FUJITSU Software
ServerView Resource Orchestrator
Virtual Edition V3.4.0

Setup Guide

Windows/Linux

J2X1-7604-09ENZ0(03)
October 2020

Preface

Purpose of This Document

This manual provides information on the operations and settings required for setup of 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 Flow of Setup for Resource Orchestrator

Explains the overall flow of setup operations when using Resource Orchestrator.

Chapter 2 Installation

Explains how to install Resource Orchestrator.

Chapter 3 Login to the ROR Console

Explains how to open and close the ROR console.

Chapter 4 License Setup and Confirmation

Explains how to set up and confirm the licenses necessary to use Resource Orchestrator.

Chapter 5 Registering Resources with Resource Orchestrator

Explains how to register, change, and delete resources used by Resource Orchestrator.

Chapter 6 Configuration after Manager Installation

Explains how to configure the HBA address rename setup service.

Chapter 7 Installing Software and Registering Agents on Managed Servers

Explains the installation of software and registration of agents on managed servers.

Chapter 8 Configuring Monitoring Information

Explains how to configure monitoring information.

Chapter 9 Settings for Server Switchover

Explains the settings and usage of the server switchover function.

Chapter 10 Saving Environment Settings

Explains how to save environment settings.

Chapter 11 Uninstallation

Explains how to uninstall Resource Orchestrator.

Appendix A Coordination with Other Products

Explains how to coordinate use of Resource Orchestrator and other products.

Appendix B Co-Existence with Other Products

Explains co-existence with other products.

Appendix C Manager Cluster Operation Settings and Deletion

Explains the settings necessary when using Resource Orchestrator on cluster systems, and the method for deleting Resource Orchestrator from cluster systems.

Appendix D Upgrading from Earlier Versions

Explains how to upgrade from earlier versions of Resource Coordinator.

Appendix E Compatibility with Earlier Versions

Explains compatibility with earlier versions of Resource Orchestrator.

Appendix F Migration Procedure when Using Active Directory with a Redundant Configuration

Explains the migration procedure for changing operation of the Active Directory used for the Single Sign-On function of ServerView Operations Manager from one server to two servers.

Appendix G Sending SNMP Traps

Explains the function used to send the details of Resource Orchestrator events to other products as SNMP traps.

Appendix H Configuring and Deleting SELinux [Linux]

Explains the methods for configuring SELinux and deleting the settings for SELinux necessary for operation using Resource Orchestrator, when SELinux is enabled (Enforcing mode).

Web Site URLs

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

Document Conventions

The notation in this manual conforms to the following conventions.

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

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

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

  [Windows Manager]

  Sections related to Windows manager

  [Linux Manager]

  Sections related to Linux manager

  [Windows]

  Sections related to Windows

  [Linux]

  Sections related to Linux

  [Red Hat Enterprise Linux]

  Sections related to Red Hat Enterprise Linux

  [Solaris]

  Sections related to Solaris

  [VMware]

  Sections related to VMware

[Horizon View]

Sections related to VMware Horizon View

[Hyper-V]

Sections related to Hyper-V

[Xen]

Sections related to RHEL5-Xen

[KVM]

Sections related to RHEL-KVM

[Solaris Zones]

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

[Solaris Zones (Solaris 10)]

Sections related to Solaris Zones with Solaris 10 VM hosts

[Solaris Zones (Solaris 11)]

Sections related to Solaris Zones with Solaris 11 VM hosts

[OVM for x86]

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

[OVM for x86 2.2]

Sections related to Oracle VM Server for x86 2.2

[OVM for x86 3.x]

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

[OVM for SPARC]

Sections related to Oracle VM Server for SPARC

[Citrix Xen]

Sections related to Citrix XenServer

[Physical Servers]

Sections related to physical servers

[Trend Micro OfficeScan]

Sections related to Trend Micro OfficeScan

[Symantec]

Sections related to Symantec Endpoint Protection

[McAfee]

Sections related to McAfee ePolicy Orchestrator

- Unless specified otherwise, the blade servers mentioned in this manual refer to PRIMERGY BX servers.
- Oracle Solaris may also be indicated as Solaris, Solaris Operating System, or Solaris OS.
- Oracle Solaris Zones may also be indicated as Solaris Containers or Solaris Container.
- Oracle VM Server for x86 may also be indicated as Oracle VM.
- In Resource Orchestrator, the following servers are referred to as SPARC Enterprise.
  - SPARC Enterprise M3000/M4000/M5000/M8000/M9000
  - SPARC Enterprise T5120/T5140/T5220/T5240/T5440

- In Resource Orchestrator, the following servers are referred to as SPARC M12.
  - SPARC M12-1/M12-2/M12-2S
- In Resource Orchestrator, the following servers are referred to as SPARC M10.
  - SPARC M10-1/M10-4/M10-4S
- Fujitsu SPARC M12 is the product name used for SPARC M12 when they are sold outside Japan.
- Fujitsu M10 is the product name used for SPARC M10 when they are sold outside Japan.
- In this manual, Fujitsu SPARC M12 is referred to as SPARC M12.
- In this manual, Fujitsu M10 is referred to as SPARC M10.
- In this manual, Fujitsu SPARC M12 and Fujitsu M10 are collectively referred to as SPARC M10/M12.
- In Resource Orchestrator, the following software is referred to as GLS.
  - PRIMECLUSTER GLS 4.4 or earlier
- In Resource Orchestrator, the following software is referred to as GDS.
  - PRIMECLUSTER GDS 4.4 or earlier
- References and character strings or values requiring emphasis are indicated using double quotes (").
- GUI items are shown enclosed by brackets ([ ]).
- The order of selecting menus is indicated using [ ]-[ ].
- Text to be entered by the user is indicated using bold text.
- Variables are indicated using italic text and underscores.
- The ellipses ("...") in menu names, indicating settings and operation window startup, are not shown.
- The ">" used in Windows is included in usage examples. When using Linux, read ">" as meaning "#".
- When using Resource Orchestrator on Windows 8 and Windows Server 2012, please note the following.
  When OS operations are explained in this manual, the examples assume OSs up to Windows 7 and Windows Server 2008. When using Resource Orchestrator on Windows 8 or Windows Server 2012, take explanations regarding the [Start] menu as indicating the [Apps] screen.
  The [Apps] screen can be displayed by right-clicking on the [Start] screen and then right-clicking [All apps].
- When using Resource Orchestrator on Windows 8.1 and Windows Server 2012 R2, please note the following.
  When OS operations are explained in this manual, the examples assume OSs up to Windows 7 and Windows Server 2008. When using Resource Orchestrator on Windows 8.1 or Windows Server 2012 R2, take explanations regarding the [Start] menu as indicating the [Apps] screen.
  The [Apps] screen can be displayed by swiping the [Start] screen from bottom to top, or clicking the downward facing arrow on the lower-left of the [Start] screen.

Menus in the ROR console

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

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

Regarding Installation Folder Paths

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

Replace it as shown below.

[Virtual Edition]

- When using Windows 64-bit (x64)

  C:\Program Files (x86)\Resource Orchestrator

- When using Windows 32-bit (x86)

  C:\Program Files\Resource Orchestrator

[Cloud Edition]

C:\Program Files (x86)\Resource Orchestrator

Command Examples

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

Abbreviations

The following abbreviations are use in this manual.

Category

Abbreviation

- Products

Windows

Windows

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

Windows Server 2012

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

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

Windows Server 2016

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

Windows Server 2019

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

Windows PE

- Microsoft(R) Windows(R) Preinstallation Environment

Windows 7

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

Windows 8.1

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

Windows 10

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

DOS

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

MSFC

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

SCVMM

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

Linux

Linux

- Red Hat(R) Enterprise Linux(R) 6.0 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.0 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.1 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.1 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.2 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.3 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.3 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.4 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.4 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.5 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.5 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.6 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.6 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.7 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.7 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.8 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.8 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.9 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.9 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.10 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.10 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 7.0 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 7.1 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 7.2 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 7.4 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 7.5 (for Intel64)
- SUSE(R) Linux Enterprise Server 10 Service Pack 2 for x86
- SUSE(R) Linux Enterprise Server 10 Service Pack 2 for AMD64 & Intel64
- SUSE(R) Linux Enterprise Server 10 Service Pack 3 for x86
- SUSE(R) Linux Enterprise Server 10 Service Pack 3 for AMD64 & Intel64
- SUSE(R) Linux Enterprise Server 11 for x86
- SUSE(R) Linux Enterprise Server 11 for AMD64 & Intel64
- SUSE(R) Linux Enterprise Server 11 Service Pack 1 for x86
- SUSE(R) Linux Enterprise Server 11 Service Pack 1 for AMD64 & Intel64
- Oracle Enterprise Linux Release 6.7 for x86 (32-bit)
- Oracle Enterprise Linux Release 6.7 for x86_64 (64-bit)
- Oracle Enterprise Linux Release 7.2 for x86 (32-bit)
- Oracle Enterprise Linux Release 7.2 for x86_64 (64-bit)

Red Hat Enterprise Linux

- Red Hat(R) Enterprise Linux(R) 6.0 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.0 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.1 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.1 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.2 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64)

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

Red Hat Enterprise Linux 6

- Red Hat(R) Enterprise Linux(R) 6.0 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.0 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.1 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.1 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.2 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.3 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.3 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.4 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.4 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.5 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.5 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.6 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.6 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.7 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.7 (for Intel64)

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

Red Hat Enterprise Linux 7

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

SUSE Linux Enterprise Server

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

Oracle Enterprise Linux

- Oracle Enterprise Linux Release 6.7 for x86 (32-bit)
- Oracle Enterprise Linux Release 6.7 for x86_64 (64-bit)
- Oracle Enterprise Linux Release 7.2 for x86 (32-bit)
- Oracle Enterprise Linux Release 7.2 for x86_64 (64-bit)

KVM

RHEL-KVM

- Red Hat(R) Enterprise Linux(R) 6.1 (for x86) Virtual Machine Function
- Red Hat(R) Enterprise Linux(R) 6.1 (for Intel64) Virtual Machine Function
- Red Hat(R) Enterprise Linux(R) 6.2 (for x86) Virtual Machine Function
- Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64) Virtual Machine Function
- Red Hat(R) Enterprise Linux(R) 6.3 (for x86) Virtual Machine Function
- Red Hat(R) Enterprise Linux(R) 6.3 (for Intel64) Virtual Machine Function
- Red Hat(R) Enterprise Linux(R) 6.4 (for x86) Virtual Machine Function
- Red Hat(R) Enterprise Linux(R) 6.4 (for Intel64) Virtual Machine Function
- Red Hat(R) Enterprise Linux(R) 6.5 (for x86) Virtual Machine Function

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

Xen

Xen

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

Citrix

Citrix XenServer

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

XenServer 6

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

Citrix XenApp

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

Citrix XenDesktop

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

Oracle Solaris

Solaris

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

- Oracle Solaris 11.2
- Oracle Solaris 11.3

Oracle VM

OVM for x86 2.2

- Oracle(R) VM Server for x86 2.2

OVM for x86 3.x

OVM for x86 3.2

- Oracle VM Server for x86 v3.2.*x*

OVM for x86 3.3

- Oracle VM Server for x86 v3.3.*x*

OVM for SPARC

- Oracle(R) VM Server for SPARC

Oracle VM Manager

- Oracle(R) VM Manager

EMC

Navisphere

- EMC Navisphere Manager

Solutions Enabler

- EMC Solutions Enabler

VMware

VMware vSphere or vSphere

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

VMware ESX

- VMware(R) ESX(R)

VMware ESX 4

- VMware(R) ESX(R) 4

VMware ESXi

- VMware(R) ESXi(TM)

VMware ESXi 5.0

- VMware(R) ESXi(TM) 5.0

VMware ESXi 5.1

- VMware(R) ESXi(TM) 5.1

VMware ESXi 5.5

- VMware(R) ESXi(TM) 5.5

VMware ESXi 6.0

- VMware(R) ESXi(TM) 6.0

VMware ESXi 6.5

- VMware(R) ESXi(TM) 6.5

VMware ESXi 6.7

- VMware(R) ESXi(TM) 6.7

VMware Infrastructure Client

- VMware(R) Infrastructure Client

VMware Tools

- VMware(R) Tools

VMware vSphere 4.0 or vSphere 4.0

- VMware vSphere(R) 4.0

VMware vSphere 4.1 or vSphere 4.1

- VMware vSphere(R) 4.1

VMware vSphere 5 or vSphere 5

- VMware vSphere(R) 5

VMware vSphere 5.1 or vSphere 5.1

- VMware vSphere(R) 5.1

VMware vSphere 5.5 or vSphere 5.5

- VMware vSphere(R) 5.5

VMware vSphere 6.0 or vSphere 6.0

- VMware vSphere(R) 6.0

VMware vSphere 6.5 or vSphere 6.5

- VMware vSphere(R) 6.5

VMware vSphere 6.7 or vSphere 6.7

- VMware vSphere(R) 6.7

VMware vSphere Client or vSphere Client

- VMware vSphere(R) Client

VMware vCenter Server or vCenter Server

- VMware(R) vCenter(TM) Server

VMware vCenter Server Appliance or vCenter Server Appliance

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

VMware vClient

- VMware(R) vClient(TM)

VMware FT

- VMware(R) Fault Tolerance

VMware DRS

- VMware(R) Distributed Resource Scheduler

VMware DPM

- VMware(R) Distributed Power Management

VMware Storage VMotion

- VMware(R) Storage VMotion

VMware vDS

- VMware(R) vNetwork Distributed Switch

VMware Horizon View

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

VMware VSAN or VSAN

- VMware(R) Virtual SAN(TM)

VMware vSphere Web Client or vSphere Web Client

- VMware vSphere(R) Web Client

VMware NSX

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

VMware NSX Controller or NSX Controller

- VMware NSX(R) Controller(TM)

VMware NSX Edge or NSX Edge

- VMware NSX(R) Edge(TM)

VMware NSX Manager or NSX Manager

- VMware NSX(R) Manager(TM)

Excel

Excel

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

Excel 2007

- Microsoft(R) Office Excel(R) 2007

Excel 2010

- Microsoft(R) Office Excel(R) 2010

Excel 2013

- Microsoft(R) Office Excel(R) 2013

Browsers

Internet Explorer

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

Firefox

- Firefox(R)

Antivirus Software

OfficeScan

- Trend Micro OfficeScan

McAfee ePolicy Orchestrator

- McAfee(R) ePolicy Orchestrator(R)

McAfee ePO

- McAfee(R) ePolicy Orchestrator(R)

McAfee Agent

- McAfee(R) Agent

McAfee Endpoint Security

- McAfee(R) Endpoint Security

Symantec Endpoint Protection

- Symantec(TM) Endpoint Protection

Symantec Endpoint Protection Manager

- Symantec(TM) Endpoint Protection Manager

BMC

BladeLogic

- BMC BladeLogic Server Automation

ETERNUS

ESC

- ETERNUS SF Storage Cruiser

ServerView

ServerView Agent

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

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

VIOM

- ServerView Virtual-IO Manager

ISM

- ServerView Infrastructure Manager
- Infrastructure Manager

SVOM

- ServerView Operations Manager

SVFAB

- ServerView Fabric Manager

RCVE

- ServerView Resource Coordinator VE

ROR

- FUJITSU Software ServerView Resource Orchestrator

ROR VE

- FUJITSU Software ServerView Resource Orchestrator Virtual Edition

ROR CE

- FUJITSU Software ServerView Resource Orchestrator Cloud Edition

Resource Coordinator

- Systemwalker Resource Coordinator
- Systemwalker Resource Coordinator Virtual server Edition

Resource Coordinator VE

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

Resource Orchestrator

- FUJITSU Software ServerView Resource Orchestrator

Export Administration Regulation Declaration

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

Trademark Information

- BMC, BMC Software, and the BMC Software logo are the exclusive properties of BMC Software, Inc., are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries.
- Citrix, Citrix Virtual Apps and Desktops, Citrix Virtual Apps, Citrix Hypervisor, XenApp, XenDesktop, XenServer, Citrix Essentials are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.
- Dell is a registered trademark of Dell Computer Corp.

- HP is a registered trademark of Hewlett-Packard Company.
- IBM is a registered trademark or trademark of International Business Machines Corporation in the U.S.
- Linux(R) is a trademark or registered trademark of Linus Torvalds in the United States and other countries.
- McAfee and the McAfee logo, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the United States and other countries.
- Microsoft, Windows, MS-DOS, Windows Server, Windows Vista, Excel, Active Directory, and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.
- Firefox is a trademark or registered trademark of the Mozilla Foundation in the United States and other countries.
- Oracle and Java are registered trademarks of Oracle and/or its affiliates.
- Red Hat, RPM and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries.
- Spectrum is a trademark or registered trademark of Computer Associates International, Inc. and/or its subsidiaries.
- SUSE and the SUSE logo are trademarks of SUSE IP Development Limited or its subsidiaries or affiliates.
- Symantec and the Symantec logo are trademarks or registered trademarks of the Symantec Corporation or its subsidiaries in the United States and other countries.
- TREND MICRO and OfficeScan are registered trademarks of Trend Micro, Inc.
- VMware, the VMware "boxes" logo and design, Virtual SMP, and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.
- ServerView and Systemwalker are registered trademarks of FUJITSU LIMITED.
- All other brand and product names are trademarks or registered trademarks of their respective owners.

Notices

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

Revision History

Month/Year Issued, Edition	Manual Code
November 2011, First Edition	J2X1-7604-01ENZ0(00)
December 2011, Edition 1.1	J2X1-7604-01ENZ0(01)
January 2012, Edition 1.2	J2X1-7604-01ENZ0(02)
February 2012, Edition 1.3	J2X1-7604-01ENZ0(03)
March 2012, Edition 1.4	J2X1-7604-01ENZ0(04)
April 2012, Edition 1.5	J2X1-7604-01ENZ0(05)
July 2012, Second Edition	J2X1-7604-02ENZ0(00)
October 2012, Third Edition	J2X1-7604-03ENZ0(00)
December 2012, Fourth Edition	J2X1-7604-04ENZ0(00)
January 2013, Fifth Edition	J2X1-7604-05ENZ0(00)
January 2013, Edition 5.1	J2X1-7604-05ENZ0(01)
January 2013, Edition 5.2	J2X1-7604-05ENZ0(02)
June 2013, Edition 5.3	J2X1-7604-05ENZ0(03)

Month/Year Issued, Edition	Manual Code
August 2013, Edition 5.4	J2X1-7604-05ENZ0(04)
August2013, Edition 5.5	J2X1-7604-05ENZ0(05)
December 2013, Sixth Edition	J2X1-7604-06ENZ0(00)
December 2013, Edition 6.1	J2X1-7604-06ENZ0(01)
February 2014, Edition 6.2	J2X1-7604-06ENZ0(02)
April 2014, Edition 6.3	J2X1-7604-06ENZ0(03)
June 2014, Edition 6.4	J2X1-7604-06ENZ0(04)
April 2015, Seventh Edition	J2X1-7604-07ENZ0(00)
May 2015, Edition 7.1	J2X1-7604-07ENZ0(01)
July 2015, Edition 7.2	J2X1-7604-07ENZ0(02)
August 2015, Edition 7.3	J2X1-7604-07ENZ0(03)
September 2015, Edition 7.4	J2X1-7604-07ENZ0(04)
December 2015, Edition 7.5	J2X1-7604-07ENZ0(05)
January 2016, Edition 7.6	J2X1-7604-07ENZ0(06)
June 2016, Edition 7.7	J2X1-7604-07ENZ0(07)
September 2016, Edition 7.8	J2X1-7604-07ENZ0(08)
December 2016, Edition 7.9	J2X1-7604-07ENZ0(09)
February 2017, Edition 7.10	J2X1-7604-07ENZ0(10)
April 2017, Eighth Edition	J2X1-7604-08ENZ0(00)
May 2017, Edition 8.1	J2X1-7604-08ENZ0(01)
August 2017, Edition 8.2	J2X1-7604-08ENZ0(02)
September 2017, Edition 8.3	J2X1-7604-08ENZ0(03)
December r 2017, Edition 8.4	J2X1-7604-08ENZ0(04)
February 2018, Edition 8.5	J2X1-7604-08ENZ0(05)
March 2018, Edition 8.6	J2X1-7604-08ENZ0(06)
October 2018, Ninth Edition	J2X1-7604-09ENZ0(00)
December 2018, Edition 9.1	J2X1-7604-09ENZ0(01)
December 2018, Edition 9.2	J2X1-7604-09ENZ0(02)
October 2020, Edition 9.3	J2X1-7604-09ENZ0(03)

Copyright

Contents

Chapter 1 Flow of Setup for Resource Orchestrator

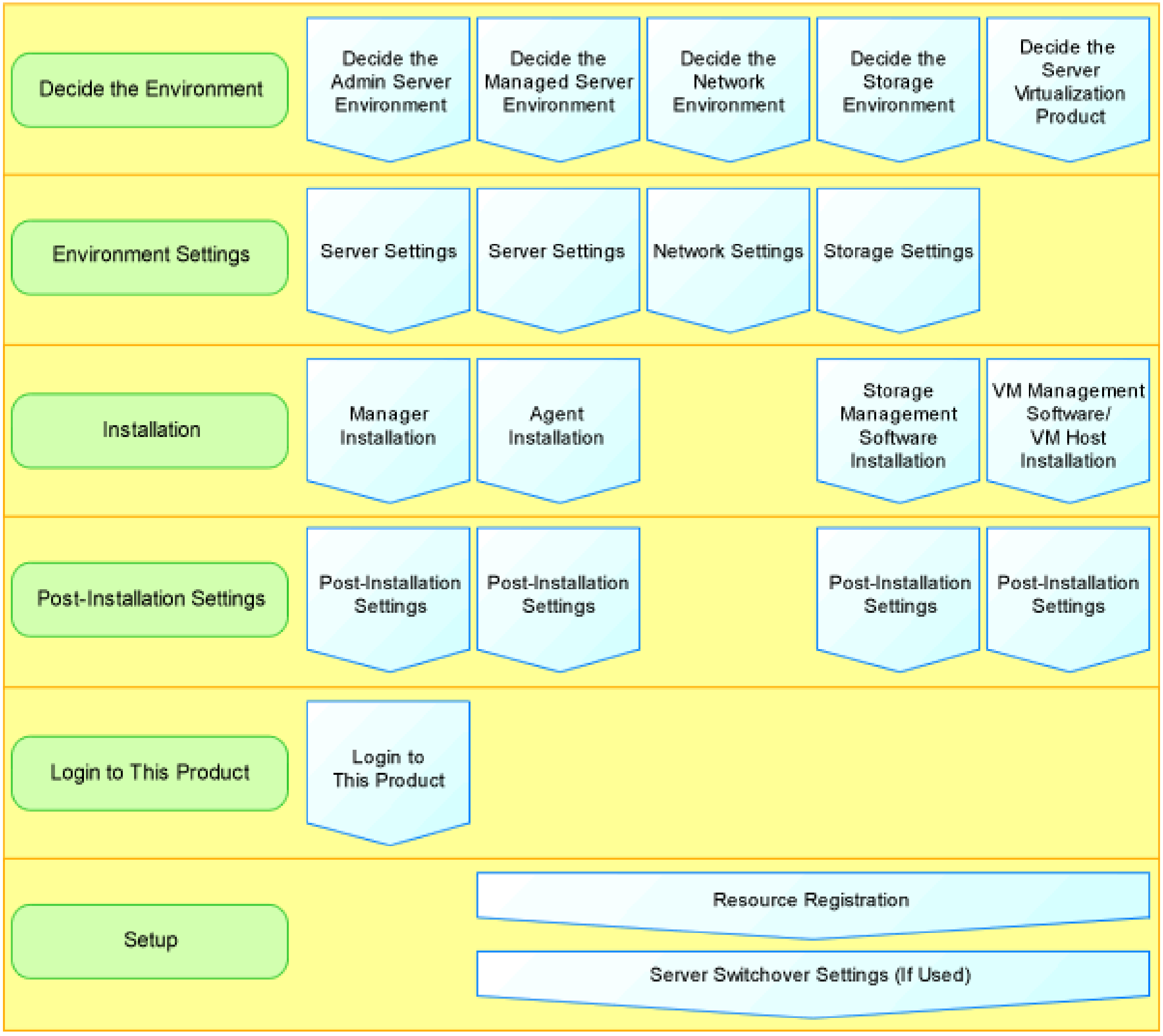
This chapter explains the overall flow of setup when using Resource Orchestrator.

An overview of setup operations when using Resource Orchestrator is given below.

Flow of Setup Operations for Special Administrators

The flow of setup operations for special administrators is indicated below.

Figure 1.1 Flow of Setup Operations for Special Administrators


Decide the Environment
Decide the Admin Server Environment
Decide the Managed Server Environment
Decide the Network Environment
Decide the Storage Environment
Decide the Server Virtualization Product
Environment Settings
Server Settings
Server Settings
Network Settings
Storage Settings
Installation
Manager Installation
Agent Installation
Storage Management Software Installation
VM Management Software/ VM Host Installation
Post-Installation Settings
Post-Installation Settings
Post-Installation Settings
Post-Installation Settings
Post-Installation Settings
Login to This Product
Login to This Product
Setup
Resource Registration
Server Switchover Settings (If Used)

1. Definition for Resource Orchestrator Setup

   Define the following settings:

   For details, refer to the "Design Guide VE".

   - Defining Servers, Storage, and Networks
   - Deciding Server Virtualization Software

2. Configuring Resource Orchestrator Setup Settings

   Define the following settings:

   For details, refer to the "Design Guide VE".

   - Server, Storage, and Network Settings

- Settings for Server Virtualization Software

3. Install Software on Admin Servers

    a. Install an OS

    b. Install required software

    c. Install the manager

4. Install the Resource Orchestrator Manager and Perform Configuration

    For details, refer to "2.1 Manager Installation" and "Chapter 6 Configuration after Manager Installation".

5. Create a Windows PE

    It is necessary to create a Windows PE after installing the manager of Resource Orchestrator.

    For details, refer to the "Windows PE Creation Script Guide".

6. Log in to Resource Orchestrator

    Log in to Resource Orchestrator.

    For details, refer to "Chapter 1 Login and Logout" in the "User's Guide VE".

7. License Setup

    Set up licenses after logging in to Resource Orchestrator.

    For details, refer to "Chapter 4 License Setup and Confirmation".

8. Resource Registration

    Register the required resources in Resource Orchestrator.

    - When Using Blade Servers

        - Register VIOM (when using rack mount servers supported by VIOM)

        - Register VM management software (when using VM management software)

        - Register chassis

        - Register admin LAN subnets (when there are multiple admin LAN subnets)

            Refer to "7.9 Registering Admin LAN Subnets" in the "User's Guide VE".

        - Register managed servers (within chassis)

        - Register LAN switch blades

        - Configure VLANs for LAN switch blades manually

        - Register LAN switches (when monitoring with the NetworkViewer)

        - Manually configure VLANs for LAN switches

        - Configure power monitoring devices (when using devices)

        - Configure HBA address rename (when using HBA address rename)

        - Configure the HBA address rename setup service (when using the HBA address rename setup service)

        - Install software and register agents on managed servers

            Install software on managed servers (physical servers, VM hosts) and then register agents in Resource Orchestrator.

            - Install an OS

            - Install required software

            - Install the agent

            - Register the agent

- When Using Rack Mount or Tower Servers
  - Register VIOM or ISM (when using rack mount servers supported by VIOM or ISM)
  - Register VM management software (when using VM management software)
  - Register admin LAN subnets (when there are multiple admin LAN subnets)

    Refer to "7.9 Registering Admin LAN Subnets" in the "User's Guide VE".
  - Register Managed Servers
  - Register LAN Switches
  - Manually configure VLANs for LAN switches
  - Configure power monitoring devices (when using devices)
  - Configure HBA address rename (when using HBA address rename)
  - Configure the HBA address rename setup service (when using the HBA address rename setup service)
  - Install software and register agents on managed servers

    Install software on managed servers (physical servers, VM hosts) and then register agents in Resource Orchestrator.

    - Install an OS
    - Install required software
    - Install the agent
    - Register the agent
- When using PRIMEQUEST
  - Register VM management software (when using VM management software)
  - Register chassis
  - Register admin LAN subnets (when there are multiple admin LAN subnets)

    Refer to "7.9 Registering Admin LAN Subnets" in the "User's Guide VE".
  - Register managed servers (within chassis)
  - Install software and register agents on managed servers

    Install software on managed servers (physical servers, VM hosts) and then register agents in Resource Orchestrator.

    - Install an OS
    - Install required software
    - Install the agent
    - Register the agent
- When Using SPARC Enterprise M3000/T series or SPARC M10-1/M10-4/M12-1/M12-2
  - Register admin LAN subnets (when there are multiple admin LAN subnets)

    Refer to "7.9 Registering Admin LAN Subnets" in the "User's Guide VE".
  - Register Managed Servers
  - Configure power monitoring devices (when using devices)
  - Install software and register agents on managed servers

    Install software and register agents on managed servers (physical servers, VM hosts).

    - Install an OS
    - Install required software
    - Install the agent

- Register the agent

- When Using SPARC Enterprise M4000/M5000/M8000/M9000 or SPARC M10-4S/M12-2S
    - Register chassis
    - Register admin LAN subnets (when there are multiple admin LAN subnets)

      Refer to "7.9 Registering Admin LAN Subnets" in the "User's Guide VE".
    - Register managed servers (within chassis)
    - Configure power monitoring devices (when using devices)
    - Install software and register agents on managed servers

      Install software and register agents on managed servers (physical servers, VM hosts).

      - Install an OS

      - Install required software

      - Install the agent

      - Register the agent

9. Settings for Server Switchover

   To use server switchover, specify the server switchover settings.

   For details, refer to "Chapter 4 Server Switchover" in the "Operation Guide VE".

Chapter 2 Installation

This chapter explains the installation of FUJITSU Software ServerView Resource Orchestrator.

2.1 Manager Installation

This section explains installation of managers.

2.1.1 Manager Installation [Windows Manager]

This section explains installation of Windows managers.

2.1.1.1 Preparations

This section explains the preparations and checks required before commencing installation.

- Host Name Checks
- System Time Checks
- Exclusive Software Checks
- Required Software Preparation and Checks
- Required Patch Checks
- Collecting and Checking Required Information
- Checking Used Port Numbers
- Configuration Parameter Checks

2.1.1.2 Software Preparation and Checks

Software preparation and checks are explained in the following sections.

This section explains the preparations and checks required before commencing the installation of Resource Orchestrator.

Host Name Checks

It is necessary to set the host name (FQDN) for the admin server to operate normally. Describe the host name in the hosts file, using 256 characters or less. In the hosts file, for the IP address of the admin server, configure the host name (FQDN) and then the computer name.

hosts File

```
System_drive\Windows\System32\drivers\etc\hosts
```

Note

When configuring the hosts file, note the following.

- Do not set the host name (FQDN) and the computer name to "127.0.0.1".

Example

When configuring the admin server with the IP address "10.10.10.10", the host name (FQDN) "remote1.example.com", and the computer name "remote1"

```
10.10.10.10 remote1.example.com remote1
127.0.0.1 localhost.localdomain localhost
```

For the admin client, either configure the hosts file so access to the admin server is possible using the host name (FQDN), or name resolution using a DNS server.

System Time Checks

Set the same system time for the admin server and managed servers.

Exclusive Software Checks

Uninstall exclusive software before installing Resource Orchestrator.

For details of exclusive software, refer to "6.1.1.5 Exclusive Software" in "Overview".

Note

- When uninstalling exclusive software, there are cases where other system operation administrators might have installed the software, so check that deleting the software causes no problems before actually doing so.

Required Software Preparation and Checks

Before installing Resource Orchestrator, perform the following operations.
In addition, check that the required software given in "6.1.1.4 Required Software" in the "Overview" has been installed. If it has not been installed, install it before continuing.

When operating managers in cluster environments, refer to "Appendix C Manager Cluster Operation Settings and Deletion" and "C.2.1 Preparations", and perform preparations and checks in advance.

ServerView Operations Manager Settings

When using ServerView Operations Manager, in order to open the console screen of the managed server, register the account of the Remote Management Controller with the ServerView Operations Manager.
For the setting method, refer to the ServerView Operations Manager manual.

- Required settings for ServerView Operations Manager 4.X for Windows

  In order for Resource Orchestrator to operate correctly, ensure that when installing ServerView Operations Manager 4.X for Windows you do not select "IIS (MS Internet Information Server)" for Select Web Server.

  For the settings, refer to the ServerView Operations Manager 4.X for Windows manual.

SNMP Trap Service Settings

In order for Resource Orchestrator to operate correctly, the following settings for the standard Windows SNMP trap service are required.

- Open [Services] from [Administrative Tools] on the Windows Control Panel, and then configure the startup type of SNMP Trap service as [Manual] or [Automatic] on the [Services] window.

  Set the service status to "Started".

Settings for ServerView Virtual-IO Manager

When using VIOM, in order for Resource Orchestrator to operate correctly, ensure that the following settings are made when installing ServerView Virtual-IO Manager for Windows.

- When using the I/O Virtualization Option

  Clear the [Select address ranges for IO Virtualization] checkbox on the virtual I/O address range selection window.

- When not using the I/O Virtualization Option

  Check the [Select address ranges for IO Virtualization] checkbox on the virtual I/O address range selection window, and then select address ranges for the MAC address and the WWN address.
  When there is another manager, select address ranges which do not conflict those of the other manager.

  For details, refer to the ServerView Virtual-IO Manager for Windows manual.

ETERNUS SF Storage Cruiser

When using ESC, configure the Fibre Channel switch settings in advance.

Settings for ISM Coordination

When both of the following apply, it is necessary to install a DHCP server on a Windows server other than the admin server.

- I/O virtualization using ISM is used
- PXE boot is used in ISM

After installing the manager, perform "6.2 Settings for ISM Coordination".

When Managing Managed Servers that Belong to Different Subnets from the Admin Server

When managing managed servers that belong to different subnets from the admin server, it is necessary to perform the following:

- DHCP server installation

  Install a DHCP server.

  When it is necessary to perform configuration for ISM coordination and both of the following apply, it is necessary to install the DHCP server on a Windows server other than the admin server.

  - I/O virtualization using ISM is used
  - PXE boot is used in ISM

  After installing the manager, perform "6.2 Settings for ISM Coordination".

  In all other cases, it is necessary to install a standard Windows DHCP server on the admin server.

  Install the DHCP Server following the procedure below:

  1. Add DHCP Server to the server roles.
     Perform binding of the network connections for the NIC to use as the admin LAN.
     For the details on adding and binding, refer to the Windows documentation.
  2. 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.
  3. From the [Services] window, stop the DHCP Server service.
     When an admin server is a member of a domain, perform step 4.
  4. Authorize DHCP servers.

     a. Open [DHCP] from [Administrative Tools] on the Windows Control Panel, and select [Action]-[Managed authorized servers] on the [DHCP] window.
        The [Manage Authorized Servers] window will be displayed.

     b. Click the [Authorize] button.

     c. The [Authorize DHCP Server] window will be displayed.

     d. Enter the admin IP address of the admin server in [Name or IP address].

     e. Click the [OK] button.

        The [Confirm Authorization] window will be displayed.

     f. Check the [Name] and [IP Address].

     g. Click the [OK] button.

  The server will be displayed in the [Authorized DHCP servers] of the [Manage Authorized Servers] window.

- Router configuration

  Depending on the functions used, it may be necessary to configure the router settings.
  For details, refer to "7.6 Configuring the Network Environment" in the "Design Guide VE".

- Registration of admin LAN subnets

  It is necessary to register admin LAN subnets in advance.
  For details, refer to "5.11 Registering Admin LAN Subnets" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Required Patch Checks

Before installing Resource Orchestrator, check that the required patches for the manager listed in "6.1.1.2 Required Patches" in the "Overview" have been applied.

If they have not been applied, apply them before continuing.

User Account Checks

This product automatically creates the user accounts listed below - if an application is using these OS user accounts, ensure there is no impact on the application before deleting them:

- rcxdb (for connecting to the database)

Single Sign-On Preparation and Checks (when used)

To use Single Sign-On (SSO) coordination, before installing Resource Orchestrator, certificate preparation and user registration of an administrator (privileged user) with the directory service are required.
For details, refer to "Chapter 10 Configuring Single Sign-On" in the "Design Guide VE".

2.1.1.3 Collecting and Checking Required Information

Before installing Resource Orchestrator, collect required information and check the system status, then determine the information to be specified on the installation window. The information that needs to be prepared is given below.

- Installation Folder

  Decide the installation folder for Resource Orchestrator.
  Note that folders on removable disks cannot be specified.
  Check that there are no files or folders in the installation folder.
  Check that the necessary disk space can be secured on the drive for installation.
  For the amount of disk space necessary for Resource Orchestrator, refer to "6.1.1.6 Static Disk Space" and "6.1.1.7 Dynamic Disk Space" in the "Overview".

- Image File Storage Folder

  The image file storage folder is located in the installation folder.
  Check that sufficient disk space can be secured on the drive where the storage folder will be created.
  For the necessary disk space, refer to "6.1.1.7 Dynamic Disk Space" in the "Overview".

  For details of how to change the image file storage folder, refer to "5.8 rcxadm imagemgr" in the "Reference Guide (Command) VE".

- Port number

  For details on port numbers, refer to "2.1.1.4 Checking Used Port Numbers".

- Directory Service Connection Information for Single Sign-On of ServerView Operations Manager

  Confirm that the directory service used for Single Sign-On of ServerView Operations Manager is correctly configured.

  This can be performed using either of the following procedures:

- Log in to ServerView Operations Manager.

  Refer to the following manuals:

  - Manual for ServerView Operations Manager:

    "ServerView user management via an LDAP directory service" in "FUJITSU ServerView Suite User Management in ServerView"

  - Manual for ServerView Operations Manager:

    "Starting ServerView Operations Manager" in "FUJITSU Software ServerView Suite ServerView Operations Manager" (User's guide)

- Perform modification installation of ServerView Operations Manager.

  When performing modification installation, the settings of directory service can be checked.

  Refer to the following manuals:

  - Manual for ServerView Operations Manager:

    "ServerView user management via an LDAP directory service" in "FUJITSU ServerView Suite User Management in ServerView"

  - Manual for ServerView Operations Manager:

    "Modify installation of Operations Manager software" in "FUJITSU Software ServerView Suite ServerView Operations Manager Installing ServerView Operations Manager Software under Windows"

  If the settings of the directory service for ServerView Operations Manager are correct, exit the modification installation without making any changes.
  If there are errors in the settings of the directory service for ServerView Operations, perform modification installation of ServerView Operations Manager to correct the errors.

Parameters Used for Installation

The following table contains the parameters used for installation.

No.	Window	Entry	Description
1	Installation Folder Selection	Installation Folder	This is the folder where Resource Orchestrator is installed. - When using a 64-bit (x64) OS Default value: *System_drive*\Program Files (x86)\Resource Orchestrator - When using a 32-bit (x86) OS Default value: *System_drive*\Program Files\Resource Orchestrator The installation folder can contain 45 characters or less including the drive letter and "\". A path starting with "\\" or a relative path cannot be specified. Alphanumeric characters, blank spaces (" "), and parentheses ("()") can be used. The following folder cannot be specified for the installation folder. - When using a 64-bit (x64) OS - *System_drive*\ - *System_drive*\Program Files(x86) - When using a 32-bit (x86) OS - *System_drive*\ - *System_drive*\Program Files

No.	Window	Entry	Description
			The following folder and its subfolders cannot be specified for the installation folder. - When using a 64-bit (x64) OS - *System_drive*\Windows - *System_drive*\Program Files - When using a 32-bit (x86) OS - *System_drive*\Windows Specify an NTFS disk.
2	Admin LAN Selection	Network to use for the admin LAN	This is the network to be used as the admin LAN. Select it from the list. The maximum value for the subnet mask is 255.255.255.255 (32-bit mask). The minimum value is 255.255.0.0 (16-bit mask). However, 255.255.255.254 cannot be specified.
3	Authentication Method Selection	Authentication Method	Select one of the following options. - Internal Authentication - ServerView Single sign-on (SSO)
4	Administrative User Creation (When [Internal Authentication] is selected)	User Account	This is the user account name to be used for logging into Resource Orchestrator as an administrative user. The name must start with an alphabetic character and can be up to 16 alphanumeric characters long, including underscores ("_"), hyphens ("-"), and periods ("."). Input is case-sensitive.
		Password	The password of the administrative user. The string must be composed of alphanumeric characters and symbols (excluding blank spaces), and can be up to 16 characters long.
		Retype password	
	Administrative User Settings (When [ServerView Single sign-on (SSO)] is selected)	User Account	This is the user account name to be used for logging into Resource Orchestrator as an administrative user. Specify the user registered in the directory service in "Single Sign-On Preparation and Checks (when used)" in "2.1.1.2 Software Preparation and Checks". When using the directory service provided with ServerView Operations Manager, specifying "administrator", which is the administrator account of ServerView Operations Manager, enables Single Sign-On coordination with ServerView Operations Manager. The name must start with an alphabetic character and can be up to 16 alphanumeric characters long, including underscores ("_"), hyphens ("-"), and periods ("."). Input is case-sensitive.

2.1.1.4 Checking Used Port Numbers

Ports Automatically Set in the services File of the System

When Resource Orchestrator is installed, the following port numbers used by it will automatically be set in the services file of the system.

If the following port numbers used by Resource Orchestrator are being used for other applications, a message indicating that the numbers are in use is displayed when the installer is started, and installation will stop.
In that case, describe the entries for the following port numbers used by Resource Orchestrator in the services file using numbers not used by other software, and then start the installer.

Ports Automatically Set in the services File of the System

```
# service name   port number/protocol name
nfdomain         23457/tcp
nfagent          23458/tcp
rcxmgr           23460/tcp
rcxweb           23461/tcp
rcxtask          23462/tcp
rcxmongrel1      23463/tcp
rcxmongrel2      23464/tcp
rcxdb            23465/tcp
```

Checking Port Usage Status

Execute the "Environment setup conditions check tool" in "2.1.1.5 Configuration Parameter Checks" to check the port usage status.
For ports with "is in use" displayed for the result of "Port status", confirm that those ports are used with the purpose of usage for Resource Orchestrator defined in C:\Windows\System32\drivers\etc\services.
When ports are being used for something other than Resource Orchestrator, change the ports to use.

For the port information used by Resource Orchestrator, refer to "Appendix A Port List" in the "Design Guide VE".

Changing Port Numbers

To change port numbers after installing the manager, refer to the following:

- "8.2 Changing Port Numbers" in the "User's Guide VE"

ephemeral Port

When the range of ephemeral port numbers on Windows is changed, the ephemeral port and the port to use conflict. In that case, select a port number which is not included in the range of the ephemeral port numbers.

The range of ephemeral port numbers is as below.

- For Windows Server 2012 or later

  49152 to 65535

2.1.1.5 Configuration Parameter Checks

Check configuration parameters following the procedure below:

1. Log in as the administrator.
2. Confirm that a single folder path is set for the TEMP environment variable.

Information

If the TEMP environment variable is not configured or if multiple folder paths are set for the TEMP environment variable, the Environment setup conditions check tool outputs the following message and cancels the process.

```
The check tool cannot be processed because the temporary folder %temp% cannot be accessed.
Please set the TEMP environment variable of current user correctly, then rerun the check tool.
press enter key to exit...
```

If the above message is output, set a single folder path for the TEMP environment variable, then execute the Environment setup conditions check tool again.

3. Start the installer.

   The installer is automatically displayed when the first DVD-ROM is set in the DVD drive. If it is not displayed, execute "RcSetup.exe" to start the installer.

4. Select "Tool" on the window displayed, and then click [Environment setup conditions check tool]. Configuration parameter checking will start.

   For the check items with the edition name displayed in the check results, check only the items corresponding to the edition to be installed.

5. When configuration parameter checking is completed, the check results will be saved in the following location.

   %temp%\ror_precheckresult-*YYYY-MM-DD-hhmmss*.txt

   The check results are output to Notepad at the same time.

   The following items are displayed as the items to be checked:

   - Required Software (Windows PowerShell)
   - Required Software (ETERNUS SF Storage Cruiser)
   - Disk Space (Express/Virtual Edition)
   - Disk Space (Cloud Edition)
   - Memory Size (Express/Virtual Edition)
   - Memory Size (Cloud Edition)
   - cpu
   - SNMP Service
   - Port Status (Express/Virtual Edition)
   - Port Status (Cloud Edition)

6. Confirm that "Warning" or "NG" is not included in the check results. If there are check items that were determined as "Warning" or "NG", resolve the cause of the problem based on the output message. For details of the corrective actions, refer to "2.1.1.1 Preparations" and "6.1 Software Environment" and "6.2 Hardware Environment" in the "Overview".

2.1.1.6 Installation

The procedure for manager installation is given below.

Before installation, check if "2.1.1.1 Preparations" have been performed.

Nullifying Firewall Settings for Ports to be used by Resource Orchestrator

When installing Resource Orchestrator on systems with active firewalls, in order to enable correct communication between the manager, agents, and clients, disable the firewall settings for the port numbers to be used for communication.

For the port numbers used by Resource Orchestrator and required software, refer to "Appendix A Port List" in the "Design Guide VE".

However, when port numbers have been changed by editing the services file during installation of Resource Orchestrator, replace the default port numbers listed in "Appendix A Port List" in the "Design Guide VE" with the port numbers changed to during installation.

Installation

The procedure for manager installation is given below.

1. Log on to the system as the administrator.

   Log on to the system on which the manager is to be installed using the Administrator account of the local computer.

2. Set the first Resource Orchestrator DVD-ROM.

   Then, the installer starts automatically.

   Information

   If the installer does not start, execute "RcSetup.exe" from the DVD-ROM drive.

3. Select [Virtual Edition].

4. Click [Manager installation].

5. Perform installation according to the installer's interactive instructions.

   Enter the parameters designed and checked in "Parameters Used for Installation" in "2.1.1.3 Collecting and Checking Required Information".

Note

- In the event of installation failure, restart and then log in as the user that performed the installation, and perform uninstallation following the uninstallation procedure.
  After that, remove the cause of the failure referring to the meaning of the output message and the suggested corrective actions, and then perform installation again.

- If there are internal inconsistencies detected during installation, the messages "The problem occurred while installing it" or "Native Installer Failure" will be displayed and installation will fail. In this case, uninstall the manager and reinstall it. If the problem persists, please contact Fujitsu technical staff.

Post-installation Cautions

- The following users are added. When installing Resource Orchestrator, do not delete these accounts.

Account Name	Usage
rcxdb	rcxdb is used as the OS account for connecting to the database service of Resource Orchestrator.

- The user group below is added.

User Group Name	Usage
Deployment Admin	This user group is used to perform backup, restoration, and cloning for Resource Orchestrator.

2.1.2 Manager Installation [Linux Manager]

This section explains installation of Linux managers.

2.1.2.1 Preparations

This section explains the preparations and checks required before commencing installation.

- Host Name Checks
- System Time Checks
- Exclusive Software Checks
- Required Software Preparation and Checks
- Required Patch Checks
- Required Package Checks

- Collecting and Checking Required Information
- Checking Used Port Numbers
- Configuration Parameter Checks

2.1.2.2 Software Preparation and Checks

Software preparation and checks are explained in the following sections.

This section explains the preparations and checks required before commencing the installation of Resource Orchestrator.

Host Name Checks

It is necessary to set the host name (FQDN) for the admin server to operate normally. Describe the host name in the hosts file, using 256 characters or less. In the hosts file, for the IP address of the admin server, configure the host name (FQDN) and then the computer name.

hosts File

```
/etc/hosts
```

Note

When configuring the hosts file, note the following.

- Do not set the host name (FQDN) and the computer name to "127.0.0.1".

  Example

  When configuring the admin server with the IP address "10.10.10.10", the host name (FQDN) "remote1.example.com", and the computer name "remote1"

  ```
  10.10.10.10 remote1.example.com remote1
  127.0.0.1 localhost.localdomain localhost
  ```

For the admin client, either configure the hosts file so access to the admin server is possible using the host name (FQDN), or name resolution using a DNS server.

System Time Checks

Set the same system time for the admin server and managed servers.

Exclusive Software Checks

Uninstall exclusive software before installing Resource Orchestrator.

For details of exclusive software, refer to "6.1.1.5 Exclusive Software" in "Overview".

Note

- When uninstalling exclusive software, there are cases where other system operation administrators might have installed the software, so check that deleting the software causes no problems before actually doing so.

Required Software Preparation and Checks

Before installing Resource Orchestrator, perform the following operations.
In addition, check that the required software, such as ServerView Operations Manager, given in "6.1.1.4 Required Software" in the "Overview" has been installed. If it has not been installed, install it before continuing.

When operating managers in cluster environments, refer to "Appendix C Manager Cluster Operation Settings and Deletion" and "C.2.1 Preparations", and perform preparations and checks in advance.

ServerView Operations Manager Settings

In order to open the console screen of the managed server, register the account of the Remote Management Controller with the ServerView Operations Manager.
For the setting method, refer to the ServerView Operations Manager manual.

Settings for SNMP Trap Daemon

In order for Resource Orchestrator to operate correctly to operate correctly, ensure that the following settings are made for the "/etc/snmp/snmptrapd.conf" file, when installing the net-snmp package. When there is no file, add the following setting after creating the file.

```
disableAuthorization yes
```

It is also necessary to enable the automatic startup setting for the snmptrapd daemon.

ETERNUS SF Storage Cruiser

When using ESC, configure the Fibre Channel switch settings in advance.

Settings for ISM Coordination

When both of the following apply, it is necessary to install a DHCP server on a Windows server other than the admin server.

- I/O virtualization using ISM is used

- PXE boot is used in ISM

  After installing the manager, perform "6.2 Settings for ISM Coordination".

When Managing Managed Servers that Belong to Different Subnets from the Admin Server

When managing managed servers that belong to different subnets from the admin server, it is necessary to perform the following:

- DHCP server installation

  Install a DHCP server.

  When it is necessary to perform configuration for ISM coordination and both of the following apply, it is necessary to install the DHCP server on a Windows server other than the admin server.

  - I/O virtualization using ISM is used

  - PXE boot is used in ISM

  After installing the manager, perform "6.2 Settings for ISM Coordination".

  In all other cases, it is necessary to install a standard Linux DHCP server on the admin server.
  Install the DHCP server following the procedure below:

  1. Install the dhcp package.

  2. Execute the following command to modify the setting so the DHCP server service (dhcpd) is not automatically started.

     ```
     # chkconfig dhcpd off <RETURN>
     ```

  3. Execute the following command to stop the DHCP server service (dhcpd):

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

- Router configuration

  Depending on the functions used, it may be necessary to configure the router settings.
  For details, refer to "9.2.4.2 Admin LAN Settings" in the "Design Guide CE".

- Registration of admin LAN subnets

  It is necessary to register admin LAN subnets in advance.
  For details, refer to "5.11 Registering Admin LAN Subnets" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Required Patch Checks

Before installing Resource Orchestrator, check that the required patches for the manager listed in "6.1.1.2 Required Patches" in the "Overview" have been applied.

If they have not been applied, apply them before continuing.

Required Package Checks

Before installing Resource Orchestrator, check that the required packages for the manager [Linux manager] listed in "6.1.1.3 Required Packages" in the "Overview" have been applied.

If they have not been installed, install them before continuing.

User Account Checks

This product automatically creates the user accounts listed below - if an application is using these OS user accounts, ensure there is no impact on the application before deleting them:

- rcxdb (for connecting to the database)

Single Sign-On Preparation and Checks (when used)

To use Single Sign-On (SSO) coordination, before installing Resource Orchestrator, certificate preparation and user registration of an administrator (privileged user) with the directory service are required.
For details, refer to "Chapter 10 Configuring Single Sign-On" in the "Design Guide VE".

Tuning System Parameters (Admin Server)

Before installation, it is necessary to tune up system parameters for the admin server. See the table below for the system parameters that need to be tuned and their values.

Point

Set the values according to the "type" of each parameter as follows:

- When the type is "setup value"

  Modification is not necessary if already set value (default or previous value) is equal to or larger than the value in the table. If it is smaller than the value in the table, change the value to the one in the table.

- When the type is "additional value"

  Add the value in the table to already set value. Before adding the value, check the upper limit for the system, and set either the resulting value or the upper limit for the system, whichever is smaller.

For details, refer to the Linux manual.

- Shared Memory

Parameter	Description	Value	Type
shmmax	Maximum Segment Size of Shared Memory	55155880	Setup value
shmall	Total amount of shared memory available for use	13466	Setup value
shmmni	Maximum number of shared memory segments	1	Additional value

- Semaphores

  To configure semaphores, specify the value for each parameter in the following format:

```
kernel.sem = para1 para2 para3 para4
```

Parameter	Description	Value	Type
para1	Maximum number of semaphores for each semaphore identifier	17	Setup value
para2	Total number of semaphores in the system	1071	Additiona l value
para3	Maximum number of operators for each semaphore call	32	Setup value
para4	Total number of semaphore operators in the system	63	Additiona l value

[Tuning Procedure]

Use the following procedure to perform tuning:

1. Use the following command to check the values of the corresponding parameters currently configured for the system.

```
# /sbin/sysctl -a
```

Example

```
# /sbin/sysctl -a
...
  (omitted)
...

kernel.sem = 250 32000 32 128
kernel.msgmnb = 65536
kernel.msgmni = 16
kernel.msgmax = 65536
kernel.shmmni = 4096
kernel.shmall = 4294967296
kernel.shmmax = 68719476736

...
  (omitted)
...
```

2. For each parameter, compare the current value to that in the above table, and then calculate the appropriate value, based on its value type (setup or additional value).

3. Edit /etc/sysctl.conf. Edit the content as in the following example:

Example

```
kernel.sem = 250 33071 32 191
kernel.shmmni = 4097
```

4. Confirm that edited content is reflected in /etc/sysctl.conf, using the following command:

```
# /bin/cat /etc/sysctl.conf
```

5. Enable the configuration on 4. using one of the following methods:

    - Reboot the system to reflect the settings

    ```
    # /sbin/shutdown -r now
    ```

    - Use /sbin/sysctl -p to reflect the settings

    ```
    # /sbin/sysctl -p /etc/sysctl.conf (*)
    ```

    *: When using this command, reboot is not necessary.

6. Confirm that configured parameters are reflected, using the following command:

```
# /sbin/sysctl -a
```

Example

```
# /sbin/sysctl -a
...
  (omitted)
...

kernel.sem = 250 33071 32 191
kernel.msgmnb = 65536
kernel.msgmni = 16
kernel.msgmax = 65536
kernel.shmmni = 4097
kernel.shmall = 4294967296
kernel.shmmax = 68719476736

...
  (omitted)
...
```

2.1.2.3 Collecting and Checking Required Information

Before installing Resource Orchestrator, collect required information and check the system status, then determine the information to be specified on the installation window. The information that needs to be prepared is given below.

- Installation Folder

  The installation directory of Resource Orchestrator is as below. It cannot be changed.

  - /opt

  - /etc/opt

  - /var/opt

Check that the necessary disk space can be secured on the drive for installation.
For the amount of disk space necessary for Resource Orchestrator, refer to "6.1.1.6 Static Disk Space" and "6.1.1.7 Dynamic Disk Space" in the "Overview".

- Image File Storage Folder

  The image file storage folder is located in the installation folder.
  Check that sufficient disk space can be secured on the drive where the storage folder will be created.
  For the necessary disk space, refer to "6.1.1.7 Dynamic Disk Space" in the "Overview".

  For details of how to change the image file storage folder, refer to "5.8 rcxadm imagemgr" in the "Reference Guide (Command) VE".

- Port number

  For details on port numbers, refer to "2.1.2.4 Checking Used Port Numbers".

- Directory Service Connection Information for Single Sign-On of ServerView Operations Manager

  Confirm that the directory service used for Single Sign-On of ServerView Operations Manager is correctly configured.

  This can be performed using either of the following procedures:

  - Log in to ServerView Operations Manager.

    Refer to the following manuals:

    - Manual for ServerView Operations Manager:

      "ServerView user management via an LDAP directory service" in "FUJITSU ServerView Suite User Management in ServerView"

    - Manual for ServerView Operations Manager:

      "Starting ServerView Operations Manager" in "FUJITSU Software ServerView Suite ServerView Operations Manager" (User's guide)

  - Perform modification installation of ServerView Operations Manager.

    When performing modification installation, the settings of directory service can be checked.

    Refer to the following manuals:

    - Manual for ServerView Operations Manager:

      "ServerView user management via an LDAP directory service" in "FUJITSU ServerView Suite User Management in ServerView"

    - Manual for ServerView Operations Manager:

      "Installing the Operations Manager software" in "FUJITSU Software ServerView Suite ServerView Operations Manager Installation ServerView Operations Manager Software under Linux"

    If the settings of the directory service for ServerView Operations Manager are correct, exit the modification installation without making any changes.
    If there are errors in the settings of the directory service for ServerView Operations, perform modification installation of ServerView Operations Manager to correct the errors.

Parameters Used for Installation

The following table contains the parameters used for installation.

No.	Window	Entry	Description
1	Admin LAN Selection	Network to use for the admin LAN	This is the network to be used as the admin LAN. Select it from the list. The maximum value for the subnet mask is 255.255.255.255 (32-bit mask). The minimum value is 255.255.0.0 (16-bit mask). However, 255.255.255.254 cannot be specified.

No.	Window	Entry	Description
2	Authentication Method Selection	Authentication Method	Select one of the following options. - Internal Authentication - ServerView Single sign-on (SSO)
3	Administrative User Creation (When [Internal Authentication] is selected)	User Account	This is the user account name to be used for logging into Resource Orchestrator as an administrative user. The name must start with an alphabetic character and can be up to 16 alphanumeric characters long, including underscores ("_"), hyphens ("-"), and periods ("."). Input is case-sensitive.
		Password	The password of the administrative user. The string must be composed of alphanumeric characters and symbols (excluding blank spaces), and can be up to 16 characters long.
		Retype password	
	Administrative User Settings (When [ServerView Single sign-on (SSO)] is selected)	User Account	This is the user account name to be used for logging into Resource Orchestrator as an administrative user. Specify the user registered in the directory service in "Single Sign-On Preparation and Checks (when used)" in "2.1.2.2 Software Preparation and Checks". When using the directory service provided with ServerView Operations Manager, specifying "administrator", which is the administrator account of ServerView Operations Manager, enables Single Sign-On coordination with ServerView Operations Manager. The name must start with an alphabetic character and can be up to 16 alphanumeric characters long, including underscores ("_"), hyphens ("-"), and periods ("."). Input is case-sensitive.

2.1.2.4 Checking Used Port Numbers

Ports Automatically Set in the services File of the System

When Resource Orchestrator is installed, the port numbers used by it will automatically be set in the services file of the system.

If the port numbers used by Resource Orchestrator are being used for other applications, a message indicating that the numbers are in use is displayed when the installer is started, and installation will stop.
In that case, describe the entries for the following port numbers used by Resource Orchestrator in the services file using numbers not used by other software, and then start the installer.

Ports Automatically Set in the services File of the System

```
# service name   port number/protocol name
nfdomain         23455/tcp
nfagent          23458/tcp
rcxmgr           23460/tcp
rcxweb           23461/tcp
rcxtask          23462/tcp
rcxmongrel1      23463/tcp
rcxmongrel2      23464/tcp
rcxdb            23465/tcp
```

Checking Port Usage Status

Execute the "Environment setup conditions check tool" in "2.1.2.5 Configuration Parameter Checks" to check the port usage status.
For ports with "is in use" displayed for the result of "Port status", confirm that those ports are used with the purpose of usage for Resource Orchestrator defined in /etc/services.
When ports are being used for something other than Resource Orchestrator, change the ports to use.

For the port information used by Resource Orchestrator, refer to "Appendix A Port List" in the "Design Guide VE".

Changing Port Numbers

To change port numbers after installing the manager, refer to the following:

- "8.2 Changing Port Numbers" in the "User's Guide VE"

2.1.2.5 Configuration Parameter Checks

Check configuration parameters following the procedure below:

1. Log in to the system as the OS administrator (root).

   Boot the admin server in multi-user mode to check that the server meets requirements for installation, and then log in to the system using root.

2. Set the first Resource Orchestrator DVD-ROM.

3. Execute the following command to mount the DVD-ROM. If the auto-mounting daemon (autofs) is used for starting the mounted DVD-ROM, the installer will fail to start due to its "noexec" mount option.

   ```
   # mount -t iso9660 -r /dev/hdc DVD-ROM_mount_point <RETURN>
   ```

4. Execute the following installation command:

   ```
   # DVD-ROM_mount_point/RcSetup.sh <RETURN>
   ```

5. Select "Environment setup conditions check tool" from the menu to execute the tool.

   For the check items with the edition name displayed in the check results, check only the items corresponding to the edition to be installed.

6. When the check is completed, the result will be sent to standard output.

   The following items are displayed as the items to be checked:

   - Required Software (ETERNUS SF Storage Cruiser)
   - Disk Space (Express/Virtual Edition)
   - Disk Space (Cloud Edition)
   - Memory Size (Express/Virtual Edition)
   - Memory Size (Cloud Edition)
   - cpu
   - SNMP Service
   - Port Status (Express/Virtual Edition)
   - Port Status (Cloud Edition)

7. Confirm that "Warning" or "NG" is not included in the check results. If there are check items that were determined as "Warning" or "NG", resolve the cause of the problem based on the output message. For details of the corrective actions, refer to "2.1.2.1 Preparations" and "6.1 Software Environment" and "6.2 Hardware Environment" in the "Overview".

2.1.2.6 Installation

The procedure for manager installation is given below.

Before installation, check if "2.1.2.1 Preparations" have been performed.

Settings in Single User Mode

In single user mode, X Window System does not start, and one of the following operations is required.

- Switching virtual consoles (using the [Ctrl] + [Alt] + [Fn] keys)
- Making commands run in the background

Nullifying Firewall Settings for Ports to be used by Resource Orchestrator

When installing Resource Orchestrator on systems with active firewalls, in order to enable correct communication between the manager, agents, and clients, disable the firewall settings for the port numbers to be used for communication.

For the port numbers used by Resource Orchestrator and required software, refer to "Appendix A Port List" in the "Design Guide VE".

However, when port numbers have been changed by editing the services file during installation of Resource Orchestrator, replace the default port numbers listed in "Appendix A Port List" in the "Design Guide VE" with the port numbers changed to during installation.

Installation

The procedure for manager installation is given below.

1. Log in to the system as the OS administrator (root).

   Boot the admin server that the manager is to be installed on in multi-user mode, and then log in to the system using root.

2. Set the first Resource Orchestrator DVD-ROM.

3. Execute the following command to mount the DVD-ROM.

   ```
   # mount -t iso9660 -r /dev/hdc DVD-ROM_mount_point <RETURN>
   ```

   Note

   - If the auto-mounting daemon (autofs) is used for DVD-ROM auto-mounting, the installer fails to start due to its "noexec" mount option.

4. Execute the following installation command:

   ```
   # cd DVD-ROM_mount_point  <RETURN>
   # ./RcSetup.sh <RETURN>
   ```

5. Select "Virtual Edition".

6. Select "Manager installation".

7. Perform installation according to the installer's interactive instructions.

   Enter the parameters designed and checked in "Parameters Used for Installation" in "2.1.2.3 Collecting and Checking Required Information".

8. Settings when SELinux is Used

   When enabling SELinux, it is necessary to perform configuration of SELinux after installing Resource Orchestrator.
   For details on configuration, refer to "H.1.1 Manager".

Note

- Corrective Action for Installation Failure

  In the event of installation failure, restart the OS and then log in as the user that performed the installation, and perform uninstallation following the uninstallation procedure.

After that, remove the cause of the failure referring to the meaning of the output message and the suggested corrective actions, and then perform installation again.

- If there are internal inconsistencies detected during installation, the messages "The problem occurred while installing it" or "It failed in the installation" will be displayed and installation will fail. In this case, uninstall the manager and reinstall it. If the problem persists, please contact Fujitsu technical staff.

- Uninstall the Related Services

  When locating ServerView Deployment Manager in the same subnet, it is necessary to uninstall the related services.

  For the method for uninstalling the related services, please refer to "5.1 deployment_service_uninstall" in the "Reference Guide (Command) VE".

Post-installation Cautions

- The following users are added. When installing Resource Orchestrator, do not delete these accounts.

Account Name	Usage
rcxdb	rcxdb is used as the OS account for connecting to the database service of Resource Orchestrator.

- The user group below is added.

User Group Name	Usage
Deployment Admin	This user group is used to perform backup, restoration, and cloning for Resource Orchestrator.
rcxdb	rcxdb is used as a user group for connecting to the database service of Resource Orchestrator.

2.2 Agent Installation

This section explains the procedure for physical server or VM host agent installation.

The relationships of installation directories and the agents that must be installed are as follows.

Table 2.1 Relationships of Installation Directories and the Agents that must be Installed

Installation Directories		Agent
VM Host	VMware	Yes (*1)
	Hyper-V	Yes
	Xen	Yes
	KVM	Yes
	Solaris Zones	Yes
	OVM for SPARC	Yes (*2)
	OVM for x86 3.x	-
Physical Server	Windows	Yes
	Linux	Yes
	Solaris	Yes

Yes: Installation is required.

- : Installation is not required.

*1: When using VMware ESXi, there is no need to install Resource Orchestrator agents on managed servers because VMs and guest OSs are managed directly from the admin server.
Install ServerView ESXi CIM Provider.
When using VMware ESXi on another vendor's servers or when not using ServerView ESXi CIM Provider on VMware ESXi on Fujitsu rack mount servers, it is not necessary to install ServerView ESXi CIM Provider.

Like with other OSs, agents must be registered.
*2: When a guest domain on OVM for SPARC is registered as a VM host, it is necessary to install agent in that guest domain.

When deploying multiple new managed servers using Windows or Linux, cloning enables copying of the data installed on a server (OS, updates, Resource Orchestrator agents, and common software installed on servers) to other servers.

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

2.2.1 Preparations

This section explains the preparations and checks required before commencing installation.

- Exclusive Software Checks

  Refer to "Exclusive Software Checks".

- Required Software Checks

  Refer to "Required Software Preparation and Checks".

- Required Patch Checks

  Refer to "Required Patch Checks".

- Required Package Checks

  Refer to "Required Package Checks [Linux]".

2.2.1.1 Software Preparation and Checks

Software preparation and checks are explained in the following sections.

Exclusive Software Checks

Uninstall exclusive software before installing Resource Orchestrator.

For details of exclusive software, refer to "6.1.1.5 Exclusive Software" in "Overview".

Note

- When uninstalling exclusive software, there are cases where other system operation administrators might have installed the software, so check that deleting the software causes no problems before actually doing so.

Required Software Preparation and Checks

Before installing Resource Orchestrator, check that the required software given in "6.1.1.4 Required Software" in the "Overview" has been installed. If it has not been installed, install it before continuing.

Note

- ServerView Agents Settings

  To operate Resource Orchestrator correctly on PRIMERGY or PRIMEQUEST series servers, perform the necessary settings for SNMP services during installation of ServerView Agents, and start ServerView Agents.
  For how to perform SNMP service settings, refer to the ServerView Agents manual.

  - For the SNMP community name, specify the same value as the SNMP community name set for the management blade.

  - For the SNMP community name, set Read (reference) or Write (reference and updating) authority.

- For the host that receives SNMP packets, select [Accept SNMP packets from any host] or [Accept SNMP packets from these hosts] and set the admin LAN IP address of the admin server.
- For the SNMP trap target, set the IP address of the admin server.
  When an admin server with multiple NICs is set as the SNMP trap target, specify the IP address of the admin LAN used for communication with the managed server.

Required Patch Checks

Before installing Resource Orchestrator, check that the required patches for the agent listed in "6.1.1.2 Required Patches" in the "Overview" have been applied.

If they have not been applied, apply them before continuing.

Required Package Checks [Linux]

Before installing Resource Orchestrator, check that the required packages for the agent [Linux] listed in "6.1.1.3 Required Packages" in the "Overview" have been applied.

If they have not been installed, install them before continuing.

Check the Network Interface Definition File

This configuration is necessary in the following case.

- Red Hat Enterprise Linux 4 AS/ES
- Red Hat Enterprise Linux 6
- SUSE Linux Enterprise Server

When using the following functions, check the definition files of network interfaces and perform configuration before installing Resource Orchestrator.

- Server Switchover
- Cloning

When Using Red Hat Enterprise Linux 4 AS/ES

Refer to the /etc/sysconfig/network-scripts/ifcfg-eth*X* file (eth*X* is an interface name such as eth0 or eth1), and check that there is no line starting with "HWADDR=" in the file.
If there is a line starting with "HWADDR=", this is because the network interface is bound to a MAC address. In that case, comment out the line.

Example

When the admin LAN interface is eth0

```
DEVICE=eth0
#HWADDR=xx:xx:xx:xx:xx:xx <- If this line exists, comment it out.
ONBOOT=yes
TYPE=Ethernet
```

When using Red Hat Enterprise Linux 6

Use the following procedure to modify the configuration file:

1. Execute the following command.

```
# systool -c net <RETURN>
```

Example

```
# systool -c net <RETURN>
Class = "net"
Class Device = "eth0"
Device =
"0000:01:00.0"
Class Device = "eth1"
Device =
"0000:01:00.1"
Class Device = "eth2"
Device =
"0000:02:00.0"
Class Device = "eth3"
Device =
"0000:02:00.1"
Class Device = "lo"
Class Device = "sit0"
```

2. Confirm the device name which is displayed after "Class Device =" and the PCI bus number which is displayed after "Device =" in the command output results.

3. Correct the configuration file.

   After confirming support for device name and MAC address in the following configuration file, change ATTR{address}=="*MAC_address*" to KERNELS=="*PCI_bus_number*".

   All corresponding lines should be corrected.

   #### Configuration File Storage Location

   /etc/udev/rules.d/70-persistent-net.rules

   ### Example

   - Before changing

   ```
   SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
   ATTR{address}=="MAC_address", ATTR{type}=="1", KERNEL=="eth*",
   NAME="Device_name"
   ```

   - After changing

   ```
   SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
   KERNELS=="PCI_bus_number", ATTR{type}=="1", KERNEL=="eth*",
   NAME="Device_name"
   ```

4. After restarting the managed servers, check if communication with the entire network is possible.

When Using SUSE Linux Enterprise Server

Use the following procedure to modify the configuration file:

1. Execute the following command.

```
# systool -c net <RETURN>
```

Example

```
# systool -c net <RETURN>
Class = "net"

  Class Device = "eth0"
    Device = "0000:01:00.0"

  Class Device = "eth1"
    Device = "0000:01:00.1"

  Class Device = "eth2"
    Device = "0000:02:00.0"

  Class Device = "eth3"
    Device = "0000:2:00.1"

  Class Device = "lo"

  Class Device = "sit0"
```

2. Confirm the device name which is given after "Class Device =" and PCI bus number which is given after "Device =" in the command output results.

3. Modify the configuration file.

When using SUSE Linux Enterprise Server 10

a. a. After confirming support for device name and MAC address in the following configuration file, change SYSFS{address}=="*MAC_address*" to ID=="*PCI_bus_number*".
All corresponding lines should be corrected.
Support of the device name and MAC address will be used after step b.

/etc/udev/rules.d/30-net_persistent_names.rules

Before changing

```
SUBSYSTEM=="net", ACTION=="add", SYSFS{address}=="MAC_address",
IMPORT="/lib/udev/rename_netiface %k device_name"
```

After changing

```
SUBSYSTEM=="net", ACTION=="add", ID=="PCI_bus_number", IMPORT="/lib/
udev/rename_netiface %k device_name"
```

b. Based on the results of step 1 and a in step 3, change the name of the following file will be to a name that includes the PCI bus number.

Before changing

/etc/sysconfig/network/ifcfg-eth-id-MAC address

After changing

/etc/sysconfig/network/ifcfg-eth-bus-pci-PCI bus number

When using SUSE Linux Enterprise Server 11

a. Change ATTR{address}=="*MAC address*" to KERNELS=="*PCI_bus_number*" in the following configuration file.
All corresponding lines should be corrected.

/etc/udev/rules.d/70-persistent-net.rules

Before changing

```
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="MAC_address", ATTR{type}=="1", KERNEL=="eth*",
NAME="device_name"
```

After changing

```
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
KERNELS=="PCI_bus_number", ATTR{type}=="1", KERNEL=="eth*",
NAME="device_name"
```

4. After restarting the managed servers, check if communication with the entire network is possible.

Information

When using cloning or the backup and restore method for server switchover, during installation perform partition settings so that names of device paths are defined using the "Device Name" format (for example: /dev/sda1) in the /etc/fstab file.

When installation is already complete, change the names of device paths defined in the boot configuration files /boot/efi/SuSE/elilo.conf and /boot/grub/menu.lst, and the /etc/fstab file so they use the "Device Name" format (for example: /dev/sda1).For specific details about the mount definition, please refer to the following URL and search for the Document ID:3580082.

```
http://www.suse.com/documentation/
```

Disabling the NetworkManager Service

1. Execute the following command to disable the NetworkManager service.

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

    ```
    # service NetworkManager stop <RETURN>
    # chkconfig NetworkManager off <RETURN>
    ```

    - When using Red Hat Enterprise Linux 7

    ```
    # systemctl stop NetworkManager <RETURN>
    # systemctl disable NetworkManager <RETURN>
    ```

2. After modifying the "/etc/sysconfig/network-scripts/ifcfg-e*xxx*" file, configure "no" for "NM_CONTROLLED".

    e*xxx* is the configuration file for the Ethernet interface.
    When using Red Hat Enterprise Linux 5 and Red Hat Enterprise Linux 6, "eth0", "eth1", or "eth2" will be used as the file name.
    When using Red Hat Enterprise Linux 7, "enp1s0f1" or "enp5s0f1" will be used as the file name.

    Example

    - Before modifying

    ```
    DEVICE="eth0"
    HWADDR="xx:xx:xx:xx:xx:xx"
    NM_CONTROLLED="yes"
    ONBOOT="yes"
    TYPE=Ethernet
    ```

    - After modifying

    ```
    DEVICE="eth0"
    HWADDR="xx:xx:xx:xx:xx:xx"
    ```

```
NM_CONTROLLED="no"
ONBOOT="yes"
TYPE=Ethernet
```

3. Execute the following command to restart the Network service.

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

     ```
     # service network restart <RETURN>
     ```

   - When using Red Hat Enterprise Linux 7

     ```
     # systemctl restart network <RETURN>
     ```

2.2.1.2 Collecting and Checking Required Information

Before installing Resource Orchestrator, collect required information and check the system status, then determine the information to be specified on the installation window. The information that needs to be prepared is given below.

- Installation folder and available disk space

  Decide the installation folder for Resource Orchestrator. Check that the necessary disk space can be secured on the drive for installation. For the amount of disk space necessary for Resource Orchestrator, refer to "6.1.1.6 Static Disk Space" and "6.1.1.7 Dynamic Disk Space" in the "Overview".

- Port number

  When Resource Orchestrator is installed, the port numbers used by it will automatically be set in the services file of the system. So usually, there is no need to pay attention to port numbers.
  If the port numbers used by Resource Orchestrator are being used for other applications, a message indicating that the numbers are in use is displayed when the installer is started, and installation will stop.
  In that case, describe the entries for the port numbers used by Resource Orchestrator in the services file using numbers not used by other software, and then start the installer.
  For details, refer to "9.1.6 Changing Port Numbers" in the "User's Guide VE".

- Check the status of the admin LAN and NIC

  Decide the network (IP addresses) to be used for the admin LAN.
  Check that the NIC used for communication with the admin LAN is enabled.
  For details on admin LANs, refer to "7.2 IP Addresses (Admin LAN)" in the "Design Guide VE".

  [Linux] [Xen] [KVM]
  Make the numeral of the managed server's network interface name (ethX) one of a consecutive sequence starting from 0. For the settings, refer to the manual for the OS.

- Check the target disk of image operations

  For backup and restoration of system images to disks, refer to "16.1 Overview" in the "User's Guide VE".
  For details on disks for cloning, refer to "17.1 Overview" in the "User's Guide VE".

- Windows Volume License Information [Windows]

  When using the following functions, you must have a volume license for the version of Windows to be installed on managed servers by Resource Orchestrator.
  Check whether the Windows license you have purchased is a volume license.

  - Server switchover (HBA address rename method/VIOM server profile switchover method/ISM profile switchover method)

  - Cloning

  - Restoration after server replacement

  - Server replacement using HBA address rename

When using cloning, you must enter volume license information when installing Resource Orchestrator.
Depending on the version of Windows being used, check the following information prior to installation.

- For Windows Server 2012 or Later

  Check the information necessary for license authentication (activation).
  The two activation methods are Key Management Service (KMS) and Multiple Activation Key (MAK). Check which method you will use.

  Check the following information required for activation depending on the method you will use.

  - Activation Information

    Table 2.2 Activation Information Methods and Information to Check

Method	Information to Check
KMS (*1)	- The KMS host name (FQDN) or the computer name or IP address - Port number (Default 1688) (*2)
MAK	The MAK key

    *1: When using Domain Name Service (DNS) to automatically find the KMS host, checking is not necessary.
    *2: When changing the port number from the default (1688), correct the definition file after installing agents. Refer to "17.2 Collecting" in the "User's Guide VE".

  - Proxy Server Information

    When using a proxy server to connect to the KMS host (KMS method) or the Volume Activation Management Tool (VAMT) to authenticate a proxy license (MAK method), check the host name or IP address, and the port number of the proxy server.

  - Administrator's Password

    Check the password as it is necessary for performing activation.

- Windows Administrator accounts

  When using Windows Server 2012 or later, check whether Administrator accounts have been changed (renamed).
  Environments which have been changed (renamed) are not supported.

2.2.2 Installation [Windows] [Hyper-V]

This section explains the procedure for agent installation.

Before installation, check if "2.2.1 Preparations" have been performed.

1. Log on to the system as the administrator.

   Log on to the system on which the agent is to be installed using the Administrator account.

2. Set the first Resource Orchestrator DVD-ROM.

   Then, the installer starts automatically.

   Information

   If the installer does not start, execute "RcSetup.exe" from the DVD-ROM drive.

3. Select [Virtual Edition].

4. Click [Agent installation].

5. The Resource Orchestrator setup window will be displayed.

   Check the contents of the license agreement window etc. and then click [Yes].

6. The [Choose Install Location] window is displayed.

   Click [Next>] to use the default Installation Folder. To change folders, click [Browse], change folders, and then click [Next>].

Note

When changing the folders, be careful about the following points.

- Do not specify the installation folder of the system (such as C:\).
- Enter the location using 100 characters or less. Do not use double-byte characters or the following symbols in the folder name.

  """", "|", ":", "*", "?", "/", ".", "<", ">", ",", "%", "&", "^", "=", "!", ";", "#", "'", "+", "[", "]", "{", "}"

- When using a 64-bit Windows Server OS, the following folder name cannot be specified for the installation folder.
  - "%SystemRoot%\System32\"
- When using cloning, installation on the OS system drive is advised, because Sysprep initializes the drive letter during deployment of cloning images.

7. The [Admin Server Registration] window will be displayed.

   Specify the admin LAN IP address of the admin server, and then click [Next>].

   Admin Server IP Address

   Specify the IP address of the admin server. When the admin server has multiple IP addresses, specify the IP address used for communication with managed servers.

8. The [License Authentication] window will be displayed.

   Enter the license authentication information for the Windows volume license.
   As license authentication information is not necessary if cloning will not be used, click [Next>] without selecting [Using the cloning feature of this product].

   If cloning will be used, depending on the version of Windows being used, specify the following information collected in "Windows Volume License Information [Windows]" of "2.2.1.2 Collecting and Checking Required Information", and click [Next>].

   For Windows Server 2012 or Later

   License Authentication Method

   Select the license authentication method from Key Management Service (KMS) and Multiple Activation Key (MAK).

   - When Key Management Service (KMS) is selected

     KMS host

     Enter the host name of the KMS host name, and the computer name or IP address.
     When using Domain Name Service (DNS) to automatically find the KMS host, this is not necessary.

   - When Multiple Activation Key (MAK) is selected

     The MAK key

     Enter the MAK key for the computer the agent is to be installed on.

     Confirm Multiple Activation Key

     Enter the MAK key again to confirm it.

   Proxy server used for activation

   Enter the host name or IP address of the proxy server.
   When the proxy server has a port number, enter the port number.

   Administrator's Password

   Enter the administrator password for the computer the agent is to be installed on.

Note

If an incorrect value is entered for [Product Key], [Key Management Service host], [The MAK Key], or [Proxy server used for activation] on the [License Authentication Information Entry] window, cloning will be unable to be used.
Check that the correct values have been entered.

9. The [Start Copying Files] window will be displayed.

   Check that there are no mistakes in the contents displayed on the window, and then click [Install>].
   Copying of files will start.
   To change the contents, click [<Back].

10. The Resource Orchestrator setup completion window will be displayed.

    When setup is completed, the [Installshield Wizard Complete] window will be displayed.
    Click [Finish] and close the window.

Note

- Corrective Action for Installation Failure

  When installation is stopped due to errors (system errors, processing errors such as system failure, or errors due to execution conditions) or cancellation by users, remove the causes of any problems, and then take corrective action as follows.

  - Open [Programs and Functions] from the Windows Control Panel, and when "ServerView Resource Orchestrator Agent" is displayed, uninstall it and then install the agent again.
    For uninstallation, refer to "11.2 Agent Uninstallation"

  - If [ServerView Resource Orchestrator Agent] is not displayed, install it again.

- Nullifying Firewall Settings for Ports to be used by Resource Orchestrator

  When installing Resource Orchestrator on systems with active firewalls, in order to enable the manager to communicate with agents correctly, disable the firewall settings for the port numbers to be used for communication.
  For the port numbers used by Resource Orchestrator and required software, refer to "Appendix A Port List" in the "Design Guide VE".
  However, when port numbers have been changed by editing the services file during installation of Resource Orchestrator, replace the default port numbers listed in "Appendix A Port List" in the "Design Guide VE" with the port numbers changed to during installation.

- Uninstall the Related Services

  When installing ServerView Deployment Manager after Resource Orchestrator has been installed, or using ServerView Deployment Manager in the same subnet, it is necessary to uninstall the related services.

  For the method for uninstalling the related services, please refer to "5.1 deployment_service_uninstall" in the "Reference Guide (Command) VE".

2.2.3 Installation [Linux] [VMware] [Xen] [KVM]

This section explains the procedure for agent installation.

Before installation, check if "2.2.1 Preparations" have been performed.

1. Log in to the system as the OS administrator (root).

   Boot the managed server that the agent is to be installed on in multi-user mode, and then log in to the system using root.

   [Xen] [KVM]
   Log in from the console.

2. Set the first Resource Orchestrator DVD-ROM.

3. Execute the following command to mount the DVD-ROM.

```
# mount -t iso9660 -r /dev/hdc DVD-ROM_mount_point <RETURN>
```

Note

If the auto-mounting daemon (autofs) is used for starting the mounted DVD-ROM, the installer will fail to start due to its "noexec" mount option.

4. Execute the following installation command:

   ```
   # cd DVD-ROM_mount_point <RETURN>
   # ./RcSetup.sh <RETURN>
   ```

5. Select "Virtual Edition".

6. Select "Agent installation".

7. Perform installation according to the installer's interactive instructions.

8. Enter the host name or IP address of a connected admin server.

9. Settings when SELinux is Used

   When enabling SELinux, it is necessary to perform configuration of SELinux after installing Resource Orchestrator.
   For details on configuration, refer to "H.1.2 Agent".

[Citrix Xen]
When using Citrix XenServer, restart the managed server.

[Xen]
When using the Linux virtual machine function of Red Hat Enterprise Linux 5 and not using I/O Virtualization (VIOM or ISM), use the following procedure.

1. After using the following command to disable the automatic startup setting of the xend daemon, restart the managed server.

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

2. After the restart is complete, use the following command to update the bind settings of the MAC address. Then, enable the automatic startup setting of the xend daemon and start the xend daemon.

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

Note

- Corrective Action for Installation Failure

  In the event of installation failure, restart and then log in as the user that performed the installation, and perform uninstallation following the uninstallation procedure.
  After that, remove the cause of the failure referring to the meaning of the output message and the suggested corrective actions, and then perform installation again.

- Nullifying Firewall Settings for Ports to be used by Resource Orchestrator

  When installing Resource Orchestrator on systems with active firewalls, in order to enable the manager to communicate with agents correctly, disable the firewall settings for the port numbers to be used for communication.

  #### Example

  [VMware]

  ```
  # /usr/sbin/esxcfg-firewall -openPort 23458,tcp,in,"nfagent" <RETURN>
  ```

For the port numbers used by Resource Orchestrator and required software, refer to "Appendix A Port List" in the "Design Guide VE". However, when port numbers have been changed by editing the services file during installation of Resource Orchestrator, replace the default port numbers listed in "Appendix A Port List" in the "Design Guide VE" with the port numbers changed to during installation.

- When Installation was Performed without using the Console [Xen] [KVM]

  When installation is performed by logging in from somewhere other than the console, the network connection will be severed before installation is complete, and it is not possible to confirm if the installation was successful. Log in from the console and restart the managed server. After restarting the server, follow the procedure in "Corrective Action for Installation Failure" and perform installation again.

- Uninstall the Related Services

  When installing ServerView Deployment Manager after Resource Orchestrator has been installed, or using ServerView Deployment Manager in the same subnet, it is necessary to uninstall the related services.

  For the method for uninstalling the related services, please refer to "5.1 deployment_service_uninstall" in the "Reference Guide (Command) VE".

2.2.4 Installation [Solaris] [Solaris Zones] [OVM for SPARC]

This section explains the procedure for agent installation.

Before installation, check if "2.2.1 Preparations" have been performed.

1. Log in to the system as the OS administrator (root).

   Boot the managed server that the agent is to be installed on in multi-user mode, and then log in to the system using root.

2. Set the first Resource Orchestrator DVD-ROM.

3. Execute the following installation command:

```
# cd DVD-ROM_mount_point <RETURN>
# ./RcSetup.sh <RETURN>
```

4. Select "Virtual Edition".

5. Select "Agent installation".

6. Perform installation according to the installer's interactive instructions.

Information

When a guest domain on OVM for SPARC is registered as a VM host, it is necessary to install agent in that guest domain.

Note

- Corrective Action for Installation Failure

  Execute the following command, delete the packages from the environment in which installation failed, and then perform installation again.

```
# cd DVD-ROM_mount_point/DISK1/Agent/Solaris/agent <RETURN>
# ./rcxagtuninstall <RETURN>
```

- Nullifying Firewall Settings for Ports to be used by Resource Orchestrator

  When installing Resource Orchestrator on systems with active firewalls, in order to enable the manager to communicate with agents correctly, disable the firewall settings for the port numbers to be used for communication.

For the port numbers used by Resource Orchestrator and required software, refer to "Appendix A Port List" in the "Design Guide VE". However, when port numbers have been changed by editing the services file during installation of Resource Orchestrator, replace the default port numbers listed in "Appendix A Port List" in the "Design Guide VE" with the port numbers changed to during installation.

2.3 HBA address rename Setup Service Installation

This section explains installation of the HBA address rename setup service.

The HBA address rename setup service is only necessary when using HBA address rename.
For details, refer to "Chapter 4 System Configuration Design" in the "Design Guide VE".

2.3.1 Preparations

This section explains the preparations and checks required before commencing installation.

- Exclusive Software Checks

  Refer to "Exclusive Software Checks".

- Required Software Checks

  Refer to "Required Software Checks".

- Required Patch Checks

  Refer to "Required Patch Checks".

- Required Package Checks

  Refer to "Required Package Checks [Linux]".

2.3.1.1 Software Preparation and Checks

Software preparation and checks are explained in the following sections.

Exclusive Software Checks

Uninstall exclusive software before installing Resource Orchestrator.

For details of exclusive software, refer to "6.1.1.5 Exclusive Software" in "Overview".

Required Software Checks

Before installing Resource Orchestrator, check that the required software given in "6.1.1.4 Required Software" in the "Overview" has been installed. If it has not been installed, install it before continuing.

Required Patch Checks

Before installing Resource Orchestrator, check that the required patches for the HBA address rename setup service listed in "6.1.1.2 Required Patches" in the "Overview" have been applied.

If they have not been applied, apply them before continuing.

Required Package Checks [Linux]

Before installing Resource Orchestrator, check that the required packages for the HBA address rename setup service [Linux] listed in "6.1.1.3 Required Packages" in the "Overview" have been applied.

If they have not been installed, install them before continuing.

2.3.1.2 Collecting and Checking Required Information

Before installing Resource Orchestrator, collect required information and check the system status, then determine the information to be specified on the installation window. The information that needs to be prepared is given below.

- Installation folder and available disk space

  Decide the installation folder for Resource Orchestrator. Check that the necessary disk space can be secured on the drive for installation. For the amount of disk space necessary for Resource Orchestrator, refer to "6.1.1.6 Static Disk Space" and "6.1.1.7 Dynamic Disk Space" in the "Overview".

2.3.2 Installation [Windows]

Install the HBA address rename setup service using the following procedure.

Before installation, check if "2.3.1 Preparations" have been performed.

1. Log on to the system as the administrator.

   Log on to the system on which the HBA address rename setup service is to be installed using the Administrator account.

2. Set the first Resource Orchestrator DVD-ROM.

   Then, the installer starts automatically.

   Information

   If the installer does not start, execute "RcSetup.exe" from the DVD-ROM drive.

3. Select [Virtual Edition].

4. Click [HBA address rename setup service installation].

5. The Resource Orchestrator setup window will be displayed.

   Check the contents of the license agreement window etc. and then click [Yes].

6. The [Choose Install Location] window is displayed.

   Click [Next>] to use the default Installation Folder. To change folders, click [Browse], change folders, and then click [Next>].

   Note

   When changing the folders, be careful about the following points.

   - Do not specify the installation folder of the system (such as C:\).
   - Enter the location using 100 characters or less. Do not use double-byte characters or the following symbols in the folder name.

     """", "|", ":", "*", "?", "/", ".", "<", ">", ",", "%", "&", "^", "=", "!", ";", "#", "'", "+", "[", "]", "{", "}"

   - When using a 64-bit Windows Server OS, the following folder name cannot be specified for the installation folder.
     - "%SystemRoot%\System32\"
     - Folder names including "Program Files" (except the default "C:\Program Files (x86)")

7. The [Start Copying Files] window will be displayed.

   Check that there are no mistakes in the contents displayed on the window, and then click [Install>].

   Copying of files will start.

   To change the contents, click [<Back].

8. The Resource Orchestrator setup completion window will be displayed.

   When using the HBA address rename setup service immediately after configuration, check the [Yes, launch it now.] checkbox.

   Click [Finish] and close the window.

   - If the check box is checked

     The HBA address rename setup service will start after the window is closed.

   - If the check box is not checked

     Refer to "6.1 Settings for the HBA address rename Setup Service", and start the HBA address rename setup service.

Note

- Corrective Action for Installation Failure

  When installation is stopped due to errors (system errors, processing errors such as system failure, or errors due to execution conditions) or cancellation by users, remove the causes of any problems, and then take corrective action as follows.

  - Open [Programs and Features] from the Windows Control Panel, and when "ServerView Resource Orchestrator HBA address rename setup service" is displayed, uninstall it and then install the agent again.
    For uninstallation, refer to "11.3 HBA address rename Setup Service Uninstallation.

  - If [ServerView Resource Orchestrator HBA address rename setup service] is not displayed, install it again.

- Nullifying Firewall Settings for Ports to be used by Resource Orchestrator

  When installing Resource Orchestrator on systems with active firewalls, in order to enable correct communication between the manager, agents, and clients, disable the firewall settings for the port numbers to be used for communication.

  For the port numbers used by Resource Orchestrator and required software, refer to "Appendix A Port List" in the "Design Guide VE".

  However, when port numbers have been changed by editing the services file during installation of Resource Orchestrator, replace the default port numbers listed in "Appendix A Port List" in the "Design Guide VE" with the port numbers changed to during installation.

2.3.3 Installation [Linux]

Install the HBA address rename setup service using the following procedure.

Before installation, check if "2.3.1 Preparations" have been performed.

1. Log in to the system as the OS administrator (root).

   Boot the managed server that the HBA address rename setup service is to be installed on in multi-user mode, and then log in to the system using root.

2. Set the first Resource Orchestrator DVD-ROM.

3. Execute the following command to mount the DVD-ROM.

```
# mount -t iso9660 -r /dev/hdc DVD-ROM_mount_point <RETURN>
```

   Note

   If the auto-mounting daemon (autofs) is used for starting the mounted DVD-ROM, the installer will fail to start due to its "noexec" mount option.

4. Execute the following installation command:

```
# cd DVD-ROM_mount_point <RETURN>
# ./RcSetup.sh <RETURN>
```

5. Select "Virtual Edition".

6. Select "HBA address rename setup service installation".
7. Perform installation according to the installer's interactive instructions.
8. Settings when SELinux is Used

   When enabling SELinux, it is necessary to perform configuration of SELinux after installing Resource Orchestrator.
   For details on configuration, refer to "H.1.3 HBA address rename Setup Service".

Note

- Corrective Action for Installation Failure

  Execute the following command, delete the packages from the environment in which installation failed, and then perform installation again.

  ```
  # cd DVD-ROM_mount_point/DISK1/HBA/Linux/hbaar <RETURN>
  # ./rcxhbauninstall <RETURN>
  ```

- Nullifying Firewall Settings for Ports to be used by Resource Orchestrator

  When installing Resource Orchestrator on systems with active firewalls, in order to enable correct communication between the manager, agents, and clients, disable the firewall settings for the port numbers to be used for communication.

  For the port numbers used by Resource Orchestrator and required software, refer to "Appendix A Port List" in the "Design Guide VE".

  However, when port numbers have been changed by editing the services file during installation of Resource Orchestrator, replace the default port numbers listed in "Appendix A Port List" in the "Design Guide VE" with the port numbers changed to during installation.

Chapter 3 Login to the ROR Console

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

Preparations

Preparations are necessary for log in to the ROR console.

Refer to "Chapter 1 Login and Logout" in the "User's Guide VE".

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.

For details on Single Sign-On, refer to "Chapter 10 Configuring Single Sign-On" in the "Design Guide VE".

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

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

Information

For details, refer to "Chapter 1 Login and Logout" in the "User's Guide VE".

Login

In the login screen, enter the following items, and click [Login].
The ROR console is displayed after a successful login.

- User ID
- Password

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"

- 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.

If Single Sign-On has been configured, when login to the ROR console fails, configuration of the environment may have failed.

Stop the manager, and reconfigure Single Sign-On.

For details on how to reconfigure Single Sign-On, refer to "13.1 When Configuring Single Sign-On" in the "Operation Guide VE".

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, the user may stay logged in, making it possible to access the ROR console without authentication.
  It is advised that the users log out properly after using the ROR console or BladeViewer.
- If the ROR console has been opened simultaneously in several Web browser windows, those login sessions may also be terminated.

Exit

To exit the ROR console, simply close the Web browser window.

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 the [Add] button in the displayed dialog.

   The [Register License] dialog is displayed.

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

3. Click the [OK] button.

   The license will be registered.

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".

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".

Point

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

Chapter 5 Registering Resources with Resource Orchestrator

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 way of registering each resource individually, it is also possible to register or change registration settings of multiple resources together 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.

  For details on the order for registering the resources to manage with Resource Orchestrator, refer to "5.1 Managed Resources and Registration Order".

- Registering or modifying multiple resources collectively

  This method is used when there are many (five or more) servers to be installed.
  For information on registering or changing multiple resources in batches, refer to "Chapter 12 Pre-configuration for Resource Registration and Modification" in the "User's Guide VE".

Information

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 details on backing up, refer to "9.2 Backup" in the "Operation Guide VE".

5.1 Managed Resources and Registration Order

This section explains managed resources and the registration order for resources.

Managed Resources

The following resources can be managed with Resource Orchestrator.

- VIOM
- ISM
- VM management software
- Server management software
- Chassis
- Managed servers
- LAN Switches
- LAN switch blades
- Power monitoring devices
- Network devices

Registration Order of Resources

Use the following procedure to register resources:

- When Using Blade Servers

    1. Register VIOM (when using VIOM)

        Refer to "7.1 Registering VIOM/ISM Coordination" in the "User's Guide VE".

    2. Register VM Management Software (when using VM Management Software)

        Refer to "7.2 Registering VM Management Software" in the "User's Guide VE".

    3. Register Chassis

        Refer to "7.3.1 Registering Chassis" in the "User's Guide VE".

    4. Register admin LAN subnets (when there are multiple admin LAN subnets)

        Refer to "7.9 Registering Admin LAN Subnets" in the "User's Guide VE".

    5. Register Managed Servers (within Chassis)

        Refer to "7.3.2 Registering Blade Servers" in the "User's Guide VE".

    6. Register LAN switch blades

        For details, refer to "7.3.3 Registering LAN Switch Blades" in the "User's Guide VE".

    7. Register Power Monitoring Devices

        For details, refer to "7.8 Registering Power Monitoring Devices" in the "User's Guide VE".

- When Using Rack Mount or Tower Servers

    1. Register VIOM or ISM (when using rack mount servers supported by VIOM or ISM)

        Refer to "7.1 Registering VIOM/ISM Coordination" in the "User's Guide VE".

    2. Register VM Management Software (when using VM Management Software)

        Refer to "7.2 Registering VM Management Software" in the "User's Guide VE".

    3. Register admin LAN subnets (when there are multiple admin LAN subnets)

        Refer to "7.9 Registering Admin LAN Subnets" in the "User's Guide VE".

    4. Register Managed Servers

        Refer to "7.4.1 Registering Rack Mount or Tower Servers" in the "User's Guide VE".
        When configuring public LAN information, refer to "7.4.3 Registering the Public LAN (MAC Address) Information" in the "User's Guide VE".

    5. Register LAN Switches

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

    6. Register Power Monitoring Devices

        For details, refer to "7.8 Registering Power Monitoring Devices" in the "User's Guide VE".

- When Using PRIMEQUEST Servers

    1. Register VM Management Software (when using VM Management Software)

        Refer to "7.2 Registering VM Management Software" in the "User's Guide VE".

    2. Register Chassis

        Refer to "7.6.1 Registering Chassis (For PRIMEQUEST Servers)" in the "User's Guide VE".

    3. Register admin LAN subnets (when there are multiple admin LAN subnets)

        Refer to "7.9 Registering Admin LAN Subnets" in the "User's Guide VE".

4. Register Managed Servers (within Chassis)

   Refer to "7.6.2 Registering PRIMEQUEST Servers" in the "User's Guide VE".

- When using SPARC Enterprise M4000/M5000/M8000/M9000 or SPARC M10-4S/M12-2S

  1. Register chassis

     Refer to "7.7.1 Registering Chassis (SPARC Enterprise M4000/M5000/M8000/M9000) or SPARC M10-4S/M12-2S" in the "User's Guide VE".

  2. Register admin LAN subnets (when there are multiple admin LAN subnets)

     Refer to "7.9 Registering Admin LAN Subnets" in the "User's Guide VE".

  3. Register Managed Servers (within Chassis)

     Refer to "7.7.2 Registering SPARC Enterprise (M3000/T Series) servers or SPARC M10 M10-1/M10-4/M12-1/M12-2" in the "User's Guide VE".

  4. Register Power Monitoring Devices

     For details, refer to "7.8 Registering Power Monitoring Devices" in the "User's Guide VE".

- When using SPARC Enterprise M3000 or SPARC M10-1/M10-4/M12-1/M12-2

  1. Register admin LAN subnets (when there are multiple admin LAN subnets)

     Refer to "7.9 Registering Admin LAN Subnets" in the "User's Guide VE".

  2. Register Managed Servers

     Refer to "7.7.2 Registering SPARC Enterprise (M3000/T Series) servers or SPARC M10 M10-1/M10-4/M12-1/M12-2" in the "User's Guide VE".

  3. Register Power Monitoring Devices

     For details, refer to "7.8 Registering Power Monitoring Devices" in the "User's Guide VE".

- When Using SPARC Enterprise T5120/T5140/T5220/T5240/T5440 Servers

  1. Register admin LAN subnets (when there are multiple admin LAN subnets)

     Refer to "7.9 Registering Admin LAN Subnets" in the "User's Guide VE".

  2. Register Managed Servers

     Refer to "7.7.2 Registering SPARC Enterprise (M3000/T Series) servers or SPARC M10 M10-1/M10-4/M12-1/M12-2" in the "User's Guide VE".

  3. Register Power Monitoring Devices

     For details, refer to "7.8 Registering Power Monitoring Devices" in the "User's Guide VE".

- When Using Network Devices

  1. Enable the Management Functions of Network Devices

     Refer to "7.5.1 Enabling the Network Device Management Function" in the "User's Guide VE".

  2. Create the Network Configuration Information

     Refer to "7.5.2 Creating the Network Configuration Information (XML Definition)" in the "User's Guide VE".

  3. Edit Model Definitions (when registering unsupported models of network devices)

     Refer to "8.2 Network Device Model Definition" in the "Reference Guide (Command) VE".

  4. Register Network Devices

     Refer to "7.5.3 Registering Network Devices" in the "User's Guide VE".

Installing Software and Registering Agents on Managed Servers

When not registering agents, or registering servers with the checkbox for the automatic registration of agents cleared, refer to "Chapter 7 Installing Software and Registering Agents on Managed Servers".

Chapter 6 Configuration after Manager Installation

6.1 Settings for the HBA address rename Setup Service

This section explains settings for the HBA address rename setup service.

In Resource Orchestrator, configure the WWN on the servers according to the server operations, and adopt I/O virtualization (HBA address rename) that enables I/O control on the server side.

HBA address rename is enabled by setting the WWN of the managed server HBA from the admin server when a managed server is powered on. This WWN is kept by managed servers until powered off.

However, a managed server will not be able to receive its assigned WWN unless it can communicate with the admin server. If communication with the admin server fails, because of problems on the admin server or a failure of the managed server's NIC, the managed server will not start up properly as its HBA will not be set up with the correct WWN.
This can be avoided by using the HBA address rename setup service, which acts as a backup service in case of communication issues between the admin server and managed servers. This service, which must run on a server other than the admin server, can set up the WWNs of managed server HBAs in the same way as the admin server does.

For details on HBA address rename settings, refer to "7.4.2 HBA address rename Settings" in the "User's Guide VE".

This service must be running in order to use HBA address rename.

Use the following procedure to configure the HBA address rename setup service.

1. Open the [HBA address rename setup service] dialog.

   [Windows]
   Select [start]-[All Programs]-[ServerView Resource Orchestrator]-[HBA address rename setup service].

   [Linux]
   Execute the following command while in a desktop environment.

   ```
   # nohup /opt/FJSVrcvhb/bin/rcxhbactl start& <RETURN>
   ```

   The [HBA address rename setup service] dialog is displayed.

2. Set the following items:

   Status

   The status of the service is displayed. [Stopping] is displayed if the service is not running, and [Running] is displayed if the service is running.

   IP address of admin server

   Enter the IP address of the admin server.

   Port number

   Enter the port number that is used to communicate with the admin server. The port number at installation is 23461.
   If the "rcxweb" port number of the admin server is changed, specify the number that has been changed.

   The latest synchronous time

   Displays the latest synchronization time.
   This is the last time this service synchronized its data (managed server settings) with that of the admin server.

3. Click one of the following buttons:

   - To Start This Service:

     Click [Run].

   - To Stop This Service:

     Click [Stop].

- To Cancel the Operation:

  Click [Cancel].

To verify that this service is running properly, power off the admin server and confirm that managed servers can still start up normally.

Point

When the graphical mode cannot be used, use the service rcvhb {stop | start | status} command to stop, start, or check the status of services after starting the HBA address rename setup service once.

When operating correctly, the descriptions are displayed as below.

[Linux]

```
# service rcvhb status
rservice is running...
pxeservice is running...
SystemcastWizard TFTP service is running...
```

Information

The services related to ROR that operate on the HBA address rename setup service server are as follow:

[Windows]

- Resource Coordinator WWN Recovery Service
- Fujitsu PXE MTFTP Service
- Fujitsu PXE Services

[Linux]

- rservice
- pxeservice
- SystemcastWizard TFTP service

Note

The following remarks apply to this service.

- Keep it [Running] at all times.
- Start it on only one server for each admin server.
- OS administrator privileges are required to start and stop this service.
- Do not operate it on the server where the manager is installed.
- The admin server and the servers configured with the HBA address rename setup service must be placed in the same segment of an admin LAN.

[Windows]

- In a clustered Manager configuration, this service can be run on the standby node. In this case, configure the startup settings following the procedure in the Manager Cluster Operation Settings.
  After performing settings for this service following the procedure for cluster operation settings, it is not necessary to perform the above procedure for starting and stopping.
  For details, refer to "Appendix C Manager Cluster Operation Settings and Deletion".

[Linux]

- In a clustered Manager configuration, this service can be run on the standby node. In this case, the above procedure should be skipped as configuration and control of the HBA address rename setup service is handled during setup of the cluster system.
  For details, refer to "Appendix C Manager Cluster Operation Settings and Deletion".

6.2 Settings for ISM Coordination

This section explains configuration for using ServerView Infrastructure Manager.

1. Install the ServerView Infrastructure Manager virtual appliance on a server other than the admin server.
   For the installation method, refer to the manuals of ServerView Infrastructure Manager.

   Note

   - In ISM V2.2 or later, if the power of an iRMC is lost the virtual I/O settings applied to the profile will also be lost.
     In that case, it is necessary to re-apply the virtual I/O settings.
     For the method for re-applying the virtual I/O settings, refer to the ISM User's Manual.

   - With ISM V2.3 or later, the default version of the usable SSL/TLS protocol is set as TLSv1.2.
     When using an installation upgraded from ISM V2.2.x, the conventional TLSv1 can be used.
     When performing a new installation of ISM V2.3 or later, configure it so that ISM can also use TLSv1.
     For details of the method for specifying

     ```
     # ismadm security enable-tls TLSv1,TLSv1.1,TLSv1.2
     ```

     and an example of execution, refer to "4.20 Changing the SSL/TLS Protocol Version" in the ISM V2.3 User's Manual.

   - When performing a new installation of ISM V2.4.c or later, ISM V2.5, or ISM V2.6 or later

     1. Execute the following command within the Infrastructure Manager console with Administrator privileges

        ```
        # ismadm security set-sslcipher 1
        ```

     2. Restart ISM-VA

        ```
        # ismadm power restart
        ```

   The following steps are only necessary when using PXE boot in ISM.

2. Prepare a (Windows) server other than the admin server or managed servers.

3. Configure the server as a DHCP server using the following procedure:

   a. Add DHCP Server to the server roles.

      Bind the DHCP server to the network connection of a NIC configured with an IP address in the same network as the admin LAN of the admin server.

      For details on adding and binding, refer to the Windows documentation.

      When the DHCP server is a member of a domain, perform the following step.

   b. Authorize the DHCP server.

      1. Click [Control Panel]-[Administrative Tools]-[DHCP].

         The [DHCP] window is displayed.

      2. Select [Action]-[Manage authorized servers].

         The [Manage Authorized Servers] window will be displayed.

      3. Click the [Authorize] button.

         The [Authorize DHCP Server] window will be displayed.

      4. Enter the admin IP address of the admin server in [Name or IP address].

5. Click the [OK] button.

   The [Confirm Authorization] window will be displayed.

6. Check the [Name] and [IP Address].

7. Click the [OK] button.

   The DHCP server will be added to the [Authorized DHCP servers] on the [Manage Authorized Servers] window.

4. Install a Resource Orchestrator agent on the DHCP server.

   For details, refer to "2.2.2 Installation [Windows] [Hyper-V]".

   Note

   - Select [Express/Virtual Edition] for the agent edition.
   - On the [License Authentication Information Entry] window, click [Next>] without selecting [Using the cloning feature of this product].

Note

- The basic software which can be installed on the DHCP server is the same as that of the Resource Orchestrator agent [Windows].
- The DHCP server is also able to manage VM guests created using virtualization software.
- It is not necessary to install ServerView Agents for Windows, which is required software for the Resource Orchestrator agent [Windows], on the DHCP server.
- When using PXE boot in ISM, it is necessary to temporarily stop the PXE services of the admin server using the rcxadm pxectl command.

  For details, refer to "3.5 rcxadm pxectl" in the "Reference Guide (Command) VE".

- While the PXE services of the admin server are stopped, the following functions cannot be used.
  - HBA address rename settings
  - Server switchover and failback (based on the HBA address rename and backup-restore methods)
  - Backup and restore
  - Deletion of system images
  - Collection of cloning images
  - Deployment of cloning images
  - Deletion of cloning images
  - Execution of the rcxadm imagemgr set command
  - Registration of servers
  - Deletion of servers
  - Changing of the admin LAN IP addresses of managed servers
  - Registration of admin subnets

Information

To transfer a managed server from being managed by VIOM to being managed by ISM, perform the following procedure.

1. If a spare server is configured for the target server, release the spare server settings.

2. Start the ServerView Virtual-IO Manager Web UI.

   For details, refer to "7.1.1 Registering Profiles" in the "User's Guide VE".

   a. Delete the profile of the relevant server.

   b. Remove the server from the targets of management by VIOM.

3. Start the ServerView Infrastructure Manager Web UI.

   a. Configure the profile of the target server.

      For details, refer to the manuals of ServerView Infrastructure Manager.

4. Regular update processing of Resource Orchestrator is performed.

   The fact that the target server is now being managed by ISM is reflected on Resource Orchestrator.

5. If necessary, reconfigure the spare server for the transferred server.

6.3 Creating Windows PE

When using the following functions of this product, it is necessary to create a Windows PE after installing the manager of Resource Orchestrator. For details, refer to the "Windows PE Creation Script Guide".

List of Resource Orchestrator Functions Requiring Windows PE

- Backup and restore of physical servers
- Collection and deployment of physical server cloning images
- Server switchover for physical servers (Backup and restore method)
- Collection of information of disks that can be operated using image operations for managed servers

Chapter 7 Installing Software and Registering Agents on Managed Servers

This chapter explains how to install software and register agents on managed servers.

Use the following procedure to install required software and register an agent on a managed server.

After agent registration, the physical OS or VM host on which the agent was installed will be displayed in the server resource tree. Usually, a server agent is automatically registered during server registration. In that case, this procedure can be skipped.

It is not necessary to re-install an already-setup operating system, required software, or agent. Simply skip the steps that were already performed.

1. Install an OS

   a. Install the operating system on the managed server.

   b. Set up the admin LAN.

      Set the admin LAN IP address that was chosen for this server in "7.2 IP Addresses (Admin LAN)" in the "Design Guide VE", as well as its corresponding network mask and default gateway.

   Using storage devices in multi-path configurations

   - Install a multi-path driver on a physical OS and VM hosts. For VM hosts, use the one provided by default by either the operating system or virtualization software, when one is available.

   - When using SAN boot and HBA address rename, refer to "2. Settings for the HBA address rename Function" in "7.4.2 HBA address rename Settings" in the "User's Guide VE" to set the number of HBA paths used with HBA address rename for the number of HBA ports.
     The server is automatically restarted using a multi-path configuration.

   - When using SAN boot together with VIOM/ISM, follow the procedure described in "7.1.1 Registering Profiles" in the "User's Guide VE" to configure profiles on the Web interface of ServerView Infrastructure Manager.
     After configuration, the server will be started using a multi-path configuration.

   - When using SAN boot together with ESC, follow the procedure described in "10.1 Configuring WWN Settings for ETERNUS SF Storage Cruiser Integration" in the "User's Guide VE", and set the path name for HBA, WWNs of each HBA and the target CA, and Affinity Group. Also, correct the settings of the OS and OBP for multi-path use.
     After configuration, the server will be started using a multi-path configuration.

   Note

   After configuration of agents, the server name (computer name for [Windows] [Hyper-V] or a system node name for [Linux] [Solaris] [Solaris Zones] [VMware] [Xen] [KVM] [Citrix Xen] [OVM for SPARC]) defined during OS installation should be set according to the following guidelines.

   [Windows] [Hyper-V]
   Specify up to 63 characters, including alphanumeric characters, underscores ("_"), and hyphens ("-").
   The string cannot be composed solely of numbers.

   [Linux] [VMware] [Xen] [KVM] [Citrix Xen]
   Specify up to 64 characters, including alphanumeric characters as well as the following symbols.

   "%", "+", ",", "-", ".", "/", ":", "=", "@", "_", "~"

   [Solaris] [Solaris Zones] [OVM for SPARC]
   Specify up to 24 characters, including alphanumeric characters, underscores ("_"), and hyphens ("-"). This name should start with an alphabetical character.

However, it is recommended that the name is comprised of the following characters defined in RFC (Request For Comment) 952, to take into consideration communication with other servers.

- Alphanumeric Characters
- Hyphens, ("-")
- Periods, (".") [Linux]

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.

[Solaris] [Solaris Zones] [OVM for SPARC]
When the OS is Solaris 11 and the user account was created during installation, root is registered as a 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.

2. Install Required Software

   Install the software packages that are required for a managed server.

   For details of the required software, refer to "6.1.1.4 Required Software" in the "Overview".

Note

When installing BMC BladeLogic RSCD Agent, add managed servers to BladeLogic.
Specify the admin IP addresses of managed servers to add.

3. Install the Agent

   Refer to "2.2 Agent Installation".

4. Register the Agent

   Register the agent from the ROR console while the target server is running.

   [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 "9.2.3 Definition Files of Each Product" in the "Design Guide VE".

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

      The [Register Agent] dialog is displayed.

   b. Select the Server OS category (physical OS or VM host).

      - For servers other than SPARC M10/M12 and SPARC Enterprise

        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.

- For SPARC M10/M12 and SPARC Enterprise

  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.

User ID

Enter the user ID to log in to the VM host.

Specify the user name "root" which has VM host administrator authority.

Note

[Solaris] [Solaris Zones] [OVM for SPARC]
When the OS is Solaris 11 and the user account was created during installation, root is registered as a 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.

c. Click the [OK] button.

The admin server starts to monitor and display server information obtained from the agent.

Note

- If "unknown" is displayed in the server resource tree for the status of a server in which the agent is installed, refer to "2.2 "unknown" Server Status" in "Troubleshooting" to solve the problem.

- 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 hostname 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 "9.2.2 Functional Differences between Products" in the "Design Guide VE".

- When performing system image backup or cloning image collection, it is necessary to either reboot the managed server or restart its "Related services" (explained in "2.2 Starting and Stopping Agents" in the "Operation Guide VE") after server registration.
  For details on how to restart the agent, refer to "2.2 Starting and Stopping Agents" in the "Operation Guide VE".

- A server running a VM host can still be registered as a physical OS if "Windows/Linux" is selected in the [Server OS category] selection list.
  A VM host server that was mistakenly registered as a physical OS should be deleted and re-registered as a VM host.

Chapter 8 Configuring Monitoring Information

This chapter explains how to configure monitoring information.

Use the following procedure to configure the monitoring information.

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. Set the following items:

   [Enable ping monitoring] checkbox

   When using the ping command to monitor the admin LAN for the target physical OS or the VM host, and recovery for the error detection is enabled, select the checkboxes.

   Information

   - When performing these settings, use ping monitoring if the server status becomes "unknown".
   - When the following conditions are satisfied for the physical OS and the VM host for which ping monitoring is enabled, message number 69111 will be output to the event log and recovery triggered. For details on the above message, refer to "Message number 69111" in "Messages".

     - The status of the primary server is "unknown"

     - The period with no response to the ping command is over the time-out value

     - The active server has not been placed into maintenance mode

     - The power of the chassis is not OFF (when using PRIMERGY BX servers)

   Note

   - As this setting uses ping monitoring on the admin LAN, recovery may be triggered even when operations are being performed.
   - With target servers, if another Resource Orchestrator operation is being performed when recovery is triggered, recovery will not take place and monitoring will recommence.
   - If the configured recovery process occurs and restoration is not possible, monitoring of the server will be suspended temporarily. After that, when the status of the server becomes "normal", monitoring will recommence.
   - For VMware ESXi, this function is not supported.
   - If server switchover is performed during recovery, even if a memory dump was set to be collected in the event of an OS failure, the memory dump will not be collected.

   Timeout(sec)

   The time-out period for ping monitoring should be set as a value between 5 and 3,600 seconds.
   One of conditions for recovery is that the amount of time for which there is no response to the "ping" command exceeds the specified time-out value.

   Recovery method

   Select a recovery operation from the following:

   - Reboot

     Perform reboot.

- Reboot (Forced)

  Perform forced reboot.

- Switchover (*)

  Perform a switchover operation based on the spare server settings.

- Reboot+Switchover (*)

  First, perform reboot.
  Reboot operations are only performed the number of times specified in the Number of reboots, and recovery operations end if it is recovered during the reboot cycle.
  Perform switchover if recovery is not successful even after rebooting the specified number of times.
  If a spare server has not been set, only rebooting will take place.

- Reboot(Forced)+Switchover (*)

  First, perform forced reboot.
  Forced reboot operations are performed only the number of times specified in the Number of reboots, and recovery operations end if it is recovered during the reboot cycle.
  Perform switchover if recovery is not successful even after forced rebooting the specified number of times.
  If a spare server has not been set, only forced rebooting will take place.

Number of reboots

Specify the number of reboots or forced reboots as a number between one and three. When specifying twice or more, recovery will not be implemented when restoring.

3. Click the [OK] button.

* Note: Recovery operations including server switchover cannot be performed with PRIMEQUEST, SPARC Enterprise partition models with divided areas, or SPARC M10/M12 in Building Block configurations.

Chapter 9 Settings for Server Switchover

This chapter explains how to use server switchover settings and automatically recover from server failures.

9.1 Overview

Server switchover is a feature that allows the user to switch over applications from a primary server to a predefined spare server when the primary server fails or is stopped for maintenance.
It can also perform Auto-Recovery, which automatically switches applications over to a spare server when a hardware failure is detected on the primary server.
There are the following four methods for switchover to spare servers.
However, each method has its own restrictions regarding supported server configurations (such as hardware environment and boot format).
For details, refer to "9.2 Configuration".

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

Table 9.1 Methods of Switchover to Spare Servers

Method	Overview
Backup and Restore Method	In a local boot environment, this method restores a system image backup to a spare server, which is then automatically started up.
HBA address rename Method	In a SAN boot environment, this method sets the WWN of a spare server's HBA to the same value as that originally set on the primary server. This allows the spare server to connect to and boot from the same boot disk that was used by the primary server.
VIOM Server Profile Switchover method	This method is used in SAN boot environments where servers start from boot disks located in storage arrays. If the primary server fails, the WWN, MAC address, boot configuration, and network configuration that have been set in its server profile using virtual I/O (VIOM) are inherited by the spare server, which then automatically starts up from the same SAN disk.
ISM Profile Switchover method	This method is used in SAN boot environments where servers start from boot disks located in storage arrays. If the primary server fails, the WWN, MAC address, boot configuration, and network configuration that have been set in its server profile using virtual I/O (ISM) are inherited by the spare server, which then automatically starts up from the same SAN disk.
Storage Affinity Switchover Method	This method is used when the server is SPARC M10/M12 or SPARC Enterprise. When using this method, the boot disk connection destination is switched over to a spare server, in coordination with ETERNUS SF Storage Cruiser storage management functions.
Switchover	The operation that stops the primary server which is in operation and switches over to the spare server according to the specified server switchover method.

Information

- The VIOM server profile switchover method and the ISM profile switchover method are collectively referred to as the "Profile Switchover Method".
- The profile switchover method and the HBA address rename method are collectively referred to as "I/O virtualization methods".

Spare Server Switchover Methods

Backup and Restore Method

In a local boot environment, this method restores a system image backup to a spare server, which is then automatically started up.

This is selected under the following cases. For details on backup and restore, refer to "16.1 Overview" in the "User's Guide VE".

- When a virtual WWN or boot configuration have not been set via the HBA address rename, VIOM, or ISM profile assigned to the primary server
- When the [Local-boot with SAN data (Backup and restore method)] checkbox is selected during setting of the spare server

When HBA address rename, VIOM, or ISM has been used to set a profile for a server, the WWN and the profile also can be switched at server switchover.

After switchover, the operating system and its applications will resume on the spare server from the status they were in at the last system image backup.
Note that only the content of the first local disk (or boot disk) as seen by the BIOS of the managed server is subject to a backup or restore operation, including all partitions (Windows drives or Linux partitions) present on the boot disk.

However, since additional disks (disks used as data disks), are not subject to backup and restore, their content cannot be made automatically accessible to the spare server after server switchover.

When using more than one local disk, backup and restore of such additional data disks should be performed using external backup software.

However, when there are multiple sections on the first disk (Windows drives or Linux partitions), all sections become the targets of backup and restore.

HBA address rename Method

In a SAN boot environment, this method sets the WWN of a spare server's HBA to the same value as that originally set on the primary server. This allows the spare server to connect to and boot from the same boot disk that was used by the primary server. This method is used when HBA address rename settings have been made on the primary server.

Because this method automatically starts the spare server from the primary server's boot disk, applications can be resumed without users being aware of the hardware replacement that occurred.

Profile Switchover Method

This method is used in SAN boot environments where servers start from boot disks located in storage arrays. If the primary server fails, the WWN, MAC address, boot configuration, and network configuration that have been set in its profile using virtual I/O (VIOM or ISM) are inherited by the spare server, which then automatically starts up from the same SAN disk. This method is used when a virtual WWN has been set via the VIOM or ISM profile assigned to the primary server.

Because this method automatically starts the spare server from the primary server's boot disk, applications can be resumed without users being aware of the hardware replacement that occurred.

Storage Affinity Switchover Method

When a primary server fails in a SAN boot environment, changing the following configuration using storage management software enables access and startup from the same boot disk. When HBA WWNs are fixed, reconfiguring storage devices enables continuation of operations.

- Zoning settings for the Fibre Channel switches connected to servers
- Host affinity settings for storage CAs

Inheritance of Network Configuration During Server Switchover

For PRIMERGY BX servers, the network configuration (VLAN IDs of adjacent LAN switch ports or port groups) of the primary server will be inherited by the spare server when using the backup and restore method, HBA address rename method, or the profile switchover method.

When using the profile exchange or the backup and restore method, if a MAC address, boot configuration, or network configuration were assigned to the server (in its profile), these settings will also be inherited by the spare server. Therefore, it is no longer necessary to reconfigure applications or network devices that depend on MAC address values.

Switchover-related Terms in Resource Orchestrator

Table 9.2 Switchover-related Terms in Resource Orchestrator

Term	Description
Switchover	The operation that stops the primary server which is in operation and switches over to the spare server according to the specified server switchover method.
Failback	After server switchover is performed, this operation stops the operating spare server and switches back to the primary server.
Takeover	The operation that appoints the active spare server as the new primary server instead of performing failback after switchover.

Note

- When using ServerView Deployment Manager on the admin LAN, the backup and restore method and HBA address rename are disabled. For details, refer to "B.2 Co-Existence with ServerView Deployment Manager".

- Auto-Recovery occurs when a hardware failure is detected. However, it does not occur when the operating system has stopped as a result of a software error or when the operating system is automatically rebooted.
  Refer to "9.4 Conditions Required for Auto-Recovery" for details.
  Furthermore, since the Auto-Recovery is driven by a hardware failure, it prioritizes a fast recovery to a spare server instead of collecting an OS memory dump (which would be used to troubleshoot an OS failure).
  Thus, even if a memory dump was set to be collected in the event of an OS failure, server recovery will take precedence and the memory dump will not be collected.

- Server switchover can be realized using one of the following methods.

  - Backup and Restore Method

  - HBA address rename Method

  - Profile Switchover method

  - Storage Affinity Switchover Method

- When configuring the HBA address rename function as the switchover method, first confirm that the HBA address rename settings have been configured properly before configuring the server switchover settings.

- When server switchover is conducted using a Hyper-V VM host, prepare more than two physical NICs.
  The network which VM hosts, such as the admin LAN for VM hosts, use to communicate with external servers should be dedicated only to physical servers, and not be configured for virtual networks.
  In a network environment that has external virtual networks configured, disable all virtual networks for VM hosts. For details, refer to "9.2.1 Configuration Requirements" in the "Design Guide VE".

- It is not possible to specify spare servers for individual VM guests. It is either possible to store VM guests on a SAN or NAS shared disk and assign a spare server to the VM host, or use the VM high-availability feature provided by the server virtualization software used.
  For more details on the high-availability features available for each server virtualization software, refer to "9.2.2 Functional Differences between Products" in the "Design Guide VE".
  Switchover using Resource Orchestrator, and the high-availability of server virtualization software can be used together.
  When using a high-availability feature of server virtualization software, do not include spare servers of Resource Orchestrator in VM hosts as spare servers.

  [VMware]
  When using a high-availability feature (VMware HA) of server virtualization software, perform high-availability configuration again when performing server switchover or failback of Resource Orchestrator.

- When primary and spare servers are placed in different chassis, and both servers are connected to LAN switch blades operating in IBP mode, server switchover only works if all of the following conditions are met.

  - LAN switch blades are PRIMERGY BX900/BX400

  - The same port group name is set for both LAN switch blades

- When using Intel PROSet for LAN redundancy, the switchover destination server may inherit the same MAC address as that of the source server, as Intel PROSet keeps an internal definition of MAC addresses. When using Intel PROSet for LAN redundancy, the switchover destination server may inherit the same MAC address as that of the source server, as Intel PROSet keeps an internal definition of MAC addresses. To avoid communication issues caused by MAC address conflicts, please be sure to reconfigure MAC addresses on the destination server following a server switchover.

- For servers other than blade servers, configuration is not possible when there are managed servers belonging to different subnets from the admin server.

- Configuration is not possible when there are managed servers whose admin LAN NIC configurations are different from the primary server.

- Server switchover can be performed, even if the NIC configurations used for HBA address rename setup service on the primary server and spare server are different. After server switchover is performed, the HBA address rename setup service may not operate depending on the network configuration. Therefore, the NIC configurations used for the HBA address rename setup service should be the same on both the primary server and the spare server.

- For Linux managed servers, when the disks are recognized using the by-id name, server switchover cannot be performed using the backup and restore method.

- When performing server switchover using the backup and restore method in a SAN data server environment that uses local boot, configure a target disk for image operations on both the primary server and the spare server.

  If the switchover is performed without configuring the target disk for image operations, the data may be overwritten on an unintended disk.
  For details, refer to "9.1.13 Changing Target Disks of Image Operations" in the "User's Guide VE".

Sharing a Spare Server Between Physical OSs and VM Guests (High-availability Function of Server Virtualization Software)

In environments where there are servers running physical OSs and servers with VM hosts and VM guests, if they both use HBA address rename, VIOM or ISM, by combining the following settings it is possible for a physical OS and a VM guest to share a spare server.
For details, refer to "Figure 9.3 Sharing a Spare Server Between Physical OSs and VM Guests (High-availability Function of Server Virtualization Software)" in "9.2 Configuration".

a. Specify a VM host as the spare server used to recover VM guests within the high-availability feature (VMware HA) of the server virtualization software used.

b. Once the above settings have been made on a physical OS, a server failure will trigger the following recovery operations.

If the failed server was running a physical OS, Resource Orchestrator will shut down the VM host on the spare server and switch the failed physical OS over to the spare server. If the failed server was a VM host running VM guests, the high-availability feature provided with the server virtualization software will recover the VM guests on the spare VM host server. Since physical OSs and VM guests share a common spare server, the two types of recovery described above can perform together: once one type of recovery occurs on a spare server, another type of recovery can no longer be performed on that same spare server.

Information

- Server switchover based on backup and restore takes approximately 3 minutes, plus the time required to restore the system image. Image restoration time depends on different factors such as disk space and network usage, but as an estimate, a disk of 73 GB will take 30 to 40 minutes (the transfer of the system images takes between 10 to 20 minutes, while system restarts and other configuration changes take another 20 minutes).

- Server switchover based on HBA address rename takes approximately 5 minutes, plus the time required to start up the original operating system and services on the spare server. Server startup time is determined according to the time taken for starting the OS and the time taken for starting the services automatically when the OS is started. If a server OS was running on the spare server, the time required to shut down the spare server must also be included.

9.2 Configuration

This section provides examples of switchover configurations for each different switchover method.

Correspondence between the Configuration Examples and the Available Server Switchover Methods

The correspondence between the configuration examples and the available server switchover methods is as shown below.

Table 9.3 Correspondence between the Configuration Examples and the Available Server Switchover Methods

Configuration Example	Server Switchover Method			
	Backup and Restore Method	HBA address rename Method	Profile Switchover method	Storage Affinity Switchover Method
Spare Server Configuration for Local Boot Servers	Yes	-	-	-
Spare Server Configuration for Booting from SAN/iSCSI Storage Servers	-	Yes	Yes	-
Sharing a Spare Server Between Physical OSs and VM Guests (High-availability Function of Server Virtualization Software)	-	Yes	Yes	-
Configuration Using a Server on which a Server OS is Operating as a Spare Server	-	Yes	Yes	-
Configuration Using a Server on which a VM Guest is Operating as a Spare Server	-	Yes	Yes	-
Spare Server Configuration for Booting from SAN Storage Servers	-	-	-	Yes
Configuration Using a Server on which a Server OS is Operating as a Spare Server	-	-	-	Yes
Configuration Using a Server on which a VM Guest is Operating as a Spare Server	-	-	-	Yes

Yes: Corresponds to the configuration example.
-: Does not correspond to the configuration example.

Each method has its own restrictions regarding the supported hardware environment.
For details, refer to the corresponding "Functions Available for Agents" in "6.2.1 All Editions" in the "Overview".

Note

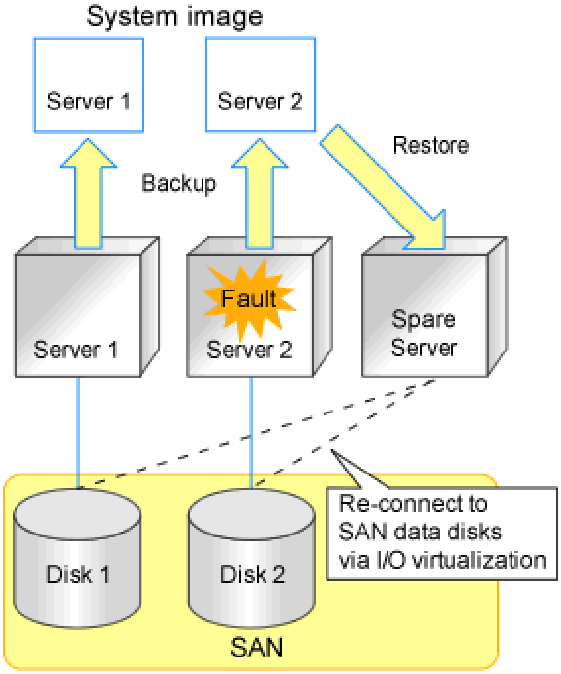
When multiple primary servers share a common spare server, the spare server cannot be shared by a local boot server, a SAN boot server, and an iSCSI boot server.

Backup and Restore Method

Spare Server Configuration for Local Boot Servers

A spare server should be set aside for servers in local boot environments.
When a primary server fails, a system image (that must be backed up beforehand) will be restored to the spare server, and the spare server will be started up. A spare server can be shared by multiple primary servers.
If a local boot server is using SAN storage for data storing purposes, I/O virtualization can make this SAN storage space accessible to the spare server.

Figure 9.1 Spare Server Configuration for Local Boot Servers

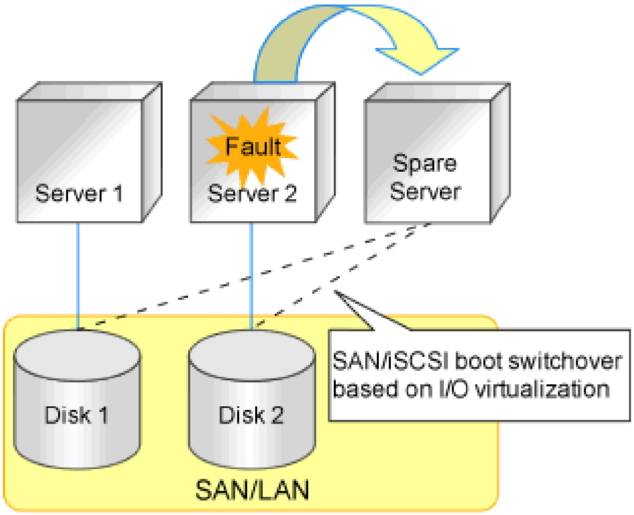


HBA address rename Method/Profile Switchover Method

Spare server configuration for booting from SAN/iSCSI storage servers (using virtual I/O)

At least one spare server using virtual I/O should be set aside for servers in a SAN/iSCSI boot environment.
When a primary server fails, the WWN set on its HBA or MAC address, boot configuration, and network configuration set on its NIC is inherited by the spare server, which can then access and start up from the same boot disk. A spare server can be shared by multiple primary servers.

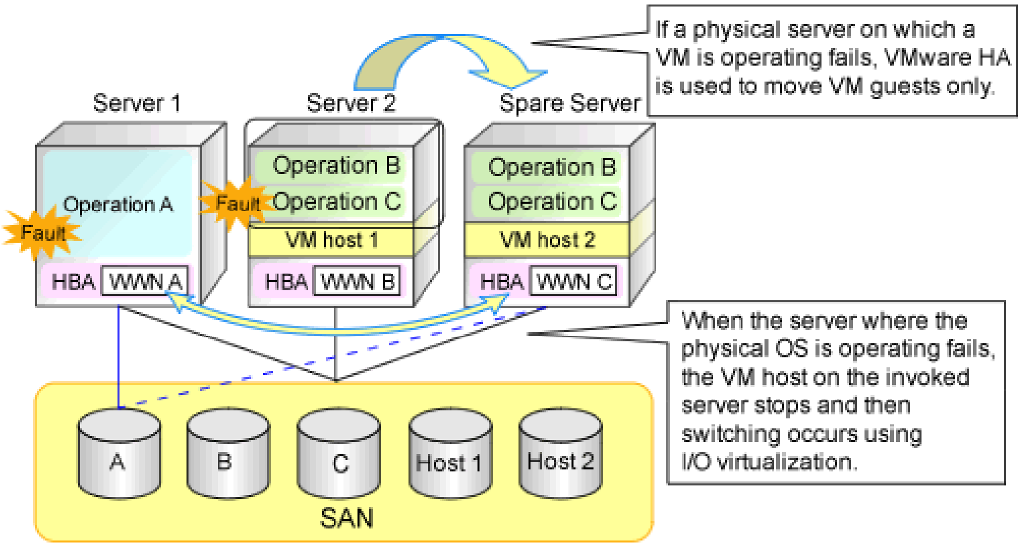
Figure 9.2 Spare Server Configuration for Booting from SAN/iSCSI Storage Servers



For spare server configurations based on I/O virtualization, a spare server can be shared by multiple physical OSs and VM guests (using the high-availability feature provided with their server virtualization software). For details on the server virtualization software supporting this configuration, refer to "9.1 Deciding Server Virtualization Software" in the "Design Guide VE".
In this case, spare servers should be set up as a VM hosts booting from a SAN, so that when a physical server hosting VM guests experiences a failure, the high-availability feature provided with their server virtualization software can be used to transfer the VM guests to this spare VM host.

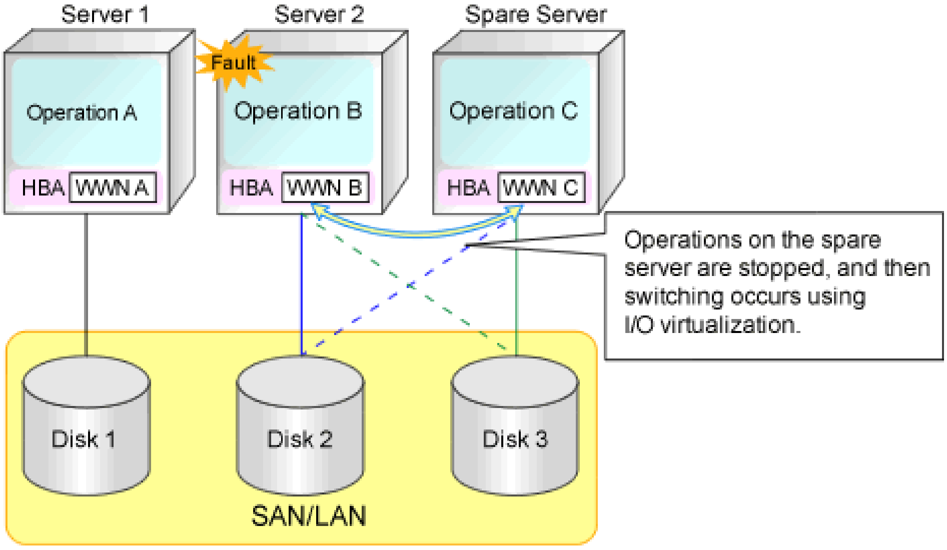
If a server running a physical OS fails, its boot disk will be reconnected to the spare server by means of an HBA address rename. When this happens, the spare server is halted, reconnected to the primary server's boot disk, and started up as the new active server.

Figure 9.3 Sharing a Spare Server Between Physical OSs and VM Guests (High-availability Function of Server Virtualization Software)


Server 1
Server 2
Spare Server
If a physical server on which a VM is operating fails, VMware HA is used to move VM guests only.
Operation A
Fault
HBA
WWN A
Operation B
Operation C
Fault
VM host 1
HBA
WWN B
Operation B
Operation C
VM host 2
HBA
WWN C
When the server where the physical OS is operating fails, the VM host on the invoked server stops and then switching occurs using I/O virtualization.
A
B
C
Host 1
Host 2
SAN

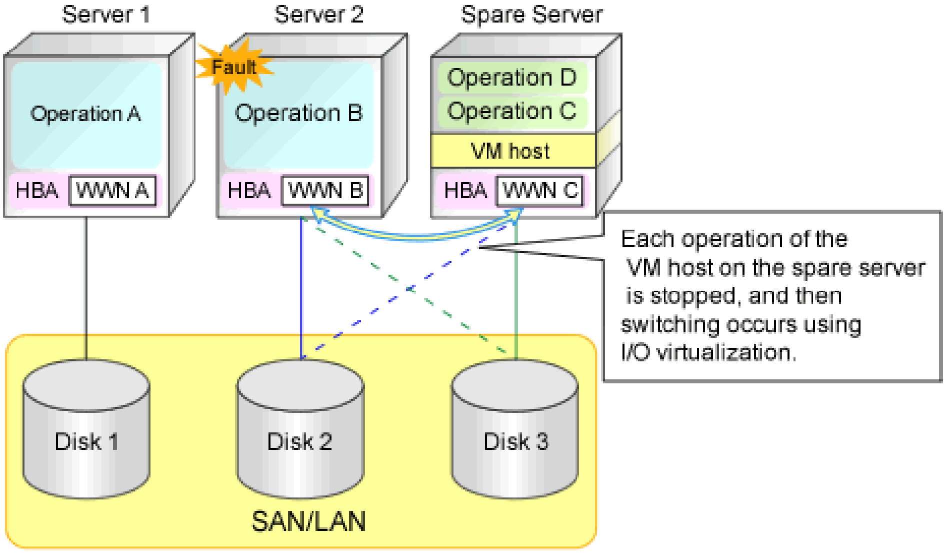
In server configurations using I/O virtualization, servers on which a server OS is operating can be used for spare servers.
If a primary server fails and its spare server boots from a SAN, the OS of the spare server will be stopped. After that, the boot disk is connected to the spare server using I/O virtualization, and the server started.

Figure 9.4 Configuration Using a Server on which a Server OS is Operating as a Spare Server



In server configurations using I/O virtualization, servers on which VM guests are operating can be used for spare servers.
When a VM host booting from a SAN is setup on a spare server, if the primary server fails, the VM host will be stopped. After that, the boot disk will be connected to the spare server using I/O virtualization, and the server will be started.

Figure 9.5 Configuration Using a Server on which a VM Guest is Operating as a Spare Server



Storage Affinity Method

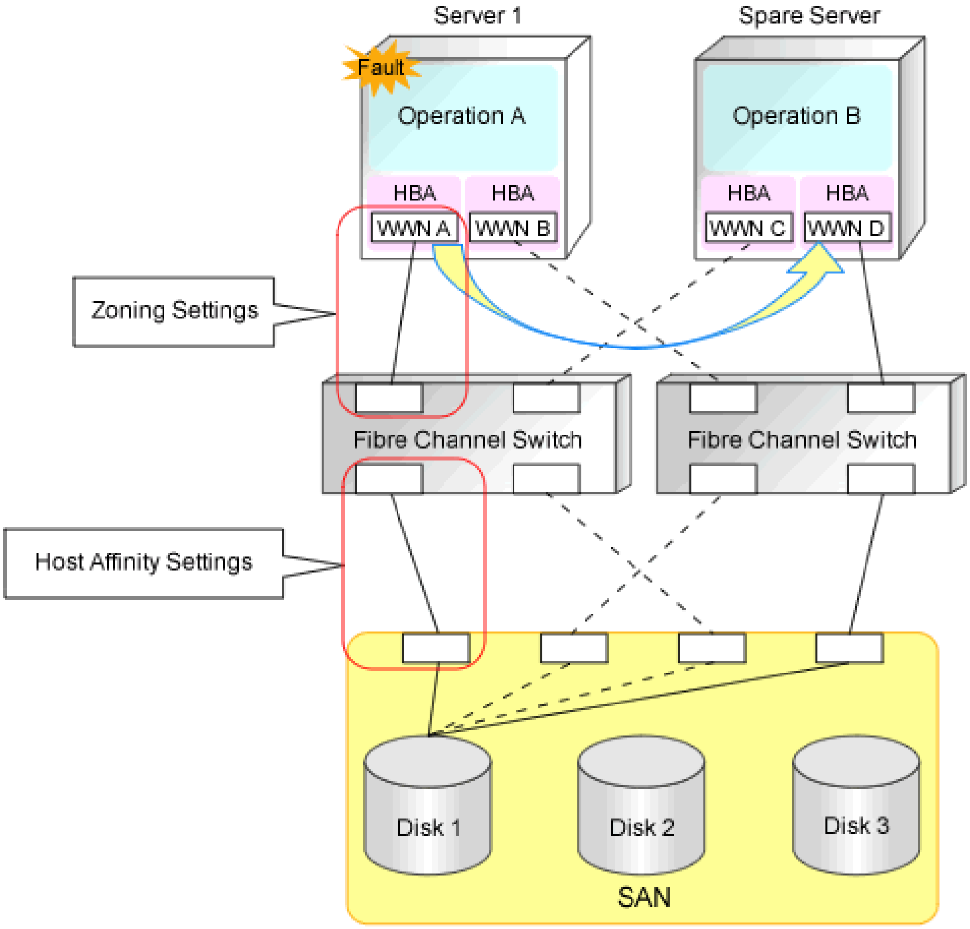
Spare server configuration for booting from SAN storage servers (using storage management software)

Storage management software should be set aside for servers in SAN boot environments.
When a primary server fails, changing the following configuration using storage management software enables access and startup from the same boot disk. A spare server can be shared by multiple primary servers.

- Zoning settings for the Fibre Channel switches connected to servers

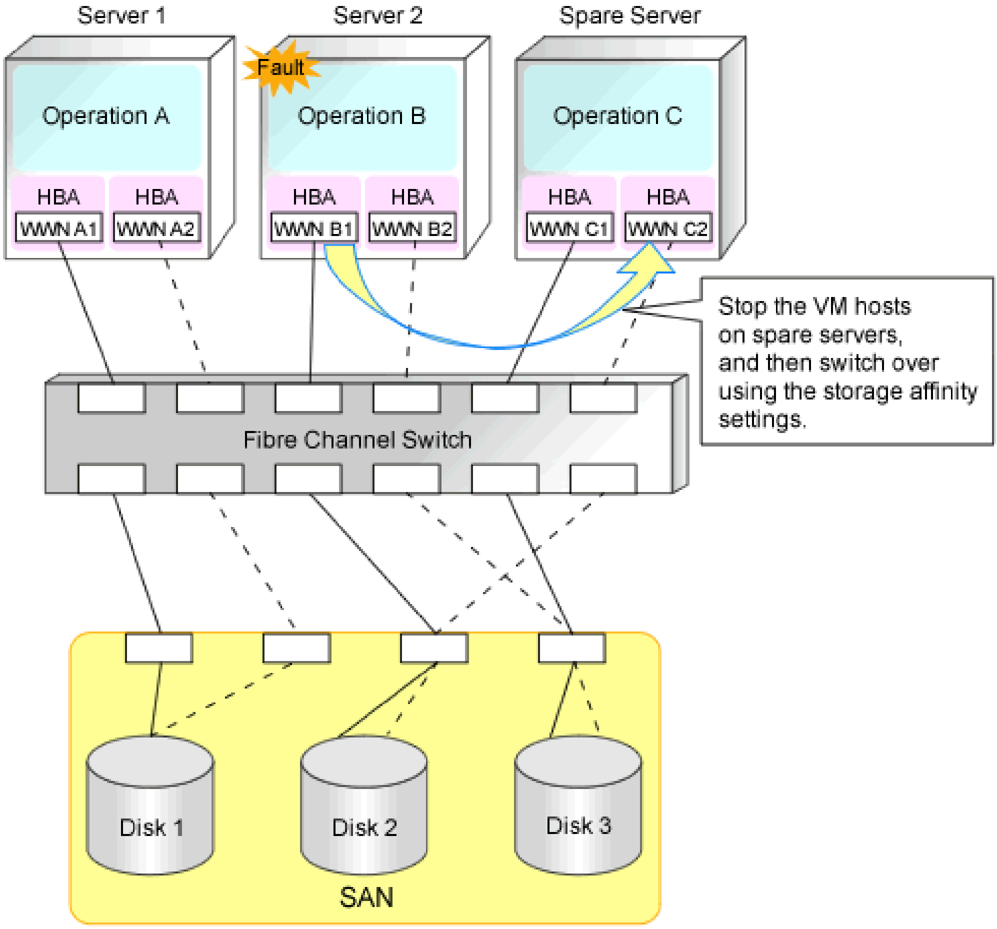
- Host affinity settings for storage CAs

Figure 9.6 Spare Server Configuration for Booting from SAN Storage Servers



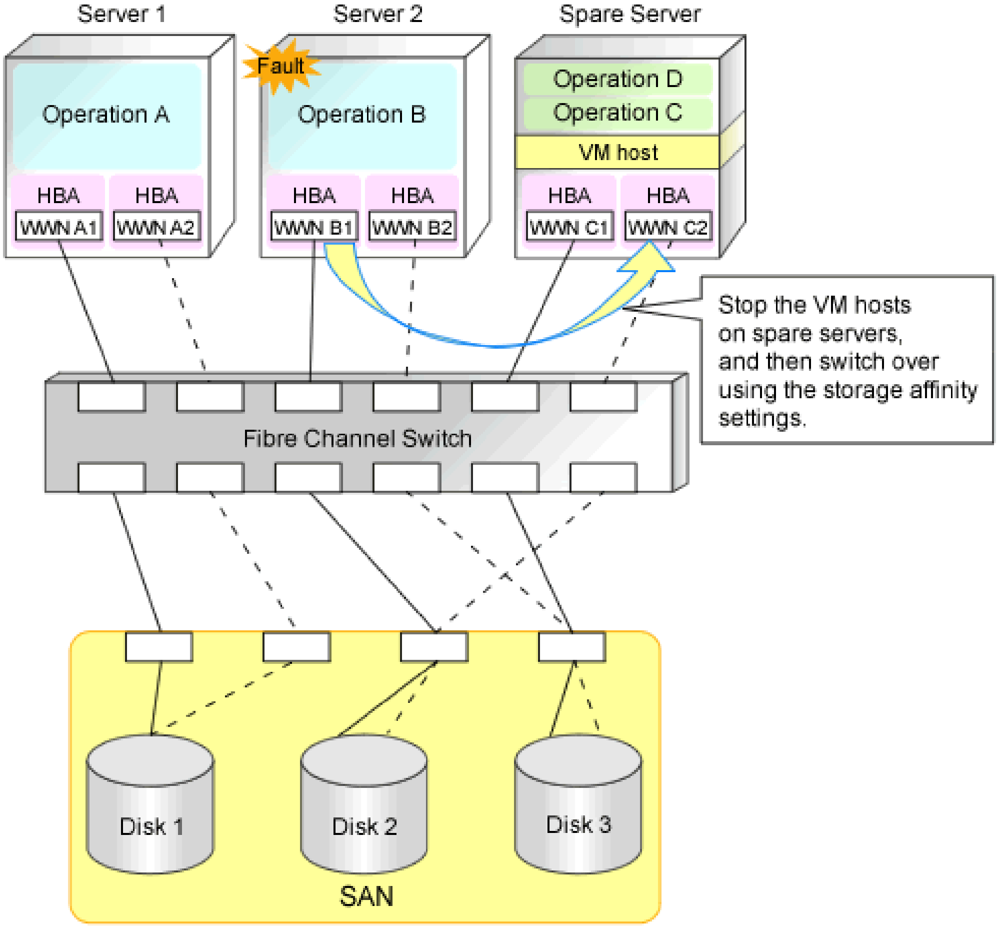
When using the storage affinity method, a server on which the server OS is operating can be used as a spare server.
Boot a server OS from a SAN on the spare server. When the primary server fails, after the OS of the spare server stops, the boot disk is connected to the spare server and started.

Figure 9.7 Configuration Using a Server on which a Server OS is Operating as a Spare Server



When using the storage affinity method, a server on which a VM guest is operating can be used as a spare server.
Boot a VM host from a SAN on the spare server. When the primary server fails, after the VM host of the spare server stops, the boot disk is connected to the spare server and started.

Figure 9.8 Configuration Using a Server on which a VM Guest is Operating as a Spare Server



9.3 Server Switchover Conditions

The following conditions must be satisfied for manual server switchover, failback, and Auto-Recovery to function correctly.

Conditions for Spare Servers

The spare server must be identical to the primary server regarding all of the following conditions.
If these conditions are not satisfied, allocation of a spare server may not be possible, server switchover may fail, or the server may malfunction after the switchover is completed.

- Server Model
- Server Hardware Configuration

  The following settings or configurations of option cards or expansion cards must be the same.

  - Model numbers
  - The locations they are mounted in
  - The number and sizes of local disks
  - RAID settings

  There are no other hardware conditions for the spare server (such as memory capacity, number of CPUs and CPU clock speed). However, the hardware configuration of the spare server must be capable of running the operating system and applications running on the primary server.

- BIOS Settings

    - 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".

- OBP Settings

    For SPARC M10/M12 and SPARC Enterprise, the OBP settings to start automatically from SAN servers of the same target disk must have been made according to the procedure in "6.2.9 Configuring OBP (Open Boot Prom) Settings (SPARC M10/M12 and SPARC Enterprise Servers)" in the "Design Guide VE".
    With the storage affinity switchover method, as setting changes are only performed for Fibre Channel switch storage devices, it is necessary to perform configuration of servers that will be changed during switchover, and HBA and OBP settings.

- LAN and SAN Access Scope

    The spare server must use the same network redundancy method, have the same redundancy paths, and have access to the same network and storage devices. Note that LAN or fibre channel switches connected in a cascade configuration are viewed as a single device.

- Firewall

    There must be no firewall between the primary server and the spare server.

- Subnet

    For servers other than blade servers, the primary server and the spare server must belong to the same subnet.

- VLAN

    For the following configurations, the primary server and the spare server must belong to the same VLAN.

    - LAN switch blades connected to managed servers are as follows:

        - Operating in Converged Fabric mode

        - PY CB 10Gb FEX Nexus B22

    - Managed servers are not blade servers

If a spare server is shared by a physical OS and one or more VM guests (using the high-availability feature provided with their server virtualization software), the spare server must be configured for SAN boot using I/O virtualization.

For details, refer to "Figure 9.3 Sharing a Spare Server Between Physical OSs and VM Guests (High-availability Function of Server Virtualization Software)" in "9.2 Configuration".

When using a server on which a server OS is operating as a spare server, both the primary server and spare server should be in a configuration that uses I/O virtualization.
For details, refer to "Figure 9.4 Configuration Using a Server on which a Server OS is Operating as a Spare Server" in "9.2 Configuration".

Also, if more than two local disks are connected to a spare server in a backup/restore configuration, and if the partitioning of the disks coming after the first in the boot order is different from the first disk, a warning message may be displayed at restart, or the operating system may not restart, causing any switchovers initiated to fail. After configuring the spare server, verify that it is operating properly by performing a switchover and failback.
If the operation fails, configure the partitions other than the first boot disk of the spare server to match the configuration of the primary server, or set up the primary server configuration so that it does not depend on any disk other than the first, using automatic service startups, and re-labeling the Windows drives as necessary.

With blade servers, if the primary server and spare server do not belong to the same subnet, if server switchover is performed to the spare server it is necessary that the VLAN ID or port group settings of the internal LAN switch ports are adjusted automatically.
For details on how to configure the settings, refer to "18.2 Settings for Server Switchover" in the "User's Guide VE".

Conditions for Server Switchover

All of the following conditions must be satisfied for server switchover or Auto-Recovery to succeed:

- The server configuration cannot already be switched over (the spare server must not be being used for operations)

- The status of the spare server must be "normal", "warning", or "stop". If a VM host has been installed on the spare server(for VMware HA), its status must be either "normal" or "warning"

- If a spare server is shared by more than one active server, none of the other primary servers may be switched over to that spare server
- If the server is in a local boot environment, its system image must have been backed up

Note

When performing server switchover using the backup and restore method in a SAN data server environment that uses local boot, configure a target disk for image operations on both the primary server and the spare server.
If the switchover is performed without configuring the target disk for image operations, the data may be overwritten on an unintended disk.
For details, refer to "9.1.13 Changing Target Disks of Image Operations" in the "User's Guide VE".

Conditions for Server Failback

All of the following conditions must be satisfied for server failback to succeed:

- The active server must have been switched over to the spare server
- The status of the primary server must be "stop"
- If the server is in a local boot environment, its system image must have been backed up

Conditions for Server Switchover of OVM for SPARC Servers

When the OS of the server is OVM for SPARC, it is also necessary to satisfy the following conditions as well as those above.

- The XCP firmware version of the primary server and the spare server are the same
- The startup settings of the primary server are configured

  For details, refer to "6.1.6 Settings when Switching Over SPARC M10/M12 or SPARC Enterprise Servers" in the "Design Guide VE".
- There are seven sets of domain configuration information of the spare server (hereinafter configuration information) or less, including the factory-default

  In SPARC M10/M12s, a maximum of eight sets of configuration information can be saved, including the factory-default.
  After switchover, the configuration information is saved on the service processor using the domain configuration name used before the switchover. Therefore, if there is configuration information with the same name on the spare server, save the configuration information after deleting the configuration information with the same name during switchover.
- Configuration information other than the factory-default has been saved on the service processor of the primary server

  When performing server switchover while the configuration information is factory-default, the configuration information cannot be saved on the switchover destination server.
- When registering the server in a VM pool, the primary server and the spare server are registered in the same VM pool

  If the servers are registered in different VM pools, the displayed information of the server in the VM pool is changed after switchover.
- An alias is not used in the boot-device settings of the OBP of the I/O domain or the control domain for the primary server

  When server switchover is performed, only boot-device settings of the primary server are carried over to the spare server.
- The admin LAN (IP address) of the control domain is allocated to a physical NIC

  The admin LAN (IP address) cannot be allocated to a virtual switch (vsw).
- CPU core activation has been applied to the spare server

  CPU core activation is not carried over during server switchover.
- No network interface which cannot communicate in the factory-default state exists in the control domain

  When a network interface created on a virtual switch (vsw) is used in the control domain, it is considered that the server switchover conditions are not satisfied.
  For example, a configuration where a virtual switch (vsw) is used for IPMP redundancy.

Note

When using an OVM for SPARC server as a spare server, only OVM for SPARC environments are supported for the primary server.

9.4 Conditions Required for Auto-Recovery

This section explains the conditions required for auto-recovery.

Auto-Recovery Using Server Switchover Settings

A server for which Auto-Recovery is enabled will be automatically switched over to its spare server if Resource Orchestrator detects both a failure from the server hardware and determines that its physical OS (or VM host) has stopped.

- Detecting hardware failures from servers

  A hardware failure can be detected by an "Error" level SNMP trap failure notification sent to the admin server from either the ServerView Agents or the server management unit. Alternatively, Resource Orchestrator can detect a failure by periodically polling the status of each managed server.

  Detectable hardware failures

  - CPU faults

  - Memory errors

  - Temperature abnormalities

  - Fan failures

    As a result of a FAN failure, it is detected as a temperature abnormality.

- Detecting that a physical OS (or VM host) has stopped

  A physical OS (or VM host) is seen to have stopped abnormally when the following conditions are met:

  - PRIMERGY BX series servers

    An abnormal server status is obtained from a server management unit, and it is not possible to communicate with either the ServerView Agents or the Resource Orchestrator agent

  - For rack mount servers, tower servers, SPARC M10/M12, and SPARC Enterprise

    Communication using the ping command is unavailable

    [OVM for SPARC]
    Communication with the control domain using the ping command is unavailable

Auto-Recovery Using Monitoring Information Settings

When ping monitoring using monitoring information is enabled, server switchover is automatically performed when there is no response from physical OS on servers or VM hosts, and restoration by executing reboot fails.
The recovery process can be changed by configuring settings. For the setting method, refer to "Chapter 8 Configuring Monitoring Information".

- No response detected by ping monitoring

  When the period with no response in the ping command is over the time-out value, no response is detected.

Note

- Notification of hardware failures on rack mount servers, tower servers, SPARC M10/M12, and SPARC Enterprise is only detected by SNMP traps.

- Auto-Recovery is not triggered on servers that are in maintenance mode.

- Even if a hardware failure is detected, Auto-Recovery will not be triggered if no response is received from the target server. In such cases, shutting down or restarting the server will temporarily stop the operating system, triggering an automatic switchover as the conditions for Auto-Recovery will be met. Under such conditions, automatic switchovers can be prevented by setting the server to maintenance mode before shutdown or restart.
- When the target server is a VM host on which a VM guest with the server role (Manager) is operating, Auto-Recovery is not triggered.

Chapter 10 Saving Environment Settings

This chapter explains how to save environment settings.

The admin server should be backed up after the entire system has been completely set up, or after registering, changing, or deleting resources.
The configuration of a Resource Orchestrator setup can be saved to guard against unexpected problems. Use the admin server backup function and troubleshooting data collection command to save settings.
This troubleshooting data can be used in conjunction with the data later collected when a problem occurs for a more effective investigation, and should therefore be stored with caution.

See

- For details on admin server backup, refer to "Chapter 9 Backup and Restoration of Admin Servers" in the "Operation Guide VE".
- For collecting troubleshooting data, refer to "1.2 Collecting Troubleshooting Data (Virtual Edition)" in "Troubleshooting".

Chapter 11 Uninstallation

This chapter explains the uninstallation of FUJITSU Software ServerView Resource Orchestrator.

The uninstallation of managers, agents, and the HBA address rename setup service is performed in the following order:

1. Uninstall the manager

   Refer to "11.1 Manager Uninstallation".

2. Agent Uninstallation

   Refer to "11.2 Agent Uninstallation".

3. HBA address rename setup service Uninstallation

   For uninstallation, refer to "11.3 HBA address rename Setup Service Uninstallation".

When uninstalling a Resource Orchestrator manager, specify Resource Orchestrator using "Uninstall (middleware)" first, and uninstall the manager.
"Uninstall (middleware)" is a common tool for Fujitsu middleware products.

The Resource Orchestrator Manager is compatible with "Uninstall (middleware)".

When a Resource Orchestrator Manager is installed, "Uninstall (middleware)" is installed first, and then "Uninstall (middleware)" will control the installation and uninstallation of Fujitsu middleware products. If "Uninstall (middleware)" has already been installed, the installation is not performed.

For the uninstallation of Uninstall (middleware), refer to "11.4 Uninstallation of "Uninstall (Middleware)"".

11.1 Manager Uninstallation

The uninstallation of managers is explained in the following sections.

The procedure for manager uninstallation is given below.

- Preparations

  Refer to "11.1.1 Preparations".

- Uninstallation

  Refer to "11.1.2 Uninstallation [Windows Manager]" or "11.1.3 Uninstallation [Linux Manager]".

11.1.1 Preparations

This section explains the preparations and checks required before commencing uninstallation.

Pre-uninstallation Advisory Notes

- Checking system images and cloning images

  The system and cloning images collected by this product are deleted.

  When the image file storage directory has been changed, system images and cloning images which were collected using Resource Orchestrator remain in the image file storage directory.

- Checking HBA address rename

  When using HBA address rename, the manager sets the WWN for the HBA of each managed server.
  When uninstalling a manager be sure to do so in the following order:

  1. Delete servers (*)

  2. Uninstall the manager

  * Note: For the server deletion method, refer to "11.2 Deleting Managed Servers" in the "User's Guide VE".

Note

When using HBA address rename, if the manager is uninstalled without servers being deleted, the WWNs of the servers are not reset to the factory default values.
Ensure uninstallation of managers is performed only after servers are deleted.

When operating without resetting the WWN, if the same WWN is setup on another server, data may be damaged if the volume is accessed at the same time.

Also, when operating managers in cluster environments, release cluster settings before uninstalling managers. For how to release cluster settings, refer to "Appendix C Manager Cluster Operation Settings and Deletion".

- Back up (copy) certificates

  When operating managers in cluster environments, back up (copy) certificates before performing uninstallation.

  Manager certificates are stored in the shared disk for managers.
  The storage folder is the following:

  [Windows Manager]
  Drive_name:\Fujitsu\ROR\SVROR\certificate

  [Linux Manager]
  Shared_disk_mount_point/Fujitsu/ROR/SVROR

- Definition Files

  All definition files created for using Resource Orchestrator will be deleted.
  If the definition files are necessary, before uninstalling Resource Orchestrator back up (copy) the folder below to another folder.

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

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

11.1.2 Uninstallation [Windows Manager]

The procedure for manager uninstallation is given below.

Before uninstalling this product, check that the preparations given in "11.1.1 Preparations" have been performed.

1. Log on to Windows as the administrator.

   Log on to the system from which the manager is to be uninstalled. Log on using the Administrator account.

2. Start the uninstaller. Select [Start]-[All Programs]-[Fujitsu]-[Uninstall (middleware)] from the Windows menu. Click the product name then [Remove], and the uninstallation window will open.

Note

- Any patches that have been applied to Resource Orchestrator will be deleted during uninstallation.

- If a manager is uninstalled and then reinstalled without agents being deleted, it will not be able to communicate with agents used before uninstallation.
  In this case, the certificates to indicate that it is the same manager are necessary.
  After installation, manager certificates are stored in the following folder:

  - *Installation_folder*\SVROR\Manager\etc\opt\FJSVssmgr\current\certificate

  - *Installation_folder*\SVROR\Manager\etc\opt\FJSVrcxdm\certificate

  When uninstalling the manager, the certificates are backed up in the following folder. When reinstalling a manager and using the same certificates, copy the backed up certificates to the appropriate folders.

  - *Installation_folder*\SVROR\back\site\certificate

    - *Installation_folder*\SVROR\back\domain\certificate

  If the certificates backed up on uninstallation are not necessary, delete them manually.

  When operating managers in cluster environments, back up the certificates as indicated in the preparations for uninstallation.
  When reinstalling a manager in a cluster environment and using the same certificates, copy the backed up certificates from the primary node to the above folders.

- Windows PE is stored in the following folders:

  Installation_folder\SVROR\ScwPro\tftp\boot\winpe

  When uninstalling the manager, Windows PE is backed up in the following folder. When reinstalling a manager and using the same Windows PE, copy the backed up Windows PE to the above folder.

  Installation_folder\SVROR\back\winpe

  If the Windows PE backed up on uninstallation is not necessary, delete it manually.

- After uninstallation, the installation folder may remain. In that case, manually delete the installation folder.

- When an admin LAN subnet has been registered, setting information of the DHCP server modified using Resource Orchestrator will not be initialized after uninstallation. Perform initialization if necessary.

- When an admin LAN subnet has been registered, after uninstallation of Resource Orchestrator, the automatic startup settings of the DHCP server (dhcpd) become "OFF" and the service is stopped.

11.1.3 Uninstallation [Linux Manager]

The procedure for manager uninstallation is given below.

Before uninstalling this product, check that the preparations given in "11.1.1 Preparations" have been performed.

1. Log in to the system as the OS administrator (root).

   Log in to the managed server from which Resource Orchestrator will be uninstalled, using root.

2. Launch the uninstallation command (cimanager.sh).

   Perform uninstallation according to the uninstaller's interactive instructions.

   ```
   # /opt/FJSVcir/cimanager.sh -c <RETURN>
   ```

Note

- When the PATH variable has been configured to enable execution of UpdateAdvisor (Middleware) commands from a user-defined location, performing uninstallation will delete any patches that have been applied to Resource Orchestrator so there is no need to return it to the state prior to application.
  When the PATH variable has not been configured, unapply patches before performing uninstallation.

- If a manager is uninstalled and then reinstalled without agents being deleted, it will not be able to communicate with agents used before uninstallation.
  In this case, the certificates to indicate that it is the same manager are necessary.
  After installation, manager certificates are stored in the following directory:

  /etc/opt/FJSVrcvmr/opt/FJSVssmgr/current/certificate

  When uninstalling the manager, the certificates are backed up in the following directory.
  When reinstalling a manager and using the same certificates, copy the backed up certificates to the above folder.

  /var/tmp/back/site/certificate

  If the certificates backed up on uninstallation are not necessary, delete them manually.

  When operating managers in cluster environments, back up the certificates as indicated in the preparations for uninstallation.
  When reinstalling a manager in a cluster environment and using the same certificates, copy the backed up certificates from the primary node to the above folders.

- Windows PE is stored in the following directory.

  /var/opt/FJSVscw-tftpsv/tftproot/boot/winpe

  When uninstalling the manager, Windows PE is backed up in the following directory. When reinstalling a manager and using the same Windows PE, copy the backed up Windows PE to the above folder.

  /var/tmp/back/winpe

  If the Windows PE backed up on uninstallation is not necessary, delete it manually.

- When passwords were saved using the rcxlogin command during operation of Resource Orchestrator, those passwords are stored in the following directory for the OS user account by which the command was executed.

  ```
  /Directory_set_for_each_user's_HOME_environment_variable/.rcx/
  ```

  Delete those manually after uninstalling Resource Orchestrator.

- When an admin LAN subnet has been registered, setting information of the DHCP server modified using Resource Orchestrator will not be initialized after uninstallation. Perform initialization if necessary.

- When an admin LAN subnet has been registered, after uninstallation of Resource Orchestrator, the automatic startup settings of the DHCP server (dhcpd) become "OFF" and the service is stopped.

- If SELinux was configured when Resource Orchestrator was installed, delete the settings for SELinux after uninstalling Resource Orchestrator.

  For details on how to delete the settings, refer to "H.2.1 Manager".

11.2 Agent Uninstallation

The uninstallation of agents is explained in the following sections.

11.2.1 Uninstallation [Windows] [Hyper-V]

This section explains the procedure for uninstallation of agents.

1. Log on to Windows as the administrator.

   Log on to the system from which the agent is to be uninstalled. Log on using the Administrator account.

2. Delete agents.

   Open [Programs and Features] from the Windows Control Panel, and select "ServerView Resource Orchestrator Agent" to delete the agent.

3. The [Confirm Uninstall] dialog will be displayed.

   Click the [OK] button.

   The services of Resource Orchestrator are automatically stopped and deleted.

4. When uninstallation is completed, the confirmation window will be displayed.

   Click the [Finish] button.

   Note

   - Any patches that have been applied to Resource Orchestrator will be deleted during uninstallation.

   - When uninstallation is stopped due to errors (system errors or processing errors such as system failure) or cancellation by users, resolve the causes of any problems, and then attempt uninstallation again.

     If uninstallation fails even when repeated, the executable program used for uninstallation may have become damaged somehow.

     In this case, set the first Resource Orchestrator DVD-ROM, open the command prompt, and execute the following command:

```
>"DVD-ROM_drive\DISK1\Agent\Windows\agent\win\setup.exe" /z"UNINSTALL" <RETURN>
```

Open [Programs and Features] from the Windows Control Panel, and if "ServerView Resource Orchestrator Agent" is not displayed, manually delete any remaining folders.

11.2.2 Uninstallation [Linux] [VMware] [Xen] [KVM]

This section explains the procedure for uninstallation of agents.

1. Log in to the system as the OS administrator (root).

   Log in to the managed server from which Resource Orchestrator will be uninstalled, using root.

2. Execute the rcxagtuninstall command.

   Executing this command performs uninstallation, and automatically deletes the packages of Resource Orchestrator.

   ```
   # /opt/FJSVrcxat/bin/rcxagtuninstall <RETURN>
   ```

   When uninstallation is completed successfully, the following message will be displayed.

   ```
   INFO : ServerView Resource Orchestrator Agent was uninstalled successfully.
   ```

   If uninstallation fails, the following message will be displayed.

   ```
   ERROR : Uninstalling package_name was failed.
   ```

   When the uninstaller of Resource Orchestrator is started, its services are stopped.

3. If uninstallation fails, use the rpm command to remove the packages given in the message, and start the process from step 1 again.

   ```
   # rpm -e package_name <RETURN>
   ```

Note

- When the PATH variable has been configured to enable execution of UpdateAdvisor (Middleware) commands from a user-defined location, performing uninstallation will delete any patches that have been applied to Resource Orchestrator so there is no need to return it to the state prior to application.
  When the PATH variable has not been configured, unapply patches before performing uninstallation.

- After uninstallation, the installation directories and files below may remain. In that case, delete any remaining directories and files manually.

  - Directory in /opt

FJSVnrmp	FJSVrcxat	FJSVrcximg	FJSVrcxkvm
FJSVssagt	systemcastwizard		

  - Directory in /etc/opt

FJSVnrmp	FJSVrcxat	FJSVssagt

  - Directory in /var/opt

systemcastwizard	FJSVnrmp	FJSVrcxat	FJSVssagt

  - Files

/boot/clcomp2.dat	/etc/init.d/scwagent	/etc/scwagent.conf

- If SELinux was configured when Resource Orchestrator was installed, delete the settings for SELinux after uninstalling Resource Orchestrator.

  For details on how to delete the settings, refer to "H.2.2 Agent".

11.2.3 Uninstallation [Solaris] [Solaris Zones] [OVM for SPARC]

This section explains the procedure for uninstallation of agents.

1. Log in to the system as the OS administrator (root).

   Log in to the managed server from which Resource Orchestrator will be uninstalled, using root.

2. Execute the rcxagtuninstall command.

   Executing this command performs uninstallation, and automatically deletes the packages of Resource Orchestrator.

   ```
   # /opt/FJSVrcvat/bin/rcxagtuninstall <RETURN>
   ```

   When uninstallation is completed successfully, the following message will be displayed.

   ```
   INFO : ServerView Resource Orchestrator Agent was uninstalled successfully.
   ```

   If uninstallation fails, the following message will be displayed.

   ```
   ERROR : Uninstalling package_name was failed.
   ```

   When the uninstaller of Resource Orchestrator is started, its services are stopped.

3. If uninstallation fails, use the pkgrm command to remove the packages given in the message, and start the process from step 1 again.

   ```
   # pkgrm package_name <RETURN>
   ```

Note

- When the PATH variable has been configured to enable execution of UpdateAdvisor (Middleware) commands from a user-defined location, performing uninstallation will delete any patches that have been applied to Resource Orchestrator so there is no need to return it to the state prior to application.
  When the PATH variable has not been configured, unapply patches before performing uninstallation.

- After uninstallation, the installation directories below may remain. In that case, delete any remaining directories and files manually.

  - Directory in /opt

    ```
    FJSVrcvat
    ```

  - Directory in /etc/opt

    ```
    FJSVrcvat
    ```

  - Directory in /var/opt

    ```
    FJSVrcvat
    ```

11.3 HBA address rename Setup Service Uninstallation

This section explains uninstallation of the HBA address rename setup service.

11.3.1 Uninstallation [Windows]

The procedure for uninstallation of the HBA address rename setup service is given below.

1. Log on to Windows as the administrator.

   Log on to the system from which the HBA address rename setup service is to be uninstalled. Log on using the Administrator account.

2. Delete the HBA address rename setup service.

   Open [Programs and Features] from the Windows Control Panel, and select "ServerView Resource Orchestrator HBA address rename setup service" to delete the service.

3. The [Confirm Uninstall] dialog will be displayed.

   Click the [OK] button.

   The services of Resource Orchestrator are automatically stopped and deleted.

4. When uninstallation is completed, the confirmation window will be displayed.

   Click the [Finish] button.

Note

- Any patches that have been applied to Resource Orchestrator will be deleted during uninstallation.

- When uninstallation is stopped due to errors (system errors or processing errors such as system failure) or cancellation by users, resolve the causes of any problems, and then attempt uninstallation again.

  If uninstallation fails even when repeated, the executable program used for uninstallation may have become damaged somehow.

  In this case, set the first Resource Orchestrator DVD-ROM, open the command prompt, and execute the following command:

  ```
  >"DVD-ROM_drive\DISK1\HBA\Windows\hbaar\win\setup.exe" /z"UNINSTALL" <RETURN>
  ```

  Open [Programs and Features] from the Windows Control Panel, and if "ServerView Resource Orchestrator HBA address rename setup service" is not displayed, manually delete any remaining folders.

11.3.2 Uninstallation [Linux]

The procedure for uninstallation of the HBA address rename setup service is given below.

1. Log in to the system as the OS administrator (root).

   Log in to the managed server from which Resource Orchestrator will be uninstalled, using root.

2. Execute the rcxhbauninstall command.

   ```
   # /opt/FJSVrcvhb/bin/rcxhbauninstall <RETURN>
   ```

   Starting the uninstaller displays the following message which explains that before uninstallation the Resource Orchestrator services will be automatically stopped.

   ```
   Any Resource Orchestrator service that is still running will be stopped and removed.
   Do you want to continue ? [y,n,?,q]
   ```

   To stop the services and uninstall Resource Orchestrator enter "y", to discontinue the uninstallation enter "n".

   If "n" or "q" is entered, the uninstallation is discontinued.

   If "?" is entered, an explanation of the entry method will be displayed.

3. Enter "y" and the uninstallation will start.

   When uninstallation is completed successfully, the following message will be displayed.

   ```
   INFO : ServerView Resource Orchestrator HBA address rename setup service was uninstalled successfully.
   ```

   If uninstallation fails, the following message will be displayed.

```
ERROR : Uninstalling "package_name" was failed
```

4. If uninstallation fails, use the rpm command to remove the packages given in the message, and start the process from step 1 again.

```
# rpm -e package_name <RETURN>
```

Note

- When the PATH variable has been configured to enable execution of UpdateAdvisor (Middleware) commands from a user-defined location, performing uninstallation will delete any patches that have been applied to Resource Orchestrator so there is no need to return it to the state prior to application.
  When the PATH variable has not been configured, unapply patches before performing uninstallation.

- After uninstallation, the installation directories below may remain. In that case, delete any remaining directories and files manually.

  - Directory in /opt

FJSVrcvhb	FJSVscw-common	FJSVscw-tftpsv

  - Directory in /etc/opt

FJSVrcvhb	FJSVscw-common	FJSVscw-tftpsv

  - Directory in /var/opt

FJSVrcvhb	FJSVscw-common	FJSVscw-tftpsv

- If SELinux was configured when Resource Orchestrator was installed, delete the settings for SELinux after uninstalling Resource Orchestrator.

  For details on how to delete the settings, refer to "H.2.3 HBA address rename Setup Service".

11.4 Uninstallation of "Uninstall (Middleware)"

The uninstallation of "Uninstall (middleware)" is explained in this section.

Note

"Uninstall (middleware)" also manages product information on Fujitsu middleware other than Resource Orchestrator. Do not uninstall "Uninstall (middleware)" unless it is necessary for some operational reason.

In the event of accidental uninstallation, reinstall it following the procedure below.

[Windows]

1. Log on to Windows as the administrator.
2. Set the first Resource Orchestrator DVD-ROM.
3. Execute the installation command.

```
>DVD-ROM_drive\DISK1\CIR\cirinst.exe <RETURN>
```

[Linux]

1. Log in to the system as the superuser (root).
2. Set the first Resource Orchestrator DVD-ROM.

3. Execute the following command to mount the DVD-ROM.

   If the auto-mounting daemon (autofs) is used for DVD-ROM auto-mounting, the installer fails to start due to its "noexec" mount option.

   ```
   # mount -t iso9660 -r /dev/hdc DVD-ROM_mount_point <RETURN>
   # cd DVD-ROM_mount_point <RETURN>
   ```

4. Execute the installation command.

   ```
   # ./DISK1/CIR/cirinst.sh <RETURN>
   ```

Uninstallation of "Uninstall (Middleware)"

To uninstall "Uninstall (middleware)", follow the procedure below.

1. Start "Uninstall (middleware)" and check that other Fujitsu middleware products do not remain.

   The starting method is as follows.

   [Windows]
   Select [Start]-[All Programs]-[Fujitsu]-[Uninstall (middleware)].

   [Linux] [Solaris]

   ```
   # /opt/FJSVcir/cimanager.sh -c <RETURN>
   ```

   Note

   If the command path contains a blank space, it will fail to start. Do not specify a directory with a name containing blank spaces.

2. After checking that no Fujitsu middleware product has been installed, execute the following uninstallation command.

   [Windows]

   ```
   >%SystemDrive%\FujitsuF4CR\bin\cirremove.exe <RETURN>
   ```

   [Linux] [Solaris]

   ```
   # /opt/FJSVcir/bin/cirremove.sh <RETURN>
   ```

3. When "This software is a common tool of Fujitsu products. Are you sure you want to remove it? [y/n]:" is displayed, enter "y" to continue. Uninstallation will be completed in seconds.

4. After uninstallation is complete, delete the following directory and contained files.

   [Windows]
   %SystemDrive%FujitsuF4CR
   %ProgramData%\Fujitsu\FujitsuF4CR

   [Linux] [Solaris]
   /var/opt/FJSVcir

Appendix A Coordination with Other Products

This appendix explains how to coordinate Resource Orchestrator with other products.

A.1 SNMP Trap Settings Using CA Spectrum

This section explains the settings for CA Spectrum to receive Resource Orchestrator SNMP traps.
Also refer to "Appendix G Sending SNMP Traps".

For details on CA Spectrum, refer to the CA Spectrum manual.

External Software

The information in this manual has been based on that of CA Spectrum Infrastructure Manager r9.1.2.
Depending on the version of CA Spectrum Infrastructure Manager, some of the terms and procedures may differ slightly from those given here.

Installing CA Spectrum

Perform installation of CA Spectrum referring to the CA Spectrum manual.
The following are advisory notices regarding coordination with Resource Orchestrator.

- Installation Order

  The order of installation of Resource Orchestrator and CA Spectrum is not important. Therefore, you can install in any order you like.

- Manager Installation

  [Windows Manager]
  The Resource Orchestrator manager and CA Spectrum's manager, SpectroSERVER cannot be installed on the same server.
  Install the Resource Orchestrator manager and the CA Spectrum manager on separate servers.

  [Linux Manager]
  The Resource Orchestrator manager and CA Spectrum's manager, SpectroSERVER can be installed on the same server or on separate servers. However, when they are installed on the same server, it is necessary to perform the settings given in "Preparations".

Preparations

Register the admin server on which the Resource Orchestrator manager has been installed as a management target of CA spectrum.

[Linux Manager]
When installing the Resource Orchestrator manager and SpectroSERVER on the same server, in order to share SNMP traps between Resource Orchestrator and CA Spectrum, ServerView Trap Server for Linux (trpsrvd) is necessary.
ServerView Trap Server for Linux is a program that is used to transfer SNMP traps received at UDP port 162 to other UDP port numbers.

The ServerView Trap Server for Linux is included in some versions of ServerView Operations Manager. In this case, install ServerView Trap Server for Linux referring to the ServerView Operations Manager manual.

If ServerView Trap Server for Linux is not included with ServerView Operations Manager, download it from the following web site, and install it referring to the documents provided with it.

URL: http://download.ts.fujitsu.com/prim_supportcd/SVSSoftware/html/ServerView_e.html

Perform the following settings after installing ServerView Trap Server for Linux.

1. Log in as OS administrator (root).

2. Change the SpectroSERVER SNMP trap reception port to one other than 162.

   The port number can be changed by editing the file shown below.

{*SpectroSERVER_installation_folder*}/CC/.vnmrc

Example

When changing the port number to 9162:

```
snmp_trap_port=9162
```

3. Restart SpectroSERVER.

4. Edit the /usr/share/SMAWtrpsv/conf/trpsrvtargets file and add the SpectroSERVER SNMP trap reception port.

   Before editing

```
##########################################################################
# Copyright (C) Fujitsu Siemens Computers 2007
# All rights reserved
# Configuration File for trpsrv (SMAWtrpsv)
##########################################################################
# Syntax
# port [(address | -) [comment]]

# examples
# 8162
# 9162 - test
# 162 145.25.124.121
```

   After editing (When making the SpectroSERVER SNMP trap reception port 9162)

```
##########################################################################
# Copyright (C) Fujitsu Siemens Computers 2007
# All rights reserved
# Configuration File for trpsrv (SMAWtrpsv)
##########################################################################

# Syntax
# port [(address | -) [comment]]

# examples
# 8162
# 9162 - test
# 162 145.25.124.121

#Transfer to UDP port 9162.
9162
```

5. When SELinux is made effective, it is necessary to set SELinux.

   For details on the settings, refer to "H.1.4 ServerView Trap Server for Linux".

6. Restart the system.

Setup Procedure

In this section, the procedures for checking SNMP traps that CA Spectrum receives from Resource Orchestrator, as event messages on OneClick (CA Spectrum's console) are explained.
Refer to the CA Spectrum manual for details on each procedure.

1. Start CA Spectrum's MIB Tools.

2. Click [Add MIB] on the "Navigation" panel.

   The [MIB Tools: Add MIB] dialog is displayed.

3. Click [Browse] and select the Resource Orchestrator MIB file.

4. Click [Compile].

   Confirm that compiling of the MIB file was successful in the messages displayed in "Compiler" of the [MIB Tools: Add MIB] dialog.

5. Click [Add & Close].

   The loaded MIB is displayed in the MIB Tools "Navigation" panel.

6. On "Navigation" panel, select the Resource Orchestrator MIB, and click the [Map] tab on the "Contents" panel.

7. Select the trap displayed in "Trap Support", and click [Information] to check the trap details.

8. Select the trap displayed in "Trap Support", and click [Map Traps].

   The [MIB Tools: Assign Trap Alarms] dialog is displayed.

9. Click [set] in "Alarm Severity", and select the severity of alarms for each trap.

10. Click the [OK] button.

    The [MIB Tools: Trap Support Results] dialog will be displayed, and you can check the results of the operation.

11. Click [Close].

    Check that event codes have been allocated for each trap in the MIB Tools "Trap Support".

12. Select a trap from "Trap Support", and click [Edit Traps].

    The Event Configuration application will start.

13. On the "Navigation" panel, select the event code allocated to the trap.

14. In "Event Message" of the "Contents" panel, the event message to be displayed when the trap is received is displayed.

    The message can be edited following the format specified by CA Spectrum.
    For details of the format, refer to the CA Spectrum manual.

15. After changing a message, select [Save All] or [Save Selected] from the Event Configuration application menu and save the settings.

After performing the above settings, perform the operation check described in "Appendix G Sending SNMP Traps".

Appendix B Co-Existence with Other Products

This appendix explains co-existence with other products.

B.1 Advisory Notes for Environments with Systemwalker Centric Manager or ETERNUS SF Storage Cruiser

This section explains advisory notes for use of Resource Orchestrator in combination with Systemwalker Centric Manager or ETERNUS SF Storage Cruiser.

Changing the Desktop Heap Value [Windows Manager]

When Resource Orchestrator is used in combination with Systemwalker Centric Manager or ETERNUS SF Storage Cruiser, there are cases where launching of services fails due to the desktop heap of the system being exhausted.
Therefore, refer to "13.1 When the Desktop Heap is Exhausted" in "Troubleshooting" and increase the area of the desktop heap.

Installation [Linux Manager]

When using the following products on servers that a manager has been installed on, in order to share SNMP Traps between servers it is necessary to perform the following procedure.

- Systemwalker Centric Manager (Operation management servers and section admin servers)

  When using Systemwalker Centric Manager in RHEL6 or later environments, refer to the procedure for sharing SNMP traps that is given in the manuals of Systemwalker Centric Manager.
  When using Systemwalker Centric Manager in RHEL5 or earlier environments, ServerView Trap Server for Linux (trpsrvd) is necessary.

- ETERNUS SF Storage Cruiser Manager 14.1 or earlier

  ServerView Trap Server for Linux (trpsrvd) is necessary.

ServerView Trap Server for Linux (trpsrvd) is used to transfer snmp traps received at UDP port number 162 to other UDP port numbers.
The ServerView Trap Server for Linux is included in some versions of ServerView Operations Manager. In this case, install ServerView Trap Server for Linux referring to the ServerView Operations Manager manual.

If ServerView Trap Server for Linux is not included with ServerView Operations Manager, download it from the following web site, and install it referring to the documents provided with it.

URL: http://download.ts.fujitsu.com/prim_supportcd/SVSSoftware/html/ServerView_e.html

Perform the following settings after installing ServerView Trap Server for Linux.

1. Log in as OS administrator (root).

2. Edit the /etc/services file, and add the following line.

   ```
   mpwksttr-trap    49162/udp
   ```

3. Edit the /usr/share/SMAWtrpsv/conf/trpsrvtargets file, and add port 49162.

   Before editing

   ```
   ##########################################################################
   # Copyright (C) Fujitsu Siemens Computers 2007
   # All rights reserved
   # Configuration File for trpsrv (SMAWtrpsv)
   ##########################################################################
   ```

```
# Syntax
# port [(address | -) [comment]]

# examples
# 8162
# 9162 - test
# 162 145.25.124.121
```

After editing

```
############################################################################
# Copyright (C) Fujitsu Siemens Computers 2007
# All rights reserved
# Configuration File for trpsrv (SMAWtrpsv)
############################################################################

# Syntax
# port [(address | -) [comment]]

# examples
# 8162
# 9162 - test
# 162 145.25.124.121

#Transfer to UDP port 49162.
49162
```

4. When SELinux is made effective, it is necessary to set SELinux.

   For details on the settings, refer to "H.1.4 ServerView Trap Server for Linux".

5. Restart the system.

Upgrading from Earlier Versions

- When upgrading managers of V2.1.3 or earlier versions

  [Windows Manager]
  The SNMP trap service (SystemWalker MpWksttr service) installed by the manager of V2.1.3 or earlier versions will be deleted by upgrading Resource Orchestrator.
  As the SystemWalker MpWksttr service is shared in environments where the following software exists, if the SystemWalker MpWksttr service is deleted when upgrading to Resource Orchestrator, perform installation and setup operation of the SystemWalker MpWksttr service referring to the manual of the following software.

  - Systemwalker Centric Manager (Operation management servers and department admin servers)

  - ETERNUS SF Storage Cruiser Manager 14.1 or earlier

  [Linux Manager]
  The SNMP trap service (SystemWalker MpWksttr service) installed by the manager of V2.1.3 or earlier versions will be deleted by upgrading Resource Orchestrator.
  As the SystemWalker MpWksttr service is shared in environments where the following software exists, if the SystemWalker MpWksttr service is deleted when upgrading to Resource Orchestrator, perform installation and setup operation of the SystemWalker MpWksttr service referring to the manual of the following software.

  - Systemwalker Centric Manager (Operation management servers and department admin servers)

  In environments where the above software has not been installed but the following software has, when upgrading managers of V2.1.3 or earlier versions, the SystemWalker MpWksttr service will remain even after upgrading, but the SystemWalker MpWksttr service is not required.

- ETERNUS SF Storage Cruiser Manager 14.2 or later

In this case, execute the following command as the OS administrator (root) and delete the SystemWalker MpWksttr service.

```
# rpm -e FJSVswstt <RETURN>
```

B.2 Co-Existence with ServerView Deployment Manager

This section explains how to use both Resource Orchestrator and ServerView Deployment Manager on the same network.

B.2.1 Overview

Resource Orchestrator and ServerView Deployment Manager can be installed either on the same server or on two different servers. In both cases, they can share the same subnet (admin LAN) to control managed servers. In a shared subnet configuration, ServerView Deployment Manager should be used instead of Resource Orchestrator for all image operations such as server cloning, backup and restore.

Resource Orchestrator and ServerView Deployment Manager use PXE boot via the network.
Therefore, if Resource Orchestrator and ServerView Deployment Manager both exist in the same network, problems resulting from conflict may occur.

Execute the deployment_service_uninstall command and uninstall services related to Resource Orchestrator (TFTP Service, PXE Services, and DHCP Server).

For details on the command, refer to "5.1 deployment_service_uninstall" in the "Reference Guide (Command) VE".

Figure B.1 System Configuration Example (Separate Server Installation)

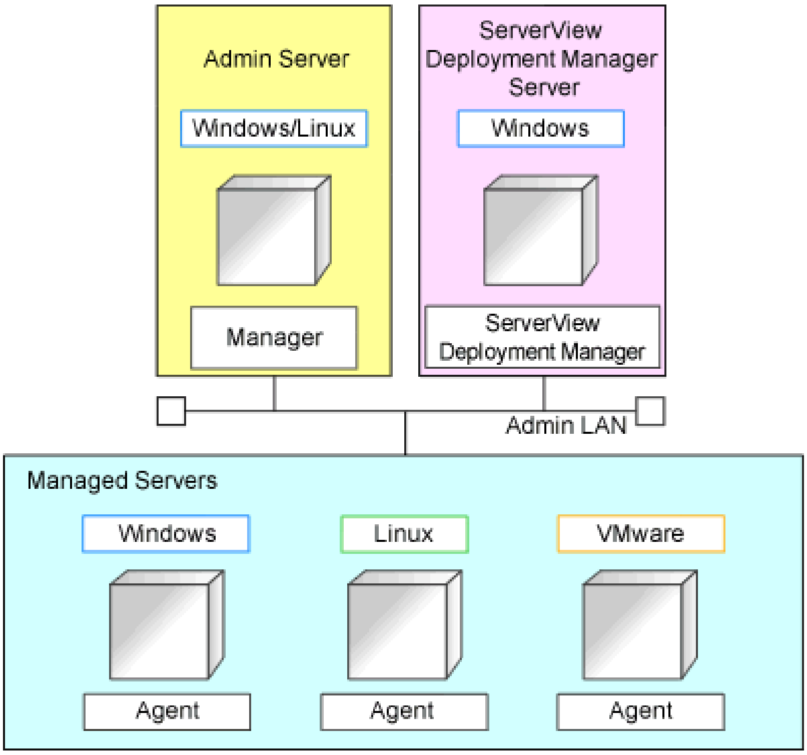
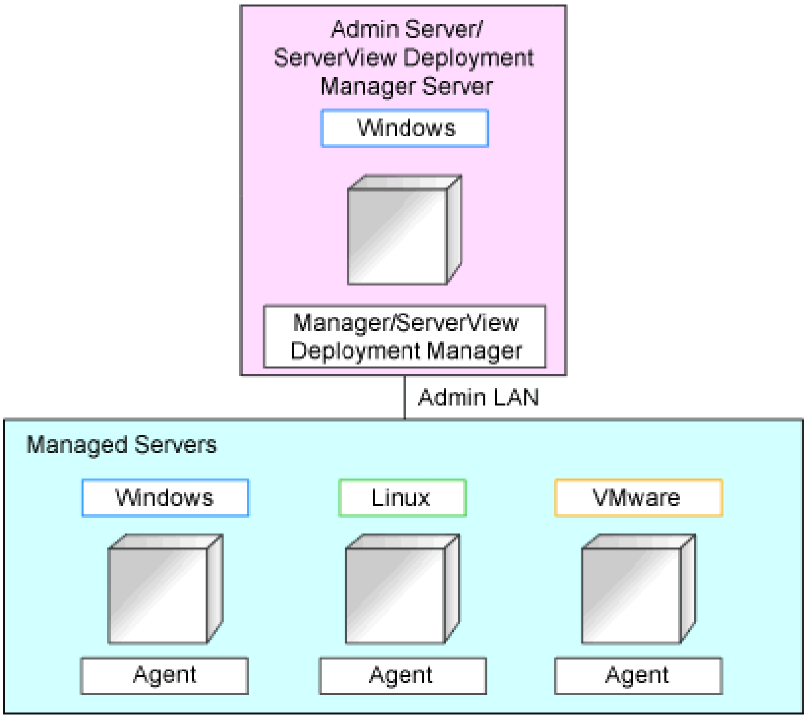


Figure B.2 System Configuration Example (Single Server Installation)



B.2.2 Restricted Functions

In shared subnet configurations, the following functions are no longer available from Resource Orchestrator.

- Backup and restore
- Cloning
- I/O virtualization (HBA address rename)
- Server switchover (based on the backup-restore and HBA address rename methods)
- Settings for the HBA address rename setup service
- Registration of admin LAN subnets

In Resource Orchestrator, the switchover of the VIOM method or the ISM method can be used.

However, users are recommended to use the following ServerView products.

- ServerView Deployment Manager (for cloning, backup and restore)
- ServerView Virtual-IO Manager or ServerView Infrastructure Manager 2.2 or later

B.3 Co-Existence with ServerView Infrastructure Manager (1.x)

This appendix explains how to use both Resource Orchestrator and ServerView Infrastructure Manager on the same network.

B.3.1 Overview

Resource Orchestrator and ServerView Infrastructure Manager use PXE boot via the network.
Therefore, if Resource Orchestrator and ServerView Infrastructure Manager both exist in the same network, problems resulting from conflict may occur.

Execute the deployment_service_uninstall command and uninstall services related to Resource Orchestrator (TFTP Service, PXE Services, and DHCP Server).

For details on the command, refer to "5.1 deployment_service_uninstall" in the "Reference Guide (Command) VE".

Information

For ServerView Infrastructure Manager V2.2 or later, use the ISM coordination function.

Restricted Functions

In shared subnet configurations, the following functions are no longer available from Resource Orchestrator.

- Backup and restore
- Cloning
- I/O virtualization (HBA address rename)
- Server switchover (based on the backup-restore and HBA address rename methods)
- Settings for the HBA address rename setup service
- Registration of admin LAN subnets

Appendix C Manager Cluster Operation Settings and Deletion

This appendix explains the settings necessary for operating Resource Orchestrator in cluster systems and the procedures for deleting this product from cluster systems.

Note

When coordination with VIOM/ISM is being used, or when Single Sign-On is configured, clustered manager operation is not supported.
When storage affinity switchover has been performed, clustered operation of Windows managers is not supported.

C.1 What are Cluster Systems

In cluster systems, two or more servers are operated as a single virtual server in order to enable high availability.

If a system is run with only one server, and the server or an application operating on it fails, all operations would stop until the server is rebooted.

In a cluster system where two or more servers are linked together, if one of the servers becomes unusable due to trouble with the server or an application being run, by restarting the applications on the other server it is possible to resume operations, shortening the length of time operations are stopped.
Switching from a failed server to another, operational server in this kind of situation is called failover.

In cluster systems, groups of two or more servers are called clusters, and the servers comprising a cluster are called nodes.

Clusters are classified into the following types:

- Standby clusters

  This type of cluster involves standby nodes that stand ready to take over from operating nodes. The mode can be one of the following modes:

  - 1:1 hot standby

    A cluster consisting of one operating node and one standby node. The operating node is operational and the standby node stands ready to take over if needed.

  - *n*:1 hot standby

    A cluster consisting of *n* operating nodes and one standby node. The *n* operating nodes run different operations and the standby node stands ready to take over from all of the operating nodes.

  - *n*:*i* hot standby

    A cluster consisting of *n* operating nodes and *i* standby nodes. The style is similar to *n*:1 hot standby, only there are i standby nodes standing ready to take over from all of the operating nodes.

  - Mutual standby

    A cluster consisting of two nodes with both operating and standby applications. The two nodes each run different operations and stand ready to take over from each other. If one node fails, the other node runs both of the operations.

  - Cascade

    A cluster consisting of three or more nodes. One of the nodes is the operating node and the others are the standby nodes.

- Scalable clusters

  This is a cluster that allows multiple server machines to operate concurrently for performance improvement and reduced degrading during trouble. It differs from standby clusters as the nodes are not divided into operating and standby types. If the system fails on one of the nodes in the cluster, the other servers take over the operations.

Resource Orchestrator managers support failover clustering of Microsoft(R) Windows Server(R) 2012 (Standard, Datacenter), and 1:1 hot standby of PRIMECLUSTER.

When operating managers in cluster systems, the HBA address rename setup service can be started on the standby node.
Using this function enables starting of managed servers without preparing a dedicated server for the HBA address rename setup service, even when managers and managed servers cannot communicate due to problems with the manager or the failure of the NIC used for connection to the admin LAN.

Information

For details of failover clustering, refer to the Microsoft web site.

For PRIMECLUSTER, refer to the PRIMECLUSTER manual.

C.2 Installation

This section explains installation of managers on cluster systems.

Perform installation only after configuration of the cluster system.

Note

In order to distinguish between the two physical nodes, one is referred to as the primary node and the other the secondary node. The primary node is the node that is active when the cluster service (cluster application) is started. The secondary node is the node that is in standby when the cluster service (cluster application) is started.

C.2.1 Preparations

This section explains the resources necessary before installation.

[Windows Manager]

- Client Access Point

  An access point is necessary in order to enable communication between the ROR console, managed servers, and managers. The IP addresses and network names used for access are allocated.

  - When the same access point will be used for access by the ROR console and the admin LAN

    Prepare a single IP address and network name.

  - When different access points will be used for access by the ROR console and the admin LAN

    Prepare a pair of IP addresses and network names.

- Shared Disk for Managers

  Prepare at least one storage volume (LUN) to store data shared by the managers.

  For the necessary disk space for the shared disk, total the values for *Installation_folder* and *Image_file_storage_folder* indicated for managers in "Table-Dynamic Disk Space" in "6.1.1.7 Dynamic Disk Space" in the "Overview", and secure the necessary amount of disk space.

- Generic Scripts for Manager Services

  Create the generic script files for (starting and stopping) the following manager services:

  - Resource Coordinator Web Server(Apache)

  - Resource Coordinator Sub Web Server(Mongrel)

  - Resource Coordinator Sub Web Server(Mongrel2)

  Create a script file with the following content for each of the services.

  The name of the file is optional, but the file extension must be ".vbs".

For Resource Coordinator Web Server (Apache)

```
Function Online()

    Dim objWmiProvider
    Dim objService
    Dim strServiceState

    ' Check to see if the service is running
    set objWmiProvider = GetObject("winmgmts:/root/cimv2")
    set objService = objWmiProvider.get("win32_service='Service_name'")
    strServiceState = objService.state

    If ucase(strServiceState) = "RUNNING" Then
        Online = True
    Else

        ' If the service is not running, try to start it.
        response = objService.StartService()

        ' response = 0  or 10 indicates that the request to start was accepted
        If ( response <> 0 ) and ( response <> 10 ) Then
            Online = False
        Else
            Online = True
        End If
    End If
End Function

Function Offline()

    Dim objWmiProvider
    Dim objService
    Dim strServiceState

    ' Check to see if the service is running
    set objWmiProvider = GetObject("winmgmts:/root/cimv2")
    set objService = objWmiProvider.get("win32_service='Service_name'")
    strServiceState = objService.state

    If ucase(strServiceState) = "RUNNING" Then

        response = objService.StopService()

        If ( response <> 0 ) and ( response <> 10 ) Then
            Offline = False
        Else
            Offline = True
        End If
    Else
            Offline = True
    End If
End Function

Function LooksAlive()

    Dim objWmiProvider
    Dim objService
    Dim strServiceState

    set objWmiProvider = GetObject("winmgmts:/root/cimv2")
    set objService = objWmiProvider.get("win32_service='Service_name'")
    strServiceState = objService.state

    if ucase(strServiceState) = "RUNNING" Then
```

```
        LooksAlive = True
    Else
        LooksAlive = False
    End If
End Function

Function IsAlive()

    Dim objWmiProvider
    Dim objService
    Dim strServiceState

    set objWmiProvider = GetObject("winmgmts:/root/cimv2")
    set objService = objWmiProvider.get("win32_service='Service_name'")
    strServiceState = objService.state

    if ucase(strServiceState) = "RUNNING" Then
        IsAlive= True
    Else
        IsAlive = False
    End If

End Function
```

Specify the following service names for four occurrences of "*service_name*" in the script.

- ResourceCoordinatorWebServer(Apache)

For Resource Coordinator Sub Web Server (Mongrel)

For Resource Coordinator Sub Web Server (Mongrel2)

```
Function Online()

    Dim objWmiProvider
    Dim objService
    Dim strServiceState

    ' Check to see if the service is running
    set objWmiProvider = GetObject("winmgmts:/root/cimv2")
    set objService = objWmiProvider.get("win32_service='service_name'")
    strServiceState = objService.state

    If ucase(strServiceState) = "RUNNING" Then
        Online = True
    Else

        ' If the service is not running, try to start it.
        response = objService.StartService()

        ' response = 0  or 10 indicates that the request to start was accepted
        If ( response <> 0 ) and ( response <> 10 ) Then
            Online = False
        Else
            Online = True
        End If
    End If
End Function

Function Offline()

    Dim objWmiProvider
    Dim objService
    Dim strServiceState
    ' Check to see if the service is running
    set objWmiProvider = GetObject("winmgmts:/root/cimv2")
    set objService = objWmiProvider.get("win32_service='service_name'")
    strServiceState = objService.state

    If ucase(strServiceState) = "RUNNING" Then

        response = objService.StopService()

        If ( response <> 0 ) and ( response <> 10 ) Then
            Offline = False
        Else
            Offline = True
        End If
    Else
            Offline = True
    End If
End Function

Function LooksAlive()

    Dim objWmiProvider
    Dim objService
    Dim strServiceState
    Dim objFile

    set objWmiProvider = GetObject("winmgmts:/root/cimv2")
    set objService = objWmiProvider.get("win32_service='service_name'")
    strServiceState = objService.state

    if ucase(strServiceState) = "RUNNING" Then
        LooksAlive = True
    Else
        liveflag=False
        set objFile = CreateObject("Scripting.FileSystemObject")
        if objFile.FileExists("Installation_folder\SVROR\Manager\Rails\db
\rcx.restarting") Then
            liveflag = True
        End If
        LooksAlive = liveflag
    End If
End Function

Function IsAlive()

    Dim objWmiProvider
    Dim objService
    Dim strServiceState
    Dim objFile

    set objWmiProvider = GetObject("winmgmts:/root/cimv2")
    set objService = objWmiProvider.get("win32_service='service_name'")
    strServiceState = objService.state

    if ucase(strServiceState) = "RUNNING" Then
        IsAlive= True
    Else
        liveflag=False
        set objFile = CreateObject("Scripting.FileSystemObject")
        if objFile.FileExists("Installation_folder\SVROR\Manager\Rails\db
\rcx.restarting") Then
            liveflag = True
        End If
        IsAlive = liveflag
    End If
End Function
```

Specify the following service names for four occurrences of "*service_name*" in the script.

- Resource Coordinator Sub Web Server(Mongrel)
- Resource Coordinator Sub Web Server(Mongrel2)

Specify the installation folder of the manager for the two occurrences of "*Installation_folder*" in the script.

[Linux Manager]

- Takeover Logical IP Address for the Manager

  When operating managers in cluster systems, allocate a new, unique IP address on the network to GLS.
  If the IP address used for access from the ROR console differs from the above IP address, prepare another logical IP address and allocate it to GLS.
  When using an IP address that is already being used for an existing operation (cluster application), there is no need to allocate a new IP address for the manager.

- Shared Disk for Managers

  Prepare a GDS volume to store shared data for managers.

  For the necessary disk space for the shared disk, total the values indicated for "[Linux Manager]" in "Table-Dynamic Disk Space" in "6.1.1.7 Dynamic Disk Space" in the "Overview", and secure the necessary amount of disk space.

C.2.2 Installation

This section explains installation of managers on cluster systems.

Install managers on both the primary and secondary nodes.

Install managers referring to "2.1 Manager Installation".

Note

- Do not install on the shared disk for managers.

[Windows Manager]

- On the [Choose Install Location] window, specify the same folder names on the primary node and secondary node for the installation folders.
  However, do not specify a folder on the shared disk for managers.
- On the [Administrative User Creation] window, specify the same character strings for the user account names and passwords on the primary node and the secondary node.
- On the [Admin LAN Selection] window of the installer, select the network with the same subnet for direct communication with managed servers.

[Linux Manager]

- Specify the same character strings for the primary node and the secondary node when entering administrative user account names and passwords during installation.
- Select a network of the same subnet from which direct communication with managed servers is possible when selecting the admin LAN network interface during installation.

After installation, stop the manager.

Stop the manager using the rcxadm mgrctl stop command.

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

[Windows Manager]
Change the startup type of the following manager services to "Manual".

- Resource Coordinator Task Manager
- Resource Coordinator Web Server(Apache)
- Resource Coordinator Sub Web Server(Mongrel)
- Resource Coordinator Sub Web Server(Mongrel2)
- Deployment Service (*)
- TFTP Service (*)
- PXE Services (*)
- Resource Coordinator DB Server (PostgreSQL)

* Note: Not necessary when ServerView Deployment Manager is used in the same subnet.

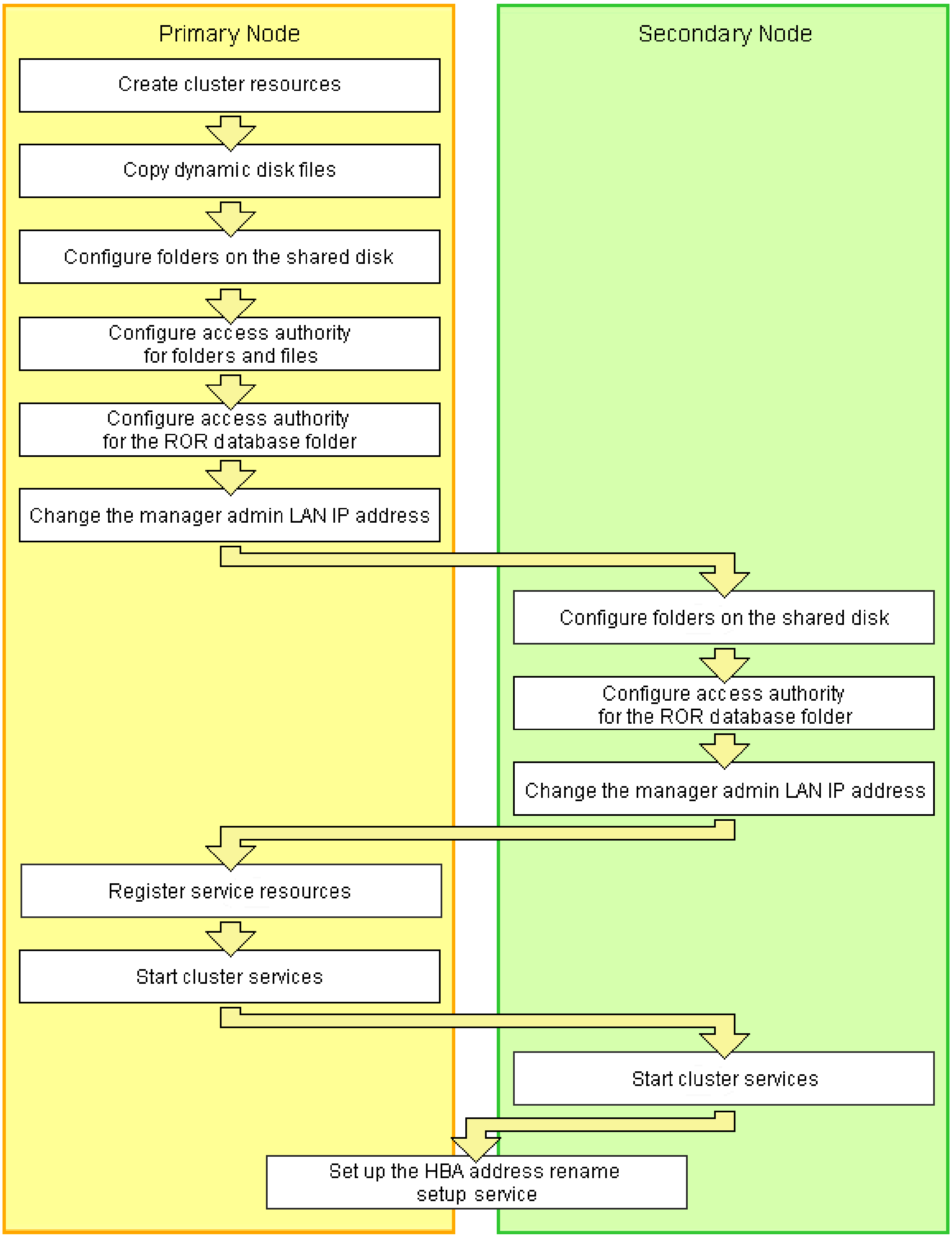
C.3 Configuration

This section explains the procedure for setting up managers as cluster services (cluster applications) in cluster systems.

C.3.1 Configuration [Windows Manager]

Perform setup on the admin server.
The flow of setup is as shown below.

Figure C.1 Manager Service Setup Flow


Primary Node
Secondary Node
Create cluster resources
Copy dynamic disk files
Configure folders on the shared disk
Configure access authority for folders and files
Configure access authority for the ROR database folder
Change the manager admin LAN IP address
Configure folders on the shared disk
Configure access authority for the ROR database folder
Change the manager admin LAN IP address
Register service resources
Start cluster services
Start cluster services
Set up the HBA address rename setup service

Setup of managers as cluster services (cluster applications) is performed using the following procedure.
This explanation assumes that the shared disk for managers has been allocated to the primary node.

Create cluster resources

1. Store the generic scripts.

   Store the generic scripts created in "C.2.1 Preparations" in the manager installation folders on the primary node and the second node.
   After storing the scripts, set the access rights for the script files.
   Use the command prompt to execute the following command on each script file.

   ```
   >cacls File_name /P "NT AUTHORITY\SYSTEM:F" "BUILTIN\Administrators:F" <RETURN>
   ```

   Note

   When using the following language versions of Windows, replace the specified local system name (NT AUTHORITY\SYSTEM) and administrator group name (BUILTIN\Administrators) with those in the following list:

Language	Local System Name	Administrator Group Name
German	NT-AUTORITÄT\SYSTEM	VORDEFINIERT\Administratoren
French	AUTORITE NT\SYSTEM	BUILTIN\Administrateurs
Spanish	NT AUTHORITY\SYSTEM	BUILTIN\Administradores
Russian	NT AUTHORITY\SYSTEM	BUILTIN\Администраторы

2. Open the [Failover Cluster Management] window and connect to the cluster system.

   When using Windows Server 2012 or later, "Roles" is described as "Failover Cluster Manager".
   When using Windows Server 2012 or later, replace "Failover Cluster Manager" with "Roles" in this manual.

3. Configure a manager "service or application".

   When using Windows Server 2012 or later, "Roles" is described as "Services and applications".
   When using Windows Server 2012 or later, replace "Services and applications" with "Roles" in this manual.

   a. Right-click [Services and Applications] on the Failover Cluster Management tree, and select [More Actions]-[Create Empty Service or Application].

      [New service or application] will be created under [Services and Applications].

   b. Right-click [New service or application], and select [Properties] from the displayed menu.

      The [New service or application properties] dialog is displayed.

   c. Change the "Name" on the [General] tab, select the resource name of the primary node from "Preferred owners:", and click [Apply].

   d. Once settings are applied, click [OK].

   From this point, the explanation assumes that the name of the "service or application" for Resource Orchestrator has been configured as "RC-manager".

4. Allocate the shared disk to the manager "service or application".

   a. Right-click [Services and Applications]-[RC-manager], and select [Add storage] from the displayed menu.

      The [Add Storage] window will be displayed.

   b. From the "Available disks:", select the shared disk for managers and click [OK].

5. Allocate the client access point to the manager "service or application".

   a. Right-click [Services and Applications]-[RC-manager], select [Add a resource]-[1 - Client Access Point] from the displayed menu.

      The [New Resource Wizard] window will be displayed.

b. Configure the following parameters on the [General] tab and then click [Next>].

   Name

   Set the network name prepared in "C.2.1 Preparations".

   Networks

   Check the network to use.

   Address

   Set the IP address prepared in "C.2.1 Preparations".

   "Confirmation" will be displayed.

c. Check the information displayed for "Confirmation" and click [Next>].

   If configuration is successful, the "Summary" will be displayed.

d. Click [Finish].

   "Name: *Network_Name*" and "IP Address:*IP_Address*" will be created in the "Server Name" of the "Summary of RC-manager" displayed in the center of the window.
   The specified value in step b is displayed for *Network_Name* and *IP_Address*.

When a network other than the admin LAN has been prepared for ROR console access, perform the process in step 6.

6. Allocate the IP address to the manager "service or application".

   a. Right-click [Services and Applications]-[RC-manager], select [Add a resource]-[More resources]-[4 - Add IP Address] from the displayed menu.

      "IP Address: [not configured]" will be created in the "Other Resources" of the "Summary of RC-manager" displayed in the center of the window.

   b. Right-click "IP Address: [not configured]", and select [Properties] from the displayed menu.

      The [IP Address: [not configured] Properties] window is displayed.

   c. Configure the following parameters on the [General] tab and then click [Apply].

      Resource Name

      Set the network name prepared in "C.2.1 Preparations".

      Network

      Select the network to use from the pull-down menu.

      Static IP Address

      Set the IP address prepared in "C.2.1 Preparations".

   d. Once settings are applied, click [OK].

Copy dynamic disk files

Copy the files from the dynamic disk of the manager on the primary node to the shared disk for managers.

1. Use Explorer to create the "*Drive_name*:\Fujitsu\ROR\SVROR\" folder on the shared disk.
2. Use Explorer to copy the files and folders from the local disk of the primary node to the folder on the shared disk.

Table C.1 List of Files and Folders to Copy

Local Disk (Source)	Shared Disk (Target)
Installation_folder\SVROR\Manager\etc\customize_data	*Drive_name*:\Fujitsu\ROR\SVROR \customize_data

Local Disk (Source)	Shared Disk (Target)
Installation_folder\SVROR\Manager\etc\opt\FJSVssmgr\current \certificate	*Drive_name*:\Fujitsu\ROR\SVROR\certificate
Installation_folder\SVROR\Manager\Rails\config\rcx_secret.key	*Drive_name*:\Fujitsu\ROR\SVROR \rcx_secret.key
Installation_folder\SVROR\Manager\Rails\config\rcx\rcxdb.pwd	*Drive_name*:\Fujitsu\ROR\SVROR\rcxdb.pwd
Installation_folder\SVROR\Manager\Rails\db	*Drive_name*:\Fujitsu\ROR\SVROR\db
Installation_folder\SVROR\Manager\Rails\log	*Drive_name*:\Fujitsu\ROR\SVROR\log
Installation_folder\SVROR\Manager\Rails\tmp	*Drive_name*:\Fujitsu\ROR\SVROR\tmp
Installation_folder\SVROR\Manager\sys\apache\conf	*Drive_name*:\Fujitsu\ROR\SVROR\conf
Installation_folder\SVROR\Manager\sys\apache\logs	*Drive_name*:\Fujitsu\ROR\SVROR\logs
Installation_folder\SVROR\Manager\var	*Drive_name*:\Fujitsu\ROR\SVROR\var
Installation_folder\SVROR\ScwPro\Bin\ipTable.dat (*)	*Drive_name*:\Fujitsu\ROR\SVROR\ipTable.dat
Installation_folder\SVROR\ScwPro\scwdb (*)	*Drive_name*:\Fujitsu\ROR\SVROR\scwdb
Installation_folder\SVROR\ScwPro\tftp\rcbootimg (*)	*Drive_name*:\Fujitsu\ROR\SVROR\rcbootimg
User_specified_folder\ScwPro\depot (*)	*Drive_name*:\Fujitsu\ROR\SVROR\depot

* Note: Not necessary when ServerView Deployment Manager is used in the same subnet.

3. Use Explorer to change the names of the folders below that were copied.

   - *Installation_folder*\SVROR\Manager\etc\customize_data
   - *Installation_folder*\SVROR\Manager\etc\opt\FJSVssmgr\current\certificate
   - *Installation_folder*\SVROR\Manager\Rails\config\rcx_secret.key
   - *Installation_folder*\SVROR\Manager\Rails\config\rcx\rcxdb.pwd
   - *Installation_folder*\SVROR\Manager\Rails\db
   - *Installation_folder*\SVROR\Manager\Rails\log
   - *Installation_folder*\SVROR\Manager\Rails\tmp
   - *Installation_folder*\SVROR\Manager\sys\apache\conf
   - *Installation_folder*\SVROR\Manager\sys\apache\logs
   - *Installation_folder*\SVROR\Manager\var
   - *Installation_folder*\SVROR\ScwPro\Bin\ipTable.dat (*)
   - *Installation_folder*\SVROR\ScwPro\scwdb (*)
   - *Installation_folder*\SVROR\ScwPro\tftp\rcbootimg (*)

   * Note: Not necessary when ServerView Deployment Manager is used in the same subnet.

   Note

   When folders or files are in use by another program, attempts to change folder names and file names may fail.
   If attempts to change names fail, change the names after rebooting the server.

4. Delete the following file from the shared disk:

   - *Drive_name*:\Fujitsu\ROR\SVROR\db\rmc_key

Configure Folders on the Shared Disk (Primary node)

1. On the primary node, configure symbolic links to the files and folders on the shared disk.

   Use the command prompt to configure a symbolic link from the files and folders on the local disk of the primary node to the files and folders on the shared disk.

   Execute the following command.

   - Folder

     ```
     >mklink /d Link_source Link_target <RETURN>
     ```

   - File

     ```
     >mklink Link_source Link_target <RETURN>
     ```

     Specify the folders or files copied in "Copy dynamic disk files" for *Link_source*.

     Specify the folders or files copied to the shared disk in "Copy dynamic disk files" for *Link_target*.

   The folders and files to specify are as given below:

   Table C.2 Folders to Specify

Local Disk (Link Source)	Shared Disk (Link Target)
Installation_folder\SVROR\Manager\etc\customize_data	*Drive_name*:\Fujitsu\ROR\SVROR\customize_data
Installation_folder\SVROR\Manager\etc\opt\FJSVssmgr\current\certificate	*Drive_name*:\Fujitsu\ROR\SVROR\certificate
Installation_folder\SVROR\Manager\Rails\db	*Drive_name*:\Fujitsu\ROR\SVROR\db
Installation_folder\SVROR\Manager\Rails\log	*Drive_name*:\Fujitsu\ROR\SVROR\log
Installation_folder\SVROR\Manager\Rails\tmp	*Drive_name*:\Fujitsu\ROR\SVROR\tmp
Installation_folder\SVROR\Manager\sys\apache\conf	*Drive_name*:\Fujitsu\ROR\SVROR\conf
Installation_folder\SVROR\Manager\sys\apache\logs	*Drive_name*:\Fujitsu\ROR\SVROR\logs
Installation_folder\SVROR\Manager\var	*Drive_name*:\Fujitsu\ROR\SVROR\var
Installation_folder\SVROR\ScwPro\scwdb (*)	*Drive_name*:\Fujitsu\ROR\SVROR\scwdb
Installation_folder\SVROR\ScwPro\tftp\rcbootimg (*)	*Drive_name*:\Fujitsu\ROR\SVROR\rcbootimg

   * Note: Not necessary when ServerView Deployment Manager is used in the same subnet.

   Table C.3 Files to Specify

Local Disk (Link Source)	Shared Disk (Link Target)
Installation_folder\SVROR\Manager\Rails\config\rcx_secret.key	*Drive_name*:\Fujitsu\ROR\SVROR\rcx_secret.key
Installation_folder\SVROR\Manager\Rails\config\rcx\rcxdb.pwd	*Drive_name*:\Fujitsu\ROR\SVROR\rcxdb.pwd
Installation_folder\SVROR\ScwPro\Bin\ipTable.dat (*)	*Drive_name*:\Fujitsu\ROR\SVROR\ipTable.dat

   * Note: Not necessary when ServerView Deployment Manager is used in the same subnet.

   Note

   Before executing the above command, move to a folder one level higher than the link source folder.

Example

When specifying a link from "*Installation_folder*\SVROR\Manager\sys\apache\logs" on the local disk to "*Drive_name*:\Fujitsu\ROR\SVROR\logs" on the shared disk

```
>cd Installation_folder\SVROR\Manager\sys\apache <RETURN>
>mklink /d logs Drive_name:\Fujitsu\ROR\SVROR\logs <RETURN>
```

2. Change the registry of the primary node.

   Not necessary when ServerView Deployment Manager is used in the same subnet.

   a. Backup the registry to be changed.

      Execute the following command.

      - x64

      ```
      >reg save HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard
      scw.reg <RETURN>
      ```

      - x86

      ```
      >reg save HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\SystemcastWizard scw.reg <RETURN>
      ```

   b. Change the registry.

      Execute the following command.

      - x64

      ```
      >reg add HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard
      \ResourceDepot /v BasePath /d Drive_name:\Fujitsu\ROR\SVROR\depot\ /f <RETURN>

      >reg add HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard
      \DatabaseBroker\Default /v LocalPath /d Drive_name:\Fujitsu\ROR\SVROR\scwdb /f <RETURN>

      >reg add HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard
      \DHCP /v IPtableFilePath /d Drive_name:\Fujitsu\ROR\SVROR /f <RETURN>
      ```

      - x86

      ```
      >reg add HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\SystemcastWizard\ResourceDepot /v
      BasePath /d Drive_name:\Fujitsu\ROR\SVROR\depot\ /f <RETURN>

      >reg add HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\SystemcastWizard\DatabaseBroker
      \Default /v LocalPath /d Drive_name:\Fujitsu\ROR\SVROR\scwdb /f <RETURN>

      >reg add HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\SystemcastWizard\DHCP /v
      IPtableFilePath /d Drive_name:\Fujitsu\ROR\SVROR /f <RETURN>
      ```

      Change *Drive_name* based on your actual environment.

   c. If changing the registry fails, restore the registry.

      Execute the following command.

      - x64

      ```
      >reg restore HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard
      scw.reg <RETURN>
      ```

- x86

```
>reg restore HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\SystemcastWizard scw.reg <RETURN>
```

Note

Do not use the backup registry file created using this procedure for any other purposes.

Configure Access Authority for Folders and Files

- Set the access authority for the folders and files copied to the shared disk.

  Use the command prompt to set the access authority for the folders and files on the shared disk.

  The folders and files to specify are as given below:

  - Folder

    Drive_name:\Fujitsu\ROR\SVROR\certificate
    Drive_name:\Fujitsu\ROR\SVROR\conf\ssl.key
    Drive_name:\Fujitsu\ROR\SVROR\var\log

  - Files

    Drive_name:\Fujitsu\ROR\SVROR\rcx_secret.key

  Execute the following command.

  - Folder

```
>cacls Folder_name /T /P "NT AUTHORITY\SYSTEM:F" "BUILTIN\Administrators:F" <RETURN>
```

  - File

```
>cacls File_name /P "NT AUTHORITY\SYSTEM:F" "BUILTIN\Administrators:F" <RETURN>
```

Note

When using the following language versions of Windows, replace the specified local system name (NT AUTHORITY\SYSTEM) and administrator group name (BUILTIN\Administrators) with those in the following list:

Language	Local System Name	Administrator Group Name
German	NT-AUTORITÄT\SYSTEM	VORDEFINIERT\Administratoren
French	AUTORITE NT\SYSTEM	BUILTIN\Administrateurs
Spanish	NT AUTHORITY\SYSTEM	BUILTIN\Administradores
Russian	NT AUTHORITY\SYSTEM	BUILTIN\Администраторы

Configure Access Authority for the Resource Orchestrator Database Folder (Primary node)

Set the access authority for the folder for the Resource Orchestrator database copied to the shared disk.

Execute the following command using the command prompt of the primary node:

```
>cacls Drive_name:\Fujitsu\ROR\SVROR\db\data /T /P "NT AUTHORITY\SYSTEM:F" "BUILTIN\Administrators:F" "rcxdb:C"
<RETURN>
```

Change the Manager Admin LAN IP Address (Primary node)

Change the admin LAN IP address of the manager.

Specify the admin LAN IP address set in step 5 of "Create cluster resources".

1. Bring the admin LAN IP address for the manager "service or application" online.
2. Execute the following command using the command prompt of the primary node:

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

3. Allocate the shared disk 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*.

   Point

   When using Windows Server 2012 or later, use the following procedure to move resources between nodes.

   1. Right-click [Roles]-[RC-manager] on the Failover Cluster Management tree, and select [Move]-[Select Node] from the displayed menu.
   2. Select the name of secondary node in the dialog, and click [OK].

   In the following procedure, when migrating resources between nodes, use this procedure to select the node name.

Configure Folders on the Shared Disk (Secondary node)

- On the secondary node, configure symbolic links to the folders on the shared disk.

  a. Use Explorer to change the names of the folders and files below.

  - *Installation_folder*\SVROR\Manager\etc\customize_data
  - *Installation_folder*\SVROR\Manager\etc\opt\FJSVssmgr\current\certificate
  - *Installation_folder*\SVROR\Manager\Rails\config\rcx_secret.key
  - *Installation_folder*\SVROR\Manager\Rails\config\rcx\rcxdb.pwd
  - *Installation_folder*\SVROR\Manager\Rails\db
  - *Installation_folder*\SVROR\Manager\Rails\log
  - *Installation_folder*\SVROR\Manager\Rails\tmp
  - *Installation_folder*\SVROR\Manager\sys\apache\conf
  - *Installation_folder*\SVROR\Manager\sys\apache\logs
  - *Installation_folder*\SVROR\Manager\var
  - *Installation_folder*\SVROR\ScwPro\Bin\ipTable.dat (*)
  - *Installation_folder*\SVROR\ScwPro\scwdb (*)
  - *Installation_folder*\SVROR\ScwPro\tftp\rcbootimg (*)

  * Note: Not necessary when ServerView Deployment Manager is used in the same subnet.

Note

When folders or files are in use by another program, attempts to change folder names and file names may fail.
If attempts to change names fail, change the names after rebooting the server.

b. Use the command prompt to configure a symbolic link from the folder on the local disk of the secondary node to the folder on the shared disk.

   Execute the following command.

   - Folder

     ```
     >mklink /d Link_source Link_target <RETURN>
     ```

   - File

     ```
     >mklink Link_source Link_target <RETURN>
     ```

     Specify a file or folder on the local disk of the secondary node for *Link_source*.

     Specify a file or folder on the shared disk of the secondary node for *Link_target*.

   The folders to specify are as given below:

Table C.4 Folders to Specify

Local Disk (Link Source)	Shared Disk (Link Target)
Installation_folder\SVROR\Manager\etc\customize_data	*Drive_name*:\Fujitsu\ROR\SVROR\customize_data
Installation_folder\SVROR\Manager\etc\opt\FJSVssmgr\current\certificate	*Drive_name*:\Fujitsu\ROR\SVROR\certificate
Installation_folder\SVROR\Manager\Rails\db	*Drive_name*:\Fujitsu\ROR\SVROR\db
Installation_folder\SVROR\Manager\Rails\log	*Drive_name*:\Fujitsu\ROR\SVROR\log
Installation_folder\SVROR\Manager\Rails\tmp	*Drive_name*:\Fujitsu\ROR\SVROR\tmp
Installation_folder\SVROR\Manager\sys\apache\conf	*Drive_name*:\Fujitsu\ROR\SVROR\conf
Installation_folder\SVROR\Manager\sys\apache\logs	*Drive_name*:\Fujitsu\ROR\SVROR\logs
Installation_folder\SVROR\Manager\var	*Drive_name*:\Fujitsu\ROR\SVROR\var
Installation_folder\SVROR\ScwPro\scwdb (*)	*Drive_name*:\Fujitsu\ROR\SVROR\scwdb
Installation_folder\SVROR\ScwPro\tftp\rcbootimg (*)	*Drive_name*:\Fujitsu\ROR\SVROR\rcbootimg

* Note: Not necessary when ServerView Deployment Manager is used in the same subnet.

Table C.5 Files to Specify

Local Disk (Link Source)	Shared Disk (Link Target)
Installation_folder\SVROR\Manager\Rails\config\rcx_secret.key	*Drive_name*:\Fujitsu\ROR\SVROR\rcx_secret.key
Installation_folder\SVROR\Manager\Rails\config\rcx\rcxdb.pwd	*Drive_name*:\Fujitsu\ROR\SVROR\rcxdb.pwd
Installation_folder\SVROR\ScwPro\Bin\ipTable.dat (*)	*Drive_name*:\Fujitsu\ROR\SVROR\ipTable.dat

* Note: Not necessary when ServerView Deployment Manager is used in the same subnet.

Note

Before executing the above command, move to a folder one level higher than the link source folder.

Example

When specifying a link from "*Installation_folder*\SVROR\Manager\sys\apache\logs" on the local disk to "*Drive_name*:\Fujitsu\ROR\SVROR\logs" on the shared disk

```
>cd Installation_folder\SVROR\Manager\sys\apache <RETURN>
>mklink /d logs Drive_name:\Fujitsu\ROR\SVROR\logs <RETURN>
```

Configure Access Authority for the Resource Orchestrator Database Folder (Secondary node)

Set the access authority for the folder for the Resource Orchestrator database copied to the shared disk.

Execute the following command using the command prompt of the secondary node:

```
>cacls Drive_name:\Fujitsu\ROR\SVROR\db\data /T /G "rcxdb:C" /E <RETURN>
```

Change the Manager Admin LAN IP Address (Secondary node)

Change the admin LAN IP address of the manager.

Specify the admin LAN IP address set in step 5 of "Create cluster resources".

1. Execute the following command using the command prompt of the secondary node:

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

2. 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*.

Register service resources

1. Add the manager service to the manager "service or application".
   Add the following six services.

   - Resource Coordinator Manager
   - Resource Coordinator Task Manager
   - Deployment Service (*)
   - TFTP Service (*)
   - PXE Services (*)
   - Resource Coordinator DB Server (PostgreSQL)

   * Note: Not necessary when ServerView Deployment Manager is used in the same subnet.

   Perform the following procedure for each of the above services:

a. Right-click [Services and Applications]-[RC-manager] on the Failover Cluster Management tree, and select [Add a resource]-[4 - Generic Service] from the displayed menu.

   The [New Resource Wizard] window will be displayed.

b. Select the above services on "Select Service" and click [Next>].

   "Confirmation" will be displayed.

c. Check the information displayed for "Confirmation" and click [Next>].

   If configuration is successful, the "Summary" will be displayed.

d. Click [Finish].

   After completing the configuration of all of the services, check that the added services are displayed in "Other Resources" of the "Summary of RC-manager" displayed in the center of the window.

2. Configure registry replication as a service in the manager "service or application".

   Not necessary when ServerView Deployment Manager is used in the same subnet.

   Configure the registry replication of resources based on the following table.

   - x64

Resource for Configuration	Registry Key
Deployment Service	[HKEY_LOCAL_MACHINE\]SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard\ResourceDepot
	[HKEY_LOCAL_MACHINE\]SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard\DatabaseBroker\Default
PXE Services	[HKEY_LOCAL_MACHINE\]SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard\DHCP
	[HKEY_LOCAL_MACHINE\]SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard\PXE\ClientBoot\

   - x86

Resource for Configuration	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\

   During configuration, enter the section of the registry keys after the brackets ([ ]).

   Perform the following procedure for each of the above resources:

   - For Windows Server 2012 or later

     Execute the following cmdlets in Windows PowerShell

```
Add-ClusterCheckpoint -ResourceName Target_resource_name -RegistryCheckpoint Registry_key <RETURN>
```

     Also, when configuring the second registry key, execute the cmdlets described above.

3. Add the generic scripts to the manager "service or application".

   Add the three generic scripts from the script files that were created in step 1 of "Create cluster resources". Perform the following procedure for each generic script.

   a. Right-click [Services and Applications]-[RC-manager] on the Failover Cluster Management tree, and select [Add a resource]-[3 - Generic Script] from the displayed menu.

      The [New Resource Wizard] window will be displayed.

   b. Set the script files created in step 1 of "Create Cluster Resources" in the "Script file path" of the "Generic Script Info", and click [Next>].

      "Confirmation" will be displayed.

   c. Check the information displayed for "Confirmation" and click [Next>].

      If configuration is successful, the "Summary" will be displayed.

   d. Click [Finish].

      After completing the configuration of all of the generic scripts, check that the added generic scripts are displayed in "Other Resources" of the "Summary of RC-manager" displayed in the center of the window.

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

   Configure the dependencies of resources based on the following table.

Table C.6 Configuring Resource Dependencies

Resource for Configuration	Dependent Resource
Resource Coordinator Manager	Shared Disks
Resource Coordinator Task Manager	Shared Disks
Resource Coordinator Sub Web Server (Mongrel) Script	Resource Coordinator Task Manager
Resource Coordinator Sub Web Server (Mongrel2) Script	Resource Coordinator Task Manager
Resource Coordinator Web Server (Apache) Script	Shared Disks
Deployment Service (*)	PXE Services
TFTP Service (*)	Deployment Service
PXE Services (*)	Admin LAN IP Address
Resource Coordinator DB Server (PostgreSQL)	Shared Disks

   * Note: Not necessary when ServerView Deployment Manager is used in the same subnet.

   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 "Resource" of the [Dependencies] tab select the name of the "Dependent Resource" from "Table C.6 Configuring Resource Dependencies" and click [Apply].

   c. Once settings are applied, click [OK].

Start the cluster service

1. 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.

   Confirm that all resources have been brought online.

2. Switch the manager "service or application" to the secondary node.

   Confirm that all resources of the secondary node have been brought online.

Note

When registering the admin LAN subnet, additional settings are required.

For the setting method, refer to the [Windows Manager] section of "Settings for Clustered Manager Configurations" in "7.9 Registering Admin LAN Subnets" in the "User's Guide VE".

Set up the HBA address rename Setup Service

When configuring managers and the HBA address rename setup service in cluster systems, perform the following procedure.

Not necessary when ServerView Deployment Manager is used in the same subnet.

Performing the following procedure starts the HBA address rename setup service on the standby node in the cluster.

1. Switch the manager "service or application" to the primary node.

   Right-click [Services and Applications]-[RC-manager] on the Failover Cluster Management tree, and select the primary node using [Move this service or application to another node] from the displayed menu.
   Switch the "Current Owner" of the "Summary of RC-manager" displayed in the center of the window to the primary node.

2. Configure the startup settings of the HBA address rename setup service of the secondary node.

   a. Execute the following command using the command prompt:

      ```
      >"Installation_folder\SVROR\WWN Recovery\opt\FJSVrcxrs\bin\rcxhbactl.exe" <RETURN>
      ```

      The [HBA address rename setup service] dialog is displayed.

   b. Define the following settings:

      IP address of admin server

      Specify the admin LAN IP address set in step 5 of "Create Cluster Resources".

      Port number

      Enter the port number that is used to communicate with the admin server. The port number at installation is 23461.
      If the "rcxweb" port number of the admin server is changed, specify the number that has been changed.

   c. Click [Run].

      Confirm that the "Status" becomes "Running".

   d. Click [Stop].

      Confirm that the "Status" becomes "Stopping".

   e. Click [Cancel] and close the [HBA address rename setup service] dialog.

3. Switch the manager "service or application" to the secondary node.

   Right-click [Services and Applications]-[RC-manager] on the Failover Cluster Management tree, and select the resource name of the secondary node from the [Move this service or application to another node] from the displayed menu.
   The "Current Owner" of the "Summary of RC-manager" switches to the secondary node.

4. Configure the startup settings of the HBA address rename setup service of the primary node.

   The procedure is the same as step 2.

5. Take the manager "service or application" offline.

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

6. Configure a "service or application" for the HBA address rename service.

   a. Right-click [Services and Applications] on the Failover Cluster Management tree, and select [More Actions]-[Create Empty Service or Application].

      [New service or application] will be created under [Services and Applications].

   b. Right-click [New service or application], and select [Properties] from the displayed menu.

      The [New service or application properties] dialog is displayed.

   c. Change the "Name" on the [General] tab, select the resource name of the primary node from "Preferred owners", and click [Apply].

   d. Once settings are applied, click [OK].

   From this point, this explanation assumes that the name of the "service or application" for the HBA address rename setup service has been configured as "RC-HBAar".

7. Add the generic scripts to the manager "service or application" for the HBA address rename service.

   a. Right-click [Services and Applications]-[RC-HBAar] on the Failover Cluster Management tree, and select [Add a resource]-[3 - Generic Script] from the displayed menu.

      The [New Resource Wizard] window will be displayed.

   b. Set the script files in the "Script file path" of the "Generic Script Info", and click [Next>].

      "Confirmation" will be displayed.

      Script File Path
      Installation_folder\SVROR\Manager\cluster\script\HBAarCls.vbs

   c. Check the information displayed for "Confirmation" and click [Next>].

      The "Summary" will be displayed.

   d. Click [Finish].

      Check that the added "HBAarCls Script" is displayed in "Other Resources" of the "Summary of RC-manager" displayed in the center of the window.

8. Add the generic scripts for the coordinated starting of the "service or application" for the HBA address rename setup service, to the "service or application" for the manager.

   a. Right-click [Services and Applications]-[RC-manager] on the Failover Cluster Management tree, and select [Add a resource]-[3 - Generic Script] from the displayed menu.

      The [New Resource Wizard] window will be displayed.

   b. Set the script files in the "Script file path" of the "Generic Script Info", and click [Next>].

      "Confirmation" will be displayed.

      Script File Path
      Installation_folder\SVROR\Manager\cluster\script\HBAarClsCtl.vbs

   c. Check the information displayed for "Confirmation" and click [Next>].

      The "Summary" will be displayed.

   d. Click [Finish].

      Check that the added "HBAarClsCtl Script" is displayed in "Other Resources" of the "Summary of RC-manager" displayed in the center of the window.

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

   Configure the dependencies of resources based on the following table.

Table C.7 Configuring Resource Dependencies

Resource for Configuration	Dependent Resource
PXE Services (*)	HBAarClsCtl Script
HBAarClsCtl Script	Admin LAN IP Address

* Note: The PXE Services have been configured in step 4, "Register service resources", but change them using the above procedure.

Configure the dependencies of resources based on the following table for each of the above resources:
Refer to step 4, "Register service resources" for how to perform the settings of Resource Dependencies.

10. Configure the property to refer to when executing the "HBAarClsCtl Script".

    Execute the following command using the command prompt of the primary node:

    ```
    >CLUSTER RES "HBAarClsCtl_Script" /PRIV HBAGroupName="RC-HBAar"<RETURN>
    ```

    Note

    - Specify the name of the generic script added in step 8 for *HBAarClsCtl_Script*, and the name of the "service or application" for the HBA address rename service for *RC-HBAar*.

    - For Windows Server 2012 or later, the CLUSTER commands are not installed by default.

      When the commands are not installed, execute the following commands using the command prompt to enable the CLUSTER commands.
      Enable the commands on both the primary node and the secondary node.

      ```
      >dism /online /enable-feature /FeatureName:FailoverCluster-CmdInterface /All /Source:C:\MOUNT\Windows
      \WinSxS <RETURN>
      ```

11. Bring the manager "service or application" online.

    a. 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.

       Confirm that all resources of the "RC-manager" have been brought online.

    b. Click [Services and Applications]-[RC-HBAar] on the Failover Cluster Management tree.

       Check that the "Status" of the "Summary of RC-HBAar" is online, and the "Current Owner" is the primary node.

12. Configure the startup settings of the HBA address rename setup service of the primary node.

    a. Execute the following command using the command prompt:

       ```
       >"Installation_folder\WWN Recovery\opt\FJSVrcxrs\bin\rcxhbactl.exe" <RETURN>
       ```

       The [HBA address rename setup service] dialog is displayed.

    b. Confirm that the "Status" is "Running".

    c. Click [Cancel] and close the [HBA address rename setup service] dialog.

13. Switch the manager "service or application" to the primary node.

    a. Right-click [Services and Applications]-[RC-manager] on the Failover Cluster Management tree, and select the primary node using [Move this service or application to another node] from the displayed menu.

       The "Current Owner" of the "Summary of RC-manager" switches to the primary node.

    b. Click [Services and Applications]-[RC-HBAar] on the Failover Cluster Management tree.

       Check that the "Status" of the "Summary of RC-HBAar" is online, and the "Current Owner" is the secondary node.

14. Confirm the status of the HBA address rename setup service of the secondary node.

    The procedure is the same as step 12.

Note

- Set the logging level of Failover Cluster to 3 (the default) or higher.

  It is possible to confirm and change the logging level by executing the following command using the command prompt:

  Logging level confirmation

  ```
  >CLUSTER /PROP:ClusterLogLevel <RETURN>
  ```

  Changing the logging level (Specifying level 3)

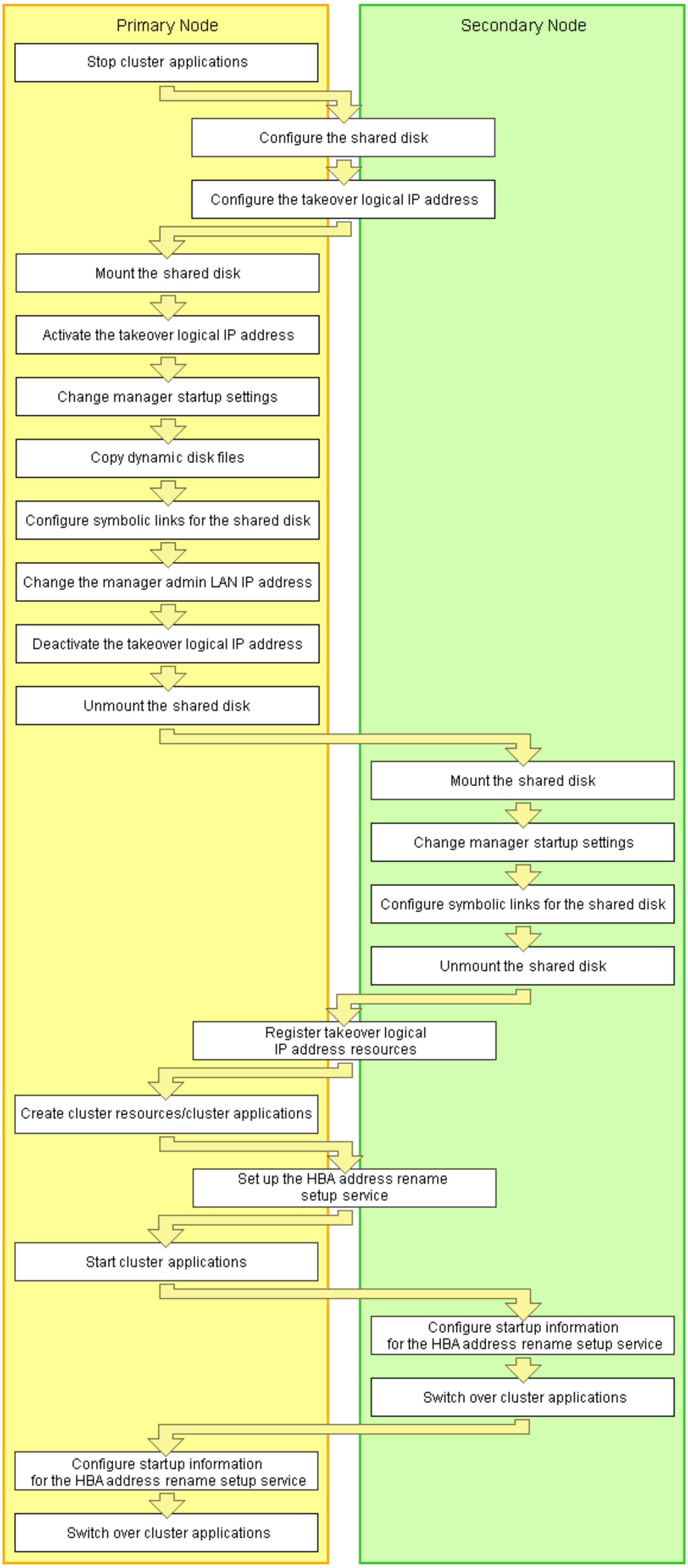
  ```
  >CLUSTER LOG /LEVEL:3 <RETURN>
  ```

- The "service or application" configured in "Set up the HBA address rename Setup Service" for the HBA address rename setup service, is controlled so that it is online on the other node, and online processing is performed in coordination with the manager "service or application".
  For "service or application" for the HBA address rename setup service, do not move the node using operations from the [Failover Cluster Management] window.

C.3.2 Configuration [Linux Manager]

Perform setup on the admin server.
The flow of setup is as shown below.

Figure C.2 Manager Service Setup Flow


Primary Node
Secondary Node
Stop cluster applications
Configure the shared disk
Configure the takeover logical IP address
Mount the shared disk
Activate the takeover logical IP address
Change manager startup settings
Copy dynamic disk files
Configure symbolic links for the shared disk
Change the manager admin LAN IP address
Deactivate the takeover logical IP address
Unmount the shared disk
Mount the shared disk
Change manager startup settings
Configure symbolic links for the shared disk
Unmount the shared disk
Register takeover logical IP address resources
Create cluster resources/cluster applications
Set up the HBA address rename setup service
Start cluster applications
Configure startup information for the HBA address rename setup service
Switch over cluster applications
Configure startup information for the HBA address rename setup service
Switch over cluster applications

Setup of managers as cluster services (cluster applications) is performed using the following procedure.
Perform setup using OS administrator authority.
If the image file storage directory is changed from the default directory (/var/opt/FJSVscw-deploysv/depot) during installation, in a of step 6 perform settings so that the image file storage directory is also located in the shared disk.

Not necessary when ServerView Deployment Manager is used in the same subnet.

1. Stop cluster applications (Primary node)

   When adding to existing operations (cluster applications)
   When adding a manager to an existing operation (cluster application), use the cluster system's operation management view (Cluster Admin) and stop operations (cluster applications).

2. Configure the shared disk and takeover logical IP address (Primary node/Secondary node)

   a. Shared disk settings

      Use GDS and perform settings for the shared disk.
      For details, refer to the GDS manual.

   b. Configure the takeover logical IP address

      Use GLS and perform settings for the takeover logical IP address.
      As it is necessary to activate the takeover logical IP address using the following procedure, do not perform registration of resources with PRIMECLUSTER (by executing the /opt/FJSVhanet/usr/sbin/hanethvrsc create command) at this point.

      When adding to existing operations (cluster applications)
      When using an existing takeover logical IP address, delete the GLS virtual interface information from the resources for PRIMECLUSTER.
      For details, refer to the GLS manual.

3. Mount the shared disk (Primary node)

   Mount the shared disk for managers on the primary node.

4. Activate the takeover logical IP address (Primary node)

   On the primary node, activate the takeover logical IP address for the manager.
   For details, refer to the GLS manual.

5. Change manager startup settings (Primary node)

   Perform settings so that the startup process of the manager is controlled by the cluster system, not the OS.
   Execute the following command on the primary node.

   ```
   # /opt/FJSVrcvmr/cluster/bin/rcxclchkconfig setup <RETURN>
   ```

6. Copy dynamic disk files (Primary node)

   Copy the files from the dynamic disk of the manager on the primary node to the shared disk for managers.

   a. Create the directory "*shared_disk_mount_point*/Fujitsu/ROR/SVROR" on the shared disk.

   b. Copy the directories and files on the local disk of the primary node to the created directory.
      Execute the following command.

      ```
      # tar cf - copy_target | tar xf - -C shared_disk_mount_point/Fujitsu/ROR/SVROR/ <RETURN>
      ```

      Note

      The following messages may be output when the tar command is executed. They have no effect on operations, so ignore them.

      - tar: Removing leading `/' from member names

      - tar: *file_name*: socket ignored

      Directories and Files to Copy

- /opt/FJSVrcvmr/rails/config/rcx/rcxdb.pwd
- /etc/opt/FJSVrcvmr/customize_data
- /etc/opt/FJSVrcvmr/opt/FJSVssmgr/current/certificate
- /etc/opt/FJSVrcvmr/rails/config/rcx_secret.key
- /etc/opt/FJSVrcvmr/sys/apache/conf
- /var/opt/FJSVrcvmr
- /etc/opt/FJSVscw-common (*)
- /var/opt/FJSVscw-common (*)
- /etc/opt/FJSVscw-tftpsv (*)
- /var/opt/FJSVscw-tftpsv (*)
- /etc/opt/FJSVscw-pxesv (*)
- /var/opt/FJSVscw-pxesv (*)
- /etc/opt/FJSVscw-deploysv (*)
- /var/opt/FJSVscw-deploysv (*)
- /etc/opt/FJSVscw-utils (*)
- /var/opt/FJSVscw-utils (*)

* Note: Not necessary when ServerView Deployment Manager is used in the same subnet.

c. Change the names of the copied directories and files listed below.

Execute the following command. Make sure a name such as *source_file_name(source_directory_name)*_old is specified for the *target_file_name(target_directory_name)*.

```
# mv -i source_file_name(source_directory_name) target_file_name(target_directory_name) <RETURN>
```

- /opt/FJSVrcvmr/rails/config/rcx/rcxdb.pwd
- /etc/opt/FJSVrcvmr/customize_data
- /etc/opt/FJSVrcvmr/opt/FJSVssmgr/current/certificate
- /etc/opt/FJSVrcvmr/rails/config/rcx_secret.key
- /etc/opt/FJSVrcvmr/sys/apache/conf
- /var/opt/FJSVrcvmr
- /etc/opt/FJSVscw-common (*)
- /var/opt/FJSVscw-common (*)
- /etc/opt/FJSVscw-tftpsv (*)
- /var/opt/FJSVscw-tftpsv (*)
- /etc/opt/FJSVscw-pxesv (*)
- /var/opt/FJSVscw-pxesv (*)
- /etc/opt/FJSVscw-deploysv (*)
- /var/opt/FJSVscw-deploysv (*)
- /etc/opt/FJSVscw-utils (*)
- /var/opt/FJSVscw-utils (*)

* Note: Not necessary when ServerView Deployment Manager is used in the same subnet.

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

   a. Configure symbolic links for the copied directories and files.

      Configure symbolic links from the directories and files on the local disk of the primary node for the directories and files on the shared disk.
      Execute the following command.

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

      For *shared_disk* specify the shared disk in "Table C.8 Directories to Link" or "Table C.9 Files to Link".
      For *local_disk*, specify the local disk in "Table C.8 Directories to Link" or "Table C.9 Files to Link".

Table C.8 Directories to Link

Shared Disk	Local Disk
Shared_disk_mount_point/Fujitsu/ROR/SVROR/etc/opt/FJSVrcvmr/customize_data	/etc/opt/FJSVrcvmr/customize_data
shared_disk_mount_point/Fujitsu/ROR/SVROR/etc/opt/FJSVrcvmr/opt/FJSVssmgr/current/certificate	/etc/opt/FJSVrcvmr/opt/FJSVssmgr/current/certificate
shared_disk_mount_point/Fujitsu/ROR/SVROR/etc/opt/FJSVrcvmr/sys/apache/conf	/etc/opt/FJSVrcvmr/sys/apache/conf
Shared_disk_mount_point/Fujitsu/ROR/SVROR/var/opt/FJSVrcvmr	/var/opt/FJSVrcvmr
Shared_disk_mount_point/Fujitsu/ROR/SVROR/etc/opt/FJSVscw-common (*)	/etc/opt/FJSVscw-common
Shared_disk_mount_point/Fujitsu/ROR/SVROR/var/opt/FJSVscw-common (*)	/var/opt/FJSVscw-common
Shared_disk_mount_point/Fujitsu/ROR/SVROR/etc/opt/FJSVscw-tftpsv (*)	/etc/opt/FJSVscw-tftpsv
Shared_disk_mount_point/Fujitsu/ROR/SVROR/var/opt/FJSVscw-tftpsv (*)	/var/opt/FJSVscw-tftpsv
Shared_disk_mount_point/Fujitsu/ROR/SVROR/etc/opt/FJSVscw-pxesv (*)	/etc/opt/FJSVscw-pxesv
Shared_disk_mount_point/Fujitsu/ROR/SVROR/var/opt/FJSVscw-pxesv (*)	/var/opt/FJSVscw-pxesv
Shared_disk_mount_point/Fujitsu/ROR/SVROR/etc/opt/FJSVscw-deploysv (*)	/etc/opt/FJSVscw-deploysv
Shared_disk_mount_point/Fujitsu/ROR/SVROR/var/opt/FJSVscw-deploysv (*)	/var/opt/FJSVscw-deploysv
Shared_disk_mount_point/Fujitsu/ROR/SVROR/etc/opt/FJSVscw-utils (*)	/etc/opt/FJSVscw-utils
Shared_disk_mount_point/Fujitsu/ROR/SVROR/var/opt/FJSVscw-utils (*)	/var/opt/FJSVscw-utils

* Note: Not necessary when ServerView Deployment Manager is used in the same subnet.

Table C.9 Files to Link

Shared Disk	Local Disk
Shared_disk_mount_point/Fujitsu/ROR/SVROR/opt/FJSVrcvmr/rails/config/rcx/rcxdb.pwd	/opt/FJSVrcvmr/rails/config/rcx/rcxdb.pwd
Shared_disk_mount_point/Fujitsu/ROR/SVROR/etc/opt/FJSVrcvmr/rails/config/rcx_secret.key	/etc/opt/FJSVrcvmr/rails/config/rcx_secret.key

b. When changing the image file storage directory, perform the following.

When changing the image file storage directory, refer to "5.8 rcxadm imagemgr" in the "Reference Guide (Command) VE", and change the path for the image file storage directory.

Also, specify a directory on the shared disk for the new image file storage directory.

Not necessary when ServerView Deployment Manager is used in the same subnet.

8. Change the Manager Admin LAN IP Address (Primary node)

Change the admin LAN IP address of the manager.
Execute the following command.

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

For *IP_address*, specify the admin LAN IP address activated in step 4.

9. Deactivate the takeover logical IP address (Primary node)

On the primary node, deactivate the takeover logical IP address for the manager.
For details, refer to the GLS manual.

10. Unmount the shared disk (Primary node)

Unmount the shared disk for managers from the primary node.

11. Mount the shared disk (Secondary node)

Mount the shared disk for managers on the secondary node.

12. Change manager startup settings (Secondary node)

Perform settings so that the startup process of the manager is controlled by the cluster system, not the OS.
On the secondary node, execute the same command as used in step 5.

13. Configure symbolic links for the shared disk (Secondary node)

a. Change the directory names and file names given in c of step 6.

b. Configure symbolic links for the shared disk.

Configure symbolic links from the directories and files on the local disk of the secondary node for the directories and files on the shared disk.
The directories and files to set symbolic links for are the same as those for "Table C.8 Directories to Link" and "Table C.9 Files to Link".

14. Unmount the shared disk (Secondary node)

Unmount the shared disk for managers from the secondary node.

15. Register takeover logical IP address resources (Primary node/Secondary node)

On GLS, register the takeover logical IP address as a PRIMECLUSTER resource.

Note

When using an existing takeover logical IP address, as it was deleted in step 2, registration as a resource is necessary.

For details, refer to the GLS manual.

16. Create cluster resources/cluster applications (Primary node)

a. Use the RMS Wizard of the cluster system to create the necessary PRIMECLUSTER resources on the cluster service (cluster application).

When creating a new cluster service (cluster application), select Application-Create and create the settings for primary node as Machines[0] and the secondary node as Machines[1]. Then create the following resources on the created cluster service (cluster application).

Perform the RMS Wizard settings for any of the nodes comprising the cluster.
For details, refer to the PRIMECLUSTER manual.

- Cmdline resources

  Create the Cmdline resources for Resource Orchestrator.
  On RMS Wizard, select "CommandLines" and perform the following settings.

  - Start script: /opt/FJSVrcvmr/cluster/cmd/rcxclstartcmd

  - Stop script: /opt/FJSVrcvmr/cluster/cmd/rcxclstopcmd

  - Check script: /opt/FJSVrcvmr/cluster/cmd/rcxclcheckcmd

  Note

  When specifying a value other than nothing for the attribute value StandbyTransitions of a cluster service (cluster application), enable the Flag of ALLEXITCODES(E) and STANDBYCAPABLE(O).

  When adding to existing operations (cluster applications)
  When adding Cmdline resources to existing operations (cluster applications), decide the startup priority order considering the restrictions of the other components that will be used in combination with the operation (cluster application).

- Gls resources

  Configure the takeover logical IP address to use for the cluster system.
  On the RMS Wizard, select "Gls:Global-Link-Services", and set the takeover logical IP address.
  When using an existing takeover logical IP address this operation is not necessary.

- Fsystem resources

  Set the mount point of the shared disk.
  On the RMS Wizard, select "LocalFileSystems", and set the file system. When no mount point has been defined, refer to the PRIMECLUSTER manual and perform definition.

- Gds resources

  Specify the settings created for the shared disk.
  On the RMS Wizard, select "Gds:Global-Disk-Services", and set the shared disk. Specify the settings created for the shared disk.

b. Set the attributes of the cluster application.

   When you have created a new cluster service (cluster application), use the cluster system's RMS Wizard to set the attributes.

   - In the Machines+Basics settings, set "yes" for AutoStartUp.

   - In the Machines+Basics settings, set "HostFailure|ResourceFailure|ShutDown" for AutoSwitchOver.

   - In the Machines+Basics settings, set "yes" for HaltFlag.

   - When using hot standby for operations, in the Machines+Basics settings, set "ClearFaultRequest|StartUp|SwitchRequest" for StandbyTransitions.
     When configuring the HBA address rename setup service in cluster systems, ensure that hot standby operation is configured.

c. After settings are complete, save the changes and perform Configuration-Generate and Configuration-Activate.

Note

When registering the admin LAN subnet, additional settings are required.
For the setting method, refer to the [Linux Manager] section of "Settings for Clustered Manager Configurations" in "7.9 Registering Admin LAN Subnets" in the "User's Guide VE".

17. Set up the HBA address rename setup service (Primary node/Secondary node)

    Configuring the HBA address rename setup service for cluster systems
    When configuring managers and the HBA address rename setup service in cluster systems, perform the following procedure.

    Not necessary when ServerView Deployment Manager is used in the same subnet.

    Performing the following procedure starts the HBA address rename setup service on the standby node in the cluster.

    a. HBA address rename setup service startup settings (Primary node)

       Configure the startup settings of the HBA address rename setup service.
       Execute the following command.

       ```
       # /opt/FJSVrcvhb/cluster/bin/rcvhbclsetup <RETURN>
       ```

    b. Configuring the HBA address rename setup service (Primary node)

       Configure the settings of the HBA address rename setup service.
       Execute the following command on the primary node.

       ```
       # /opt/FJSVrcvhb/bin/rcxhbactl modify -ip IP_address <RETURN>
       # /opt/FJSVrcvhb/bin/rcxhbactl modify -port port_number <RETURN>
       ```

       IP Address

       Specify the takeover logical IP address for the manager.

       Port number

       Specify the port number for communication with the manager. The port number at installation is 23461.

    c. HBA address rename setup service Startup Settings (Secondary node)

       Configure the startup settings of the HBA address rename setup service.
       On the secondary node, execute the same command as used in step a.

    d. Configuring the HBA address rename setup service (Secondary node)

       Configure the settings of the HBA address rename setup service.
       On the secondary node, execute the same command as used in step b.

18. Start cluster applications (Primary node)

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

19. Set up the HBA address rename setup service startup information (Secondary node)

    a. Execute the following command.

       ```
       # nohup /opt/FJSVrcvhb/bin/rcxhbactl start& <RETURN>
       ```

       The [HBA address rename setup service] dialog is displayed.

    b. Click [Stop].

       Confirm that the "Status" becomes "Stopping".

    c. Click [Run].

       Confirm that the "Status" becomes "Running".

    d. Click [Stop].

       Confirm that the "Status" becomes "Stopping".

    e. Click [Cancel] and close the [HBA address rename setup service] dialog.

20. Switch over cluster applications (Secondary node)

    Use the cluster system's operation management view (Cluster Admin) and switch the manager cluster service (cluster application) to the secondary node.

21. Set up the HBA address rename setup service startup information (Primary node)

    The procedure is the same as step 19.

22. Switch over cluster applications (Primary node)

    Use the cluster system's operation management view (Cluster Admin) and switch the manager cluster service (cluster application) to the primary node.

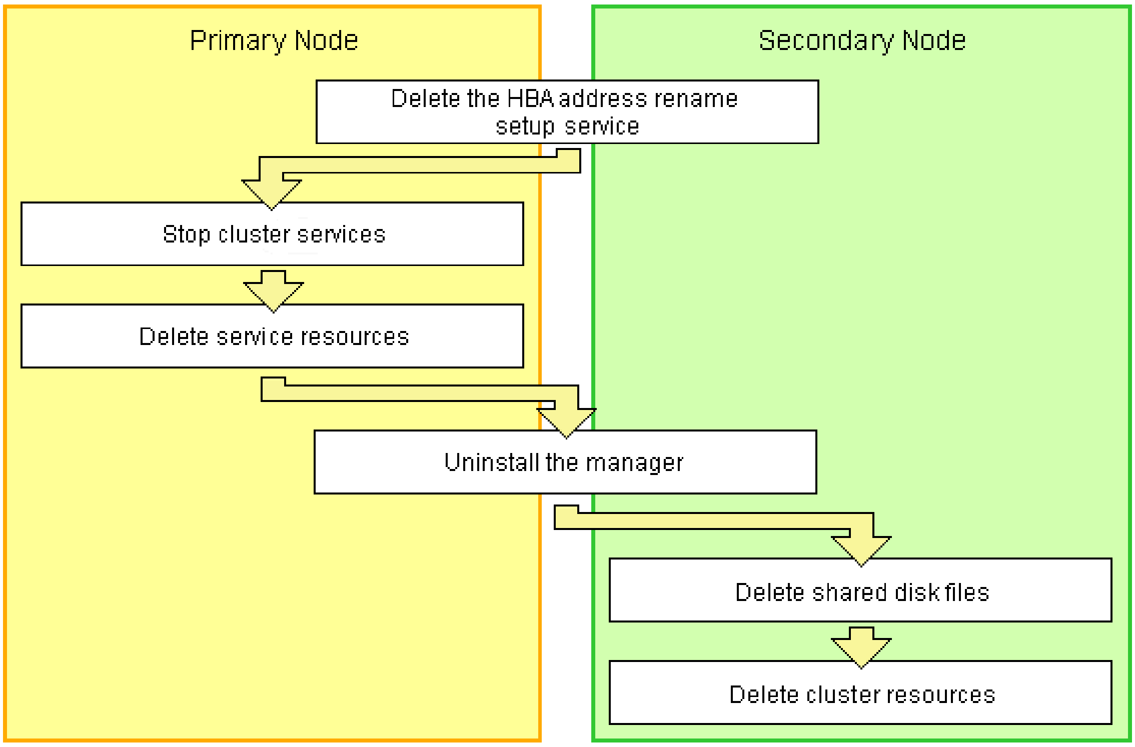
C.4 Releasing Configuration

This section explains how to delete the cluster services of managers being operated on cluster systems.

C.4.1 Releasing Configuration [Windows Manager]

The flow of deleting cluster services of managers is as indicated below.

Figure C.3 Flow of Deleting Manager Service Settings



Delete settings for manager cluster services using the following procedure.
This explanation assumes that the manager is operating on the primary node.

Delete the HBA address rename Setup Service

When the HBA address rename setup service and managers in cluster systems have been configured, perform the following procedure.

Not necessary when ServerView Deployment Manager is used in the same subnet.

1. Take the "service or application" for the HBA address rename setup service offline.

    a. Open the [Failover Cluster Management] window and connect to the cluster system.

    b. Right-click [Services and Applications]-[RC-HBAar] on the Failover Cluster Management tree, and select [Take this service or application offline] from the displayed menu.

2. Take the manager "service or application" offline.

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

3. Delete the scripts of the "service or application" for the HBA address rename service.

   a. Click [Services and Applications]-[RC-HBAar] on the Failover Cluster Management tree.

   b. Right-click the "HBAarCls Script" of the "Other Resources" on the "Summary of RC-HBAar" displayed in the middle of the [Failover Cluster Management] window, and select [Delete] from the displayed menu.

4. Delete the "service or application" for the HBA address rename setup service.

   Right-click [Services and Applications]-[RC-HBAar] on the Failover Cluster Management tree, and select [Delete] from the displayed menu.

5. Configure the dependencies of the resources in the "service or application" for the manager back to the status they were in before setting up the HBA address rename setup service.

   a. Right-click the "PXE Services" 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 [PXE Services Properties] window will be displayed.

   b. In the "Resource" of the [Dependencies] tab, select the name of the Admin LAN IP Address and click [Apply].

   c. Once settings are applied, click [OK].

6. Delete the generic scripts for the coordinated boot of the "service or application" for the HBA address rename service from the "service or application" for the manager.

   a. Click [Services and Applications]-[RC-manager] on the Failover Cluster Management tree.

   b. Right-click the "HBAarCls Script" of the "Other Resources" on the "Summary of RC-manager" displayed in the middle of the [Failover Cluster Management] window, and select [Delete] from the displayed menu.

Stop the cluster service

When configuring the "Delete the HBA address rename Setup Service", perform the procedure from step 3.

1. Open the [Failover Cluster Management] window and connect to the cluster system.

2. Take the manager "service or application" offline.

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

3. Bring the shared disk for the manager "service or application" online.

   Right-click the shared disk on "Disk Drives" on the "Summary of RC-manager" displayed in the middle of the [Failover Cluster Management] window, and select [Bring this resource online] from the displayed menu.

Delete service resources

Delete the services, scripts, and IP address of the manager "service or application".
Using the following procedure, delete all the "Other Resources".

1. Click [Services and Applications]-[RC-manager] on the Failover Cluster Management tree.

2. Right-click the resources on "Other Resources" on the "Summary of RC-manager" displayed in the middle of the [Failover Cluster Management] window, and select [Delete] from the displayed menu.

3. Using the following procedure, delete the resources displayed in the "Server Name" of the "Summary of RC-manager" in the middle of the [Failover Cluster Management] window.

   a. Right-click "IP Address: *IP_address*", and select [Delete] from the displayed menu.

b. Right-click "Name: *Network_name*", and select [Delete] from the displayed menu.

When registering the admin LAN subnet, delete the "DHCP Service" using the following procedure.

4. Set the path of the "DHCP Service".

   a. Right-click the resources of the "DHCP Service" on the "Summary of RC-manager" displayed in the middle of the [Failover Cluster Management] window, and select [Properties] from the displayed menu.

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

   b. Configure the path on the [General] tab based on the following table.

Item	Value to Specify
Database path	%SystemRoot%\System32\dhcp\
Audit file path	%SystemRoot%\System32\dhcp\
Backup path	%SystemRoot%\System32\dhcp\backup\

5. Right-click the resources of the "DHCP Service" on the "Summary of RC-manager" displayed in the middle of the [Failover Cluster Management] window, and select [Delete] from the displayed menu.

Manager Uninstallation

1. Refer to "11.1.2 Uninstallation [Windows Manager]", and uninstall the manager on the primary node.
2. Allocate the shared disk 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*.

3. Uninstall the manager of the secondary node.

Delete shared disk files

Use Explorer to delete the "*Drive_name*:\Fujitsu\ROR\SVROR\" folder on the shared disk.

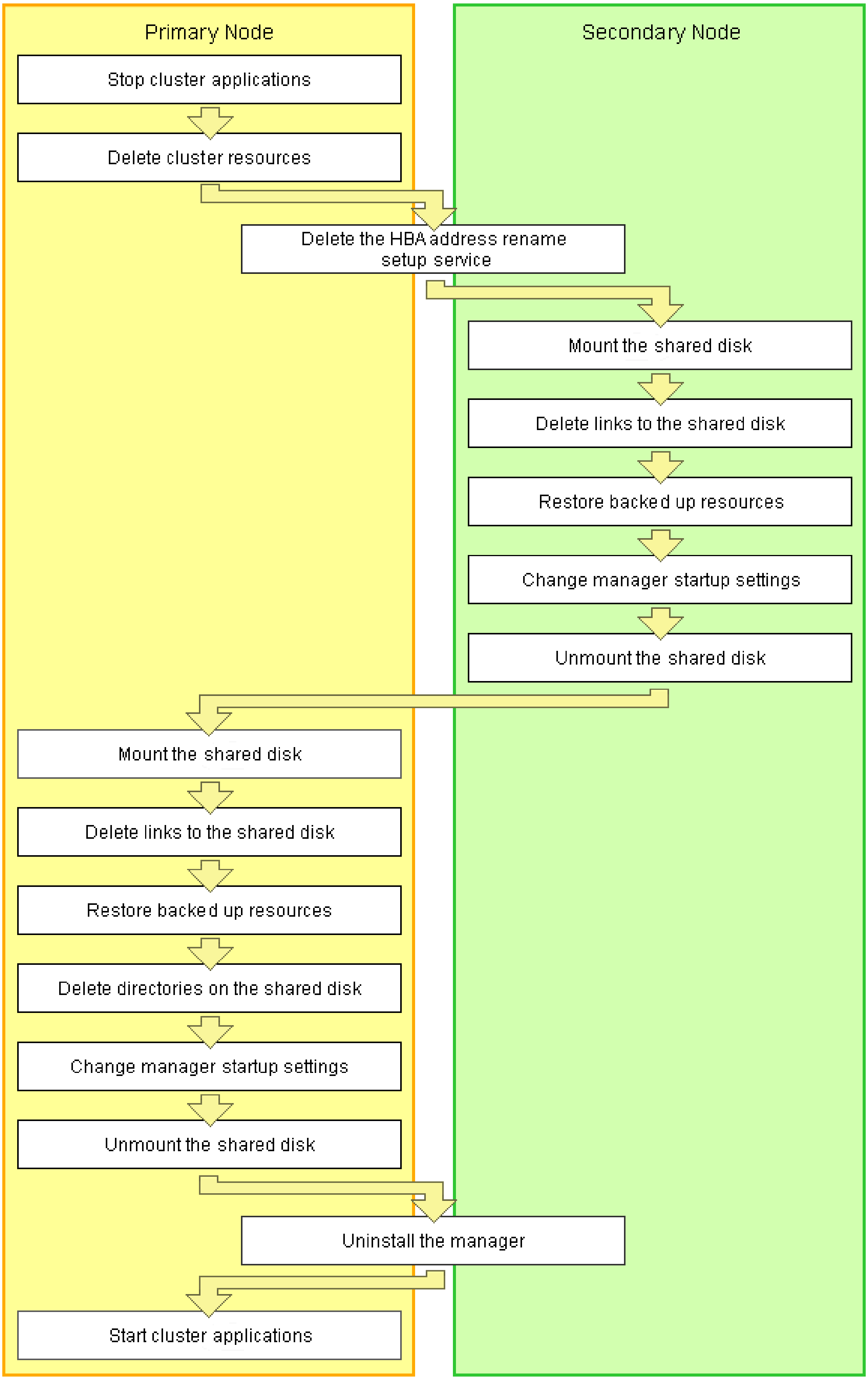
Delete cluster resources

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

C.4.2 Releasing Configuration [Linux Manager]

The flow of deleting cluster services (cluster applications) of managers is as indicated below.

Figure C.4 Flow of Deleting Manager Service Settings


Primary Node
Secondary Node
Stop cluster applications
Delete cluster resources
Delete the HBA address rename setup service
Mount the shared disk
Delete links to the shared disk
Restore backed up resources
Change manager startup settings
Unmount the shared disk
Mount the shared disk
Delete links to the shared disk
Restore backed up resources
Delete directories on the shared disk
Change manager startup settings
Unmount the shared disk
Uninstall the manager
Start cluster applications

Releasing of manager cluster services (cluster applications) is performed using the following procedure.
Perform releasing of configuration using OS administrator authority.

1. Stop cluster applications (Primary node)

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

2. Delete cluster resources (Primary node)

   Use the RMS Wizard of the cluster system, and delete manager operation resources registered on the target cluster service (cluster application).

   When a cluster service (cluster application) is in a configuration that only uses resources of Resource Orchestrator, also delete the cluster service (cluster application).

   On the RMS Wizard, if only deleting resources, delete the following:

   - Cmdline resources (Only script definitions for Resource Orchestrator)

   - Gls resources (When they are no longer used)

   - Gds resources (When they are no longer used)

   - Fsystem resources (The mount point for the shared disk for managers)

   Release the RMS Wizard settings for any of the nodes comprising the cluster.
   For details, refer to the PRIMECLUSTER manual.

3. Delete the HBA address rename setup service (Primary node/Secondary node)

   When the HBA address rename setup service has been configured for a cluster system
   When the HBA address rename setup service and managers in cluster systems have been configured, perform the following procedure.

   Not necessary when ServerView Deployment Manager is used in the same subnet.

   a. Stopping the HBA address rename setup service (Secondary node)

      Stop the HBA address rename setup service.
      Execute the following command, and check if the process of the HBA address rename setup service is indicated.

      ```
      # ps -ef | grep rcvhb | grep -v grep <RETURN>
      ```

      When processes are output after the command above is executed, execute the following command and stop the HBA address rename setup service. If no processes were output, this procedure is unnecessary.

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

   b. Releasing HBA address rename setup service Startup Settings (Secondary node)

      Release the startup settings of the HBA address rename setup service.
      Execute the following command.

      ```
      # /opt/FJSVrcvhb/cluster/bin/rcvhbclunsetup <RETURN>
      ```

   c. Deleting links (Secondary node)

      If processes of the HBA address rename setup service were not indicated in a., this procedure is unnecessary.
      Execute the following command and delete symbolic links.

      ```
      # rm symbolic_link <RETURN>
      ```

      - Symbolic Links to Delete

        - /var/opt/FJSVscw-common

        - /var/opt/FJSVscw-tftpsv

- /etc/opt/FJSVscw-common
- /etc/opt/FJSVscw-tftpsv

d. Reconfiguring symbolic links

If processes of the HBA address rename setup service were not indicated in a., this procedure is unnecessary.
Execute the following command, and reconfigure the symbolic links from the directory on the local disk for the directory on the shared disk.

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

For *shared_disk*, specify the shared disk in "Table C.10 Directories to Relink".
For *local_disk*, specify the local disk in "Table C.10 Directories to Relink".

Table C.10 Directories to Relink

Shared Disk	Local Disk
Shared_disk_mount_point/Fujitsu/ROR/SVROR/var/opt/FJSVscw-common	/var/opt/FJSVscw-common
Shared_disk_mount_point/Fujitsu/ROR/SVROR/var/opt/FJSVscw-tftpsv	/var/opt/FJSVscw-tftpsv
Shared_disk_mount_point/Fujitsu/ROR/SVROR/etc/opt/FJSVscw-common	/etc/opt/FJSVscw-common
Shared_disk_mount_point/Fujitsu/ROR/SVROR/etc/opt/FJSVscw-tftpsv	/etc/opt/FJSVscw-tftpsv

e. Stopping the HBA address rename setup service (Primary node)

Stop the HBA address rename setup service.
On the primary node, execute the same command as used in step a.

f. Releasing the HBA address rename setup service Startup Settings (Primary node)

Release the startup settings of the HBA address rename setup service.
On the primary node, execute the same command as used in step b.

g. Deleting links (Primary node)

If processes of the HBA address rename setup service were not indicated in step e, this procedure is unnecessary.
On the primary node, execute the same command as used in step c.

h. Reconfiguring symbolic links

If processes of the HBA address rename setup service were not indicated in step e, this procedure is unnecessary.
On the primary node, execute the same command as used in step d.

4. Mount the shared disk (Secondary node)

When it can be confirmed that the shared disk for managers has been unmounted from the primary node and the secondary node, mount the shared disk for managers on the secondary node.

5. Delete links to the shared disk (Secondary node)

Delete the symbolic links specified for the directories and files on the shared disk from the directories and files on the local disk of the secondary node.

Execute the following command.

```
# rm symbolic_link <RETURN>
```

Symbolic links to directories to delete

- /etc/opt/FJSVrcvmr/customize_data
- /etc/opt/FJSVrcvmr/opt/FJSVssmgr/current/certificate
- /etc/opt/FJSVrcvmr/sys/apache/conf
- /var/opt/FJSVrcvmr
- /etc/opt/FJSVscw-common (*)

- /var/opt/FJSVscw-common (*)
- /etc/opt/FJSVscw-tftpsv (*)
- /var/opt/FJSVscw-tftpsv (*)
- /etc/opt/FJSVscw-pxesv (*)
- /var/opt/FJSVscw-pxesv (*)
- /etc/opt/FJSVscw-deploysv (*)
- /var/opt/FJSVscw-deploysv (*)
- /etc/opt/FJSVscw-utils (*)
- /var/opt/FJSVscw-utils (*)

* Note: Not necessary when ServerView Deployment Manager is used in the same subnet.

Symbolic links to files to delete

- /opt/FJSVrcvmr/rails/config/rcx/rcxdb.pwd
- /etc/opt/FJSVrcvmr/rails/config/rcx_secret.key

When registering the admin LAN subnet, also delete symbolic links to the following files and directories:

- /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

6. Restore backed up resources (Secondary node)

Restore the directories and files that were backed up when configuring the cluster environment.
Execute the following command. Specify the files and directories that were backed up when configuring the cluster environment using names such as *source_file_name(source_directory_name)_*old for the *source_restoration_file_name(source_restoration_directory_name*). For *restoration_target_file_name(restoration_target_directory_name)*, specify file names or directory names corresponding to the *source_restoration_file_name(source_restoration_directory_name).*

```
# mv -i source_restoration_file_name(source_restoration_directory_name)
restoration_target_file_name(restoration_target_directory_name) <RETURN>
```

Restore the following directory names and file names.

- /opt/FJSVrcvmr/rails/config/rcx/rcxdb.pwd
- /etc/opt/FJSVrcvmr/opt/FJSVssmgr/current/certificate
- /etc/opt/FJSVrcvmr/rails/config/rcx_secret.key
- /etc/opt/FJSVrcvmr/sys/apache/conf
- /var/opt/FJSVrcvmr
- /etc/opt/FJSVscw-common (*1)
- /var/opt/FJSVscw-common (*1)
- /etc/opt/FJSVscw-tftpsv (*1)
- /var/opt/FJSVscw-tftpsv (*1)
- /etc/opt/FJSVscw-pxesv (*1)
- /var/opt/FJSVscw-pxesv (*1)

  - /etc/opt/FJSVscw-deploysv (*1)
  - /var/opt/FJSVscw-deploysv (*1)
  - /etc/opt/FJSVscw-utils (*1)
  - /var/opt/FJSVscw-utils (*1)

   When registering the admin LAN subnet, also restore the following file and directory names:

  - /etc/dhcpd.conf (*2)
  - /etc/dhcp/dhcpd.conf (*3)
  - /var/lib/dhcpd

   *1: Not necessary when ServerView Deployment Manager is used in the same subnet.
   *2: When using Red Hat Enterprise Linux 5
   *3: When using Red Hat Enterprise Linux 6

7. Change manager startup settings (Secondary node)

   Perform settings so that the startup process of the manager is controlled by the OS, not the cluster system.
   Execute the following command on the secondary node.

   ```
   # /opt/FJSVrcvmr/cluster/bin/rcxclchkconfig unsetup <RETURN>
   ```

8. Unmount the shared disk (Secondary node)

   Unmount the shared disk for managers from the secondary node.

9. Mount the shared disk (Primary node)

   Mount the shared disk for managers on the primary node.

10. Delete links to the shared disk (Primary node)

    Delete the symbolic links specified for the directories and files on the shared disk from the directories and files on the local disk of the primary node.

    The directories and files to delete are the same as those for "Symbolic links to directories to delete" and "Symbolic links to files to delete" in step 5.

11. Restore backed up resources (Primary node)

    Restore the directories and files that were backed up when configuring the cluster environment.
    Refer to step 6. for the procedure.

12. Delete directories on the shared disk (Primary node)

    Delete the created directory "*Shared_disk_mount_point*/Fujitsu/ROR/SVROR" on the shared disk.
    Execute the following command.

    ```
    # rm -r shared_disk_mount_point/Fujitsu/ROR/SVROR <RETURN>
    ```

    When there is no need to check with the rm command, add the -f option. For the rm command, refer to the manual for the OS.

13. Change manager startup settings (Primary node)

    Perform settings so that the startup process of the manager is controlled by the OS, not the cluster system.
    Refer to step 7. for the command to execute on the primary node.

14. Unmount the shared disk (Primary node)

    Unmount the shared disk for managers from the primary node.

15. Uninstall the manager (Primary node/Secondary node)

    Refer to "11.1.3 Uninstallation [Linux Manager]", and uninstall the managers on the primary node and the secondary node.
    When releasing the cluster configuration and returning to a single configuration, uninstall the manager from one of the nodes.

When operating managers in cluster environments, if the admin server settings are modified, change the admin server settings before using it in a single configuration.

For the method for changing the admin server settings, refer to "Chapter 8 Changing Admin Server Settings" in the "User's Guide VE".

16. Start cluster applications (Primary node)

    When there are other cluster services (cluster applications), use the cluster system's operation management view (Cluster Admin) and start the cluster services (cluster applications).

C.5 Advisory Notes

This section explains advisory notes regarding the settings for managers in cluster operations, and their deletion.

Switching Cluster Services (Cluster Applications)

Events that occur when switching cluster services (cluster applications) cannot be displayed.
Also, the message number 65529 may be displayed on the ROR console.
Perform login again.

For details on the messages, refer to "Message number 65529" in "Messages".

Troubleshooting Information

Collect troubleshooting information referring to the instructions in "1.2 Collecting Troubleshooting Data (Virtual Edition)" in "Troubleshooting". At that time, execute the commands from the primary node of the admin server, and collect information from the primary node and managed servers.

Commands

Do not use the start or stop subcommand of rcxadm mgrctl to start or stop the manager.
Right-click the manager "service or application" on the Failover Cluster Management tree, and select [Bring this service or application online] or [Take this service or application offline] from the displayed menu.
Other commands can be executed as they are in normal cluster operation.

ROR Console

The registration state of server resources on the resource tree when an admin server is included in a chassis is as indicated below.

- The server resources being operated by the manager on the cluster node are displayed as "[Admin Server]".
- The server resources not being operated by the manager on the cluster node are displayed as "[Unregistered]".

Do not register the server resources of the cluster node that are displayed as "[Unregistered]".

Services (Daemons) Managed with PRIMECLUSTER [Linux Manager]

The following services (daemons) are managed with the Check script provided by Resource Orchestrator.

- /etc/init.d/scwdepsvd
- /etc/init.d/scwpxesvd
- /etc/init.d/scwtftpd
- /opt/FJSVrcvmr/opt/FJSVssmgr/bin/cimserver
- /opt/FJSVrcvmr/sys/rcxtaskmgr
- /opt/FJSVrcvmr/sys/rcxmongrel1

- /opt/FJSVrcvmr/sys/rcxmongrel2
- /opt/FJSVrcvmr/sys/rcxhttpd
- /etc/init.d/dhcpd (*)

* Note: When registering the admin LAN subnet

Appendix D Upgrading from Earlier Versions

This appendix explains the upgrade procedures.

D.1 Overview

This section explains an overview of upgrades.

D.1.1 Upgrading from Earlier Versions

Upgrading from earlier versions indicates how to upgrade the following environments to this version of ROR VE.

- Environments configured using RCVE
- Environments configured using an earlier version of ROR VE

Upgrade Procedure

Perform upgrade using the following procedure:

1. Upgrade the Manager.
2. Upgrade the Agent.
3. Upgrade the HBA address rename Setup Service.
4. Perform the operations for the Client side.
   This operation can be performed after upgrading the manager.

Information

Combinations with agents of earlier versions

- The manager of this version can be used in combination with agents without upgrading, as the combinations with agents of earlier versions (*1) are supported.
  In this case, the scope of available functions is limited to the one provided by the earlier version of agents.

  *1: RCVE V2.1.0 - ROR V3.3.0

- When using Server Switchover with a manager of this version and agents of Solaris version, agent version must be upgraded V3.1.2(T009947SP-01 or later) or V3.2.0 or later.

Upgradability

Upgradability of the environments to this version of ROR VE is as indicated below.

Product Name	Version	Edition	Upgradability						
			Manager		Agent			HBA address rename Setup Service	
			Windows	Linux	Windows	Linux	Solaris	Windows	Linux
RCVE	V2.1.x		No	No	Yes	Yes	Yes	Yes	Yes
	V2.2.0		No	No	Yes	Yes	Yes	Yes	Yes
	V2.2.2		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ROR	V2.x.x		No	No	Yes	Yes	Yes	Yes	Yes
	V3.0.0	VE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
		CE	No	No					

Product Name	Version	Edition	Upgradability						
			Manager		Agent			HBA address rename Setup Service	
			Windows	Linux	Windows	Linux	Solaris	Windows	Linux
	V3.1.x	VE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
		CE	No	No					
	V3.2.0	VE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
		CE	No	No					
	V3.3.0	VE	Yes	-	Yes	-	-	Yes	-
		CE	No						

Yes: Upgrade is possible

No: Upgrade is not possible

-: Upgrade is not necessary (an unavailable upgrade pattern)

Note

After upgrading the manager from RCVE V2.2.2 to ROR VE, it is not possible to upgrade from ROR VE to ROR CE.

D.2 Manager

This section explains the upgrading of managers.

When operating managers in clusters, transfer using upgrade installation cannot be performed. Perform "Transfer of the Manager Using Re-installation or the Pre-configuration Function".

Point

- In the following procedure, please understand that sections referring to the manuals of an earlier version of ServerView Resource Coordinator VE are actually referring to the manuals of an earlier version of ServerView Resource Orchestrator.
- When maintaining compatibility with earlier versions, refer to "2.1.1 Maintaining Compatibility with Earlier Versions" in the "Release Notes", and change each setting.

[Windows Manager]

- When upgrading an environment configured using ServerView Resource Coordinator VE to this version of FUJITSU Software ServerView Resource Orchestrator Virtual Edition, replace the "*Installation_folder*\SVROR\Manager" used in Resource Orchestrator manuals with "*Installation_folder*\Manager".

Transferred Data

The following manager data is transferred:

- Resource Orchestrator setting information (Setting information for the environment of the earlier version)
- Certificates
- System images and cloning images (Files in the image file storage folder)

Also, with transfer using upgrade installation the following data is also transferred:

- Port number settings
- Power consumption data

- Batch files and script files for event-related functions

Data which is transferred during upgrade installation, except for system images and cloning images, is created and stored in the following folder.
For system images and cloning images, the installation folder of the earlier version is used.
Ensure that the folder is not deleted until after the upgrade is complete.
After the upgrade is complete, the following folder may remain. In that case, check that Resource Orchestrator is operating correctly and then manually delete the folder.

[Windows Manager]
32-bit (x86) OS
Drive_name\Program Files\RCVE-upgradedata
64-bit (x64) OS
Drive_name\Program Files (x86)\RCVE-upgradedata

[Linux Manager]
/var/opt/RCVE-upgradedata
/var/opt/backupscwdir
/var/opt/FJSVctmg-upgradedata
/var/tmp/FJSVctmg-upgrade

Preparations

Perform the following preparations and checks before upgrading:

- Check that the environment is one in which managers of this version can be operated.
  For the operational environment, refer to "6.1 Software Environment" and "6.2 Hardware Environment" in the "Overview".
  Take particular care regarding the memory capacity.
- To enable recovery in case there is unexpected trouble during the upgrade process, please back up the system.
- When using GLS to perform redundancy of NICs for the admin LAN of managed servers, activate the admin LAN on the primary interface.
- To confirm that the upgrade is complete, if there are registered VM hosts on which there are VM guests, check from the ROR console that all of the VM guests are displayed and record their information before upgrading.
- When server switchover settings have been performed, it is not possible to upgrade when spare servers have been switched to. Restore any such servers before starting the upgrade. For how to restore, refer to the information about Server Switchover in the "ServerView Resource Coordinator VE Operation Guide".
- It is necessary to prepare as many agent licenses as were covered in the SupportDesk contract held for the earlier version.

  After upgrading, it is possible to manage the same number of managed servers as the number of agent licenses prepared.
- When the settings for restarting of managers have been changed, check and record the settings, referring to "Restarting Managers" in "Appendix A Notes on Operating ServerView Resource Orchestrator" in the "Operation Guide VE".

[Windows Manager]

- Confirm that the disk space necessary for upgrade installation has been secured.

  Use the following procedure to confirm the necessary disk space:

  1. Log in to the system as the administrator.
  2. The installer is automatically displayed when the first DVD-ROM is set in the DVD drive.
     If the installer does not start, execute "RcSetup.exe" from the DVD-ROM drive.
  3. Select [Express/Virtual Edition], and then click [Displays the hard disk space for upgrade installation] on the displayed window.
     The necessary disk space is displayed.

Upgrade using Upgrade Installation

When upgrading to this version, upgrade can be performed using upgrade installation. Perform the upgrade using the following procedure:

Note

- Do not change the hardware settings or configurations of managers, agents, or any other devices until upgrading is completed.
- When performing an upgrade installation, please do not access the installation folder of the earlier version or any of the files and folders inside it using the command prompt, Explorer, or an editor.
  While it is being accessed, attempts to perform upgrade installation will fail.
  If upgrade installation fails, stop accessing the files or folders and then perform the upgrade installation again.
- To revert to the status before an upgrade was performed, restore the system that was backed up in the preparation stage.
- Upgrade installation will delete patches that were applied to the earlier version.

  [Linux Manager]
  When the PATH variable has not been configured to enable execution of UpdateAdvisor (Middleware) commands from a user-defined location, performing upgrade installation will delete any patches that have been applied to the old version, but it will not delete product information or component information. Refer to the UpdateAdvisor (Middleware) manual and delete software and component information from the applied modification checklist.
- When operating managers in clusters, transfer using upgrade installation cannot be performed. Perform transfer using re-installation or the pre-configuration function.
- When the path of the installation folder before the upgrade is 46 characters or longer, transfer using upgrade installation is not possible. Perform transfer using re-installation or the pre-configuration function.
- When the settings for restarting of managers have been changed, reconfigure the settings after the completion of the upgrade installation, based on the information which was recorded during preparation. For details, refer to "Restarting Managers" in "Appendix A Notes on Operating ServerView Resource Orchestrator" in the "Operation Guide VE".
- If the manager and ServerView Deployment Manager are on the same server, it is not possible to upgrade.

1. Upgrade Installation

   [Windows Manager]

   Refer to steps 1 to 5 in the installation section in "2.1.1.6 Installation", and execute the Resource Orchestrator installer.

   The Resource Orchestrator setup window will be displayed.
   Check the contents of the license agreement, etc. and then click [Next] or enter "y".
   The settings to be inherited from the earlier version will be displayed. After checking them, click [Confirm] or enter "y".
   Upgrade installation will begin.

   [Linux Manager]

   Refer to steps 1 to 7 in the installation section in "2.1.2.6 Installation", and execute the Resource Orchestrator installer.

   Check the contents of the license agreement, etc. and then enter "y".
   The setting information that will be taken over from the earlier version will be displayed. Please check it and then enter "y".
   Upgrade installation will begin.

2. Restarting after Upgrade Installation is Finished

   After upgrade installation is finished, restart the system in order to complete the upgrade.

3. Registration of license

   When performing upgrade installation from the following products to Virtual Edition, it is necessary to register the license.

   - RCVE

   Access the ROR console, and register the license of Virtual Edition.

   For the registration of the license, refer to the setting of the license of "Chapter 4 License Setup and Confirmation".

Note

- When using backup system images or collecting cloning images without upgrading agents, either reboot managed servers after the manager upgrade is completed, or restart the related services.

  For restarting managed servers and the related services, refer to "5.2 Agent" in the "ServerView Resource Coordinator VE Setup Guide".

- After the upgrade is complete, check that Resource Orchestrator is operating correctly, and then manually delete the folder that was used to back up the transferred data.
  For the folder created to back up the transferred data, refer to "Transferred Data".

Transfer of the Manager Using Re-installation or the Pre-configuration Function

In the following cases, import system configuration files (import) and export system configuration files (export) using pre-configuration.

- Transfer from RCVE manager to this version of ROR VE
- Transfer of a cluster operated using RCVE manager to this version of ROR VE manager
- Transfer of a cluster operated using ROR VE manager to this version of ROR VE manager
- When the path of the installation folder before transfer is 46 characters or longer

Use the following procedure to perform "Transfer of the Manager Using Re-installation or the Pre-configuration Function".

See

For pre-configuration, refer to the following manuals:

[RCVE]

- "Chapter 7 Pre-configuration" in the "ServerView Resource Coordinator VE Setup Guide"
- "Appendix D Format of CSV System Configuration Files" in the "ServerView Resource Coordinator VE Setup Guide"

[ROR VE V3.0.0]

- "Chapter 6 Pre-configuration" in the "ServerView Resource Orchestrator Virtual Edition V3.0.0 User's Guide"
- "Appendix A Format of CSV System Configuration Files" in the "ServerView Resource Orchestrator Virtual Edition V3.0.0 User's Guide"

Also, when transferring the manager using the pre-configuration function, perform the following preparations and checks.

- To confirm that transfer using the pre-configuration function is complete, if there are registered VM hosts on which there are VM guests, check from the ROR console that all of the VM guests are displayed, and record their information.
- When server switchover settings have been performed, it is not possible to transfer using the pre-configuration function when spare servers have been switched to. Perform restoration before starting transfer using the pre-configuration function.

  For the restoration method, refer to the following manuals:

  [RCVE]

  - "Chapter 10 Server Switchover" in the "ServerView Resource Coordinator VE Operation Guide"

  [ROR VE V3.0.0]

  - "Chapter 10 Server Switchover" in the "ServerView Resource Orchestrator Virtual Edition V3.0.0 Operation Guide"

- The following information will not be transferred. Reconfiguration is necessary when performing transfer using the pre-configuration function.

  Record the following configuration information from the RC console or the ROR Console.

    - User account information
    - Registration status of the agent of each managed server, and maintenance mode settings
    - Spare server settings
    - Agent registration information of OVM for SPARC guest domains
    - ETERNUS SF Storage Cruiserの登録情報 (*1)
    - ETERNUS SF Storage Cruiser連携によるWWN情報の設定
    - LANスイッチブレード以外のLANスイッチの登録情報
    - ネットワークデバイスの登録情報 (*2)

  *1: 本情報については、コマンド(rcxadm storagemgr)で確認してください。

  *2: 情報については、管理機能の定義ファイルおよび構成情報（xml定義）も確認してください。

- Power consumption data

  When monitoring of power consumption is being performed, collected power consumption data will not be transferred.

  When the power consumption data is necessary, export it in CSV format.

  For the export method, refer to the following manuals:

  [RCVE]

    - "13.2 Exporting Power Consumption Data" in the "ServerView Resource Coordinator VE Operation Guide"

  [ROR VE V3.0.0]

    - "13.2 Exporting Power Consumption Data" in the "ServerView Resource Orchestrator Virtual Edition V3.0.0 Operation Guide"

Note

Do not change the settings of the manager, agents, or any other hardware devices, or their configuration, until transfer using the pre-configuration function is complete.

1. Set Maintenance Mode

   From the RC console of the RCVE manager, or the ROR console of ROR VE, place all managed servers into maintenance mode.

2. System Configuration File Export

   Use the pre-configuration function to export a system configuration file in CSV format. During the export, do not perform any other operations with Resource Orchestrator.
   For the export method, refer to the following manuals:

   [RCVE]

   - "Chapter 7 Pre-configuration" in the "ServerView Resource Coordinator VE Setup Guide"

   [ROR VE V3.0.0]

   - "Chapter 6 Pre-configuration" in the "ServerView Resource Orchestrator Virtual Edition V3.0.0 User's Guide"

3. Backup (copy) Assets to Transfer

   a. Back up (copy) certificates.

      Back up (copy) the following folders and directories:

      - RCVE Windows Manager

        Installation_folder\Manager\etc\opt\FJSVssmgr\current\certificate
        Installation_folder\Manager\etc\opt\FJSVrcxdm\certificate
        Installation_folder\Manager\sys\apache\conf\ssl.crt
        Installation_folder\Manager\sys\apache\conf\ssl.key

- ROR VE Windows Manager

  Installation_folder\SVROR\Manager\etc\opt\FJSVssmgr\current\certificate
  Installation_folder\SVROR\Manager\etc\opt\FJSVrcxdm\certificate
  Installation_folder\SVROR\Manager\sys\apache\conf\ssl.crt
  Installation_folder\SVROR\Manager\sys\apache\conf\ssl.key

- RCVE and ROR VE Linux Manager

  /etc/opt/FJSVrcvmr/opt/FJSVssmgr/current/certificate
  /etc/opt/FJSVrcvmr/sys/apache/conf/ssl.crt
  /etc/opt/FJSVrcvmr/sys/apache/conf/ssl.key

b. Back up (copy) the folder containing the collected system images and cloning images to a location other than the installation folder and the image file storage folder.
When using the default image file storage folder, back up (copy) the following folder or directory:

- RCVE Windows Manager

  Installation_folder\ScwPro\depot\Cloneimg

- ROR VE Windows Manager

  Installation_folder\SVROR\ScwPro\depot\Cloneimg

- RCVE and ROR VE Linux Manager

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

When using a folder or directory other than the default, back up (copy) the "Cloneimg" folder or "CLONEIMG" directory used.

c. Back up (copy) the following file.

- Port Number Settings

  [Windows Manager]
  System_drive\WINDOWS\system32\drivers\etc\services

  [Linux Manager]
  /etc/services

- Batch Files and Script Files for Event-related Functions

  RCVE Windows Manager
  Installation_folder\Manager\etc\trapop.bat

  ROR VE Windows Manager
  Installation_folder\SVROR\Manager\etc\trapop.bat

  Linux Manager
  /etc/opt/FJSVrcvmr/trapop.sh

Note

- When operating managers in clusters, the above folders or directories are stored on the shared disk. Check if files, folders, or directories stored in the above locations are correctly backed up (copied).
The backup (copy) storage target can be set to be stored in a folder or directory on the shared disk other than "RCoordinator" or "SVROR" which are created during setup of the manager cluster service.

- When operating managers in clusters, the backup (copy) of folders or directories should be executed on the primary node.

- Before making a backup (copy) of system images and cloning images, check the available disk space. For the disk space necessary for system images and cloning images, refer to the following manuals:

  [RCVE]

  - "1.1.2.5 Dynamic Disk Space" in the "ServerView Resource Coordinator VE Installation Guide"

  [ROR VE V3.0.0]

- "1.4.2.5 Dynamic Disk Space" in the "ServerView Resource Orchestrator Virtual Edition V3.0.0 Setup Guide"

When there is no storage folder for system images and cloning images, this step is not necessary.

4. Uninstall Earlier Products or Managers of Earlier Versions

   Refer to the "ServerView Resource Coordinator VE Installation Guide" or the "ServerView Resource Orchestrator Virtual Edition V3.0.0 Installation Guide", and uninstall the manager.

   When operating managers in clusters, refer to the following manuals, delete the cluster service and uninstall the manager.

   [RCVE]

   - "Appendix B Manager Cluster Operation Settings and Deletion" in the "ServerView Resource Coordinator VE Installation Guide"

   [ROR VE V3.0.0]

   - "Appendix B Manager Cluster Operation Settings and Deletion" in the "ServerView Resource Orchestrator Virtual Edition V3.0.0 Installation Guide"

   Note

   - Do not perform "Delete servers" as given in the Preparations in the "ServerView Resource Coordinator VE Installation Guide" or the "ServerView Resource Orchestrator Virtual Edition V3.0.0 Installation Guide".
     When managed servers using HBA address rename have been deleted, it is necessary to reboot managed servers after upgrading of the manager is completed.

   - User account information is deleted when managers are uninstalled. Refer to step 6 and perform reconfiguration from the ROR console.

5. Installation of Managers of This Version

   Install managers of this version.
   For installation, refer to "2.1 Manager Installation".

   When operating managers in cluster environments, refer to "Appendix C Manager Cluster Operation Settings and Deletion", uninstall the manager and then configure the cluster services.

   Note

   - When installing managers, specify the same admin LAN as used for the RCVE manager on the [Admin LAN Selection] window.

   - When the settings for restarting of managers have been changed, reconfigure the settings after the manager is installed, based on the information which was recorded during preparation. For details, refer to "Restarting Managers" in "Appendix A Notes on Operating ServerView Resource Orchestrator" in the "Operation Guide VE".

   After installing managers, use the following procedure to restore the certificates and image file storage folder backed up (copied) in step 3.

   a. Stop the manager.

      For the method for stopping managers, refer to "2.1 Starting and Stopping Managers" in the "Operation Guide VE".

   b. Return the image file storage folder backup (copy) to the folder specified during installation.

      When using the default image file storage folder, restore to the following folder or directory:

      [Windows Manager]
      Installation_folder\ScwPro\depot\Cloneimg

      [Linux Manager]
      /var/opt/FJSVscw-deploysv/depot/CLONEIMG

When using a folder other than the default, restore to the new folder.
When the image file storage folder was not backed up, this step is not necessary.

c. Restore the backed up (copied) certificates to the manager *installation_folder*.

   Restore to the following folder or directory:

   [Windows Manager]
   Installation_folder\SVROR\Manager\etc\opt\FJSVssmgr\current\certificate
   Installation_folder\SVROR\Manager\etc\opt\FJSVrcxdm\certificate
   Installation_folder\SVROR\Manager\sys\apache\conf\ssl.crt
   Installation_folder\SVROR\Manager\sys\apache\conf\ssl.key

   [Linux Manager]
   /etc/opt/FJSVrcvmr/opt/FJSVssmgr/current/certificate
   /etc/opt/FJSVrcvmr/sys/apache/conf/ssl.crt
   /etc/opt/FJSVrcvmr/sys/apache/conf/ssl.key

d. Restore the information that was backed up during preparations.

   - Port number settings

     Change the port numbers based on the information that was backed up during preparations.
     For details on how to change port numbers, refer to "8.2 Changing Port Numbers" in the "User's Guide VE".
     When the port number has not been changed from the default, this step is not necessary.

   - Batch files and script files for event-related functions

     Restore them by replacing the following file.

     [Windows Manager]
     Installation_folder\SVROR\Manager\etc\trapop.bat

     [Linux]
     /etc/opt/FJSVrcvmr/trapop.sh

e. Start the manager.

   For the methods for starting and stopping managers, refer to "2.1 Starting and Stopping Managers" in the "Operation Guide VE".

6. User Account Settings

   Using the information recorded during preparations, perform setting of user accounts using the ROR console.
   For details on how to configure user accounts, refer to "Chapter 5 Managing User Accounts" in the "User's Guide VE".

7. Registration of license

   Access the ROR console, and register the license of Virtual Edition.

   For the registration of the license, refer to the setting of the license of "Chapter 4 License Setup and Confirmation".

8. Edit System Configuration Files

   Based on the environment created for the RCVE manager, edit the system configuration file (CSV format) exported in 2.
   Change the operation column of all resources to "new".

   For how to edit system configuration files (CSV format), refer to "Appendix B Format of CSV System Configuration Files" in the "User's Guide VE".

   Note

   When the spare server information is configured, use the following procedure to delete the spare server information.

   - In the "SpareServer" section, set "operation" as a hyphen ("-").

9. Creating an Environment of This Version

   Import the system configuration file and create an environment of this version.
   Use the following procedure to configure an environment of this version.

   a. Import of the system configuration file

      Import the edited system configuration file.
      For the import method, refer to "12.2 Importing the System Configuration File" in the "User's Guide VE".

   b. Register the Agent

      Using the information recorded during preparations, perform agent registration using the ROR console. Perform agent registration with the OS of the managed server booted.

      For details on registering agents, refer to "Chapter 7 Installing Software and Registering Agents on Managed Servers".

      After completing agent registration, use the ROR console to check that all physical OSs and VM hosts are displayed. When there are VM hosts (with VM guests) registered, check that all VM guests are displayed.

   c. Spare Server Information Settings

      Using the information recorded during preparations, perform registration of spare server information using the ROR console.
      For registration of spare server information, refer to "18.2 Settings for Server Switchover" in the "User's Guide VE".

   d. Registration of Labels, Comments, and Contact Information

      When label, comment, and contact information has been registered, change the contents of the operation column of the system configuration file (CSV format) that were changed to "new" in 7 back to hyphens ("-"), and change the contents of the operation column of resources contained in the [Memo] section to "new".
      For how to edit system configuration files (CSV format), refer to "Appendix B Format of CSV System Configuration Files" in the "User's Guide VE".
      Import the edited system configuration file.
      For the import method, refer to "12.2 Importing the System Configuration File" in the "User's Guide VE".

10. Set Maintenance Mode

    Using the information recorded during preparation, place the managed serves placed into maintenance mode before the transfer using the pre-configuration function into maintenance mode again.
    For maintenance mode settings, refer to "Appendix C Maintenance Mode" in the "User's Guide VE".

Note

When using backup system images or collecting cloning images without upgrading agents, either reboot managed servers after reinstallation of the manager or transfer using the pre-configuration function is completed, or restart the related services.

For restarting the Related Services, refer to "2.2 Starting and Stopping Agents" in the "Operation Guide VE".

D.3 Agent

This section explains the upgrading of agents.
Upgrading of agents is not mandatory even when managers have been upgraded to this version. Perform upgrades if necessary.

Transferred Data

Before upgrading, note that the following agent resources are transferred:

- Definition files of the network parameter auto-configuration function (when the network parameter auto-configuration function is being used)

  [Windows] [Hyper-V]
  Installation_folder\Agent\etc\event_script folder
  Installation_folder\Agent\etc\ipaddr.conf file
  Installation_folder\Agent\etc\ipaddr.conf file

[Linux] [VMware] [Xen] [KVM]
/etc/opt/FJSVrcxat/event_script directory
/etc/opt/FJSVnrmp/lan/ipaddr.conf file
/etc/FJSVrcx.conf file

[Solaris]
The command does not have to be executed.

Data and work files which are transferred during upgrade installation are stored in the following folder. Ensure that the folder is not deleted until after the upgrade is complete.
After the upgrade is complete, the following folder may remain. In that case, check that Resource Orchestrator is operating correctly and then manually delete the folder.

[Windows] [Hyper-V]
32-bit (x86) OS
Drive_name\Program Files\RCVE-upgradedata
64-bit (x64) OS
Drive_name\Program Files (x86)\RCVE-upgradedata

[Linux] [VMware] [Xen] [KVM]
/var/opt/RCVE-upgradedata

[Solaris]
/var/opt/RCVE-upgradedata

Preparations

Perform the following preparations and checks before upgrading:

- Check that the environment is one in which agents of this version can be operated.
  For the operational environment, refer to "6.1 Software Environment" and "6.2 Hardware Environment" in the "Overview".
- To enable recovery in case there is unexpected trouble during the upgrade process, back up the folders and files listed in "Transferred Data" to a folder other than the agent installation folder.

Upgrade using Upgrade Installation

When performing upgrade installation from V2.1.1 of agents in Windows environments, upgrade installation can be performed using the installer of this version.

Use the following procedure to upgrade agents of earlier versions to agents of this version on all of the managed servers that are being upgraded.

Note

- Do not perform any other operations with Resource Orchestrator until the upgrade is completed.
- Perform upgrading of agents after upgrading of managers is completed.
- In the event that upgrade installation fails, please resolve the cause of the failure and perform upgrade installation again. If the problem cannot be resolved and upgrade installation fails again, please contact Fujitsu technical staff.
- When performing an upgrade installation, please do not access the installation folder of the earlier version or any of the files and folders inside it using the command prompt, Explorer, or an editor.
  While it is being accessed, attempts to perform upgrade installation will fail.
  If upgrade installation fails, stop accessing the files or folders and then perform the upgrade installation again.
- When stopping the upgrade and restoring the earlier version, please re-install the agent of the earlier version and then replace the information that was backed up during the preparations.
  When performing restoration and an agent of this version or an earlier version has been installed, please uninstall it.
  After restoration, please delete the folder containing the backed up assets.

- Upgrade installation will delete patches that were applied to the earlier version.

  [Linux]
  When the PATH variable has not been configured to enable execution of UpdateAdvisor (Middleware) commands from a user-defined location, performing upgrade installation will delete any patches that have been applied to the old version, but it will not delete product information or component information. Refer to the UpdateAdvisor (Middleware) manual and delete software and component information from the applied modification checklist.

1. Set Maintenance Mode

   When server switchover settings have been performed for managed servers, place them into maintenance mode.
   When managed servers are set as spare servers, place the managed servers set as spare servers into maintenance mode.

2. Backing up (copying) of Network Parameter Auto-configuration Function Definition Files

   When using the network parameter auto-configuration function during deployment of cloning images, back up (copy) the following folders and files to a location other than the agent installation folder.

   [Windows] [Hyper-V]
   Installation_folder\Agent\etc\event_script folder
   Installation_folder\Agent\etc\ipaddr.conf file
   Installation_folder\Agent\etc\ipaddr.conf file

   [Linux] [VMware] [Xen] [KVM]
   /etc/opt/FJSVrcxat/event_script directory
   /etc/opt/FJSVnrmp/lan/ipaddr.conf file
   /etc/FJSVrcx.conf file

   [Solaris]
   The command does not have to be executed.

3. Upgrade Installation

   [Windows] [Hyper-V]
   Refer to "2.2.2 Installation [Windows] [Hyper-V]", and execute the Resource Orchestrator installer.
   The Resource Orchestrator setup window will be displayed. Check the contents of the license agreement, etc. and then click [Yes].
   The setting information that will be taken over from the earlier version will be displayed. Please check it and then click [Install].
   Upgrade installation will begin.

   [Linux] [VMware] [Xen] [KVM]
   Refer to "2.2.3 Installation [Linux] [VMware] [Xen] [KVM]", and execute the Resource Orchestrator installer.
   Check the contents of the license agreement, etc. and then enter "y".
   The setting information that will be taken over from the earlier version will be displayed. Please check it and then enter "y". Upgrade installation will begin.

   [Solaris]
   Refer to "2.2.4 Installation [Solaris] [Solaris Zones] [OVM for SPARC]", and execute the Resource Orchestrator installer.
   Check the contents of the license agreement, etc. and then enter "y". Upgrade installation will begin.

   Note

   - When upgrade installation is conducted on SUSE Linux Enterprise Server, upgrade installation will be conducted successfully even if the following message is displayed.

     ```
     insserv: Warning, current runlevel(s) of script 'scwagent' overwrites defaults.
     ```

4. Restoration of Network Parameter Auto-configuration Function Definition Files

   When using the network parameter auto-configuration function during deployment of cloning images, restore the definition files that were backed up (copied) in step 2. When step 2 was not performed, this step is not necessary.

   a. Stop agents.

      For the method for stopping agents, refer to "2.2 Starting and Stopping Agents" in the "Operation Guide VE".

b. Restore the definition file.

   Restore the folders and files backed up (copied) in step 2 to the following locations in the installation folder of this version:

   [Windows] [Hyper-V]
   Installation_folder\Agent\etc\event_script folder
   Installation_folder\Agent\etc\ipaddr.conf file
   Installation_folder\Agent\etc\ipaddr.conf file

   [Linux] [VMware] [Xen] [KVM]
   /etc/opt/FJSVrcxat/event_script directory
   /etc/opt/FJSVnrmp/lan/ipaddr.conf file
   /etc/FJSVrcx.conf file

   [Solaris]
   There is no definition file to restore.

c. Start agents.

   For the method for starting agents, refer to "2.2 Starting and Stopping Agents" in the "Operation Guide VE".

5. Release Maintenance Mode

   Release the maintenance mode of managed servers placed into maintenance mode in step 1.

Note

- After upgrading agents, use the ROR console to check if the upgraded managed servers are being displayed correctly.
- Updating of system images and cloning images is advised after agents have been upgraded.
- After the upgrade is complete, check that Resource Orchestrator is operating correctly, and then manually delete the folder that was used to back up the transferred data.
  For the folder created to back up the transferred data, refer to "Transferred Data".

Transfer of Agents Using Re-installation or the Pre-configuration Function

Use the following procedure to perform transfer from agents of earlier versions to agents on this version on all managed servers for which transfer using the pre-configuration function will be performed.

Note

- Do not perform any other operations with Resource Orchestrator until the transfer using the pre-configuration function is completed.
- Perform transfer of agents after transfer of the manager using the pre-configuration function is completed.
- When using the network parameter auto-configuration function during deployment of cloning images, specify the same installation folder for agents of the earlier version and those of this version.

1. Set Maintenance Mode

   - When server switchover settings have been performed for managed servers

     Place them into maintenance mode.

   - When managed servers are set as spare servers

     Place the managed servers set as spare servers into maintenance mode.

2. Backing up (copying) of Network Parameter Auto-configuration Function Definition Files

   When using the network parameter auto-configuration function during deployment of cloning images, back up (copy) the following folders and files to a location other than the agent installation folder.

[Windows] [Hyper-V]
Installation_folder\Agent\etc\event_script folder
Installation_folder\Agent\etc\ipaddr.conf file
Installation_folder\Agent\etc\ipaddr.conf file

[Linux] [VMware] [Xen] [KVM]
/etc/opt/FJSVrcxat/event_script directory
/etc/opt/FJSVnrmp/lan/ipaddr.conf file
/etc/FJSVrcx.conf file

[Solaris]
The command does not have to be executed.

3. Uninstall RCVE or the earlier version ROR agents

   Uninstall the agent, referring to the manuals of RCVE or the earlier version of ROR.

4. Install ROR VE Agents

   Install ROR VE agents.
   For installation, refer to "2.2 Agent Installation".

5. Restoration of Network Parameter Auto-configuration Function Definition Files

   When using the network parameter auto-configuration function during deployment of cloning images, restore the definition files that were backed up (copied) in step 2. When step 2 was not performed, this step is not necessary.

   a. Stop agents.

      For the method for stopping agents, refer to "2.2 Starting and Stopping Agents" in the "Operation Guide VE".

   b. Restore the definition file.

      Restore the folders and files backed up (copied) in step 2 to the following locations in the installation folder of this version:

      [Windows] [Hyper-V]
      Installation_folder\Agent\etc\event_script folder
      Installation_folder\Agent\etc\ipaddr.conf file
      Installation_folder\Agent\etc\ipaddr.conf file

      [Linux] [VMware] [Xen] [KVM]
      /etc/opt/FJSVrcxat/event_script directory
      /etc/opt/FJSVnrmp/lan/ipaddr.conf file
      /etc/FJSVrcx.conf file

      [Solaris]
      There is no definition file to restore.

   c. Start agents.

      For the method for starting agents, refer to "2.2 Starting and Stopping Agents" in the "Operation Guide VE".

6. Release Maintenance Mode

   Release the maintenance mode of managed servers placed into maintenance mode in 1.

Note

- After transferring agents, use the ROR console to check that the upgraded managed servers are being displayed correctly.
- Updating of system images and cloning images is advised after agents have been transferred.

Upgrading with ServerView Update Manager or ServerView Update Manager Express

Upgrade installation can be performed with ServerView Update Manager or ServerView Update Manager Express when upgrading to this version from RCVE V2.2.2 or later.

Refer to the manual of ServerView Update Manager or ServerView Update Manager Express for the procedure.

Note

- To upgrade with ServerView Update Manager, the server to be upgrade must be managed by ServerView Operations Manager.
- OSs and hardware supported by ServerView Update Manager or ServerView Update Manager Express can be updated.
- For Linux or VMware, the installed ServerView Agents must be at least V5.01.08.
- Do not perform any other operations with Resource Orchestrator until the upgrade is completed.
- Perform upgrading of agents after upgrading of managers is completed.
- In the event that upgrade installation fails, please resolve the cause of the failure and perform upgrade installation again. If the problem cannot be resolved and upgrade installation fails again, please contact Fujitsu technical staff.
- When performing an upgrade installation, please do not access the installation folder of the earlier version or any of the files and folders inside it using the command prompt, Windows Explorer, or an editor. While it is being accessed, attempts to perform upgrade installation will fail.
- If upgrade installation fails, stop accessing the files or folders and then perform the upgrade installation again.
- When stopping the upgrade and restoring the earlier version, please re-install the agent of the earlier version and then replace the information that was backed up during the preparations.

  When performing restoration and an agent of this version or an earlier version has been installed, please uninstall it.

  After restoration, please delete the folder containing the backed up assets.
- Upgrade installation will delete patches that were applied to the earlier version.

[Linux]

- When the PATH variable has not been configured to enable execution of UpdateAdvisor (Middleware) commands from a user-defined location, performing upgrade installation will delete any patches that have been applied to the old version, but it will not delete product information or component information. Refer to the UpdateAdvisor (Middleware) manual and delete software and component information from the applied modification checklist.
- After upgrading agents, use the ROR console to check that the upgraded managed servers are being displayed correctly.
- Updating of system images and cloning images is advised after agents have been upgraded.

D.4 HBA address rename Setup Service

This section explains upgrading of the HBA address rename setup service.

Transferred Data

There is no HBA address rename setup service data to transfer when upgrading from an earlier version to this version.

Preparations

Perform the following preparations and checks before upgrading:

- Check that the environment is one in which agents of this version can be operated.

  For the operational environment, refer to "6.1 Software Environment" and "6.2 Hardware Environment" in the "Overview".

Upgrade using Upgrade Installation

When upgrading to this version from RCVE V2.2.2, upgrade can be performed using upgrade installation. Perform the upgrade using the following procedure:

Note

- Do not perform any other operations with Resource Orchestrator until the upgrade is completed.
- Perform upgrading of the HBA address rename setup service after upgrading of managers is completed.
- In the event that upgrade installation fails, please resolve the cause of the failure and perform upgrade installation again. If the problem cannot be resolved and upgrade installation fails again, please contact Fujitsu technical staff.
- When performing an upgrade installation, please do not access the installation folder of the earlier version or any of the files and folders inside it using the command prompt, Explorer, or an editor.
  While it is being accessed, attempts to perform upgrade installation will fail.
  If upgrade installation fails, stop accessing the files or folders and then perform the upgrade installation again.
- When stopping the upgrade and restoring the earlier version, please re-install the HBA address rename setup service of the earlier version.
  When performing restoration and the HBA address rename setup service of this version or an earlier version has been installed, please uninstall it.
- Upgrade installation will delete patches that were applied to the earlier version.

  [Linux]
  When the PATH variable has not been configured to enable execution of UpdateAdvisor (Middleware) commands from a user-defined location, performing upgrade installation will delete any patches that have been applied to the old version, but it will not delete product information or component information. Refer to the UpdateAdvisor (Middleware) manual and delete software and component information from the applied modification checklist.

1. Upgrade Installation

   [Windows]
   Refer to "2.3.2 Installation [Windows]", and execute the Resource Orchestrator installer.
   The Resource Orchestrator setup window will be displayed. Check the contents of the license agreement, etc. and then click [Yes].
   The setting information that will be taken over from the earlier version will be displayed. Please check it and then click [Install].
   Upgrade installation will begin.

   [Linux]
   Refer to "2.3.3 Installation [Linux]", and execute Resource Orchestrator installer.
   The Resource Orchestrator setup window will be displayed. Check the contents of the license agreement, etc. and then enter "y".
   A message checking about performing the upgrade installation will be displayed.
   To perform upgrade installation, enter "y". Upgrade installation will begin.

2. Display the Resource Orchestrator Setup Completion Window [Windows]

   When using the HBA address rename setup service immediately after configuration, check the [Yes, launch it now.] checkbox.
   Click [Finish] and close the window. If the checkbox was checked, the HBA address rename setup service will be started after the window is closed.

3. Start the HBA address rename setup Service

   [Windows]
   When the HBA address rename setup service was not started in step 2, refer to "6.1 Settings for the HBA address rename Setup Service", and start the HBA address rename setup service.

   [Linux]
   Refer to "6.1 Settings for the HBA address rename Setup Service", and start the HBA address rename setup service.

D.5 Client

This section explains the necessary operations for clients after upgrading of managers.

Web browsers are used as clients of this version.

When upgrading managers, it is necessary to clear the Web browser's cache (temporary internet files), before accessing the ROR console.

Use the following procedure to clear the Web browser's cache.

1. Select [Tools]-[Internet Options].

   The [Internet Options] dialog is displayed.

2. Select the [General] tab on the [Internet Options] dialog.

3. Select [Delete] in the "Browsing history" area.

   The [Delete Browsing History] dialog is displayed.

4. Check the [Temporary Internet files] checkbox in the [Delete Browsing History] dialog and unselect the other checkboxes.

5. Click the [Delete] button.

   The Web browser's cache is cleared.

Appendix E Compatibility with Earlier Versions

For details on compatibility with earlier versions of Resource Orchestrator, refer to "Release Notes".

Appendix F Migration Procedure when Using Active Directory with a Redundant Configuration

This appendix explains the migration procedure when changing the number of Active Directories for performing the Single Sign-On function of ServerView Operations Manager from one to two. It is assumed that an Active Directory in a redundant configuration is used in this procedure.

It is possible to continue operation by using an Active Directory in a redundant configuration that automatically switches to the other domain controller when one of the domain controllers fails.

Preparations

- Active Directory Settings
  - Configure the domain controller to use as a backup host.
- ServerView Operations Manager Settings
  - Register the backup host in the directory service settings.

  For details, refer to "ServerView user management via an LDAP directory service" in "FUJITSU ServerView Suite User Management in ServerView".

Migration Procedure

1. Stop the manager.

   For the method for stopping managers, refer to "2.1 Starting and Stopping Managers" in the "Operation Guide VE".

2. Register the directory service connection information for performing Single Sign-On.

   Execute the rcxadm authctl sync command to register the connection information for the two Active Directories registered in the ServerView Operations Manager in the manager.

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

3. Check the certificate of the backup host.

   Execute the rcxadm authctl diffcert command to check the alias of the CA certificate (keystore) of the backup host.

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

4. Register the certificate of the backup host.

   Register the alias of the CA certificate (keystore) of the backup host checked in step 3.
   For details on how to register, refer to "13.1.1.2 Registering Certificates" in the "Operation Guide VE".

5. Start the manager.

   Refer to Section "2.1 Starting and Stopping Managers" in the "Operation Guide VE" for information on starting the manager.

Appendix G Sending SNMP Traps

This appendix explains the function used to send the details of Resource Orchestrator events to other products as SNMP traps.

Functional Overview

By receiving SNMP traps sent by Resource Orchestrator on other products (operation management products, etc.) it is possible to monitor major Resource Orchestrator events on other products. With this function, in operating environments where monitoring is mainly performed using the consoles of other products, as it is not necessary to constantly display the Resource Orchestrator console, centralization of the monitoring console is possible.

Function Details

- SNMPv1 traps are sent to servers registered as destinations. Destination servers are registered, changed, and deleted using the rcxadm eventctl command.
  For details on this command, refer to "5.7 rcxadm eventctl" in the "Reference Guide (Command) VE".
- The SNMP traps sent by Resource Orchestrator contain information about the operation details of Resource Orchestrator. For events related to status changes of resources managed by Resource Orchestrator and events internal to resources, the SNMP traps will be sent by the resource itself.
- The events that are the target of sending as SNMP traps are as follow:

  FJSVrcx:INFO:21143:*operation*:started
  FJSVrcx:INFO:21144:*operation*:completed
  FJSVrcx:INFO:21145:*operation*:cancelled
  FJSVrcx:ERROR:61143:*operation*:failed
  FJSVrcx:ERROR:61144:*operation*:rollback failed
- For details of the Resource Orchestrator events that are sent as SNMP traps, check the event log of the ROR console.

Setup Procedure

This section explains the procedure for setting other products to receive Resource Orchestrator SNMP traps.
Here it is assumed that installation of other products for receiving SNMP traps has been performed, and that basic settings such as those of the SNMP trap service necessary to receive traps and the required ports, have been made.

1. Configure a SNMP community name for the product that will receive SNMP traps.
   Enter a string of up to 32 alphanumeric characters, hyphens ("-"), and underscores ("_") for the SNMP community name.
2. Load the Resource Orchestrator MIB file on the product that is to receive SNMP traps.
   The MIB file that defines the SNMP traps for Resource Orchestrator is located in the following folder on the admin server.

   [Windows Manager]
   Installation_folder\SVROR\Manager\etc\mibs\RCVE-Event-Trap-MIB.mib

   [Linux Manager]
   /etc/opt/FJSVrcvmr/mibs/RCVE-Event-Trap-MIB.mib
3. Register destination servers using the rcxadm eventctl add command of Resource Orchestrator.

Modification Procedure

Use the following procedure to change SNMP trap destination settings:

1. Delete the target destination server information using the rcxadm eventctl delete command of Resource Orchestrator.
2. Register the new destination servers using the rcxadm eventctl add command of Resource Orchestrator.

Deletion Procedure

Delete the target destination server information using the rcxadm eventctl delete command of Resource Orchestrator.

Operation Checks

Use the following procedure to confirm that SNMP trap destinations have been registered correctly.

1. From the ROR console, place the desired managed 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].

2. The managed server is released from maintenance mode.

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

      The [Release Maintenance Mode] dialog is displayed.

   b. Click [OK].

As a result of the above operation, the following four events will be sent as SNMP traps to the registered server. If the destination has been registered correctly, it is possible to check the receipt of the Resource Orchestrator SNMP traps on the destination device.
Please note that the display of SNMP traps varies depending on the product.

Event ID	OID
FJSVrcx:INFO:21143: setting maintenance mode:started	1.3.6.1.4.1.211.4.1.3.55.100.1.2.1.21143
FJSVrcx:INFO:21144: setting maintenance mode:completed	1.3.6.1.4.1.211.4.1.3.55.100.1.2.1.21144
FJSVrcx:INFO:21143: releasing maintenance mode:started	1.3.6.1.4.1.211.4.1.3.55.100.1.2.1.21143
FJSVrcx:INFO:21144: releasing maintenance mode:completed	1.3.6.1.4.1.211.4.1.3.55.100.1.2.1.21144

If the receipt of SNMP traps cannot be confirmed, use the rcxadm eventctl command to check if the desired destination has been registered correctly. If there are no problems with the registered details, check that there are no problems with the network or the settings for the SNMP trap destination. After resolving any problems, repeat the above procedure and check if the Resource Orchestrator SNMP traps can be received.

Appendix H Configuring and Deleting SELinux [Linux]

This appendix explains how to configure and delete SELinux in Resource Orchestrator when SELinux is enabled (Enforcing mode).

H.1 Configuring SELinux

This section explains how to configure SELinux.

H.1.1 Manager

After installing Resource Orchestrator, use the following procedure to configure SELinux.

1. Execute the following commands.

   ```
   # cd /etc/opt/FJSVrcvmr/selinux <RETURN>
   # /usr/sbin/semodule -i fjsvrcvmr.pp <RETURN>
   # /usr/sbin/semanage fcontext -a -t bin_t /opt/FJSVcir/jre/bin/java <RETURN>
   # /sbin/restorecon -R /etc/init.d <RETURN>
   # /sbin/restorecon /opt/FJSVcir/jre/bin/java <RETURN>
   # /sbin/restorecon /opt/FJSVrcvmr/runtime/jre6/bin/java <RETURN>
   # /sbin/restorecon /opt/FJSVrcvmr/runtime64/jre6/bin/java <RETURN>
   # /sbin/restorecon /var/opt/FJSVrcvmr/rcxtrphdl <RETURN>
   # /sbin/restorecon /opt/FJSVrcvhb/jre6/bin/java <RETURN>
   ```

   The policy modules are applied and a label is configured for each file.

2. Check if the label of each file and directory is correct.

   Execute the following commands.

   - File

     ```
     # ls -Z file <RETURN>
     ```

     For *file*, specify the target file for label check.

   - Directory

     ```
     # ls -dZ directory <RETURN>
     ```

     For *directory*, specify the directory for label check.

   Example

   To check the label of /opt/FJSVcir/jre/bin/java

   ```
   # ls -Z /opt/FJSVcir/jre/bin/java <RETURN>

   -rwxr-xr-x. root sys system_u:object_r:bin_t:s0 /opt/FJSVcir/jre/bin/java
   ```

   The files and directories to check the labels of are as follows.

   Table H.1 Files and Directories to Check the Labels Of

Files and Directories	Label
/etc/init.d/scwdepsvd	unconfined_exec_t
/etc/init.d/scwpxesvd	
/etc/init.d/scwtftpd	

Files and Directories	Label
/etc/init.d/rcvmr	
/etc/init.d/rcxdb	
/etc/init.d/rcxhttpd	
/etc/init.d/rcxmongrel[0-9]*	
/var/opt/FJSVrcvmr/rcxtrphdl/ (directory)	snmpd_var_lib_t
/opt/FJSVrcvmr/runtime64/jre6/bin/java	bin_t
/opt/FJSVrcvmr/runtime/jre6/bin/java	
/opt/FJSVrcvhb/jre6/bin/java	
/opt/FJSVcir/jre/bin/java	

3. Restart the manager.

   For the method for restarting managers, refer to "2.1 Starting and Stopping Managers" in the "Operation Guide VE".

H.1.2 Agent

After installing Resource Orchestrator, use the following procedure to configure SELinux.

1. Execute the following commands.

   - When using Red Hat Enterprise Linux 6

```
# /usr/sbin/semanage fcontext -a -t unconfined_exec_t '/etc/rc\.d/init\.d/SCruiserAgent' <RETURN>
# /usr/sbin/semanage fcontext -a -t unconfined_exec_t '/etc/rc\.d/init\.d/scwnaconfig-p[0-9]*' <RETURN>
# /usr/sbin/semanage fcontext -a -t unconfined_exec_t '/etc/rc\.d/init\.d/scwagent' <RETURN>
# /usr/sbin/semanage fcontext -a -t bin_t /opt/FJSVssagt/jre6/bin/java <RETURN>
# /sbin/restorecon -R /etc/init.d <RETURN>
# /sbin/restorecon /opt/FJSVssagt/jre6/bin/java <RETURN>
```

   - When using Red Hat Enterprise Linux 7.0

```
# /usr/sbin/semanage fcontext -a -t unconfined_exec_t /opt/FJSVssagt/bin/SCruiserAgent <RETURN>
# /usr/sbin/semanage fcontext -a -t unconfined_exec_t '/opt/systemcastwizard/scwnaconfig-p[0-9]*.sh'
<RETURN>
# /usr/sbin/semanage fcontext -a -t unconfined_exec_t /opt/systemcastwizard/scwagent <RETURN>
# /usr/sbin/semanage fcontext -a -t bin_t /opt/FJSVssagt/jre6/bin/java <RETURN>
# /sbin/restorecon /opt/FJSVssagt/bin/SCruiserAgent <RETURN>
# /sbin/restorecon /opt/systemcastwizard/scwnaconfig-p[0-9]*.sh <RETURN>
# /sbin/restorecon /opt/systemcastwizard/scwagent <RETURN>
# /sbin/restorecon /opt/FJSVssagt/jre6/bin/java <RETURN>
```

   The label is configured in the file.

2. Check if the label of each file is correct.

   Execute the following commands.

```
# ls -Z file <RETURN>
```

   For *file*, specify the target file for label check.

   ### Example

   To check the label of /opt/FJSVssagt/jre6/bin/java

```
# ls -Z /opt/FJSVssagt/jre6/bin/java <RETURN>
```

```
-rwxr-xr-x. root sys unconfined_u:object_r:bin_t:s0 /opt/FJSVssagt/jre6/bin/java
```

The files and labels to check are as follows.

Table H.2 Files to Check the Labels Of (Red Hat Enterprise Linux 6)

File	Label
/etc/init.d/SCruiserAgent	unconfined_exec_t
/etc/init.d/scwagent	
/etc/init.d/scwnaconfig-p1	
/opt/FJSVssagt/jre6/bin/java	bin_t

Table H.3 Files to Check the Labels Of (Red Hat Enterprise Linux 7)

File	Label
/opt/FJSVssagt/bin/SCruiserAgent	unconfined_exec_t
/opt/systemcastwizard/scwagent	
/opt/systemcastwizard/scwnaconfig-p1.sh	
/opt/systemcastwizard/scwnaconfig-p2.sh	
/opt/FJSVssagt/jre6/bin/java	bin_t

3. Restart the agent.

   For details on how to restart the agent, refer to "2.2 Starting and Stopping Agents" in the "Operation Guide VE".

H.1.3 HBA address rename Setup Service

After installing Resource Orchestrator, use the following procedure to configure SELinux.

1. Execute the following commands.

```
# /usr/sbin/semanage fcontext -a -t unconfined_exec_t '/etc/rc\.d/init\.d/rcvhb' <RETURN>
# /usr/sbin/semanage fcontext -a -t unconfined_exec_t '/etc/rc\.d/init\.d/PXEService' <RETURN>
# /usr/sbin/semanage fcontext -a -t unconfined_exec_t '/etc/rc\.d/init\.d/rservice' <RETURN>
# /usr/sbin/semanage fcontext -a -t unconfined_exec_t '/etc/rc\.d/init\.d/scwtftpd' <RETURN>
# /usr/sbin/semanage fcontext -a -t bin_t /opt/FJSVrcvhb/jre6/bin/java <RETURN>
# /sbin/restorecon -R /etc/init.d <RETURN>
# /sbin/restorecon /opt/FJSVrcvhb/jre6/bin/java <RETURN>
```

   The label is configured in the file.

2. Check if the label of each file is correct.

   Execute the following commands.

```
# ls -Z file <RETURN>
```

   For *file*, specify the target file for label check.

Example

To check the label of /opt/FJSVrcvhb/jre6/bin/java

```
# ls -Z /opt/FJSVrcvhb/jre6/bin/java <RETURN>

-rwxr-xr-x. root sys unconfined_u:object_r:bin_t:s0 /opt/FJSVrcvhb/jre6/bin/java
```

The files and labels to check are as follows.

Table H.4 Files to Check the Labels Of

File	Label
/etc/init.d/PXEService	unconfined_exec_t
/etc/init.d/rcvhb	
/etc/init.d/rservice	
/etc/init.d/scwtftpd	
/opt/FJSVrcvhb/jre6/bin/java	bin_t

3. Restart the HBA address rename setup service.

   For details on how to restart the HBA address rename setup service, refer to "6.1 Settings for the HBA address rename Setup Service".

H.1.4 ServerView Trap Server for Linux

After installing ServerView Trap Server for Linux (trpsrvd), execute the following command to configure the port type for the port number.

```
# /usr/sbin/semanage port -a -t snmp_port_t -p udp 8162 <RETURN>
```

H.2 Deleting the SELinux Settings

This section explains how to delete the SELinux settings.

H.2.1 Manager

After uninstalling Resource Orchestrator, use the following procedure to delete SELinux settings.

1. Execute the following command and delete the policy module.

   ```
   # /usr/sbin/semodule -r fjsvrcvmr <RETURN>
   ```

2. Execute the following command and delete the file label.

   ```
   # /usr/sbin/semanage fcontext -d /opt/FJSVcir/jre/bin/java <RETURN>
   ```

H.2.2 Agent

After uninstalling Resource Orchestrator, execute the following command to delete the label of the file:

- When using Red Hat Enterprise Linux 6

  ```
  # /usr/sbin/semanage fcontext -d '/etc/rc\.d/init\.d/SCruiserAgent' <RETURN>
  # /usr/sbin/semanage fcontext -d '/etc/rc\.d/init\.d/scwnaconfig-p[0-9]*' <RETURN>
  # /usr/sbin/semanage fcontext -d '/etc/rc\.d/init\.d/scwagent' <RETURN>
  # /usr/sbin/semanage fcontext -d /opt/FJSVssagt/jre6/bin/java <RETURN>
  ```

- When using Red Hat Enterprise Linux 7.0

  ```
  # /usr/sbin/semanage fcontext -d /opt/FJSVssagt/bin/SCruiserAgent <RETURN>
  # /usr/sbin/semanage fcontext -d '/opt/systemcastwizard/scwnaconfig-p[0-9]*.sh' <RETURN>
  # /usr/sbin/semanage fcontext -d /opt/systemcastwizard/scwagent <RETURN>
  # /usr/sbin/semanage fcontext -d /opt/FJSVssagt/jre6/bin/java <RETURN>
  ```

H.2.3 HBA address rename Setup Service

After uninstalling Resource Orchestrator, execute the following command to delete the label of the file:

```
# /usr/sbin/semanage fcontext -d '/etc/rc\.d/init\.d/rcvhb' <RETURN>
# /usr/sbin/semanage fcontext -d '/etc/rc\.d/init\.d/PXEService' <RETURN>
# /usr/sbin/semanage fcontext -d '/etc/rc\.d/init\.d/rservice' <RETURN>
# /usr/sbin/semanage fcontext -d '/etc/rc\.d/init\.d/scwtftpd' <RETURN>
# /usr/sbin/semanage fcontext -d /opt/FJSVrcvhb/jre6/bin/java <RETURN>
```

H.2.4 ServerView Trap Server for Linux

After uninstalling ServerView Trap Server for Linux (trpsrvd), execute the following command to delete the port type for the port number.

```
# /usr/sbin/semanage port -d -t snmp_port_t -p udp 8162 <RETURN>
```