

ServerView Resource Orchestrator Cloud Edition V3.0.0



Setup Guide

Windows/Linux

J2X1-7610-01ENZ0(06)
March 2013

Preface

Purpose

This manual provides an outline of ServerView Resource Orchestrator (hereinafter Resource Orchestrator) and the operations and settings required for setup.

Target Readers

This manual is written for system administrators who will use Resource Orchestrator to operate the infrastructure in private cloud or data center environments.

When setting up systems, it is assumed that readers have the basic knowledge required to configure the servers, storage, network devices, and server virtualization software to be installed. Additionally, a basic understanding of directory services such as Active Directory and LDAP is necessary.

Organization

This manual is composed as follows:

Title	Description
Chapter 1 Overview	Provides an overview of Resource Orchestrator.
Chapter 2 Overview of Resource Orchestrator Setup Operations	Explains the overall flow of setup operations when using Resource Orchestrator.
Chapter 3 Resource Orchestrator Setup Design	Explains how to design a Resource Orchestrator installation.
Chapter 4 Pre-setup Preparations	Explains how to design and prepare a Resource Orchestrator installation.
Chapter 5 Installation and Uninstallation	Explains how to install and uninstall Resource Orchestrator.
Chapter 6 Configuration After Installation	Explains configuration after installing Resource Orchestrator.
Chapter 7 Resource Orchestrator login	Explains how to log in to Resource Orchestrator.
Chapter 8 Setup	Explains how to set up Resource Orchestrator.
Appendix A Port List	Describes the ports used by Resource Orchestrator.
Appendix B HTTPS Communications	Explains the security features of the HTTPS communication protocol used by Resource Orchestrator.
Appendix C Hardware Configuration	Explains how to configure hardware.
Appendix D Design and Configuration when Creating a Physical L-Server	Explains how to perform design and configuration when creating a physical L-Server.
Appendix E Design and Configuration when Creating a Virtual L-Server	Explains how to perform design and configuration when creating a virtual L-Server.
Appendix F Installation of VM Hosts on Physical L-Servers	Explains how to install VM hosts on physical L-Servers.
Appendix G User Management Using Directory Service	Explains how to manage users using the directory service.
Appendix H Basic Mode	Explains Basic mode.
Appendix I Definition Files	Explains how to configure definition files.
Appendix J Notes on Installation	Explains points to keep in mind when setting up a Resource Orchestrator environment.
Appendix K Dashboard Customization	Explains how to customize the dashboard.

Title	Description
Appendix L Co-Existence with ServerView Deployment Manager	Explains how to use both Resource Orchestrator and ServerView Deployment Manager on the same network.
Glossary	Explains the terms used in this manual. Please refer to it when necessary.

Notational Conventions

The notation in this manual conforms to the following conventions.

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

[Windows]	Sections related to Windows (When not using Hyper-V)
[Linux]	Sections related to Linux
[VMware]	Sections related to VMware
[Hyper-V]	Sections related to Hyper-V
[Xen]	Sections related to RHEL5-Xen
[KVM]	Sections related to RHEL-KVM
[Oracle VM]	Sections related to Oracle VM
[Windows/Hyper-V]	Sections related to Windows and Hyper-V
[Windows/Linux]	Sections related to Windows and Linux
[Linux/VMware]	Sections related to Linux and VMware
[Xen/KVM]	Sections related to RHEL5-Xen and RHEL-KVM
[VM host]	Sections related to Windows Server 2008 with VMware or Hyper-V enabled

- Unless specified otherwise, the blade servers mentioned in this manual refer to PRIMERGY BX servers.
- References and character strings or values requiring emphasis are indicated using double quotes (").
- Window names, dialog names, menu names, and tab names are shown enclosed by brackets ([]).
- Button names are shown enclosed by angle brackets (< >) or square brackets ([]).
- The order of selecting menus is indicated using []-[] .
- Text to be entered by the user is indicated using bold text.
- Variables are indicated using italic text and underscores.
- The ellipses ("...") in menu names, indicating settings and operation window startup, are not shown.
- The ">" used in Windows is included in usage examples. When using Linux, read ">" as meaning "#".

Menus in the ROR console

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

Documentation Road Map

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

Manual Name	Abbreviated Form	Purpose
ServerView Resource Orchestrator Cloud Edition V3.0.0 Setup Guide	Setup Guide CE	Please read this first. Read this when you want information about the purposes and uses of basic functions, and how to install Resource Orchestrator.
ServerView Resource Orchestrator Cloud Edition V3.0.0 Installation Guide	Installation Guide CE	Read this when you want information about how to install Resource Orchestrator.
ServerView Resource Orchestrator Cloud Edition V3.0.0 Operation Guide	Operation Guide CE	Read this when you want information about how to operate systems that you have configured.
ServerView Resource Orchestrator Cloud Edition V3.0.0 User's Guide for Infrastructure Administrators (Resource Management)	User's Guide for Infrastructure Administrators (Resource Management) CE	Read this when you want information about how to operate the GUI (resource management) used by infrastructure administrators and dual-role administrators.
ServerView Resource Orchestrator Cloud Edition V3.0.0 User's Guide for Infrastructure Administrators	User's Guide for Infrastructure Administrators CE	Read this when you want information about how to operate the GUI (for operations other than resource management) used by infrastructure administrators and dual-role administrators.
ServerView Resource Orchestrator Cloud Edition V3.0.0 User's Guide for Tenant Administrators	User's Guide for Tenant Administrators CE	Read this when you want information about how to operate the GUI used by tenant administrators.
ServerView Resource Orchestrator Cloud Edition V3.0.0 User's Guide for Tenant Users	User's Guide for Tenant Users CE	Read this when you want information about how to operate the GUI used by tenant users.
ServerView Resource Orchestrator Cloud Edition V3.0.0 Reference Guide for Infrastructure Administrators (Resource Management)	Reference Guide (Resource Management) CE	Read this when you want information about commands used by infrastructure administrators and dual-role administrators to manage resources, messages output by the system, and how to perform troubleshooting.
ServerView Resource Orchestrator Cloud Edition V3.0.0 Reference Guide for Infrastructure Administrators	Reference Guide CE	Read this when you want information about the commands used by infrastructure administrators and dual-role administrators for operations other than resource management.
ServerView Resource Orchestrator Cloud Edition V3.0.0 Messages	Messages CE	Read this when you want detailed information about the corrective actions for displayed messages.

In some cases this manual may ask you to refer to the following Virtual Edition manuals.
Please refer to them when necessary:

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

Manual Name	Abbreviated Form	Purpose
ServerView Resource Orchestrator Virtual Edition V3.0.0 Messages	Messages VE	Read this when you want detailed information about the corrective actions for displayed messages.

Related Documentation

Please refer to these manuals when necessary.

- Administration Manual
- Interstage Application Server Security System Guide
- Interstage Application Server Reference Manual (Command Edition)
- Interstage Business Process Manager Analytics V11.1 Management Console Guide
- When using VMware
 - vSphere Basic System Administration
 - vSphere Resource Management Guide
 - Guest Operating System Installation Guide
- When using the Linux virtual machine function of Red Hat(R) Enterprise Linux(R) 5.4 (for x86) or Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64)
 - Red Hat Enterprise Linux 5 Virtualization Guide
 - Systemwalker Software Configuration Manager Operation Guide
- When using KVM virtual machine functions
 - Red Hat Enterprise Linux 6 Virtualization Administration Guide
 - Red Hat Enterprise Linux 6 Virtualization Getting Started Guide
 - Red Hat Enterprise Linux 6 Virtualization Host Configuration and Guest Installation Guide
- When using Oracle VM
 - Oracle VM Manager User's Guide
 - Oracle VM Server User's Guide
- When using NetApp storage
 - Data ONTAP Software Setup Guide
 - Data ONTAP System Administration Guide
 - Data ONTAP Storage Management Guide
 - Data ONTAP Block Access Management Guide for iSCSI and FC
- When using ETERNUS storage
 - ETERNUS SF Storage Cruiser User's Guide
 - ETERNUS SF Storage Cruiser Message Guide
 - ETERNUS SF Express V15.0/ AdvancedCopy Manager Operation Guide for Copy Control Module
- When using ServerView Suite
 - User Management in ServerView

Abbreviations

The following abbreviations are used in this manual:

Abbreviation	Products
Windows	Microsoft(R) Windows Server(R) 2008 Standard Microsoft(R) Windows Server(R) 2008 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Datacenter Microsoft(R) Windows Server(R) 2003 R2, Standard Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition Windows(R) 7 Professional Windows(R) 7 Ultimate Windows Vista(R) Business Windows Vista(R) Enterprise Windows Vista(R) Ultimate Microsoft(R) Windows(R) XP Professional operating system
Windows Server 2008	Microsoft(R) Windows Server(R) 2008 Standard Microsoft(R) Windows Server(R) 2008 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Datacenter
Windows 2008 x86 Edition	Microsoft(R) Windows Server(R) 2008 Standard (x86) Microsoft(R) Windows Server(R) 2008 Enterprise (x86)
Windows 2008 x64 Edition	Microsoft(R) Windows Server(R) 2008 Standard (x64) Microsoft(R) Windows Server(R) 2008 Enterprise (x64)
Windows Server 2003	Microsoft(R) Windows Server(R) 2003 R2, Standard Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
Windows 2003 x64 Edition	Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
Windows 7	Windows(R) 7 Professional Windows(R) 7 Ultimate
Windows Vista	Windows Vista(R) Business Windows Vista(R) Enterprise Windows Vista(R) Ultimate
Windows XP	Microsoft(R) Windows(R) XP Professional operating system
Linux	Red Hat(R) Enterprise Linux(R) 5 (for x86) Red Hat(R) Enterprise Linux(R) 5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.1 (for x86) Red Hat(R) Enterprise Linux(R) 5.1 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.2 (for x86) Red Hat(R) Enterprise Linux(R) 5.2 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.3 (for x86) Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.4 (for x86) Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.6 (for x86)

Abbreviation	Products
	Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.7 (for x86) Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64) Red Hat(R) Enterprise Linux(R) 6.2 (for x86) Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64) SUSE(R) Linux Enterprise Server 11 for x86 SUSE(R) Linux Enterprise Server 11 for EM64T
Red Hat Enterprise Linux	Red Hat(R) Enterprise Linux(R) 5 (for x86) Red Hat(R) Enterprise Linux(R) 5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.1 (for x86) Red Hat(R) Enterprise Linux(R) 5.1 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.2 (for x86) Red Hat(R) Enterprise Linux(R) 5.2 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.3 (for x86) Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.4 (for x86) Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.6 (for x86) Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.7 (for x86) Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64) Red Hat(R) Enterprise Linux(R) 6.2 (for x86) Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64)
Red Hat Enterprise Linux 5	Red Hat(R) Enterprise Linux(R) 5 (for x86) Red Hat(R) Enterprise Linux(R) 5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.1 (for x86) Red Hat(R) Enterprise Linux(R) 5.1 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.2 (for x86) Red Hat(R) Enterprise Linux(R) 5.2 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.3 (for x86) Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.4 (for x86) Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.6 (for x86) Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.7 (for x86) Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64)
Red Hat Enterprise Linux 6	Red Hat(R) Enterprise Linux(R) 6.2 (for x86) Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64)
RHEL5-Xen	Red Hat(R) Enterprise Linux(R) 5.4 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64) Linux Virtual Machine Function
RHEL-KVM	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
DOS	Microsoft(R) MS-DOS(R) operating system, DR DOS(R)
SUSE Linux Enterprise Server	SUSE(R) Linux Enterprise Server 11 for x86 SUSE(R) Linux Enterprise Server 11 for EM64T
Oracle VM	Oracle VM Server for x86
ESC	ETERNUS SF Storage Cruiser

Abbreviation	Products
GLS	PRIMECLUSTER GLS
Navisphere	EMC Navisphere Manager
Solutions Enabler	EMC Solutions Enabler
MSFC	Microsoft Failover Cluster
SCVMM	System Center Virtual Machine Manager 2008 R2 System Center 2012 Virtual Machine Manager
VMware	VMware vSphere(R) 4 VMware vSphere(R) 4.1 VMware vSphere(R) 5
VMware FT	VMware Fault Tolerance
VMware DRS	VMware Distributed Resource Scheduler
VMware DPM	VMware Distributed Power Management
VMware vDS	VMware vNetwork Distributed Switch
VIOM	ServerView Virtual-IO Manager
ServerView Agent	ServerView SNMP Agents for MS Windows (32bit-64bit) ServerView Agents Linux ServerView Agents VMware for VMware ESX Server
ROR VE	ServerView Resource Orchestrator Virtual Edition
ROR CE	ServerView Resource Orchestrator Cloud Edition
Resource Coordinator	Systemwalker Resource Coordinator Systemwalker Resource Coordinator Virtual server Edition

Export Administration Regulation Declaration

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

Trademark Information

- EMC, EMC², CLARiiON, Symmetrix, and Navisphere are trademarks or registered trademarks of EMC Corporation.
- HP is a registered trademark of Hewlett-Packard Company.
- Linux is a trademark or registered trademark of Linus Torvalds in the United States and other countries.
- Microsoft, Windows, MS, MS-DOS, Windows XP, Windows Server, Windows Vista, Windows 7, Excel, Active Directory, and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.
- NetApp is a registered trademark of Network Appliance, Inc. in the US and other countries. Data ONTAP, Network Appliance, and Snapshot are trademarks of Network Appliance, Inc. in the US and other countries.
- Oracle and Java are registered trademarks of Oracle and/or its affiliates in the United States and other countries.
- 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.
- SUSE is a registered trademark of SUSE LINUX AG, a Novell business.
- VMware, the VMware "boxes" logo and design, Virtual SMP, and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.
- ServerView and Systemwalker are registered trademarks of FUJITSU LIMITED.

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

Notices

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

Month/Year Issued, Edition	Manual Code
November 2011, First Edition	J2X1-7610-01ENZ0(00)
December 2011, 1.1	J2X1-7610-01ENZ0(01)
January 2012, 1.2	J2X1-7610-01ENZ0(02)
February 2012, 1.3	J2X1-7610-01ENZ0(03)
March 2012, 1.4	J2X1-7610-01ENZ0(04)
April 2012, 1.5	J2X1-7610-01ENZ0(05)
March 2013, 1.6	J2X1-7610-01ENZ0(06)

Copyright FUJITSU LIMITED 2010-2013

Contents

Chapter 1 Overview.....	1
1.1 Features.....	1
1.2 Function Overview.....	1
1.2.1 Resource Management.....	4
1.2.2 Resource Pool.....	8
1.2.3 L-Servers.....	9
1.2.4 L-Platform.....	12
1.2.5 Templates.....	12
1.2.6 Resource Visualization.....	13
1.2.7 Simplifying Networks.....	13
1.2.8 Simplifying Storage.....	17
1.2.9 Tenants.....	18
1.2.10 Resource Visualization (Dashboard).....	18
1.2.11 Disaster Recovery.....	18
1.3 Function Differences Depending on Product.....	18
1.4 Software Environment.....	20
1.4.1 Software Organization.....	20
1.4.2 Software Requirements.....	20
1.4.2.1 Required Basic Software.....	20
1.4.2.2 Required Software.....	30
1.4.2.3 Exclusive Software.....	38
1.4.2.4 Static Disk Space.....	45
1.4.2.5 Dynamic Disk Space.....	46
1.4.2.6 Memory Size.....	48
1.5 Hardware Environment.....	49
1.6 System Configuration.....	52
Chapter 2 Overview of Resource Orchestrator Setup Operations.....	57
Chapter 3 Resource Orchestrator Setup Design.....	61
3.1 System Configuration Design.....	61
3.2 Tenant and Resource Pool Design.....	61
3.2.1 Overview of Tenants.....	61
3.2.2 Tenant Operation.....	63
3.2.3 Global Pool and Local Pool Selection Policy.....	67
3.2.4 Resource Pool Types.....	68
3.2.5 Subdividing Resource Pools.....	68
3.2.6 Concept for Separating Tenants by Resource Pool.....	68
3.2.6.1 Server Pool.....	68
3.2.6.2 VM Pool.....	69
3.2.6.3 Storage Pool.....	69
3.2.6.4 Network Pool.....	69
3.2.6.5 Address Pool.....	69
3.2.6.6 Image Pool.....	70
3.3 Defining User Accounts.....	70
3.4 High Availability and Disaster Recovery Design.....	71
3.4.1 Blade Chassis High Availability Design.....	71
3.4.2 Storage Chassis High Availability Design.....	72
3.4.3 Admin Server High Availability Design.....	73
3.4.4 Disaster Recovery Design.....	75
Chapter 4 Pre-setup Preparations.....	77
4.1 Defining and Configuring the Server Environment.....	77
4.1.1 Defining the Server Environment.....	77
4.1.1.1 Preparations for Server Environments.....	77

4.1.1.2 Chassis Settings (for Blade Server Environments).....	78
4.1.1.3 Settings for Rack Mount or Tower Servers.....	78
4.1.1.4 Chassis Setting Values (For PRIMEQUEST).....	79
4.1.2 Configuring the Server Environment.....	80
4.2 Defining and Configuring the Network Environment.....	82
4.2.1 Defining the Network Environment.....	82
4.2.1.1 Admin LAN Network Design.....	84
4.2.1.2 Virtual System Design.....	89
4.2.1.3 Physical Network Design for the Public LAN and iSCSI LAN.....	91
4.2.1.4 Relationship between Physical Network Configuration and Resources.....	94
4.2.2 Defining Configuration Settings for Devices.....	96
4.2.2.1 Settings for the Admin Server.....	97
4.2.2.2 Settings for Admin Clients.....	97
4.2.2.3 Settings for Managed Network Devices.....	97
4.2.2.4 Settings for Unmanaged Network Devices.....	100
4.2.2.5 Settings for Managed Servers.....	103
4.2.2.6 Settings for LAN Switch Blades on Managed Blade Systems.....	103
4.2.2.7 Settings for Managed Storage Units.....	104
4.2.2.8 Settings for Other Managed Hardware.....	104
4.2.3 Pre-configuring Devices.....	104
4.2.3.1 Pre-configuring Admin Servers.....	105
4.2.3.2 Pre-configuring Admin Clients.....	105
4.2.3.3 Pre-configuring Managed Network Devices.....	105
4.2.3.4 Pre-configuring Unmanaged Network Devices.....	105
4.2.3.5 Pre-configuring Managed Servers.....	105
4.2.3.6 Pre-configuring LAN Switch Blades on Managed Blade Systems.....	105
4.2.3.7 Pre-configuring Managed Storage Units.....	110
4.2.3.8 Pre-configuring Other Managed Hardware.....	111
4.2.3.9 Pre-configuration for Making iSCSI LAN Usable.....	111
4.2.4 Preparations for Resource Orchestrator Network Environments.....	111
4.2.4.1 When Automatically Configuring the Network.....	112
4.2.4.2 When Using IBP.....	121
4.2.4.3 When Using an iSCSI LAN for iSCSI Boot.....	122
4.2.4.4 When Using Link Aggregation.....	123
4.2.4.5 When Using NICs other than Those in the Default Configuration of the Automatic Network Configuration.....	123
4.2.4.6 When Using Automatic Virtual Switch Configuration on Rack Mount or Tower Servers.....	123
4.2.4.7 When Deploying L-Servers even if the Service Console and Port Group are the Same.....	123
4.2.4.8 When Registering Network Devices as Resources.....	124
4.2.4.9 When Automatically Configuring Network Devices.....	126
4.2.5 When Providing IPv6 Network for Public LANs.....	135
4.3 Deciding and Configuring the Storage Environment.....	137
4.3.1 Deciding the Storage Environment.....	137
4.3.1.1 Storage Environment Preparation.....	137
4.3.1.2 Storage Configuration.....	140
4.3.1.3 HBA and Storage Device Settings.....	144
4.3.1.4 iSCSI Interface and Storage Device Settings (iSCSI).....	146
4.3.2 Configuring the Storage Environment.....	148
4.4 Deciding and Configuring Server Virtualization Software.....	149
4.4.1 Deciding Server Virtualization Software.....	149
4.4.2 Configuring Server Virtualization Software.....	150
4.5 Installing and Configuring Single Sign-On.....	152
4.5.1 Deciding the Directory Service to Use.....	152
4.5.2 Setting up ServerView Operations Manager and Directory Service Environments.....	152
4.5.2.1 Coordination with the User Registration Directory Service.....	152
4.5.2.2 To Use a User already Registered with Active Directory as a Resource Orchestrator User.....	153
4.5.2.3 Single Sign-On When Using the ServerView Operations Manager Console.....	154
4.5.2.4 When Installing ServerView Operations Manager Again.....	155

4.5.3 Preparing Certificates.....	155
4.5.4 Registering Administrators.....	156
4.5.5 When Reconfiguring Single Sign-On.....	157
4.5.5.1 Confirming Certificates.....	157
4.5.5.2 Registering Certificates.....	158
4.5.5.3 Checking Directory Service Connection Information.....	161
4.5.5.4 Modifying Directory Service Connection Information.....	161
4.5.5.5 When Certificates Have Expired.....	162
4.5.6 Updating from Earlier Versions.....	162
4.5.6.1 Registering CA Certificates of ServerView Operations Manager 1.....	164
4.5.6.2 Registering CA Certificates of ServerView Operations Manager 2.....	166
4.5.6.3 Registering CA Certificate of Individually Configured OpenDS or Active Directory 1.....	167
4.5.6.4 Registering CA Certificate of Individually Configured OpenDS or Active Directory 2.....	168
4.5.6.5 Moving Information in the Directory Service Used in Earlier Versions.....	169
4.5.6.6 Registering Users in the Directory Service.....	169
4.5.6.7 Registering Directory Service Connection Information in Resource Orchestrator.....	171
4.5.6.8 Changing Already Registered Directory Service Connection Information.....	172
4.5.6.9 Allocating Roles to Tenant Administrator.....	173
Chapter 5 Installation/Uninstallation.....	174
Chapter 6 Configuration after Installation.....	175
6.1 Creating Definition Files.....	175
6.1.1 Creating Definition Files Combining Ports of SAN Storage.....	175
6.1.2 Creating Definition Files for Registering Network Devices.....	177
6.1.3 Creating Model Definition Files for Network Devices.....	177
6.2 Preparations for the Network Device Automatic Configuration Function.....	177
6.2.1 Creating a Folder for Registering Rulesets.....	177
6.2.2 Registering Sample Scripts.....	177
6.3 SSL Communication Environment Settings.....	178
6.3.1 Stop Web Server.....	178
6.3.2 Setting the Interstage Certificate Environment Access Permissions [Linux].....	179
6.3.3 Getting and Registering a Certificate.....	179
6.3.3.1 Getting a Certificate from the Certificate Authority.....	179
6.3.3.2 Creating Test Site Certificates.....	183
6.3.4 Creating SSL Definitions.....	184
6.3.5 Importing a Certificate to ServerView SSO Authentication Server.....	185
6.3.6 Start the Web server.....	187
6.4 Settings for Sending E-mail.....	187
6.4.1 Stopping the Manager.....	188
6.4.2 Settings for Email Sent from Tenant Management.....	188
6.4.3 Settings for Email Sent from the L-Platform Management Window.....	189
6.4.4 Starting the Manager.....	190
6.4.5 Settings for Email Sent via the Application Process.....	190
6.4.6 Settings for Email Sent from the Dashboard.....	192
6.5 Application Process Settings.....	193
6.5.1 Registering an Application Process Assessor.....	193
6.5.1.1 Creating an infrastructure administrator/dual-role administrator.....	193
6.5.1.2 Adding an infrastructure administrator/dual-role administrator to IflowUsers Group.....	194
6.5.2 Stopping the Manager.....	195
6.5.3 Setting Application process settings.....	195
6.5.4 Setting Application process to be used.....	196
6.5.5 Starting the Manager.....	197
6.6 Customizing the Dashboard.....	197
Chapter 7 Logging in to Resource Orchestrator.....	198
7.1 Login.....	198
7.2 Starting and Stopping the Manager.....	200

7.3 Starting and Stopping the Agent.....	203
7.4 Importing a Certificate to a Browser.....	204
Chapter 8 Setup.....	206
8.1 Registering Resources with Resource Orchestrator.....	206
8.1.1 Managed Resources and Registration Order.....	207
8.1.1.1 Managed Resources.....	207
8.1.1.2 Necessity of Resource Registration.....	207
8.1.1.3 Registration Order and Registration Method for Resources.....	208
8.2 HBA address rename Settings.....	211
8.2.1 Settings for the HBA address rename Setup Service.....	214
8.3 Software Installation and Agent Registration.....	216
8.4 Registering Resources to the Global Pool.....	218
8.5 Creating L-Server Templates.....	220
8.6 Collecting and Registering Cloning Images.....	220
8.6.1 When Collecting Cloning Images from Physical L-Servers.....	221
8.6.2 When Collecting Cloning Images from Virtual L-Servers.....	227
8.6.3 When Registering a Cloning Image Created from a Physical Server in Advance to the Image Pool.....	229
8.6.4 When Registering an Image (Template) Created with VM Management Software in Advance to the Image Pool.....	229
8.7 Creating L-Platform Templates.....	230
8.8 Saving Environment Settings.....	230
Appendix A Port List.....	231
Appendix B HTTPS Communications.....	242
Appendix C Hardware Configuration.....	247
C.1 Connections between Server Network Interfaces and LAN Switch Ports.....	247
C.2 WWN Allocation Order during HBA address rename Configuration.....	248
C.3 Using Link Aggregation.....	249
C.3.1 Configuration of Link Aggregation and a Server.....	249
C.3.2 Preparations.....	250
C.3.3 Operating Resource Orchestrator.....	253
Appendix D Design and Configuration when Creating a Physical L-Server.....	254
D.1 System Configuration.....	254
D.2 Pre-setup Preparations (Servers).....	259
D.3 Pre-setup Preparations (Storage).....	260
D.3.1 When Using ETERNUS Storage.....	261
D.3.2 When Using NetApp FAS Storage.....	262
D.3.3 When Using EMC CLARiiON Storage.....	264
D.3.4 When Using EMC Symmetrix DMX Storage or EMC Symmetrix VMAX Storage.....	267
D.4 Pre-setup Preparations (Network).....	268
D.5 Configuration after Installation.....	271
D.5.1 Definition Files.....	271
D.6 Setup.....	280
D.6.1 Automatic Network Configuration.....	282
D.6.2 Manual Network Configuration.....	285
D.7 Creating an L-Server.....	285
D.7.1 Installation of an Operating System Using PXE Boot.....	287
D.7.2 Cloning Images.....	289
D.7.3 [OS] Tab Configuration.....	289
D.7.4 Network Redundancy and VLAN Settings of L-Servers.....	289
D.8 Selection of Physical Servers for Physical L-Servers.....	293
D.9 Advisory Notes for Creation of Physical L-Servers.....	294
Appendix E Design and Configuration for Creating Virtual L-Servers.....	296
E.1 Common Functions of Server Virtualization Software.....	296
E.1.1 Definition Files.....	296

E.2 VMware.....	307
E.2.1 System Configuration.....	307
E.2.2 Preparations.....	312
E.2.3 Installation.....	318
E.2.4 Configuration after Installation.....	318
E.2.5 Setup.....	321
E.2.6 Advisory Notes for VMware Usage.....	335
E.2.7 Overcommit.....	336
E.3 Hyper-V.....	339
E.3.1 System Configuration.....	339
E.3.2 Preparations.....	345
E.3.3 Installation.....	350
E.3.4 Setup.....	350
E.3.5 Advisory Notes for Hyper-V Usage.....	373
E.3.6 Overcommit.....	376
E.4 RHEL5-Xen.....	380
E.4.1 System Configuration.....	380
E.4.2 Preparations.....	382
E.4.3 Installation.....	383
E.4.4 Setup.....	383
E.4.5 Advisory Notes for RHEL5-Xen Usage.....	388
E.5 Oracle VM.....	389
E.5.1 System Configuration.....	389
E.5.2 Preparations.....	390
E.5.3 Installation.....	392
E.5.4 Setup.....	392
E.5.5 Advisory Notes for Oracle VM Usage.....	397
E.6 KVM.....	400
E.6.1 System Configuration.....	401
E.6.2 Preparations.....	403
E.6.3 Installation.....	405
E.6.4 Setup.....	406
E.6.5 Advisory Notes for RHEL-KVM Usage.....	411
E.6.6 Overcommit.....	412
Appendix F Installation of VM Hosts on Physical L-Servers.....	413
F.1 Installation.....	413
F.2 Changing Configuration.....	415
F.3 Deletion.....	415
F.4 Advisory Notes for Installation of VM Hosts on Physical L-Servers.....	415
Appendix G User Management Using Directory Service.....	416
G.1 Installation Method.....	416
G.2 User Confirmation of Directory Service Server.....	416
G.3 Importing Certificates.....	416
G.4 Manager Configuration.....	420
G.5 Migration from Internal Authentication Function to Directory Service.....	421
Appendix H Basic Mode.....	426
H.1 Overview.....	426
H.2 User Account Design Using the Internal Authentication Function.....	426
Appendix I Definition Files.....	427
Appendix J Notes on Installation.....	431
Appendix K To Customize Dashboard.....	432
K.1 Building the Dashboard Development Environment.....	432
K.1.1 Installing the Dashboard Development Environment.....	432

K.1.2 Setting up the Dashboard Development Environment.....	443
K.2 To Customize Dashboard.....	446
K.2.1 Customizing Email Send Settings.....	446
K.2.2 Customizing Threshold Values.....	449
K.2.3 Customizing Monitored Pools.....	450
K.3 Backup and Restore the Dashboard Development Environment.....	452
K.3.1 Backup the Definition Information.....	452
K.3.2 Restore the Definition Information.....	452
K.4 Uninstalling the Dashboard Development Environment.....	452
K.4.1 Uninstall the Interstage Business Process Manager Analytics Client.....	453
K.4.2 Uninstall Interstage Business Process Manager Studio.....	453
K.4.3 Uninstall JRE 5.0.....	454
Appendix L Co-Existence with ServerView Deployment Manager.....	455
L.1 Overview.....	455
L.2 Restricted Functions.....	456
Glossary.....	457

Chapter 1 Overview

This chapter provides an overview of Resource Orchestrator.

1.1 Features

Resource Orchestrator centrally manages private clouds and data center resources (servers, storage, and networks). This dynamic resource management software manages these resources as resource pools, reducing infrastructure costs, and strengthening ICT governance.

This section explains some of the features provided by Resource Orchestrator.

Speedy Support for Evolving Businesses

Resource Orchestrator promptly provides servers (with storage and networks) according to the user's specific needs by managing resources, such as servers, storage, networks, and images (*1), as resource pools. By simplifying the launch, expansion, and change of business operations, this software provides quick support for evolving businesses.

*1: A copy of the contents of a disk (including the operating system) collected from a server, which can be deployed to other servers.

Reduced Infrastructure Investment Costs

Resource Orchestrator provides complete visualization of servers, storage resources, and network resources, making the state of each of these resources visible to users. This allows for the effective use of unused resources and planning for the installation of required resources. Moreover, infrastructure investment costs are reduced, since resources that could not be diverted to other uses can be used effectively.

Reduced Infrastructure Operational Costs

Resource Orchestrator provides a template which defines logical specifications (number of CPUs, memory capacity, disk capacity, number of NICs, etc.) for servers with storage and networks. Using this template to standardize the configuration of a system including servers, storage, and networks, offers the following benefits:

- Simplified configuration of systems.
- Reduced risk of mistakes by using proven values for parameter settings when installing an operating system or setting up storage and networks.
- Reduced infrastructure operational costs by using a unified configuration for managing versions of security software or backup methods over multiple systems.

Practicing ICT Governance

Resource Orchestrator can perform security management, including user and role management and access control, regardless of the platform size. Pooled resources can be divided and secured by user (tenant), enabling operation in accordance with ICT governance.

Integrated Operation and Monitoring of Physical and Virtual Resources

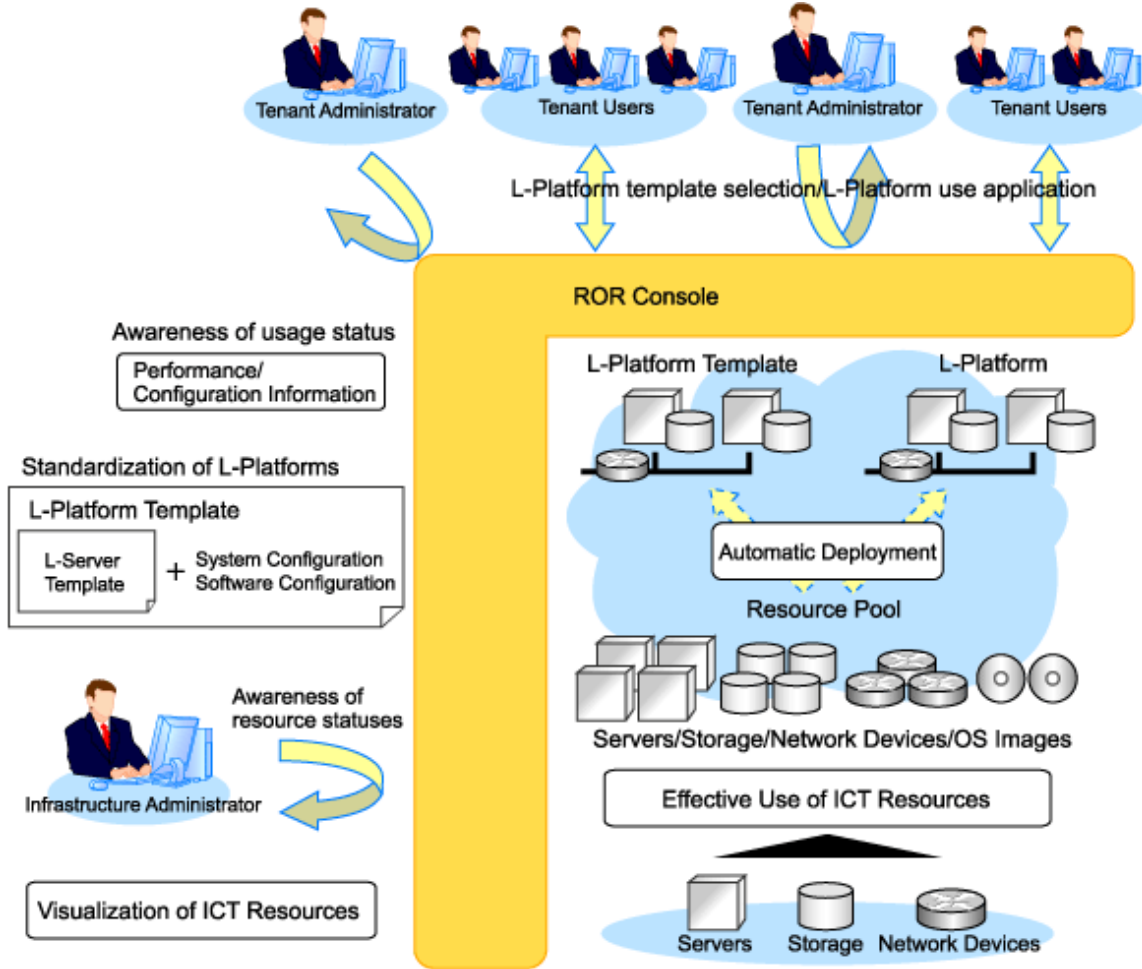
Even in environments with both physical and virtual resources, unified operations can be performed from one console for central management.

1.2 Function Overview

This section explains the Resource Orchestrator user roles and the functions available to each user.

The Resource Orchestrator user roles and the functions available to each user are as follow:

Figure 1.1 Resource Orchestrator User Roles and the Functions Available to Each User



For details on Resource Orchestrator user roles and the functions available for use, refer to "B.2 Roles and Available Operations" in the "Operation Guide CE".

The functions available to the majority of Resource Orchestrator users are as follow:

Table 1.1 Available Functions

Main Function	Description	Target Users
Use L-Platforms	L-Platforms that meet one's needs can be used, as necessary.	Tenant Users
Standardize L-Platforms (L-Platform templates)	Templates can be created for a hierarchical system configuration and OS logical configuration.	Tenant Administrators
Safe use of ICT resources by tenants in multiple departments	ICT resources can be shared by multiple departments while maintaining security.	Tenant Administrators
Effective use of ICT resources	ICT resources can be managed as a collection of resources (resource pool). They can be used effectively, according to changes in usage.	Infrastructure Administrators
Visualization of ICT resources	The status of ICT resource usage can be easily checked from the dashboard. The availability of resource pools can be monitored on the dashboard.	Infrastructure Administrators

Infrastructure Administrators

Resource Orchestrator provides a Logical Server (hereinafter L-Server) function which defines logical specifications (number of CPUs, memory capacity, disk capacity, number of NICs, etc.) for ICT resources within a private cloud (servers, storage, and networks). The system of L-Servers arranged in a hierarchy is called L-Platform.

Infrastructure administrators manage the ICT resources within a private cloud (servers, storage, and networks) and the operating systems running on L-Platforms.

Using Resource Orchestrator, infrastructure administrators collectively manage ICT resources in resource pools, while monitoring the load and performing addition, replacement, and maintenance of ICT resources when necessary.

These operations are performed from the ROR console.

The ROR console is used to manage ICT resources.

The following functions are provided by the ROR console:

- [Dashboard] tab

A function for checking the availability of resource pools. Displays the availability of the global pool. Global pools are resource pools containing resources that can be used by multiple tenants.

- [Usage Condition] tab

A function for checking the activity status of L-Platforms. Displays the activity status of L-Platforms for the entire system.

- [Resource] tab

A function used to manage the following:

- Resource pools
- Relationship between L-Platforms and resources
- Relationship between L-Servers and resources

- [Template] tab

A function for managing L-Platform templates. Used to create or modify L-Platforms for shared use over the entire system.

- [L-Platform] tab

A function for L-Platform usage applications and management.

- [Request] tab

Infrastructure administrators review applications.

System Operation Administrators

System operation administrators manage the operation of the entire system. Administrator privileges for the operating system are required.

Normally the roles of the infrastructure administrator and system operation administrator are performed concurrently.

Tenant Administrators

Tenant administrators prepare a pre-defined L-Platform environment template (L-Platform template) according to tenant user needs, and release it to tenant users.

In accordance with the application process, tenant administrators may also receive and review applications from tenant users.

Tenant administrators can check the usage status and monitor the operational statuses of tenant users.

Checking and monitoring the statuses of tenant users is performed from the ROR console.

- [Dashboard] tab

Displays the availability of the local pools allocated to a tenant.

- [Usage Condition] tab

Displays the activity status of the L-Platforms in a tenant.

- [Template] tab

L-Platform templates can be edited and released to tenant users as tenant specific L-Platform templates.

- [L-Platform] tab

Applications to use and management of L-Platforms in a tenant can be performed.

- [Request] tab

Tenant administrators authorize applications.

Tenant Users

Tenant users can apply to use L-Platforms, and use L-Platforms configured according to their application.

When the authorization of the tenant administration department manager is required for an application, tenant users must request authorization from the manager in accordance with the application process.

L-Platforms are accessed from the ROR console.

- [L-Platform] tab

Applications to use L-Platforms and L-Platform operations can be performed.

- [Request] tab

Displays the application status for L-Platforms.

1.2.1 Resource Management

The following functions are provided by Resource Orchestrator.

For details on the operational environment for Resource Orchestrator, refer to "[1.4 Software Environment](#)" and "[1.5 Hardware Environment](#)".

Table 1.2 List of Available Functions

Function	Functional Overview	Remarks
Resource pools	A function that enables you to use all resources effectively and efficiently.	For details, refer to " 1.2.2 Resource Pool ".
L-Server creation	A function that provides L-Servers, logical servers including physical and virtual servers, which are comprised of appropriate resources in a resource pool, such as servers, storage, OS images and network. Even if there are no resources to allocate to L-Servers, flexible configuration and operation, such as creating L-Server definitions in advance, is possible.	For details on L-Servers, refer to " 1.2.3 L-Servers ". For details on allocating and releasing resources to and from L-Servers, refer to "11.8 Allocating and Releasing Resources to L-Servers" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".
L-Server templates	A function that enables pre-definition of L-Server specifications (number of CPUs, memory capacity, disk capacity, number of NICs, etc.) to simplify L-Server creation.	For details, refer to " 1.2.5 Templates ".
Resource visualization	A function that displays the total size and the free space of the resources in a resource pool.	For details, refer to " 1.2.6 Resource Visualization ".
Simplifying network settings	A function that provides automatic configuration of network settings used for connecting network devices or creating L-Servers.	For details, refer to " 1.2.7 Simplifying Networks ".
Simplifying storage settings	To use storage from a physical L-Server, configure storage units and storage networks.	For details, refer to " 1.2.8 Simplifying Storage ".

Function	Functional Overview	Remarks
Changing physical server usage	This function enables effective use of server resources as the operating systems and software that are started on physical servers can be changed depending on the time and situation.	For details, refer to "11.9 Changing Physical Server Usage" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".
Linking L-Servers with configured physical servers or virtual machines	Enables uniform management of configured physical servers or virtual machines as L-Servers by linking them to an L-Server.	For details, refer to "Chapter 16 Linking L-Servers with Configured Physical Servers or Virtual Machines" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".
Managing multiple resources using resource folders	A function for managing clustered multiple resources.	For details, refer to "Chapter 13 Resource Folder and Tenant Operations" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".
Restricting access using roles	A function for configuring roles (a collection of available operations) and access scopes (resources which can be operated) for individual users. A large number of users can be configured as a single unit using user groups that manage multiple users.	For details, refer to "Appendix B Access Control by Roles" of the "Operation Guide CE".
Sharing and dividing resources between multiple departments using tenants	A tenant is a unit for division of management and operation of resources based on organizations or operations. This function enables secure operation of sharing and dividing resources between multiple departments.	Refer to "3.2 Tenant and Resource Pool Design" and "Chapter 3 Managing Tenants" in the "Operation Guide CE".
Managing and sharing user information using LDAP coordination	By using a directory service which supports LDAP, such as Active Directory, user information can be managed and shared with other services.	For details, refer to "Appendix G User Management Using Directory Service".
Realization of high availability	Functions to enable high availability systems, with features such as L-Server and admin server redundancy, server switchover for chassis failures, and storage switchover.	For details, refer to "3.4 High Availability and Disaster Recovery Design".
DR (Disaster Recovery)	Preparing a backup system (a backup site) at remote sites to handle fatal damage caused by disasters enables administrators to perform switchover when trouble occurs.	For details, refer to "Chapter 15 Disaster Recovery" in the "Operation Guide CE".
Monitoring	A function for monitoring resource statuses of servers and displaying if the status is normal or not by using the GUI.	For details, refer to "Chapter 10 Monitoring Resources" of the "Operation Guide CE".
Power control	A function for turning servers ON or OFF.	Refer to "11.1 Power Operations" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".
Hardware maintenance	Functions to simplify hardware replacement. When connected with a SAN, it is not necessary to re-configure storage units by configuring the I/O virtualization settings. By using VIOM, it is not necessary to change the settings of software or network devices to refer to MAC addresses, as the MAC address, boot settings, and network settings are automatically changed. VM host maintenance can be easily performed, using VM Home Positions.	For details, refer to "Chapter 7 Hardware Maintenance" of the "Operation Guide CE".

Function	Functional Overview	Remarks
Network device monitoring	<p>A function for monitoring resource statuses of network devices and displaying if the status is normal or not on the GUI. Periodic or SNMP trap monitoring can be specified when network devices are registered or changed.</p> <ul style="list-style-type: none"> - Periodic monitoring Network devices are periodically monitored. - Alive monitoring Executes the "ping" command to the network device, and determines the existence of the device based on the response. - Status monitoring Collects MIB information for the device with SNMP, and determines the status from the MIB information. - SNMP trap monitoring Status monitoring (SNMP monitoring) is performed for SNMP trap (issued by the network device) reception. 	<p>For details, refer to "10.2 Monitoring Networks" of the "Operation Guide CE" and "Chapter 1 User Interface" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".</p> <p>For details on how to specify the monitoring method, refer to "2.6 Network Configuration Information" of the "Reference Guide (Resource Management) CE".</p>
Network maintenance	A function for maintaining network devices.	For details, refer to "Chapter 7 Hardware Maintenance" of the "Operation Guide CE".
L-Server console screen	The L-Server console screen that displays the information of physical and virtual L-Servers can be opened with common, simple operations from the Resource Orchestrator screen.	For details, refer to "11.3 Using the L-Server Console" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Managed Resources

Resource Orchestrator can be used to manage the resources described in the table below.

For details on management of chassis, servers, VM hosts, VM management software, and LAN switches (LAN switch blades), refer to ["Chapter 4 Pre-setup Preparations"](#).

Table 1.3 Managed Resources

Resource	Description
Chassis	A chassis is an enclosure used to house server blades. It can monitor the statuses of servers, display their properties, and control their power states.
Physical server	<p>This is a general term for any physical server. This term is used to distinguish physical servers from virtual machines that are created using server virtualization software such as VMware or Hyper-V. The following usage methods are available for physical servers:</p> <ul style="list-style-type: none"> - Managing unused physical servers as L-Servers by registering them with Resource Orchestrator - Managing configured physical servers by linking them to L-Servers <p>VM hosts and physical OS's running on physical servers can be detected and registered as managed resources by Resource Orchestrator.</p>
VM host	<p>This refers to the server virtualization software running on a server to operate a virtual machine. For example, Windows Server 2008 R2, VMware ESX for VMware, domain 0 for RHEL5-Xen, VM hosts for RHEL-KVM, or Oracle VM Server with Hyper-V roles added.</p> <p>VM hosts can be managed by monitoring their statuses, displaying their properties, and performing operations such as HBA address rename and server switchover.</p>

Resource	Description
	When a VM host is registered, any VM guests on the VM host are automatically detected and displayed in the server tree. The power and migration operations of VM guests can be performed from the server tree, however, detected VM guests cannot perform operations as L-Servers.
VM management software	This software manages multiple server virtualization software. For example, for VMware, it is vCenter Server, for Hyper-V, it is SCVMM, and for Oracle VM, it is Oracle VM Manager. VM management software can be integrated (registered) into Resource Orchestrator to enable the use of functions for VM guests.
LAN switch (LAN switch blade)	The network switches that are mounted in a blade server chassis (LAN switch blades). Resource Orchestrator can monitor LAN switch blade statuses, display their properties, and manage their VLAN configurations. The following information is displayed in a comprehensive Network Map: <ul style="list-style-type: none"> - Network configurations of physical servers and virtual machines (Virtual switches, VM Guests) - Statuses of network connections between resources - VLAN configuration status within physical servers and virtual machines
VM guest	This refers to the operating system running on a virtual machine. Resource Orchestrator can monitor VM guest statuses, display their properties, and control their power states. In addition to the functions of ROR VE, the following functions are available for use: <ul style="list-style-type: none"> - Managing new VM guests as L-Servers - Managing configured virtual machines by linking them to L-Servers
Virtual switch	This is a virtual switch used to manage a VM guest network on the VM host. In Hyper-V, it represents the concept of virtual networks. It supports virtual switches, which are standard Hyper-V virtual network and VMware functions. Cisco Nexus 1000V virtual switches are not supported.
Disk resources	This refers to a disk resource allocated to a server. For EMC CLARiiON and ETERNUS storage, this is a LUN, for NetApp storage it is a FlexVol, for EMC Symmetrix DMX or EMC Symmetrix VMAX storage it is a device, and for VM guests it is a virtual disk.
Virtual storage resources	This refers to a resource that can create a disk resource. Examples include RAID groups, aggregates, DSK groups, and file systems for creating VM (VMFS (datastore) of VMware, etc.). Disk resources can be created from RAID groups of ETERNUS storage, aggregates of NetApp storage, and file systems for creating VM.
Storage management software	Software to manage and integrate one or multiple storage units. For EMC CLARiiON storage, they are Navisphere, for EMC Symmetrix DMX storage or EMC Symmetrix VMAX storage, it is Solutions Enabler, for ETERNUS storage, it is ETERNUS SF Storage Cruiser, and for NetApp storage, it is Data ONTAP. Integration (registration) with Resource Orchestrator enables the use of functions for basic management of storage units.
Network resources	This refers to a resource that defines network information for use by an L-Server or a network device. By connecting the NIC for an L-Server to a network resource, the physical and virtual network switches are configured, enabling the L-Server to communicate. If an IP address range is set for a network resource, the IP address can be automatically set when deploying an image to an L-Server.
Network device resources	This refers to a resource that defines a network device. Firewalls and L2 switches (except for LAN switch blades) are included. It is possible to monitor the statuses of network devices, display their properties, and perform automatic configuration.
Address set resources	WWNs and MAC addresses. Necessary when creating physical L-Servers.
Virtual image resources	An image that is created using a template from a VM management software for VM guest creation, or that is collected as a cloning image from an L-Server.

Resource	Description
Physical image resources	An image that is collected as a cloning image from an L-Server.

1.2.2 Resource Pool

A resource pool is a collection of physical servers, VM hosts, storage, networks, images, and other resources of the same type.

Resource pools offer the following benefits.

Until now, launching or expanding business operations required the purchase of servers, storage, networks, and other resources. Furthermore, significant time and effort was spent preparing and organizing such operations. Resource Orchestrator can save you time and effort by enabling you to configure a server simply by removing the required resource from a resource pool. This allows you to effectively plan the organization and operation of your infrastructure environment.

The resource pool management function allows you to effectively and efficiently use all resources. The types of resource pools are as described in "[Table 1.4 Resource Pool Types](#)". For details, refer to "Chapter 12 Resource Pool Operations" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

By using Resource Orchestrator to first register resources to control in a resource pool, an appropriate resource can be created from the resource pool at a user's request and be used to quickly configure a server (with storage and networks). When the server is no longer required, the resource can be reused.

Multiple resource pools can be created depending on operational requirements (hardware type, security, resource management units). If the resources in a resource pool are insufficient, a new resource can be added or a resource can be moved from another resource pool to compensate.

Table 1.4 Resource Pool Types

Resource Pool Types	Overview
VM	<p>A resource pool for storing VM hosts used when creating new servers (VM). VM hosts of different server virtualization software can be stored.</p> <p>In VM pools where different server virtualization software exists, an appropriate VM host can be selected and an L-Server created by specifying VM type during L-Server creation.</p> <p>Moving an L-Server (migration) is only possible between VM hosts belonging to the same cluster group, when two or more cluster groups are registered in the same VM pool.</p>
Servers	<p>A resource pool for storing the physical servers used when creating new servers.</p>
Storage	<p>Virtual storage resources and disk resources can be managed using Resource Orchestrator. Virtual storage resources indicate such as RAID groups controlled by storage management software, and file systems for VM guests controlled by VM management software. The resources can be managed as virtual storage resources using the same operations.</p> <p>A disk resource refers to a disk resource allocated to a server.</p> <ul style="list-style-type: none"> - When using ETERNUS storage, NetApp storage, and EMC CLARiiON LUN (Logical Unit Number) - When using EMC Symmetrix DMX or EMX Symmetrix VMAX Device - For VM guests Virtual Disk <p>In Resource Orchestrator, use the following procedure to allocate a disk resource to an L-Server:</p> <ul style="list-style-type: none"> - Create the required size of disk resources from the virtual storage resource, and allocate them to the L-Server - Allocate the disk created in advance using storage management software to the L-Server <p>The following virtual storage resources are stored in storage pools:</p> <ul style="list-style-type: none"> - For VM

Resource Pool Types	Overview
	<p>A file system for creation of VMs and virtual disks such as VMFS (datastore) of VMware, shared volumes for clusters of Hyper-V, or storage repositories of Oracle VM</p> <ul style="list-style-type: none"> - For physical servers An original resource used to create LUN such as ETERNUS RAID groups or NetApp aggregates on storage units <p>The following disk resources are stored in storage pools:</p> <ul style="list-style-type: none"> - For physical servers Resources for the disk to be allocated to the server, such as a LUN of ETERNUS and EMC CLARiiON, a FlexVol of NetApp, or a device of EMC Symmetrix DMX or EMC Symmetrix VMAX
Network	<p>The following resources are stored:</p> <ul style="list-style-type: none"> - Network resources - Network devices (Firewalls)
Address	<p>The following resources are stored:</p> <ul style="list-style-type: none"> - MAC address (Media Access Control address) - WWN
Image	<p>The following resources are stored:</p> <ul style="list-style-type: none"> - Cloning images

1.2.3 L-Servers

Resource Orchestrator can be used to create Logical Servers which define the logical specifications (number of CPUs, memory capacity, disk capacity, number of NICs, etc.) for servers (with storage and networks).

Resources can be allocated to an L-Server according to defined specifications. An L-Server with allocated resources can perform the same operations as a normal physical server and a virtual machine.

In addition, configured physical servers and virtual machines can be managed by linking them with L-Servers.

To operate the server, L-Server users only need to be aware of the specifications defined for the server, and not the resources allocated to it.

The following advantages are gained by using L-Servers:

- Simple and rapid server configuration

The ideal server can be configured simply and quickly by automatically allocating resources from resource pools according to the L-Server defined specifications.

- Reduced management costs

L-Server users do not need to manage the resources allocated to the server. Moreover, resource management is performed by an infrastructure administrator, reducing overall management costs.

- Integrated operation of physical servers and virtual machines

L-Servers can be created for both physical servers and virtual machines.

- An L-Server created using a physical server is called a "physical L-Server".
- An L-Server created using a virtual machine is called a "virtual L-Server".

After creating L-Servers, operations can be performed without differentiation between physical servers and virtual machines.

Information

Resources from resource pools can be automatically allocated or specific resources can be manually allocated to an L-Server.

L-Server Creation

By specifying server specifications (number of CPUs, memory capacity or model type), storage capacity, operating system image, and network connections, Resource Orchestrator quickly creates a practical L-Server using the applicable resources from resource pools. It is possible to choose from two operational methods: (1) only create the configuration definition of an L-Server. In this case, resources are allocated to it when it is powered on for the first time; (2) create an L-Server with resources allocated. In this case, the L-Server will be ready for use after creation.

Resources can be selected using the following two methods:

- Automatic assignment
- Specifying resources or resource pools by each user

L-Server specifications can be specified by the following two methods.

- Selecting an L-Server template

For details on how to create an L-Server using an L-Server template (with L-Server specifications pre-defined), refer to "10.1 Creation Using an L-Server Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- Manually specifying each L-Server specification without using an L-Server template

For details on how to create an L-Server individually (without using an L-Server template), refer to "10.2 Creation of Physical L-Servers Using Parameters" or "10.3 Creation of Virtual L-Servers Using Parameters" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Basic operations, such as startup, shutdown, and delete, can be performed for an L-Server in the same way as for a typical server. L-Server users do not require detailed knowledge of the resources allocated to the server in order to operate it.

The following operations can be performed:

- Changing of L-Server configurations

Configurations of resources to allocate to the L-Server can be changed.

Refer to "11.2 Modifying an L-Server" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- Moving an L-Server between servers (migration) (For virtual L-Servers)

The function that moves a virtual L-Server to another VM host without stopping it.

For details, refer to "11.7 Migration of VM Hosts between Servers" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- Snapshot (For virtual L-Servers)

The function that saves the content of the system disk and data disk of a virtual L-Server disk at a certain point of time.

For details, refer to "11.6.1 Snapshot" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- Backup (For physical L-Servers)

The function that saves the system disk of a physical L-Server.

For details, refer to "11.6.2 Backup and Restore" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

When determining the location of an L-Server, Resource Orchestrator first selects a VM pool.

The VM pool and VM host to use for the L-Server can be selected using the following two methods:

- When the VM host on which L-Server will be operated is not specified (when Resource Orchestrator automatically selects the VM host)

When multiple VM pools are accessible, the priority for L-Server creation can be specified for individual VM pools in advance. Resource Orchestrator selects the location from the VM pools, using the order of priority (1 is the highest, 10 lowest). When multiple VM pools have the same priority, the VM pool is selected at random.

- When the VM host on which an L-Server will be operated is specified (when Resource Orchestrator creates an L-Server on the specified VM host)

Select the location from the specified VM pools or VM hosts.

Then, determine the VM host on which the L-Server is to be placed.

The destination VM host must meet the following conditions:

- The VM host is powered on
- Monitoring status is "normal"
- Maintenance mode is not set

For details on maintenance mode, refer to "Appendix B Maintenance Mode" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- Maintenance mode has not been set for the server virtualization software

When a VM host is specified for "VM host", the capacity of the VM host is checked, and then the L-Server is created.

- When using L-Server templates

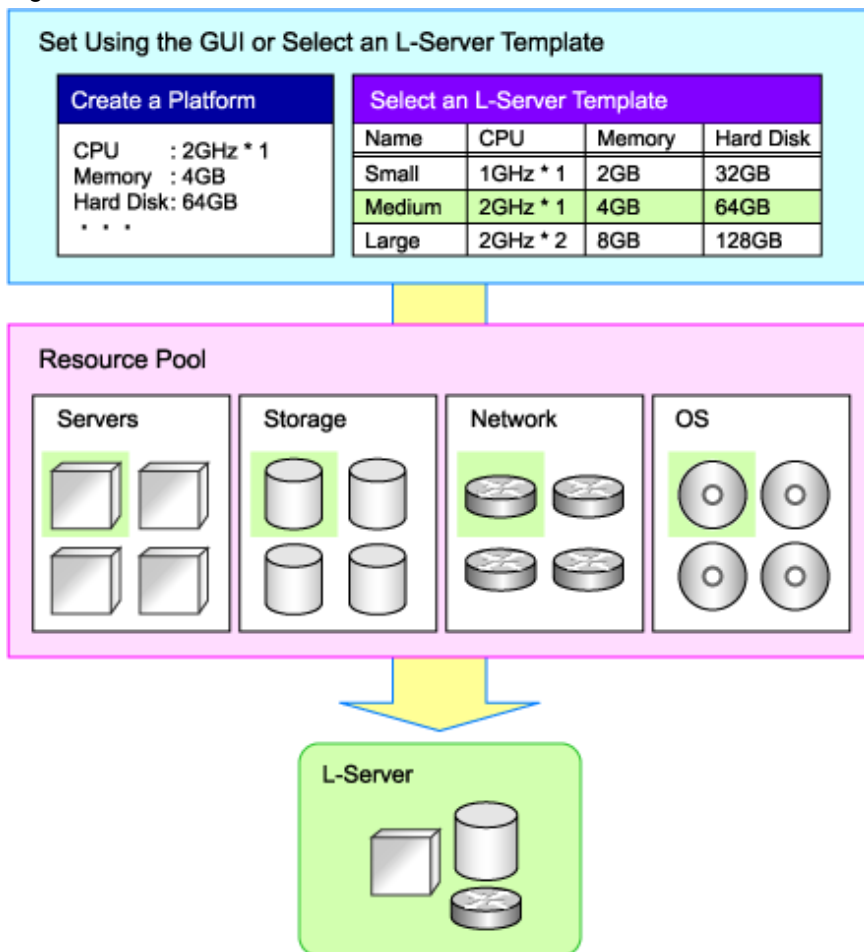
The VM host on which another L-Server that was created from the same L-Server template is placed is searched for, and then the L-Server is created.

If there is insufficient space on the VM host, a VM host that has more capacity is searched for, and then the L-Server is created.

- When not using L-Server templates

A VM host that has more capacity is searched for, and then the L-Server is created.

Figure 1.2 L-Server Creation



1.2.4 L-Platform

This section explains L-Platforms.

An L-Platform is a hierarchical system (Web/AP/DB).

Resource Orchestrator can be used to deploy and operate L-Platforms.

An L-Platform defines the following combination of resources:

- L-Server

Resource Orchestrator can be used to define a Logical Server which defines the logical specifications (number of CPUs, memory capacity, disk capacity, number of NICs, etc.) for servers (with storage and networks).

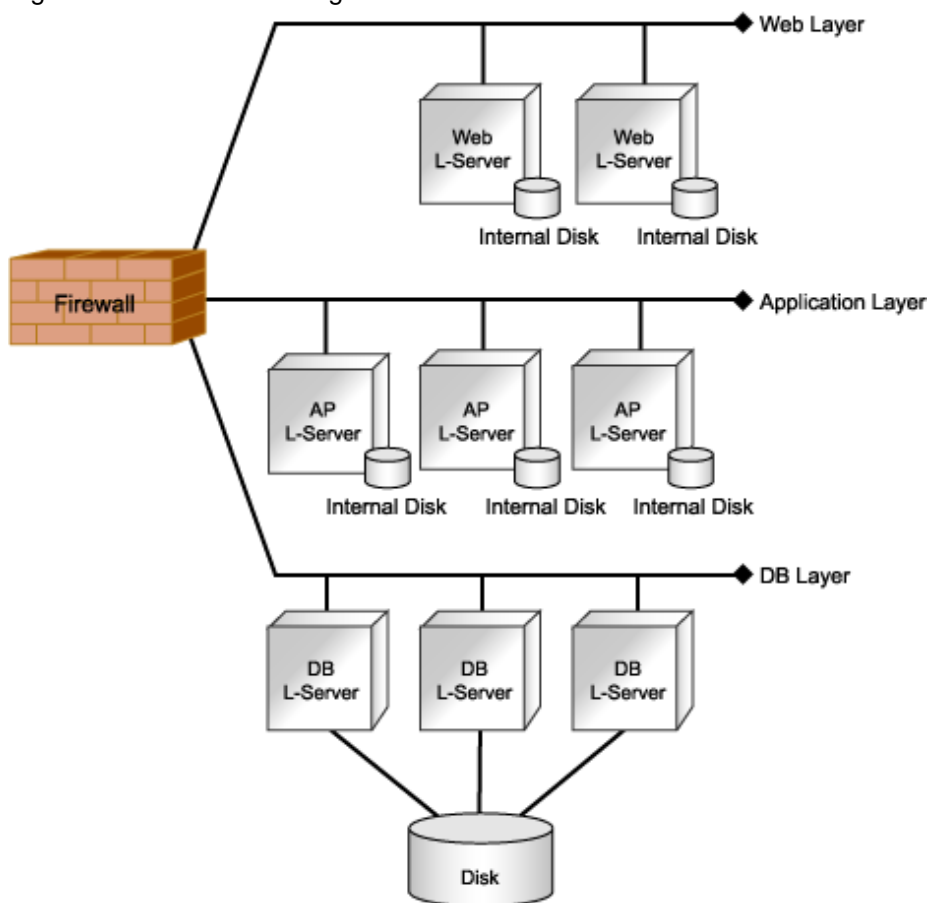
For details on L-Servers, refer to "1.2.3 L-Servers".

- Firewall Resources

In a hierarchical system, this resource ensures the security of each tier.

The configuration of an L-Platform is shown below.

Figure 1.3 L-Platform Configuration



1.2.5 Templates

This section explains templates.

The following templates can be used with Resource Orchestrator:

- L-Platform Templates

- L-Server Templates

L-Platform Templates

An L-Platform template defines L-Platform specifications.

L-Platform templates enable standardization of L-Platform specifications and easy creation of L-Platforms.

For the format of L-Platform templates and how to create L-Platform templates, refer to "Chapter 5 Template" in the "User's Guide for Infrastructure Administrators CE".

L-Server Templates

An L-Server template defines the specifications of the L-Servers comprising the L-Platform.

Specify an L-Server template when creating an L-Platform template.

For the format of L-Server templates, refer to "2.2 L-Server Template" of the "Reference Guide (Resource Management) CE".

For how to create L-Server templates, refer to "8.1.2 Creating a Template" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

1.2.6 Resource Visualization

Resource Orchestrator includes the ROR console graphical user interface.

The total size and the free space of the resources in the resource pool are displayed. The number of L-Servers that can be created for each L-Server template can also be displayed, in units of the specified L-Server template.

For details on the L-Server conversion view, refer to "12.4 Viewing a Resource Pool" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

For details on the ROR console, refer to "1.1 ROR Console Layout" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

1.2.7 Simplifying Networks

VLAN or IP address settings for LAN switch blades, virtual switches, and L2 switches is automatically performed based on the definition information of network resources in Resource Orchestrator. For L2 switches and firewalls, configuring, modifying, or deleting the definitions that include VLAN settings is automatically performed using scripts. A script is prepared for each model of the network devices by infrastructure administrators.

Timing of Automatic Network Settings

The simplified network settings will be executed when the following operations are performed:

Table 1.5 Timing of Automatic Network Settings Execution

Target	Operation	L-Server (IP Address Settings for OS)	Virtual Switch (Creation/VLAN Settings)	LAN Switch Blade (VLAN Settings)	L2 Switches (Overall Settings)	Firewall (Overall Settings)
Network resources	Creation	-	-	Yes (*1)	Yes (*2)	-
	Modification	-	-	Yes (*1)	Yes (*2)	-
	Deletion	-	Yes	-	Yes (*2)	-
Virtual L-Server	Creation	Yes	Yes	Yes	-	-
	Modification	-	-	-	-	-
	Deletion	-	-	-	-	-
Physical L-Servers	Creation	Yes	-	Yes	Yes (*2, *3)	-
	Modification	-	-	Yes	-	-
	Deletion	-	-	Yes	Yes (*2, *3)	-

Target	Operation	L-Server (IP Address Settings for OS)	Virtual Switch (Creation/VLAN Settings)	LAN Switch Blade (VLAN Settings)	L2 Switches (Overall Settings)	Firewall (Overall Settings)
L-Platform	Creation	Yes	Yes (*4)	Yes	-	Yes (*2)
	Modification	-	Yes (*4)	Yes (*5)	-	Yes (*2)
	Deletion	-	-	Yes (*5)	-	Yes (*2)

Yes: Available

-.: Not Available

*1: When automatic network settings and automatic VLAN settings for uplink ports are enabled, settings are automatically configured at the point when an uplink port (including an uplink port with link aggregation configured) is added.

*2: Modification is performed based on a script prepared for each device name (or model name).

*3: Available when using rack mount servers.

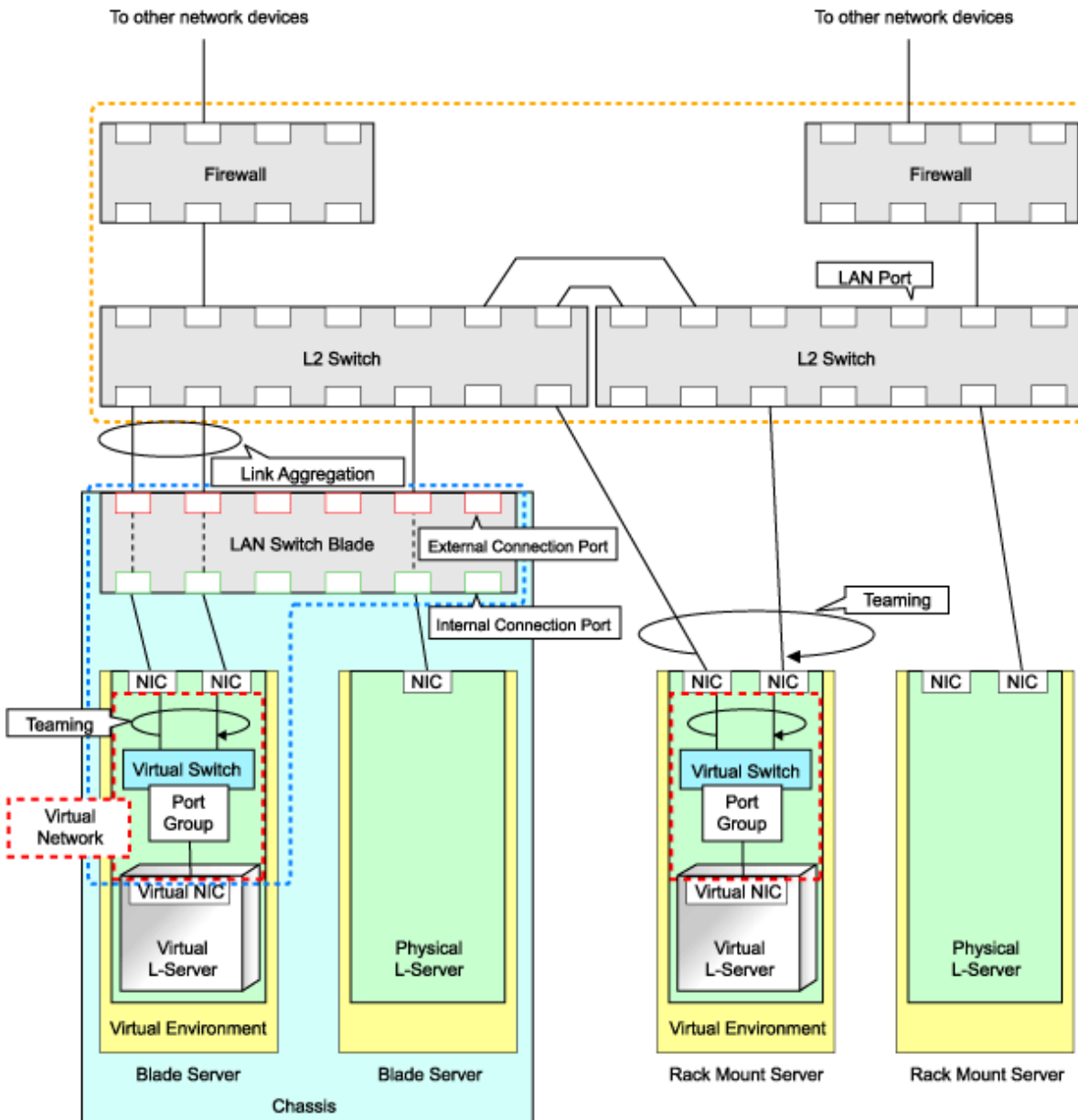
*4: Available when using virtual L-Servers.


*5: Available when using physical L-Servers.


Scope of Automatic Network Settings

The simplifying network settings will be executed for the following scope.

Figure 1.4 Scope of Automatic Network Settings Execution



 : Scope of automatic configuration using network resources

 : Scope of automatic configuration using the scripts prepared for each network device

For details on automatic network settings for virtualized environments, refer to the relevant sections explaining how to prepare and setup server virtualization software in "[Appendix E Design and Configuration for Creating Virtual L-Servers](#)".

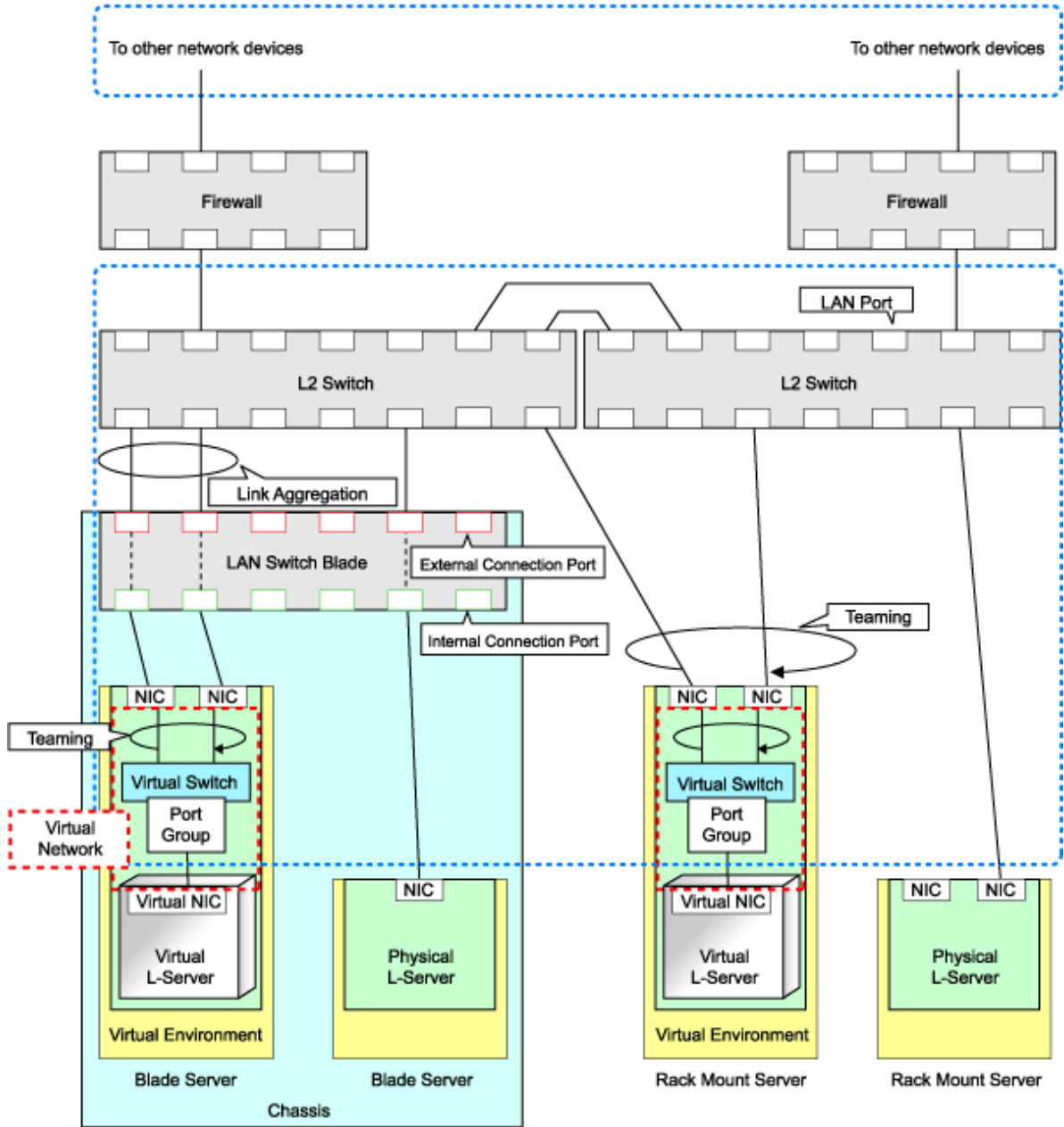
Hiding Network Information


The following network information is hidden, depending on the network resource.

- Virtual Switches
- Port Groups
- LAN Switch Blades

- L2 Switches

Figure 1.5 Hiding of Network Device Information



 : Scope of hiding by network resources

Network Device Automatic Configuration

For network devices (Firewalls and L2 switches), the following are automatically configured by registered scripts in Resource Orchestrator. Scripts need to be prepared beforehand by infrastructure administrators.

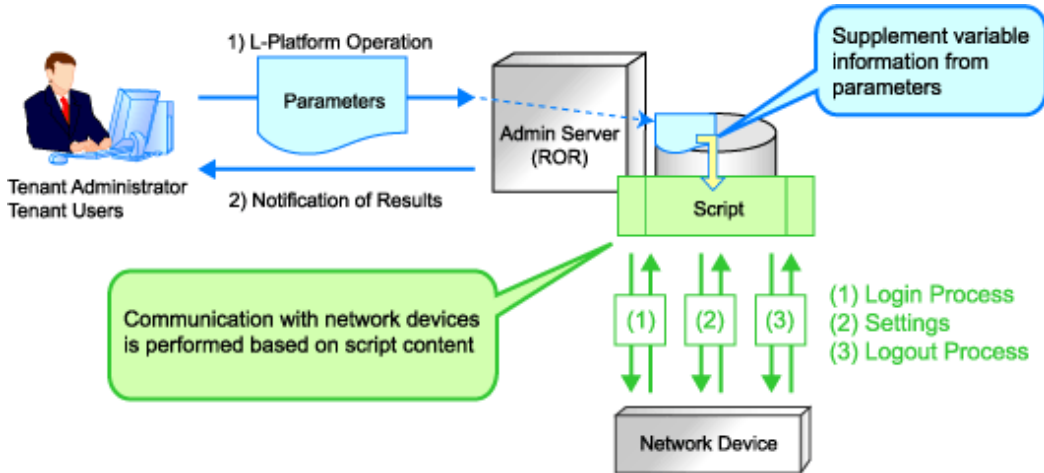
- Automatic configuration for firewalls when creation, modification, or deletion of an L-Platform is performed

The detailed timing is as follows:

- When an L-Platform is created from an L-Platform template that includes a network device (firewall)
- When L-Server addition or deletion is performed for an L-Platform

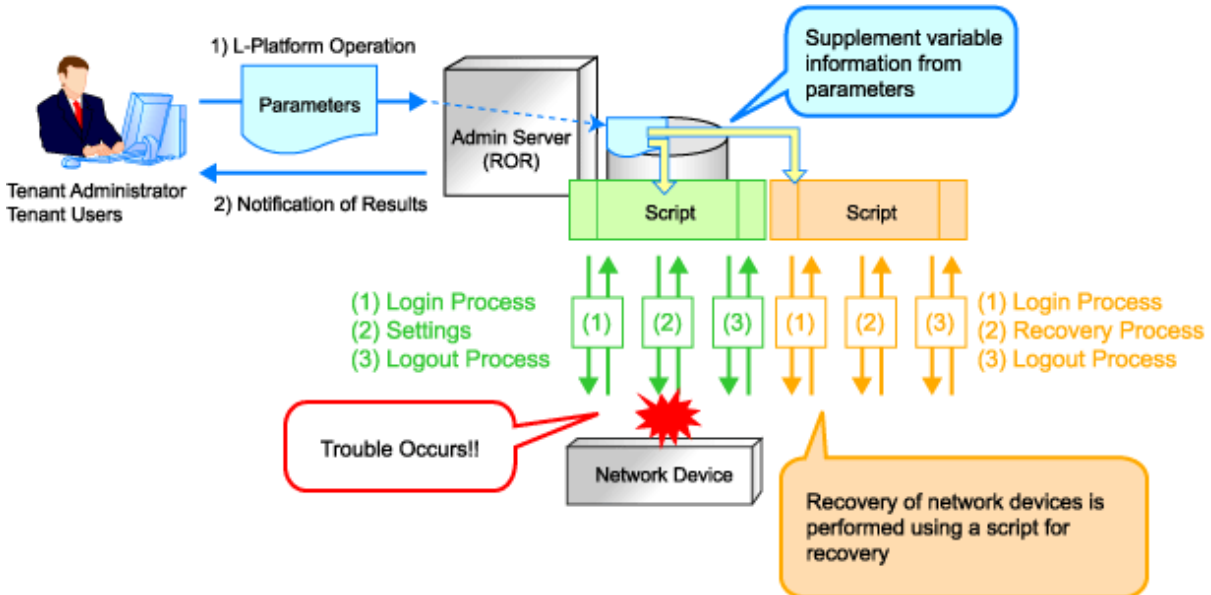
- When a network device (firewall) in an L-Platform is modified
- When an L-Platform created from an L-Platform template that includes a network device (firewall) is deleted
- Automatic configuration for L2 switches when creation, modification, or deletion of a network resource is performed
- Automatic configuration for L2 switches when creation or modification of a physical L-Server is performed on rack mount servers

Figure 1.6 Network Device Automatic Configuration Image



Recovery (deletion of incomplete settings, etc.) of network devices can be performed by preparing a recovery script in advance in case automatic configuration of network devices fails.

Figure 1.7 Network Device Automatic Configuration Image (Recovery Process)



1.2.8 Simplifying Storage

This section provides a brief overview of simplified storage setup.

When creating physical servers and virtual machines, it was difficult to smoothly provide servers as configuration of storage units and the storage network was necessary.

Resource Orchestrator enables quick allocation of storage through coordination with storage management software or VM management software.

For details, refer to "4.3 Deciding and Configuring the Storage Environment".

1.2.9 Tenants

This section explains tenants.

You may want to share some resources between departments in case of future changes or faults while maintaining the segregation of resources for each department.

A tenant is the unit for division of management and operation of resources based on organizations or operations.

An L-Platform and an exclusive resource pool for each tenant are stored in a tenant. The exclusive resource pool for each tenant is called a local pool.

There are resource pools which can be used by multiple tenants including local pools. These resource pools are called global pools.

Resources can be divided and used effectively by tenants using local pools and global pools.

For details, refer to "[3.2 Tenant and Resource Pool Design](#)".

For creating, modifying, and deleting tenants, refer to "Chapter 8 Tenants" of the "User's Guide for Infrastructure Administrators CE".

1.2.10 Resource Visualization (Dashboard)

This section explains resource visualization.

The availability of resource pools can be checked with ease from the [Dashboard] tab of the ROR console.

For how to operate the [Dashboard] tab of the ROR console, refer to the "User's Guide for Infrastructure Administrators CE".

1.2.11 Disaster Recovery

Resource Orchestrator provides simple and highly reliable Disaster Recovery.

For details, refer to "[3.4.4 Disaster Recovery Design](#)".

1.3 Function Differences Depending on Product

The functions available for Resource Orchestrator differ depending on the Resource Orchestrator product purchased.

The functions available for ServerView Resource Orchestrator Virtual Edition (hereinafter ROR VE) and ServerView Resource Orchestrator Cloud Edition (hereinafter ROR CE) differ as follows:

Table 1.6 Function Differences Depending on Product

Function	Description	ROR VE	ROR CE
Server monitoring	A function for monitoring resource statuses of servers and displaying if the status is normal or not by using the GUI.	Yes	Yes
Power control	A function for turning servers ON or OFF.	Yes	Yes
Backup and restore	Creates system image backups of servers that can be easily restored when needed. System images are centrally stored on a disk on the admin server.	Yes	Yes
Hardware maintenance	Functions to simplify hardware replacement.	Yes	Yes
Server switchover	Recover applications upon hardware failure by switching over primary servers with pre-assigned spare servers.	Yes	Yes (*1)
Cloning	Creates a cloning image of a reference server and deploys it to other managed servers. Cloning images are centrally stored on a disk on the admin server.	Yes	Yes (*2)
Resource pool	A function for effective use of resources.	No	Yes
L-Server	A function that provides L-Servers, logical servers including physical and virtual servers, which are comprised of appropriate resources in a resource pool, such as servers, storage, OS images and network.	No	Yes
L-Platform	A function that provides hierarchical systems comprised of multiple L-Servers, network resources, and network device resources.	No	Yes

Function	Description	ROR VE	ROR CE
Template	A function that defines L-Platform and L-Server specifications to enable simple configuration of L-Platforms and L-Servers.	No	Yes
Tenants	A function that enables multiple departments to divide and share resources safely.	No	Yes
Dashboard	A function that can be used to easily check resource statuses.	No	Yes
Disaster Recovery	A function that prepares a backup system (a backup site) at remote sites to handle fatal damage caused by disasters, enabling administrators to perform switchover when trouble occurs.	No	Yes (*3)

*1: Available for physical servers registered in the server tree. For details, refer to "Chapter 8 Server Switchover Settings" of the "User's Guide VE".

*2: Available for physical servers registered in the server tree. For details, refer to "Chapter 7 Cloning [Windows/Linux]" of the "User's Guide VE".

*3: Available when the Disaster Recovery option is purchased.

The support provided for managed server hardware and server virtualization software differs for ROR VE and ROR CE.

The functions of ROR VE can be used with ROR CE, even with hardware and server virtualization software that is not supported.

Example

When using SPARC Enterprise series servers for ROR CE, server management operations, such as server maintenance and switchover can be performed. However, resource pool management operations are not available.

Table 1.7 Managed Server Hardware Differences Depending on Product

Software	Hardware	ROR VE	ROR CE (*1)
Manager	PRIMERGY RX series/BX series/TX series	Yes	Yes
	PRIMEQUEST	Yes	Yes
Agent	PRIMERGY RX series/BX series/TX series	Yes	Yes
	Other PC servers	Yes	Yes
	PRIMEQUEST	Yes	Yes
	SPARC Enterprise series	Yes	No

*1: For details, refer to "1.5 Hardware Environment".

Table 1.8 Server Virtualization Software Differences Depending on Product

Software	Server Virtualization Product	ROR VE	ROR CE (*1)
Agent	VMware	Yes	Yes
	Hyper-V	Yes	Yes
	RHEL-Xen	Yes	Yes
	RHEL-KVM	Yes	Yes
	Citrix XenServer	Yes	No
	Oracle VM	No	Yes

*1: For details, refer to "1.4.2.1 Required Basic Software".

1.4 Software Environment

Resource Orchestrator is composed of the following DVD-ROM.

- ServerView Resource Orchestrator (Windows version)
- ServerView Resource Orchestrator (Linux version)

1.4.1 Software Organization

Resource Orchestrator is composed of the following software.

Table 1.9 Software Organization

Software	Functional Overview
ServerView Resource Orchestrator V3.0 Manager (hereinafter manager)	<ul style="list-style-type: none">- Used to control managed servers and neighboring network devices- Manages resource pools and L-Servers- Operates on the admin server
ServerView Resource Orchestrator V3.0 Agent (hereinafter agent)	<ul style="list-style-type: none">- Performs pre-configuration during deployment, monitors operating servers, and controls backup and cloning- Operates on managed servers (*1)
ServerView Resource Orchestrator V3.0 HBA address rename setup service (hereinafter HBA address rename setup service)	<ul style="list-style-type: none">- Realization of high availability of the HBA address rename setup used by the admin server (*2)- Operates on a separate device from the admin server or managed servers, such as a desktop computer

*1: When using a combination of a manager of this version and agents of earlier versions, only operations provided by the agent version are guaranteed.

*2: For details on HBA address rename setup, refer to "[4.3.1 Deciding the Storage Environment](#)".

1.4.2 Software Requirements

This section explains the software requirements for installation of Resource Orchestrator.

1.4.2.1 Required Basic Software

The basic software listed below is required when using Resource Orchestrator.

Required Basic Software

Table 1.10 Manager [Windows]

Basic Software (OS)	Remarks
Microsoft(R) Windows Server(R) 2008 Standard (x86, x64) Microsoft(R) Windows Server(R) 2008 Enterprise (x86, x64) Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Datacenter	The Server Core installation option is not supported.

Table 1.11 Manager [Linux]

Basic Software (OS)	Remarks
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) 5.7 (for x86) Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64)	Prepare any required driver kits, update kits, or software.

Basic Software (OS)	Remarks
Red Hat(R) Enterprise Linux(R) 5.6 (for x86) Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.4 (for x86) Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64)	For information about required software, refer to the manual of the server or the Linux installation guide. About required packages, refer to " Table 1.32 Required Packages of Manager [Linux] ". The Linux Kernel version depending on the hardware corresponds to the version supported by Fujitsu.

Table 1.12 Agent [Windows]

Basic Software (OS)	Remarks
Microsoft(R) Windows Server(R) 2008 Standard (x86, x64) Microsoft(R) Windows Server(R) 2008 Enterprise (x86, x64) Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Datacenter	The Server Core installation option is not supported.
Microsoft(R) Windows Server(R) 2003 R2, Standard Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition	SP2 or later supported.

Table 1.13 Agent [Hyper-V]

Basic Software (OS)	Remarks
Microsoft(R) Windows Server(R) 2008 R2 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Datacenter	The Server Core installation option is not supported. Switch on the role of Hyper-V. Add MSFC. Only Windows managers are supported. When using dynamic memory and memory weight, Windows Server 2008 R2 Service Pack 1 (SP1) or later must be applied to the VM host, and SCVMM must be upgraded to System Center Virtual Machine Manager 2008 R2 Service Pack 1 (SP1) or later.

Table 1.14 Agent [Linux]

Basic Software (OS)	Remarks
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) 5.7 (for x86) Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.6 (for x86) Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.4 (for x86) Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.3 (for x86) Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.2 (for x86) Red Hat(R) Enterprise Linux(R) 5.2 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.1 (for x86)	Prepare any required driver kits, update kits, or software. For information about required software, refer to the manual of the server or the Linux installation guide. About required packages, refer to " Table 1.33 Required Packages of Agent [Linux] ". The Linux Kernel version depending on the hardware corresponds to the version supported by Fujitsu.

Basic Software (OS)	Remarks
Red Hat(R) Enterprise Linux(R) 5.1 (for Intel64) Red Hat(R) Enterprise Linux(R) 5 (for x86) Red Hat(R) Enterprise Linux(R) 5 (for Intel64)	
SUSE(R) Linux Enterprise Server 11 for x86 SUSE(R) Linux Enterprise Server 11 for EM64T	

Table 1.15 Agent [VMware]

Basic Software (OS)	Remarks
VMware vSphere (R) 4 VMware vSphere (R) 4.1 VMware vSphere (R) 5	Install Resource Orchestrator on the VMware ESX host.

Table 1.16 Agent [Xen/KVM]

Basic Software (OS)	Remarks
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) 5.7 (for x86) Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.6 (for x86) Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.4 (for x86) Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64)	-

Table 1.17 Agent [Oracle VM]

Basic Software (OS)	Remarks
Oracle VM 3.0	-

Table 1.18 HBA address rename setup service [Windows]

Basic Software (OS)	Remarks
Microsoft(R) Windows Server(R) 2008 Standard (x86, x64) Microsoft(R) Windows Server(R) 2008 Enterprise (x86, x64) Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Datacenter	The Server Core installation option is not supported.
Microsoft(R) Windows Server(R) 2003 R2, Standard Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition	SP2 or later supported.
Microsoft(R) Windows Vista(R) Business Microsoft(R) Windows Vista(R) Enterprise Microsoft(R) Windows Vista(R) Ultimate	-
Microsoft(R) Windows(R) XP Professional Edition	SP2 or later supported.
Microsoft(R) Windows(R) 7 Professional Microsoft(R) Windows(R) 7 Ultimate	-

Table 1.19 HBA address rename setup service [Linux]

Basic Software (OS)	Remarks
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) 5.7 (for x86) Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.6 (for x86) Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.4 (for x86) Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64)	Prepare any required driver kits, update kits, or software. For information about required software, refer to the manual of the server or the Linux installation guide. About required packages, refer to " Table 1.34 Required Package of HBA address rename setup service [Linux] ". The Linux Kernel version depending on the hardware corresponds to the version supported by Fujitsu.

 **Note**

Installation will fail when a Resource Orchestrator agent is installed on an unsupported OS.

[Hyper-V]

When using Hyper-V on managed servers, the only supported OS of the admin server is Windows.

[Xen]

When using RHEL5-Xen on managed servers, the only supported OS of the admin server is Linux.

Use of some functions used in the server virtualization software for Resource Orchestrator at the same time with this product is not supported. Please do not use these functions.

[Hyper-V]

VMware(R) ESX and Citrix(R) XenServer(TM) can be managed by SCVMM, but only VM hosts for Hyper-V can be managed when using SCVMM in Resource Orchestrator.

Table 1.20 List of Functions with no Support of Combined Use

Server Virtualization Software	Functions with no Support of Combined Use
VMware vSphere (R) 4.0 VMware vSphere (R) 4.1 VMware vSphere (R) 5	Cisco Nexus 1000V virtual switch
Microsoft(R) System Center Virtual Machine Manager 2008 R2 Microsoft(R) System Center 2012 Virtual Machine Manager	- Movement of storage areas - Movement changing the virtual machine storage destination - Saving in the virtual machine library
Oracle VM Manager	Template

 Note

- If an L-Server is created with a specified Windows image, when deploying the image use Sysprep, provided by Microsoft, to re-configure the properties unique to the server. By executing Sysprep, the user information and OS setting information are reset. For details on Sysprep, refer to the information provided by Microsoft.
- If stopping or restarting of the manager is performed during execution of Sysprep, the operation being executed will be performed after the manager is started.
Until the process being executed is completed, do not operate the target resource.
- When using MAK license authentication for activation of Windows Server 2008 image OS, Sysprep can be executed a maximum of three times. Since Sysprep is executed when creating L-Server with images specified or when collecting cloning images, collection of cloning images and creation of L-Servers with images specified cannot be performed more than four times. Therefore, it is recommended not to collect cloning images from L-Servers that have had cloning images deployed, but to collect them from a dedicated master server. When customization of a guest OS is performed using the template function in VMware or when the template is created using SCVMM, Sysprep is executed and the number is included in the count.

[Windows] [VMware]

Note the following points when collecting cloning images from an L-Server that was created using a cloning image.

- As L-Servers which have not been used even once after creation do not have server specific information set, creation of L-Servers using cloning images collected from an L-Server may fail. When collecting cloning images, set the server specific information on L-Server, after starting the target L-Server.

[Oracle VM]

The information on the [OS] tab cannot be set when deploying the image.

Required Basic Software: Admin Clients

It is not necessary to install Resource Orchestrator on admin clients, but the following basic software is required.

Table 1.21 Required Basic Software: Admin Clients

Basic Software (OS)	Remarks
Microsoft(R) Windows(R) 7 Professional Microsoft(R) Windows(R) 7 Ultimate	-
Microsoft(R) Windows Vista(R) Business Microsoft(R) Windows Vista(R) Enterprise Microsoft(R) Windows Vista(R) Ultimate	SP1 or later supported.
Microsoft(R) Windows(R) XP Professional operating system	SP3 or later supported.
Microsoft(R) Windows Server(R) 2008 Standard (x86, x64) Microsoft(R) Windows Server(R) 2008 Enterprise (x86, x64) Microsoft(R) Windows Server(R) 2008 R2 Standard	The Server Core installation option is not supported.

Basic Software (OS)	Remarks
Microsoft(R) Windows Server(R) 2008 R2 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Datacenter	
Microsoft(R) Windows Server(R) 2003 R2, Standard Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition	SP2 or later supported.

Required Patches

Table 1.22 Manager [Windows]

Basic Software (OS)	Patch ID/Bundle Update
Microsoft(R) Windows Server(R) 2003 R2 Standard x64 Edition	Hotfix KB942589 (*1)
Microsoft(R) Windows Server(R) 2003 R2 Enterprise x64 Edition	Hotfix KB942589 (*1)
PRIMECLUSTER GLS	TP002714XP-06

*1: Necessary when managing a managed server within a separate subnet to the admin server.

Table 1.23 Manager [Linux]

Basic Software (OS)	Patch ID/Bundle Update (*1)
Red Hat(R) Enterprise Linux(R) 5 (for x86)	Bundle Update U09091 (5.4 compatible) Bundle Update U10041 (5.5 compatible)
Red Hat(R) Enterprise Linux(R) 5 (for Intel64)	Bundle Update U09091 (5.4 compatible) Bundle Update U10041 (5.5 compatible)

*1: necessary when upgrading.

Table 1.24 Agent [Windows]

Basic Software (OS)	Patch ID/Bundle Update
PRIMECLUSTER GLS	TP002714XP-06

Table 1.25 Agent [Windows/Hyper-V]

Basic Software (OS)	Patch ID/Bundle Update
None	-

Table 1.26 Agent [Linux]

Basic Software (OS)	Patch ID/Bundle Update (*1)
Red Hat(R) Enterprise Linux(R) 5 (for x86)	Bundle Update U07121 (5.1 compatible) Bundle Update U08071 (5.2 compatible) Bundle Update U09031 (5.3 compatible) Bundle Update U09091 (5.4 compatible) Bundle Update U10041 (5.5 compatible)
Red Hat(R) Enterprise Linux(R) 5 (for Intel64)	Bundle Update U07121 (5.1 compatible) Bundle Update U08071 (5.2 compatible) Bundle Update U09031 (5.3 compatible) Bundle Update U09091 (5.4 compatible) Bundle Update U10041 (5.5 compatible)

Table 1.27 Agent [VMware]

Basic Software (OS)	Patch ID/Bundle Update
None	-

Table 1.28 Agent [Xen/KVM]

Basic Software (OS)	Patch ID/Bundle Update
None	-

Table 1.29 Agent [Oracle VM]

Basic Software (OS)	Patch ID/Bundle Update
None	-

Table 1.30 HBA address rename setup service [Windows]

Basic Software (OS)	Patch ID/Bundle Update
None	-

Table 1.31 HBA address rename setup service [Linux]

Basic Software (OS)	Patch ID/Bundle Update (*1)
Red Hat(R) Enterprise Linux(R) 5 (for x86)	Bundle Update U09091 (5.4 compatible) Bundle Update U10041 (5.5 compatible)
Red Hat(R) Enterprise Linux(R) 5 (for Intel64)	Bundle Update U09091 (5.4 compatible) Bundle Update U10041 (5.5 compatible)

*1: necessary when upgrading.

[Hyper-V]

For the manager, agents, SCVMM, SCVMM agents, and Windows guest OS's, apply the latest updated program using Microsoft Update.

Installation of the latest integrated service provided by each OS on VM guests is necessary.

Required Packages [Linux]

The packages listed below are required when using Resource Orchestrator.

Install the required packages beforehand, if necessary.

The architecture of the required packages to be installed is shown enclosed by parenthesis "()".

For the items with no architecture to be installed is specified, install the package of the same architecture as the OS.

Table 1.32 Required Packages of Manager [Linux]

Basic Software (OS)	Required Packages
Red Hat(R) Enterprise Linux(R) 6.2 (for x86) Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64)	alsa-lib(i686) apr(i686) apr-util(i686) audit-libs(i686) cloog-ppl compat-expat1(i686) compat-libtermcap(i686) compat-openldap(i686) compat-readline5(i686) cpp cracklib(i686) cyrus-sasl-lib(i686)

Basic Software (OS)	Required Packages
	db4(i686) elfutils-libelf(i686) expat(i686) file gcc gcc-c++ gdb(i686) glibc(i686) glibc-devel(i686) glibc-headers kernel-headers keyutils-libs(i686) krb5-libs(i686) libattr(i686) libcap(i686) libcom_err(i686) libgcc(i686) libgomp libICE(i686) libselinux(i686) libSM(i686) libstdc++(i686) libstdc++-devel libtool-ltdl(i686) libuuid(i686) libX11(i686) libX11-common(noarch) libXau(i686) libxcb(i686) libXext(i686) libXi(i686) libxml2(i686) libXp(i686) libXt(i686) libXtst(i686) make mpfr ncurses ncurses-libs(i686) net-snmp net-snmp-utils nspr (*1) nss (*1) nss-softokn-freebl(i686) nss-util (*1) openldap (*1) openssl(i686) openssl098e(i686) pam(i686) perl perl-libs perl-Module-Pluggable perl-Pod-Escapes perl-Pod-Simple perl-version ppl

Basic Software (OS)	Required Packages
	readline(i686) redhat-lsb sqlite(i686) strace(i686) sysstat tssh unixODBC(i686) X-Window (*2) zlib(i686)
Red Hat(R) Enterprise Linux(R) 5.7 (for x86) Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.6 (for x86) Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.4 (for x86) Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64)	apr(i386) apr-util(i386) elfutils-libelf(i386) glibc(i386) libtermcap(i386) libxml2(i386) libXp(i386) libxslt(i386) net-snmp net-snmp-utils postgresql-libs(i386) readline(i386) redhat-lsb sysstat X-Window (*2) zlib(i386)

*1: Necessary when managing a managed server within a separate subnet to the admin server.

*2: Install an OS, specifying a package.

Table 1.33 Required Packages of Agent [Linux]

Basic Software (OS)	Required Packages
Red Hat(R) Enterprise Linux(R) 6.2 (for x86) Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64)	alsa-lib(i686) glibc(i686) libgcc(i686) libICE(i686) libSM(i686) libstdc++(i686) libtool-ltdl(i686) libuuid(i686) libX11(i686) libXau(i686) libxcb(i686) libXext(i686) libXi(i686) libxml2(i686) (*1) libXt(i686) libXtst(i686) ncurses (*1) ncurses-libs(i686) net-snmp-utils readline(i686) sqlite(i686) sysfsutils sysstat (*1) unixODBC(i686)

Basic Software (OS)	Required Packages
Red Hat(R) Enterprise Linux(R) 5.7 (for x86)	alsa-lib(i686)
Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64)	glibc(i686)
Red Hat(R) Enterprise Linux(R) 5.6 (for x86)	libgcc(i686)
Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64)	libICE(i686)
Red Hat(R) Enterprise Linux(R) 5.5 (for x86)	libselinux(i686)
Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64)	libsepol
Red Hat(R) Enterprise Linux(R) 5.4 (for x86)	libSM(i686)
Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64)	libstdc++(i686)
Red Hat(R) Enterprise Linux(R) 5.3 (for x86)	libX11(i686)
Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64)	libXau(i686)
Red Hat(R) Enterprise Linux(R) 5.2 (for x86)	libXdmcp
Red Hat(R) Enterprise Linux(R) 5.2 (for Intel64)	libXext(i686)
Red Hat(R) Enterprise Linux(R) 5.1 (for x86)	libXi(i686)
Red Hat(R) Enterprise Linux(R) 5.1 (for Intel64)	libXt(i686)
Red Hat(R) Enterprise Linux(R) 5 (for x86)	libXtst(i686)
Red Hat(R) Enterprise Linux(R) 5 (for Intel64)	ncurses-libs(i686)
	net-snmp-utils
	readline(i686)
	sqlite(i686)
	sysstat (*1)

*1:Necessary when installing an agent (dashboard functions).

Table 1.34 Required Package of HBA address rename setup service [Linux]

Basic Software (OS)	Required Packages
Red Hat(R) Enterprise Linux(R) 6.2 (for x86)	alsa-lib(i686)
Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64)	glibc(i686)
	libgcc(i686)
	libICE(i686)
	libSM(i686)
	libstdc++(i686)
	libtool-ltdl(i686)
	libuuid(i686)
	libX11(i686)
	libXau(i686)
	libxcb(i686)
	libXext(i686)
	libXi(i686)
	libXt(i686)
	libXtst(i686)
	ncurses-libs(i686)
	readline(i686)
	sqlite(i686)
	unixODBC(i686)
Red Hat(R) Enterprise Linux(R) 5.7 (for x86)	alsa-lib(x86_64)
Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64)	e2fsprogs-libs
Red Hat(R) Enterprise Linux(R) 5.6 (for x86)	glibc(x86_64)
Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64)	libgcc(i686)
Red Hat(R) Enterprise Linux(R) 5.5 (for x86)	libICE(x86_64)
Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64)	libSM(x86_64)
Red Hat(R) Enterprise Linux(R) 5.4 (for x86)	libstdc++(i686)
Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64)	libX11(x86_64)
Red Hat(R) Enterprise Linux(R) 5.3 (for x86)	libXau(x86_64)
Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64)	libXdmcp
	libXext(i686)

Basic Software (OS)	Required Packages
	libXi(i686) libXt(i686) libXtst(i686) ncurses(i686) readline(i686) sqlite(i686)

1.4.2.2 Required Software

The software listed below is required when using Resource Orchestrator.

Required Software

Table 1.35 Manager [Windows]

Required Software	Version	Remarks
ServerView Operations Manager for Windows (*1, *2) (previously ServerView Console for Windows)	V5.10.03 or later	This is necessary when viewing the server console window from the ROR console. Use a version of ServerView Operations Manager that supports viewing of the server console window. When displaying the console window, install ServerView Operations Manager on the same computer as the Resource Orchestrator manager. When registering monitored servers with ServerView Operations Manager, specify the IP address of the iRMC server.
	V5.30 or later	Necessary when using VMware ESXi for managed servers. Use a version of ServerView Operations Manager that supports VMware ESXi.
Microsoft(R) LAN Manager module (*1)	-	Necessary when performing backup and restore, or cloning for physical servers. Obtain it from the Microsoft FTP site. (*3)
BACS or Intel PROSet or PRIMECLUSTER GLS for Windows (*1)	-	Necessary when performing redundancy of the admin LAN for admin servers.
ServerView RAID (*1, *2)	-	Necessary when a RAID is composed of local disks (*4).
ServerView Virtual-IO Manager (*1)	2.6 or later	Necessary when creating physical L-Servers using blade servers.
VMware vCenter Server (*1) (previously VMware VirtualCenter)	4.0 4.1 5.0	[VMware] Necessary for management of VM guest and VM host. Can be placed on the same admin server as the manager or on another server.
SNMP Trap Service (*1)	-	-
DHCP Server (Standard OS service) (*1)	-	Necessary when managing a managed server within a separate subnet to the admin server.

Required Software	Version	Remarks
Microsoft(R) System Center Virtual Machine Manager 2008 R2 or Microsoft(R) System Center 2012 Virtual Machine Manager (*1)	-	[Hyper-V] Necessary for management of VM guest and VM host. Can be placed on the same admin server as the manager or on another server. Multiple library servers can be configured. Configure control settings for a maximum of 31 sessions, referring to " SCVMM Server MaxShellPerUser Settings " in " E.3.2 Preparations ". It is necessary to install Microsoft(R) SQL Server and Windows(R) Automated Installation Kit for Windows(R) 7 beforehand, when using Microsoft(R) System Center 2012 Virtual Machine Manager. For details, confirm the system requirements for the Microsoft(R) System Center 2012 Virtual Machine Manager. When only using Microsoft(R) System Center 2012 Virtual Machine Manager environments, the content of disks deleted from virtual L-Servers can be saved.
Windows PowerShell (*1)	2.0	[Hyper-V] Necessary for management of VM guest and VM host.
ETERNUS SF Storage Cruiser Manager (*1)	14.2 or later	Necessary when connecting an ETERNUS LUN to a physical L-Server. Install on the same admin server as the manager. Apply one of the following: <ul style="list-style-type: none"> - Patch TK20771 or later for ETERNUS SF Storage Cruiser14.2 manager - Patch TK30771 or later for ETERNUS SF Storage Cruiser14.2A manager
	15.0 or later	In the following cases, ETERNUS SF Storage Cruiser manager must be version 15.0 or later: <ul style="list-style-type: none"> - When linking with thin provisioning on ETERNUS storage - When using dynamic LUN mirroring on ETERNUS storage - When using Automatic Storage Layering for ETERNUS storage
ETERNUS SF AdvancedCopy Manager Copy Control Module (*1)	15.0 or later	Necessary when using dynamic LUN mirroring on ETERNUS storage.
NavisecCLI (*1)	7.30 or later	Necessary when connecting an EMC CLARiON LUN to a physical L-Server. Install on the same admin server as the manager.
SymCLI (*1)	-	Necessary when connecting an EMC Symmetrix DMX or EMC Symmetrix VMAX device to a physical L-Server. Install on the same admin server as the manager.
Solutions Enabler (*1)	7.1.2 or later	Necessary when connecting an EMC Symmetrix DMX or EMC Symmetrix VMAX device to a physical L-Server. Necessary to connect the server on which Solutions Enabler is operated to storage using a Fibre Channel connection.

Required Software	Version	Remarks
		Can be installed on the same admin server as the manager or on another admin server.
Oracle VM Manager (*1)	3.0	[Oracle VM] Necessary for management of VM guest and VM host.

*1 Unless specified otherwise, install on the same server as the manager.

*2: Required for PRIMERGY servers.

When installing managers in cluster environments, installation on both the primary and secondary nodes is necessary.

*3: Obtain it from the following Microsoft FTP site.

Microsoft FTP site

URL: <ftp://ftp.microsoft.com/bussys/clients/msclient/dsk3-1.exe> (As of February 2012)

*4: A local disk refers either to a server's internal disk, or to one stored in a storage blade.

Table 1.36 Manager [Linux]

Required Software	Version	Remarks
ServerView Operations Manager for Linux (*1)	V4.81.05 or later	Necessary when viewing the server management software Web UI from the ROR console.
	V5.10.03 or later	This is necessary when viewing the server console window from the ROR console. Use a version of ServerView Operations Manager that supports viewing of the server console window. When displaying the console window, install ServerView Operations Manager on the same computer as the Resource Orchestrator manager. When registering monitored servers with ServerView Operations Manager, specify the IP address of the iRMC server.
	V5.30 or later	Necessary when using VMware ESXi for managed servers. Use a version of ServerView Operations Manager that supports VMware ESXi.
Microsoft(R) LAN Manager module (*1)	-	Necessary when using backup and restore, or cloning. Obtain it from the Microsoft FTP site. (*2)
ServerView Virtual-IO Manager	2.6 or later	Necessary when creating physical L-Servers using blade servers.
PRIMECLUSTER Enterprise Edition (*1)	4.3A00 or later	When an admin server is in a cluster configuration, one of the following software is necessary. The supported standby cluster type is 1:1 hot standby.
PRIMECLUSTER HA Server (*1)	4.3A00 or later	
PRIMECLUSTER GLS (*1)	-	Necessary when performing redundancy of the admin LAN for admin servers.
VMware vCenter Server (*1) (previously VMware VirtualCenter)	4.0 4.1 5.0	Necessary for management of VM guest and VM host.
ETERNUS SF Storage Cruiser Manager (*1)	14.2 or later	Necessary when connecting an ETERNUS LUN to a physical L-Server. Install on the same admin server as the manager. Apply one of the following:

Required Software	Version	Remarks
		<ul style="list-style-type: none"> - Patch T01512-07 or later (x86), T01512-07 (Intel64) or later for ETERNUS SF Storage Cruiser14.2 manager - Patch T05195-01 or later (x86), T05195-01 (Intel64) or later for ETERNUS SF Storage Cruiser14.2A manager
	15.0 or later	<p>In the following cases, ETERNUS SF Storage Cruiser manager must be version 15.0 or later:</p> <ul style="list-style-type: none"> - When linking with thin provisioning on ETERNUS storage - When using dynamic LUN mirroring on ETERNUS storage - When using Automatic Storage Layering for ETERNUS storage
ETERNUS SF AdvancedCopy Manager Copy Control Module (*1)	15.0 or later	Necessary when using dynamic LUN mirroring on ETERNUS storage.
NavisecCLI (*1)	7.30 or later	Necessary when connecting an EMC CLARiiON LUN to a physical L-Server. Install on the same admin server as the manager.
SymCLI (*1)	-	Necessary when connecting an EMC Symmetrix DMX or EMC Symmetrix VMAX device to a physical L-Server. Install on the same admin server as the manager.
Solutions Enabler (*1)	7.1.2 or later	Necessary when connecting an EMC Symmetrix DMX or EMC Symmetrix VMAX device to a physical L-Server. Necessary to connect the server on which Solutions Enabler is operated to storage using a Fibre Channel connection. Can be installed on the same admin server as the manager or on another admin server.
Systemwalker Software Configuration Manager (*1)	-	Necessary when using RHEL5-Xen servers.
Oracle VM Manager (*1)	3.0	[Oracle VM] Necessary for management of VM guest and VM host.
DHCP Server (Standard OS service)	-	Necessary when managing a managed server within a separate subnet to the admin server.

*1 Unless specified otherwise, install on the same server as the manager.

*2: Obtain it from the following Microsoft FTP site.

Microsoft FTP site

URL: ftp://ftp.microsoft.com/bussys/clients/msclient/dsk3-1.exe (As of February 2012)
--

Table 1.37 Agent [Windows]

Required Software	Version	Remarks
ServerView Agents for Windows (*1)	V4.50.05 or later	-
"setupcl.exe" module "sysprep.exe" module	-	Necessary when using backup and restore, or cloning. Please refer to the Microsoft web site and obtain the latest

Required Software	Version	Remarks
		module. (*2) When using Windows Server 2008, the modules are already configured in the OS so there is no need to obtain new modules.
Intel PROSet or PRIMECLUSTER GLS for Windows (*1)	-	Necessary when performing redundancy of the admin LAN and public LAN for managed servers.
ServerView RAID (*1)	-	Necessary when a RAID is composed of local disks (*3).
ETERNUS Multipath Driver	V2.0L10 or later	Necessary for multipath connections between servers and storage units (ETERNUS). Versions differ depending on OS and storage types. Refer to ETERNUS Multipath Driver support information.
Data ONTAP DSM	3.2R1 or later	Necessary for connection between servers and storage units (NetApp). Versions differ depending on OS and storage types. Refer to Data ONTAP DSM support information.
PowerPath	5.3 or later	Necessary for multipath connections between servers and storage units (EMC CLARiiON, EMC Symmetrix DMX, or EMC Symmetrix VMAX). Versions differ depending on OS and storage types. Refer to PowerPath support information.

*1: Required for PRIMERGY servers.

When installing managers in cluster environments, installation on both the primary and secondary nodes is necessary.

*2: The necessary files vary depending on the CPU architecture (x86, x64) of the target system, and the OS version. Please refer to the Microsoft web site for the module to obtain.

Microsoft download web site

URL(x86): http://www.microsoft.com/downloads/details.aspx?familyid=93F20BB1-97AA-4356-8B43-9584B7E72556&displaylang=en (As of February 2012) URL(x64): http://www.microsoft.com/downloads/details.aspx?familyid=C2684C95-6864-4091-BC9A-52AEC5491AF7&displaylang=en (As of February 2012)
--

After obtaining the latest version of module, place it in a work folder (such as C:\temp) of the system for installation and execute it. For how to execute it, refer to "2.2.1.1 Software Preparation and Checks" of the "Installation Guide CE".

The module is not necessary after installation of agents.

*3: A local disk refers either to a server's internal disk, or to one stored in a storage blade.

Table 1.38 Agent [Linux]

Required Software	Version	Remarks
ServerView Agent for Linux (*1)	V4.90.14 or later	-
ServerView RAID (*1)	-	Necessary when a RAID is composed of local disks (*2).
ETERNUS Multipath Driver	V2.0L02 or later	Necessary for multipath connections between servers and storage units (ETERNUS). Versions differ depending on OS and storage types. Refer to ETERNUS Multipath Driver support information.
PowerPath	5.3	Necessary for multipath connections between servers and storage units (EMC CLARiiON, EMC Symmetrix DMX,

Required Software	Version	Remarks
		or EMC Symmetrix VMAX). Versions differ depending on OS and storage types. Refer to PowerPath support information.

*1: Required for PRIMERGY servers.

When installing managers in cluster environments, installation on both the primary and secondary nodes is necessary.

*2: A local disk refers either to a server's internal disk, or to one stored in a storage blade.

Table 1.39 Agent [Red Hat Enterprise Linux]

Required Software	Version	Remarks
PRIMECLUSTER GLS (*1)	4.2A00 or later	Necessary when performing redundancy of the admin LAN and public LAN for managed servers.

*1: Required for PRIMERGY servers.

When installing managers in cluster environments, installation on both the primary and secondary nodes is necessary.

Table 1.40 Agent [VMware]

Required Software	Version	Remarks
ServerView Agents for VMware (*1)	V4.30-20 or later	Not necessary when using VMware ESXi for the agent.
ServerView RAID (*1)	-	Necessary when a RAID is composed of local disks (*2).
ServerView ESXi CIM Provider	1.10.01 or later	Necessary when using VMware ESXi.

*1: Required for PRIMERGY servers.

When installing managers in cluster environments, installation on both the primary and secondary nodes is necessary.

*2: A local disk refers either to a server's internal disk, or to one stored in a storage blade.

Table 1.41 Agent [Hyper-V]

Required Software	Version	Remarks
ServerView Agents for Windows (*1)	V4.50.05 or later	-
"setupcl.exe" module "sysprep.exe" module	-	Necessary when using backup and restore, or cloning. Please refer to the Microsoft web site and obtain the latest module. (*2) When using Windows Server 2008, the modules are already configured in the OS so there is no need to obtain new modules.
Intel PROSet	15.6.25.0 or later	Necessary to automatically perform the following configurations using Intel PROSet on blade servers: <ul style="list-style-type: none"> - Virtual network creation and NIC connection - Configuration of the server blade connection ports of LAN switch blades - Connection of the server blade ports and uplink ports This is not necessary when the following applies: <ul style="list-style-type: none"> - When not performing network redundancy for L-Servers using blade servers - When using servers other than blade servers

Required Software	Version	Remarks
PRIMECLUSTER GLS for Windows (*1)	-	<p>After configuring redundancy for blade servers using PRIMECLUSTER GLS, it is necessary to perform the following configurations automatically:</p> <ul style="list-style-type: none"> - Virtual network creation and NIC connection - Configuration of the server blade connection ports of LAN switch blades - Connection of the server blade ports and uplink ports <p>This is not necessary when the following applies:</p> <ul style="list-style-type: none"> - When not performing network redundancy for L-Servers using blade servers - When using servers other than blade servers <p>For details, refer to "1.2.7 Simplifying Networks".</p>

*1: Required for PRIMERGY servers.

When installing managers in cluster environments, installation on both the primary and secondary nodes is necessary.

*2: The necessary files vary depending on the CPU architecture (x86, x64) of the target system, and the OS version. Please refer to the Microsoft web site for the module to obtain.

Microsoft download web site

<p>URL(x86): http://www.microsoft.com/downloads/details.aspx?familyid=93F20BB1-97AA-4356-8B43-9584B7E72556&displaylang=en (As of February 2012)</p> <p>URL(x64): http://www.microsoft.com/downloads/details.aspx?familyid=C2684C95-6864-4091-BC9A-52AEC5491AF7&displaylang=en (As of February 2012)</p>

After obtaining the latest version of module, place it in a work folder (such as C:\temp) of the system for installation and execute it. For how to execute it, refer to "2.2.1.1 Software Preparation and Checks" of the "Installation Guide CE".

The module is not necessary after installation of agents.

Table 1.42 Agent [Xen]

Required Software	Version	Remarks
ServerView Agents for Linux	V4.81-14 or later	Necessary when using PRIMEQUEST series servers.
ServerView RAID (*1)	-	Necessary when a RAID is composed of local disks (*2).
PRIMECLUSTER GDS	-	Necessary when using RHEL5-Xen servers.

*1: Required for PRIMERGY servers.

When installing managers in cluster environments, installation on both the primary and secondary nodes is necessary.

*2: A local disk refers either to a server's internal disk, or to one stored in a storage blade.

Table 1.43 Agent [KVM]

Required Software	Version	Remarks
ServerView Agents for Linux	V5.1 or later	-

Table 1.44 Agent [Oracle VM]

Required Software	Version	Remarks
ServerView Agents for Linux	5.0 or later	-

Table 1.45 HBA address rename setup service [Windows]

Required Software	Version	Remarks
Windows(R) Internet Explorer(R)	8 9	Necessary in the following cases: - When displaying the online help - When creating physical L-Servers using rack mount servers

Table 1.46 HBA address rename setup service [Linux]

Required Software	Version	Remarks
Firefox	3	Necessary in the following cases: - When displaying the online help - When creating physical L-Servers using rack mount servers

Required Software: Admin Clients

The following software is necessary for admin clients.

Table 1.47 List of Required Software for Admin Clients

Required Software	Version	Remarks
Windows(R) Internet Explorer(R)	8 9	Select [View]-[Encoding] in Internet Explorer, and confirm if [Auto-Select] is checked. If [Auto-Select] is not checked, select it.
Adobe Flash Player	10.3.183.5 or higher	Necessary for displaying the ROR console and the dashboard on admin clients.
Java(TM) 2 Runtime Environment Standard Edition	(*1)	Necessary for displaying the management window of ServerView Operations Manager, the VM management console, or console window on admin clients.
VMware vSphere(R) Client	4.0 4.1 5.0	[VMware] Necessary on admin clients when using the functions for coordinating with VMware or the VM management software on managed servers.
Hyper-V Manager	-	[Hyper-V] Necessary on admin clients when using the functions for coordinating with Hyper-V on managed servers. Operation on Windows XP and Windows 2003 are not supported.
Microsoft(R) System Center Virtual Machine Manager 2008 R2 VMM management console or Microsoft(R) System Center 2012 Virtual Machine Manager VMM console	-	[Hyper-V] Necessary on admin clients when using the functions for coordinating with VM management software and connecting with the L-Server console. Prepare the same version as VM management software for registration in Resource Orchestrator.
ETERNUS SF Storage Cruiser clients	14.2 or later	Necessary when checking the detailed information of storage using the admin client.

Required Software	Version	Remarks
		Operation on Windows 2003 x64 Edition is not supported.

*1: To display the management window of ServerView Operations Manager, please refer to the ServerView Operations Manager manual. To display the VM management console, version 1.5 or later is necessary.

1.4.2.3 Exclusive Software

Resource Orchestrator cannot be used in combination with Resource Coordinator, Cloud Infrastructure Management Software, or the following products.

List of Exclusive Software

Table 1.48 [Manager]

Operating System Type	Product Name	Version and Level	Remarks
Windows	INTERSTAGE	All versions	Here "INTERSTAGE" includes the following products: <ul style="list-style-type: none"> - INTERSTAGE - INTERSTAGE Standard Edition - INTERSTAGE Enterprise Edition
	Interstage Apcoordinator	All versions	-
	Interstage Application Server	All versions	Here "Interstage Application Server" includes the following products: <ul style="list-style-type: none"> - INTERSTAGE Application Server Standard Edition - INTERSTAGE Application Server Enterprise Edition - INTERSTAGE Application Server Web-J Edition - Interstage Application Server Standard Edition - Interstage Application Server Standard-J Edition - Interstage Application Server Enterprise Edition - Interstage Application Server Plus - Interstage Application Server Plus Developer - Interstage Application Server Web-J Edition
	Interstage Apworks	All versions	-
	Interstage Application Framework Suite	All versions	-
	Interstage Business Application Server	All versions	Here "Interstage Business Application Server" includes the following products: <ul style="list-style-type: none"> - Interstage Business Application Server Standard Edition - Interstage Business Application Server Enterprise Edition
	Interstage Business Process Manager	All versions	-

Operating System Type	Product Name	Version and Level	Remarks
	Interstage Business Process Manager Analytics	All versions	-
	Interstage BPM Flow	All versions	-
	Interstage Service Integrator	All versions	-
	Interstage Security Directory	All versions	-
	Interstage Shunsaku Data Manager	All versions	-
	Interstage Studio	All versions	-
	Interstage Traffic Director	All versions	-
	INTERSTAGE WEBCOORDINATOR	All versions	-
	Interstage Web Server	All versions	-
	ObjectDirectory	All versions	-
	Systemwalker Centric Manager (x64)	All versions	<p>Here "Systemwalker Centric Manager" includes the following products:</p> <ul style="list-style-type: none"> - SystemWalker/CentricMGR - SystemWalker/CentricMGR-M - SystemWalker/CentricMGR GEE - SystemWalker/CentricMGR EE - SystemWalker/CentricMGR SE - Systemwalker Centric Manager Global Enterprise Edition - Systemwalker Centric Manager Enterprise Edition - Systemwalker Centric Manager Standard Edition
	Systemwalker IT Change Manager	All versions	<p>Here "Systemwalker IT Change Manager" includes the following products:</p> <ul style="list-style-type: none"> - Systemwalker IT Change Manager Enterprise Edition - Systemwalker IT Change Manager Standard Edition
	Systemwalker IT Process Master	All versions	-
	Systemwalker Operation Manager	V13.3 or earlier	<p>Here "Systemwalker Operation Manager" includes the following products:</p> <ul style="list-style-type: none"> - SystemWalker/OperationMGR Global Enterprise Edition - SystemWalker/OperationMGR Enterprise Edition - SystemWalker/OperationMGR Standard Edition - SystemWalker OperationMGR Global Enterprise Edition - SystemWalker OperationMGR Enterprise Edition

Operating System Type	Product Name	Version and Level	Remarks
			<ul style="list-style-type: none"> - SystemWalker OperationMGR Standard Edition - Systemwalker Operation MGR Global Enterprise Edition - Systemwalker OperationMGR Enterprise Edition - Systemwalker OperationMGR Standard Edition
	Systemwalker PKI Manager	All versions	-
	Securecrypto Library	All versions	-
	Systemwalker Resource Coordinator	All versions	<p>Here "Systemwalker Resource Coordinator" includes the following products:</p> <ul style="list-style-type: none"> - Systemwalker Resource Coordinator - Systemwalker Resource Coordinator Base Edition - Systemwalker Resource Coordinator Virtual server Edition
	Systemwalker Runbook Automation (Admin Server)	14.0.0 14.1.0 (*1)	-
	Systemwalker Runbook Automation (Linked Server/Relay Server/Business Server)	All versions	-
	Systemwalker Service Quality Coordinator	All versions	-
	Systemwalker Service Catalog Manager	V14g	-
	Systemwalker Software Configuration Manager	V14.0.0	-
	Systemwalker Software Configuration Manager (Admin Server)	V14.1.0 (*2)	-
	Systemwalker Software Configuration Manager (Linked Server/Public Server)	All versions	-
	Cloud Infrastructure Management Software	All versions	-
	SystemcastWizard	All versions	-
	SystemcastWizard Professional	All versions	-
	SystemcastWizard Lite	All versions	-
	ServerView Installation Manager (*3)	All versions	-
	ServerView Resource Coordinator VE	All versions	-

Operating System Type	Product Name	Version and Level	Remarks
	ServerView Resource Orchestrator	All versions	-
	ServerView Deployment Manager (*4)	All versions	-
	Premeo Premium Agent	All versions	-
	TeamWARE Office Server	All versions	-
	TRADE MASTER	All versions	-
Linux	Interstage Application Server	All versions	Here "Interstage Application Server" includes the following products: <ul style="list-style-type: none"> - INTERSTAGE Application Server Standard Edition - INTERSTAGE Application Server Enterprise Edition - INTERSTAGE Application Server Web-J Edition - Interstage Application Server Standard Edition - Interstage Application Server Standard-J Edition - Interstage Application Server Enterprise Edition - Interstage Application Server Plus - Interstage Application Server Plus Developer - Interstage Application Server Web-J Edition
	Interstage Application Framework Suite	All versions	-
	Interstage Business Application Server	All versions	Here "Interstage Business Application Server" includes the following products: <ul style="list-style-type: none"> - Interstage Business Application Server Standard Edition - Interstage Business Application Server Enterprise Edition
	Interstage BPM Flow	All versions	-
	Interstage Business Process Manager	All versions	-
	Interstage Business Process Manager Analytics	All versions	-
	Interstage Web Server	All versions	-
	Interstage Service Integrator	All versions	Here "Interstage Service Integrator" includes the following products: <ul style="list-style-type: none"> - Interstage Service Integrator Enterprise Edition - Interstage Service Integrator Standard Edition
	Interstage Shunsaku Data Manager	All versions	-
	Interstage Traffic Director	All versions	-
	Server System Manager	All versions	-
	Systemwalker Centric Manager (Intel 64 version)	All versions	Here "Systemwalker Centric Manager" includes the following products: <ul style="list-style-type: none"> - SystemWalker/CentricMGR

Operating System Type	Product Name	Version and Level	Remarks
			<ul style="list-style-type: none"> - SystemWalker/CentricMGR-M - SystemWalker/CentricMGR GEE - SystemWalker/CentricMGR EE - SystemWalker/CentricMGR SE - Systemwalker Centric Manager Global Enterprise Edition - Systemwalker Centric Manager Enterprise Edition - Systemwalker Centric Manager Standard Edition
	Systemwalker IT Process Master	All versions	-
	Systemwalker IT Change Manager	All versions	<p>Here "Systemwalker IT Change Manager" includes the following products:</p> <ul style="list-style-type: none"> - Systemwalker IT Change Manager Enterprise Edition - Systemwalker IT Change Manager Standard Edition
	Systemwalker Operation Manager	V13.3 or earlier	<p>Here "Systemwalker Operation Manager" includes the following products:</p> <ul style="list-style-type: none"> - Systemwalker Operation Manager Enterprise Edition - Systemwalker Operation Manager Standard Edition
	Systemwalker Resource Coordinator	All versions	<p>Here "Systemwalker Resource Coordinator" includes the following products:</p> <ul style="list-style-type: none"> - Systemwalker Resource Coordinator - Systemwalker Resource Coordinator Base Edition - Systemwalker Resource Coordinator Virtual server Edition
	Systemwalker Runbook Automation (Admin Server)	14.1.0 (*1)	-
	Systemwalker Runbook Automation (Linked Server/Relay Server/Business Server)	All versions	-
	Systemwalker Service Quality Coordinator	All versions	-
	Systemwalker Service Catalog Manager	V14g	-
	Systemwalker Software Configuration Manager (Admin Server)	V14.1.0 (*2)	-
	Systemwalker Software Configuration Manager (Linked Server/Public Server)	All versions	-
	Cloud Infrastructure Management Software	All versions	-

Operating System Type	Product Name	Version and Level	Remarks
	ServerView Resource Coordinator VE	All versions	-
	ServerView Resource Orchestrator	All versions	-
	Premeo Premium Agent	All versions	-

*1: When the functions of Systemwalker Runbook Automation products are used, a license for Systemwalker Runbook Automation is necessary.

*2: When the software parameter setting function is used, the media and a license for Systemwalker Software Configuration Manager is necessary.

*3: As managers of this product include PXE server, use in combination with the PXE server required for remote installation of ServerView Installation Manager is not possible.

*4: ServerView Deployment Manager can be installed after Resource Coordinator has been installed.

Table 1.49 [Managed Server Resource Agent]

Virtual Environment	Product Name	Version and Level	Remarks
VMware	ServerView Deployment Manager (*1)	All versions	-
Hyper-V	Server System Manager	All versions	-
	SystemcastWizard	All versions	-
	SystemcastWizard Professional	All versions	-
	SystemcastWizard Lite	All versions	-
	Systemwalker Service Quality Coordinator	All versions	-
	Systemwalker Service Catalog Manager	V14g	-
Linux	Server System Manager	All versions	-
	SystemcastWizard	All versions	-
	SystemcastWizard Professional	All versions	-
	SystemcastWizard Lite	All versions	-
	ServerView Deployment Manager (*1)	All versions	-
Oracle VM	ServerView Deployment Manager (*1)	All versions	-

*1: ServerView Deployment Manager can be installed after Resource Coordinator has been installed.

Operating System Type	Product Name	Version and Level	Remarks
Windows	Systemwalker Service Quality Coordinator	All versions	-
	Systemwalker Service Catalog Manager	V14g	-
	ETERNUS SF Disk Space Monitor	All versions	-
Linux	Systemwalker Service Quality Coordinator	All versions	-
	Systemwalker Service Catalog Manager	V14g	-
	ETERNUS SF Disk Space Monitor	All versions	-

Basic mode

Exclusive software in Basic mode are as follows:

Table 1.50 List of Exclusive Software

Software	Product Name
Manager [Windows]	ServerView Installation Manager (*1)
	ServerView Deployment Manager
Manager [Linux]	Server System Manager
Agent [Windows/Hyper-V]	Server System Manager
	ServerView Deployment Manager (*2)
Agent [Linux]	Server System Manager
	ServerView Deployment Manager (*2)
Agent [VMware]	ServerView Deployment Manager (*2)
Agent [Xen/KVM]	-
Agent [Oracle VM]	ServerView Deployment Manager (*2)

*1: As managers of this product include PXE server, use in combination with the PXE server required for remote installation of ServerView Installation Manager is not possible.

*2: ServerView Deployment Manager can be installed after Resource Coordinator has been installed. For details on installation, refer to "2.2 Agent Installation" of the "Installation Guide CE".

 **Note**

- The same resource cannot be managed by the Resource Orchestrator admin server and the ServerView Resource Orchestrator admin server.
- Resource Orchestrator managers contain some functions of DHCP servers and PXE servers. Do not use products or services that use the functions of other DHCP servers or PXE servers on the admin server. Such products or services can be placed in the same network as Resource Orchestrator managers.

Examples of Products Including DHCP Servers and PXE Servers

- The Windows Server 2003 "Remote Installation Service", and the Windows Server 2008/Windows Server 2003 "Windows Deployment Service"
- ADS (Automated Deployment Services) of Windows Server 2003
- Boot Information Negotiation Layer (BINLSVC)
- ServerView Deployment Manager (*1)
- ServerStart (when using the remote installation function)
- ServerView Installation Manager
- Solaris JumpStart

*1: As PXE server is included, the use of some functions is restricted when it is used on the same admin LAN as ServerView Resource Orchestrator. For details on co-existence with ServerView Deployment Manager, refer to "[Appendix L Co-Existence with ServerView Deployment Manager](#)".

[Windows]

- Depending on the Windows Server domain type, the available functions differ as indicated in the table below.

Table 1.51 Function Restrictions Based on Domain Type

Domain Type	Backup and Restore	Cloning	Server Switchover Using Backup and Restore
Domain controller	No	No	No
Member server (*1)	Yes (*2)	Yes (*2, *3)	Yes (*2, *4)

Domain Type	Backup and Restore	Cloning	Server Switchover Using Backup and Restore
Workgroup	Yes	Yes	Yes

Yes: Use possible.

No: Use not possible.

*1: Member servers of Windows NT domains or Active Directory.

*2: After performing operations, it is necessary to join Windows NT domains or Active Directory again.

*3: Before obtaining cloning images, ensure that the server is not a member of a Windows NT domain or Active Directory.

*4: When switchover has been performed using Auto-Recovery, join Windows NT domains or Active Directory again before starting operations.

[Windows/Linux]

- Contact Fujitsu technical staff for information about ServerView Deployment Manager.

1.4.2.4 Static Disk Space

For new installations of Resource Orchestrator, the following static disk space is required.

The amount of disk space may vary slightly depending on the environment in question.

Table 1.52 Static Disk Space

Software	Folder	Required Disk Space (Unit: MB)
Manager [Windows]	<i>Installation_folder</i> (*1)	4000
Manager [Linux]	/opt	3525
	/etc/opt	255
	/var/opt	220
Agent [Windows/Hyper-V]	<i>Installation_folder</i> (*1)	300
Agent [Linux]	/opt	250
	/etc/opt	55
	/var/opt	105
Agent [VMware]	/opt	90
	/etc/opt	5
	/var/opt	5
Agent [Xen]	/opt	90
	/etc/opt	5
	/var/opt	5
Agent [KVM]	/opt	100
	/etc/opt	5
	/var/opt	5
Agent [Oracle VM]	/opt	90
	/etc/opt	5
	/var/opt	5

*1: The installation folder name specified when this software is installed.

The default folder name when Windows is installed on C:\ is as follows:

C:\Fujitsu\ROR

1.4.2.5 Dynamic Disk Space

When using Resource Orchestrator, the following disk space is required for each folder, in addition to static disk space.

Table 1.53 Dynamic Disk Space

Software	Folder	Required Disk Space (Unit: MB)
Manager [Windows]	<i>Installation_folder</i> (*1)	9000 + <i>Number_of_managed_servers</i> * 4
		<i>Environmental_data_storage_area</i>
		<i>Performance_display_information_storage_area</i> (*8)
		<i>Metering_log_storage_area</i> (*9)
	<i>Image_file_storage_folder</i> (*2)	<i>Image_file_storage_area</i> (*3)
	<i>Backup_storage_folder_for_configuration_definition_information</i>	<i>Backup_storage_area_for_configuration_definition_information</i> (*4)
	<i>L-Server_restoration_log_storage_folder</i>	<i>L-Server_restoration_log_storage_folder</i> (*4)
Manager [Linux]	/etc	2
	/var/opt	9000 + <i>Number_of_managed_servers</i> * 4
		<i>Environmental_data_storage_area</i>
		<i>Performance_display_information_storage_area</i> (*8)
		<i>Metering_log_storage_area</i> (*9)
	<i>Image_file_storage_directory</i> (*2)	<i>Image_file_storage_area</i> (*3)
<i>Backup_storage_folder_for_configuration_definition_information</i>	<i>Backup_storage_area_for_configuration_definition_information</i> (*4)	
	<i>L-Server_restoration_log_storage_folder</i>	<i>L-Server_restoration_log_storage_folder</i> (*4)
Agent [Windows]	<i>Installation_folder</i> (*1)	60
		<i>Log_data</i> (*5)
Agent [Hyper-V]	<i>Installation_folder</i> (*1)	60
		<i>Log_data</i> (*6)
Agent [Linux]	/etc	1
	/var/opt	1
		<i>Log_data</i> (*7)
Agent [VMware]	/etc	1
	/var/opt	1
HBA address rename setup service [Windows]	<i>Installation_folder</i> (*1)	60
HBA address rename setup service [Linux]	/etc	1
	/var/opt	60

Software	Folder	Required Disk Space (Unit: MB)
Agent [Xen]	/etc	1
	/var/opt	1
Agent [KVM]	/etc	1
	/var/opt	1
Agent [Oracle VM]	/etc	1
	/var/opt	1

*1: The installation folder name specified when this software is installed.
The default folder name when Windows is installed on C:\ is as follows:

C:\Fujitsu\ROR

*2: The name of the storage folder (directory) specified for image files when this software is installed.

[Windows]

The default folder name when Windows is installed on C:\ is as follows:

C:\Fujitsu\ROR\ScwPro\depot

[Linux]

The default is as follows:

/var/opt/FJSVscw-deploysv/depot

*3: The image storage area when using cloning images for cloning of physical servers.

For details on the amount of space for the image storage area, refer to "1.4.2.5 Dynamic Disk Space" in the "Setup Guide VE".

Cloning images of L-Servers are stored in image pools regardless of server types.

*4: The backup storage area for configuration definition information and the L-Server restoration log storage area can be specified in the definition file. Estimate according to the location of the specified disk. For details on disk capacity and the content of the backup storage area for configuration definition information and the L-Server restoration log storage area, refer to "Chapter 8 Backup and Restoration of Admin Servers" of the "Operation Guide CE".

*5: The approximate estimate value is 60 MB.

*6: The approximate estimate value is 60 MB * VM guest number.

*7: The approximate estimate value is 100MB.

The size of log data changes according to L-Server configurations.

When it is necessary to estimate the detailed data, refer to "2.2.1.2 How to estimate the amount of space required for the log data ("Troubleshoot" directory)" in the "Systemwalker Service Quality Coordinator Installation Guide".

*8: For information disk capacity for performance display, there are storage areas for dashboard information and usage condition information. The disk capacity necessary for resources is indicated below.

Table 1.54 Formula of Disk Space Necessary for Information Storage Area for Performance Display

Target Resource	Required Disk Space
Dashboard information	<p>The size changes depending on the number of L-Server templates and tenants changed. Prepare the disk capacity, referring to the following formula in the case where 10 L-Server templates are defined.</p> <p>When the number of tenants is 100, 6.6 GB of capacity is required.</p> <p>Disk Space = (67.0 + (55.5 * number of tenants)) * 1.2 (MB)</p>
Usage condition information	<p>The size will increase and decrease depending on the numbers of VM hosts and VM guests.</p> <p>The capacity differs depending on the VM management software.</p> <p>Prepare the disk capacity, referring to the following formula. For the information storage area with 50 hosts and 1,000 VM (20VM/host), approximately 19.4 GB of space is required.</p> <p>Disk space = ((N1 * host number) + (N2 * guest number)) * 1.2(MB)</p>

Target Resource	Required Disk Space
	[VMware] N1 = 2.0, N2 = 16.5 [Hyper-V] N1 = 92.0, N2 = 26.0 [Xen/KVM] N1 = 102.0, N2 = 7.0

*9: The necessary disk capacity for metering logs is indicated as follows:

Table 1.55 Formula of Disk Space Necessary for Metering Logs

Metering Logs per day * capacity for one year 3.5 MB * 365 = 1.3 GB
--

The conditions of the base for the formula for disk space above and the formula of the metering logs per day are indicated as below.

Table 1.56 Required Conditions for Metering Information Backup

Item	Estimated Value	
Number of operating L-Platforms	1000	
Number of resources per L-Platform	L-Server	1
	Expansion disk	1
	Software	2
Usage status	<ul style="list-style-type: none"> - The following operations are executed every day <ul style="list-style-type: none"> - Return and deployment of 10 L-Platforms - Starting of 1,000 L-Servers when starting operations - Stopping of 1,000 L-Servers when finishing operations - Obtain regular logs every day - Keep metering logs for one year 	
Online backup frequency	<ul style="list-style-type: none"> - Execute monthly base backup (every 30 days) - Execute hourly difference backup. 	

Table 1.57 Formula for Metering Logs per Day

<ul style="list-style-type: none"> - Target capacity for metering logs <ul style="list-style-type: none"> - Event Logs for an L-Platform : 2.3 KB/each time (A) - Event Logs for other than an L-Platform : 0.6 KB/each time (B) - Regular logs : 2.3 * number of L-Platforms (KB) (C) - Metering logs per day <ul style="list-style-type: none"> (A) * operation number for L-Platforms per day + (B) * operation number for other than L-Platforms per day + (C) * number of operating L-Platforms <p>= 2.3 KB * 20 + 0.6 KB * 2000 + 2.3 KB * 1000 = 3.5MB</p>

1.4.2.6 Memory Size

The memory size listed below is required when using Resource Orchestrator.

Table 1.58 Memory Size

Software	Memory Size (Unit: MB)
Manager [Windows]	10240
Manager [Linux]	10240
Agent [Windows/Hyper-V]	512
Agent [Linux]	256
Agent [VMware]	32
Agent [Xen/KVM]	32
Agent [Oracle VM]	32

1.5 Hardware Environment

The hardware conditions described in the table below must be met when using Resource Orchestrator.

Table 1.59 Required Hardware

Software	Hardware	Remarks
Manager	PRIMERGY BX series servers PRIMERGY RX series servers PRIMERGY TX series servers	The CPU must be a multi-core CPU. 10 GB or more of memory is necessary.
Agent	PRIMERGY BX620 S4 PRIMERGY BX620 S5 PRIMERGY BX620 S6 PRIMERGY BX920 S1 PRIMERGY BX920 S2 PRIMERGY BX920 S3 PRIMERGY BX922 S2 PRIMERGY BX924 S2 PRIMERGY BX924 S3 PRIMERGY BX960 S1 PRIMERGY RX100 S5 PRIMERGY RX100 S6 PRIMERGY RX200 S4 PRIMERGY RX200 S5 PRIMERGY RX200 S6 PRIMERGY RX300 S4 PRIMERGY RX300 S5 PRIMERGY RX300 S6 PRIMERGY RX600 S4 PRIMERGY RX600 S5 PRIMERGY RX900 S1 PRIMERGY TX150 S6 PRIMERGY TX150 S7 PRIMERGY TX200 S5 PRIMERGY TX200 S6 PRIMERGY TX300 S4 PRIMERGY TX300 S5 PRIMERGY TX300 S6 PRIMEQUEST 1000 series servers Other PC servers	<ul style="list-style-type: none"> - When using servers other than PRIMERGY BX servers Only configurations where Fibre Channel cards are mounted in expansion slot 2 are supported. - When using servers other than PRIMERGY BX servers It is necessary to mount an IPMI-compatible (*1) server management unit (*2). - For Physical L-Servers The following servers cannot be used: <ul style="list-style-type: none"> - PRIMERGY TX series servers - PRIMERGY RX100 series servers - PRIMEQUEST 1000 series servers - Other PC servers - When using RHEL5-Xen as the server virtualization software Only PRIMEQUEST 1000 series servers are supported for managed servers. - When using physical L-Servers for iSCSI boot PRIMERGY BX900 and VIOM are required. - When the destination of a physical L-Server is a PRIMERGY BX920 series or BX922 series server and LAN switch blades (PG-SW109 or PG-SW201) are mounted in CB1 and CB2, only NIC1 and NIC2 can be used.

*1: Supports IPMI 2.0.

*2: This usually indicates a Baseboard Management Controller (hereinafter BMC). For PRIMERGY, it is called an integrated Remote Management Controller (hereinafter iRMC).

The following hardware is required for admin clients:

Table 1.60 Required Hardware for Admin Clients

Software	Hardware	Remarks
Client	Personal computers PRIMERGY RX series servers PRIMERGY BX series servers PRIMERGY TX series servers Other PC servers	-

When connecting storage units that can be connected to the physical servers of L-Servers, the following storage units can be used:

Table 1.61 Storage Units that can be Connected with L-Servers on Physical Servers

Hardware	Remarks
ETERNUS DX8000 series ETERNUS DX8000 S2 series ETERNUS DX400 series ETERNUS DX400 S2 series ETERNUS DX90 S2 ETERNUS DX90 ETERNUS DX80 S2 ETERNUS DX80 ETERNUS DX60 S2 ETERNUS DX60 ETERNUS8000 series	Thin provisioning is available for the following storage units: <ul style="list-style-type: none"> - ETERNUS DX8000 series - ETERNUS DX8000 S2 series - ETERNUS DX400 series - ETERNUS DX400 S2 series - ETERNUS DX90 S2 - ETERNUS DX80 S2 For the following apparatuses, when disk resources are created with Resource Orchestrator, set the alias (if possible) based on the disk resource name in the LUN. <ul style="list-style-type: none"> - ETERNUS DX8000 S2 series - ETERNUS DX400 S2 series - ETERNUS DX90 S2 - ETERNUS DX80 S2 - ETERNUS DX60 S2 On ETERNUS other than the above, the alias name is set as previously, that is the default value set on the ETERNUS. For the following apparatuses, if an alias has been set for the LUN, the alias name is displayed. <ul style="list-style-type: none"> - ETERNUS DX8000 series - ETERNUS DX8000 S2 series - ETERNUS DX400 series - ETERNUS DX400 S2 series - ETERNUS DX90 S2 - ETERNUS DX90 - ETERNUS DX80 S2 - ETERNUS DX80 - ETERNUS DX60 S2 - ETERNUS DX60

Hardware	Remarks
	<p>Dynamic LUN mirroring can be used with Resource Orchestrator with the following apparatuses.</p> <ul style="list-style-type: none"> - ETERNUS DX8000 S2 series - ETERNUS DX410 S2 - ETERNUS DX440 S2 - ETERNUS DX90 S2 <p>When using the target units for the following options, Automatic Storage Layering can be used with Resource Orchestrator.</p> <ul style="list-style-type: none"> - ETERNUS SF Storage Cruiser V15 Optimization Option
ETERNUS4000 series	Model 80 and model 100 are not supported. Thin provisioning is not available for this series.
ETERNUS2000 series	When an alias name is configured for a LUN, the alias name is displayed.
NetApp FAS6000 series NetApp FAS3100 series NetApp FAS2000 series NetApp V6000 series NetApp V3100 series	Data ONTAP 7.3.3 or later Data ONTAP 8.0.1 7-Mode
EMC CLARiiON CX4-120 EMC CLARiiON CX4-240 EMC CLARiiON CX4-480 EMC CLARiiON CX4-960 EMC CLARiiON CX3-10 EMC CLARiiON CX3-20 EMC CLARiiON CX3-40 EMC CLARiiON CX3-80	Navisphere Manager and Access Logix must be installed on SP.
EMC Symmetrix DMX-3 EMC Symmetrix DMX-4 EMC Symmetrix VMAX	VolumeLogix must be installed on SP.

When using storage management software, do not change or delete the content set for storage units by Resource Orchestrator. Insufficient disk space does not cause any problems for RAID group or aggregate creation.

When connecting storage units that can be connected to the physical servers of L-Servers, the following Fibre Channel switches can be used:

Table 1.62 Fibre Channel Switches which can be used when Connecting ETERNUS Storage, NetApp Storage, EMC CLARiiON Storage, and EMC Symmetrix DMX Storage with L-Servers on Physical Servers

Hardware	Remarks
Brocade series ETERNUS SN200 series	-
PRIMERGY BX600 Fibre Channel switch blades	Connect fibre channel switch blades to the following connection blades: - NET3, NET4
PRIMERGY BX900 Fibre Channel switch blades	Connect fibre channel switch blades to the following connection blades: - CB5, CB6
PRIMERGY BX400 Fibre Channel switch blades	Connect fibre channel switch blades to the following connection blades: - CB3, CB4

Refer to the following sections for the LAN switch blades that are available when using simplifying of network settings:

- Physical L-Server
 - "D.6.1 Automatic Network Configuration"
- Virtual L-Server
 - "E.2.5 Setup"
 - "E.3.4 Setup"

Table 1.63 Supported Network Devices

Hardware		Version
L2 switches (*1)	Fujitsu SR-X 300 series Fujitsu SR-X 500 series	V01 or later
	Cisco Catalyst 2900 series Cisco Catalyst 2918 series Cisco Catalyst 2928 series Cisco Catalyst 2940 series Cisco Catalyst 2950 series Cisco Catalyst 2955 series Cisco Catalyst 2960 series Cisco Catalyst 2970 series Cisco Catalyst 2975 series Cisco Catalyst 3500 series Cisco Catalyst 3550 series Cisco Catalyst 3560 series Cisco Catalyst 3750 series	IOS 12.2 or later
Firewall (*2)	Fujitsu IPCOM EX IN series Fujitsu IPCOM EX SC series	E20L10 or later
	Cisco ASA 5500 series	ASASoftware-8.3 or later

*1: L2 switches are necessary in the following cases:

- When placing an L2 switch between a firewall and rack mount or tower servers
- When placing an L2 switch between a firewall and LAN switch blades

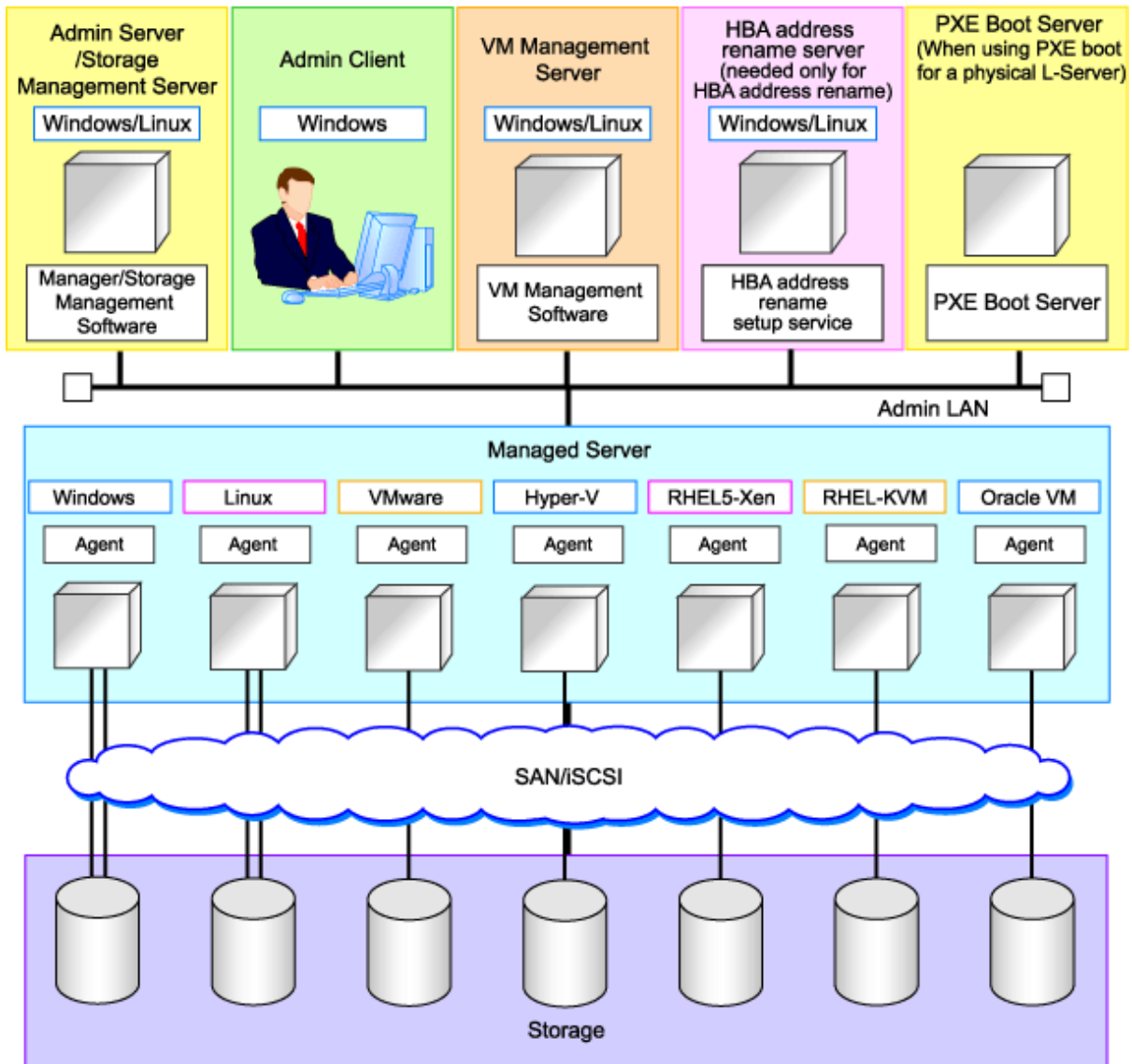
*2: Necessary when placing a firewall on an L-Platform.

In addition, an L3 switch is necessary when using a separate admin LAN network for each tenant.

1.6 System Configuration

This section provides an example of a Resource Orchestrator system configuration.

Figure 1.8 Example of System Configuration



Admin Server

The admin server is a server used to manage several managed servers.

The admin server operates in a Windows or Linux environment. An admin server can be operated on VMware and Hyper-V virtual machines.

The Resource Orchestrator manager should be installed on the admin server. The admin server can be made redundant by using clustering software. It can also be standardized with the admin client.

The Resource Orchestrator agent cannot be installed on the admin server to monitor and manage the admin server itself.

Note

Also install ServerView Virtual-IO Manager when creating physical L-Servers using blade servers.

When operating an admin server on a virtual machine on VMware or Hyper-V, do not register VM hosts that operate on the admin server in VM pools.

[VMware]

To use VMware ESXi, install ServerView Operations Manager and register the target VMware ESXi.

[Hyper-V]

When using Hyper-V on managed servers, the only supported OS of the admin server is Windows.

[Xen]

When using RHEL5-Xen on managed servers, the only supported OS of the admin server is Linux.

Managed Server

Managed servers are the servers used to run applications. They are managed by the admin server.

Install agents on managed servers.

In server virtualization environments, the agent should only be installed on the VM host.



When using VMware ESXi, Resource Orchestrator agents cannot be installed.

Install ServerView ESXi CIM Provider agents.

When using other vendor's servers, perform "[Configuration when Creating a Virtual L-Server Using VMware ESXi on Other Vendor's Servers](#)".

Admin Client

Admin clients are terminals used to connect to the admin server, which can be used to monitor and control the configuration and status of the entire system.

Admin clients should run in a Windows environment.

Storage Management Server

A server on which storage management software that manages multiple storage units has been installed.

Sharing with the admin server differs depending on the storage in use.

- When using ETERNUS storage
 - Operate ETERNUS SF Storage Cruiser in the same environments as the admin server.
Note that resources for both the admin and storage management software servers are required when operating the servers together.
 - Operate the ETERNUS SF AdvancedCopy Manager Copy Control Module in the same environment as the admin server.

- When using NetApp storage

In Resource Orchestrator, Data ONTAP can be used as storage management software, but a server for storage management software is not necessary, as Data ONTAP is an OS for NetApp storage.

- When using EMC CLARiiON storage

In Resource Orchestrator, Navisphere can be used as storage management software, but servers for storage management software are not necessary, as Navisphere is software operated on the SP of EMC CLARiiON storage.

- When using EMC Symmetrix DMX storage or EMC Symmetrix VMAX storage

In Resource Orchestrator, Solutions Enabler can be used as storage management software. Servers for storage management software can be operated on the same computer as the admin server, but the storage management software must be connected to EMC Symmetrix DMX storage or EMC Symmetrix VMAX storage using FC-HBA. Note that resources for both the admin and storage management software servers are required when operating the servers together.

VM Management Server

A server on which VM management software (such as VMware vCenter Server, System Center Virtual Machine Manager, and Oracle VM Manager) to integrate multiple server virtualization software products has been installed. The VM management server can be operated on the same machine as the admin server.

Note that resources for both the admin and VM management servers are required when operating the servers together.

PXE Boot Server

For purposes such as OS installation, it is necessary to perform PXE boot of a physical L-Server using its own PXE server. The PXE boot server must be operated on a server other than the admin server.



PXE boot is unavailable on networks that use tagged VLAN settings. Do not configure tagged VLANs for PXE boot servers.

HBA address rename Setup Service Server

A server on which the HBA address rename setup service operates. This is necessary when creating physical L-Servers using rack mount servers. This is not necessary when creating physical L-Servers using blade servers. When an admin server cannot be communicated with from a managed server, configure the necessary WWNs for starting the managed server instead of the admin server. The HBA address rename server operates in a Windows or Linux environment. Install the HBA address rename setup service on this server. Use as an admin server and managed server at the same time is not possible. Keep this server powered ON at all times, in preparation for admin server trouble or communication errors. For details, refer to ["4.3.1.3 HBA and Storage Device Settings"](#) and ["C.2 WWN Allocation Order during HBA address rename Configuration"](#).

Admin LAN

The admin LAN is the LAN used by the admin server to control managed servers and storage. The admin LAN is set up separately from the public LAN used by applications on managed servers. Using network redundancy software on the server enables redundancy for the admin LAN or the public LAN. Manually configure network redundancy software. When using a physical L-Server, the default physical network adapter numbers available for the admin LAN are as given below.

- When not performing redundancy, "1" is available
- When performing redundancy, "1" and "2" are available



When using a NIC other than the default one, the configuration at the time of physical server registration and at L-Server creation must be the same. Thus when designing systems it is recommended that physical servers registered in the same server pool use the same NIC index.



The first NIC that is available for the admin LAN can be changed. For details, refer to ["2.4.2 Registering Blade Servers"](#) of the ["User's Guide for Infrastructure Administrators \(Resource Management\) CE"](#).

iSCSI LAN

Refer to "[4.2.1.3 Physical Network Design for the Public LAN and iSCSI LAN](#)".

Chapter 2 Overview of Resource Orchestrator Setup Operations

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

Setup operations when using Resource Orchestrator are performed by the users below.

Infrastructure Administrators

Infrastructure administrators manage ICT resources such as servers, storage, networks, and images.

They collectively manage ICT resources in resource pools, and perform addition, configuration modification, and maintenance of ICT resources when necessary.

In Resource Orchestrator, the following roles can be assigned to infrastructure administrators:

- infra_admin (infrastructure administrator)

Tenant Administrators

Provide tenant users with L-Platform templates based on their needs.

In Resource Orchestrator, the following roles can be assigned to tenant administrators:

- tenant_admin (tenant administrator)

The following role combines the roles of infrastructure administrators and tenant administrators:

- administrator (administrator)

For details of roles, refer to "Appendix B Access Control by Roles" in the "Operation Guide CE".

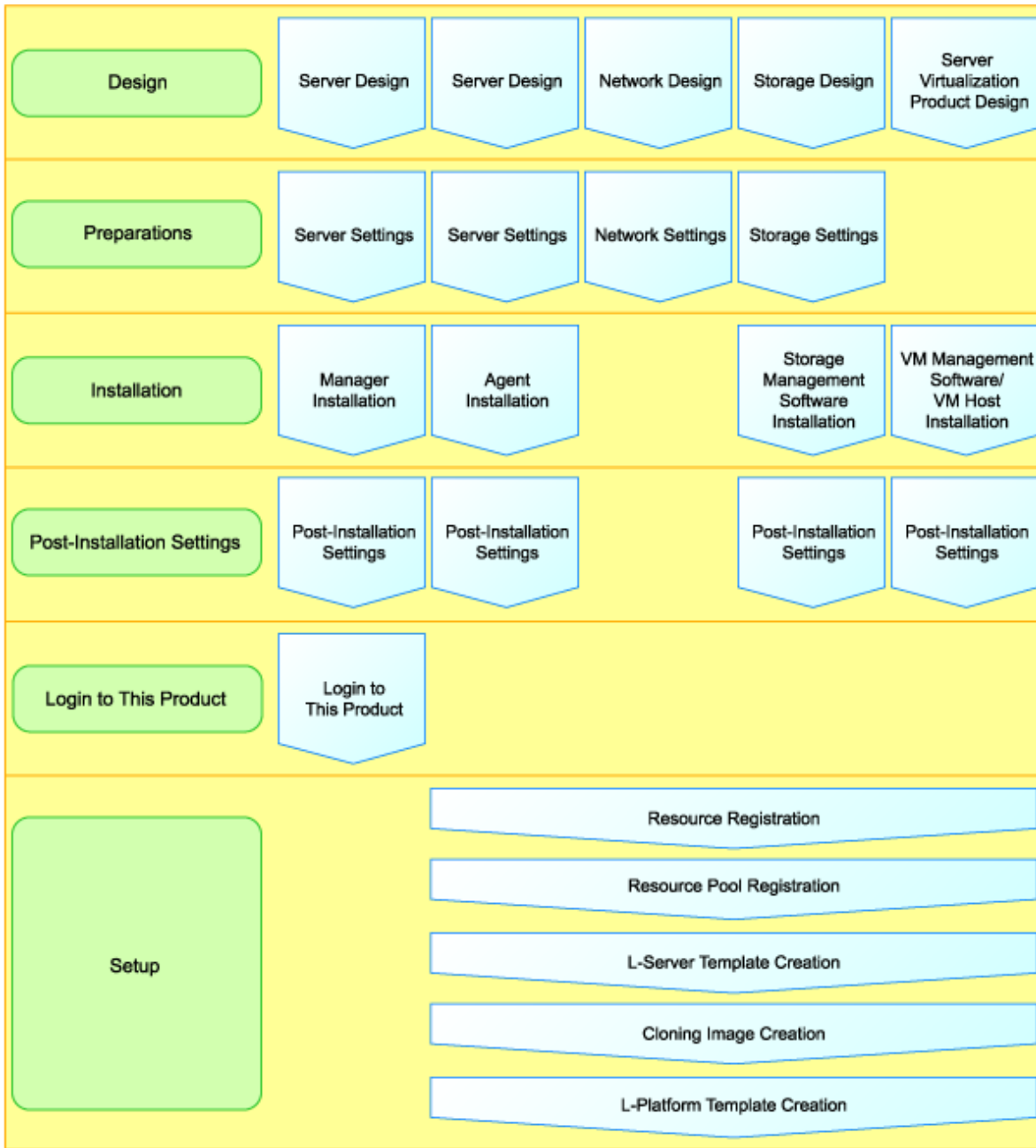
An overview of setup operations when using Resource Orchestrator is given below.

Setup Operations for Infrastructure Administrators

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

For details on creating tenants and tenant administrators, refer to the "Operation Guide CE".

Figure 2.1 Flow of Setup Operations for Infrastructure Administrators



1. Design for Resource Orchestrator Setup

Design the following items:

For details, refer to "[Chapter 3 Resource Orchestrator Setup Design](#)".

- Tenants and resource pools
- User accounts
- Design for High Availability and Disaster Recovery
- Design servers, storage, and networks
- Design server virtualization software

2. Settings for Resource Orchestrator Setup

Define the following settings:

For details, refer to ["Chapter 4 Pre-setup Preparations"](#).

- Server, Storage, and Network Settings
- Settings for Server Virtualization Software

3. Installation

Install the following software:

For details, refer to the "Installation Guide CE".

- Manager
- Agents for physical servers and VM hosts

4. Configuration after Installation

Define the following settings:

For details, refer to ["Chapter 6 Configuration after Installation"](#).

- Network Script Settings
- Definition File Settings

5. Resource Orchestrator Login

Log in to Resource Orchestrator.

After logging into Resource Orchestrator, set up the license.

For details, refer to ["Chapter 7 Logging in to Resource Orchestrator"](#).

6. Resource Registration

Register the required resources in Resource Orchestrator.

For details, refer to ["8.1 Registering Resources with Resource Orchestrator"](#).

When using HBA address rename, refer to ["8.2 HBA address rename Settings"](#).

7. OS Installation on Managed Servers and Agent Registration

Install an OS on managed servers and register agents.

For details, refer to ["8.3 Software Installation and Agent Registration"](#).

8. Resource Registration for Resource Pools

Register resources in a resource pool.

For details, refer to ["8.4 Registering Resources to the Global Pool"](#).

9. L-Server Template Creation

Create an L-Server template.

For details, refer to ["8.5 Creating L-Server Templates"](#).

10. Cloning Image Creation

Create a cloning image.

To create a cloning image, an L-Server for the infrastructure administrator must be created.

For details, refer to ["8.6 Collecting and Registering Cloning Images"](#).

11. L-Platform Template Creation

Create an L-Platform template.

For details, refer to ["8.7 Creating L-Platform Templates"](#).

12. Tenant Creation

Create tenants.

For details, refer to "8.3 Creating a Tenant" in the "User's Guide for Infrastructure Administrators CE".

13. Tenant Administrator Creation

Create the tenant administrator.

For details, refer to "Chapter 9 Account" in the "User's Guide for Infrastructure Administrators CE".

Setup Operations for Tenant Administrators

Tenant administrators perform the following operations:

For details, refer to the "User's Guide for Tenant Administrators CE".

1. Duplicate L-Platform Templates
2. Modify L-Platform Templates
3. Release L-Platform Templates
4. Create Tenant Users

Setup Operations for Tenant Users

Tenant users perform the following operation:

For details, refer to the "User's Guide for Tenant Users CE".

1. Create L-Platforms

Chapter 3 Resource Orchestrator Setup Design

This chapter explains how to design a Resource Orchestrator installation.

3.1 System Configuration Design

This section explains how to design a system configuration.

The procedure differs depending on whether the L-Server is physical or virtual.

- For Physical L-Servers

For details, refer to "[D.1 System Configuration](#)".

- For Virtual L-Servers

[VMware]

For details, refer to "[E.2.1 System Configuration](#)".

[Hyper-V]

For details, refer to "[E.3.1 System Configuration](#)".

[RHEL5-Xen]

For details, refer to "[E.4.1 System Configuration](#)".

[Oracle VM]

For details, refer to "[E.5.1 System Configuration](#)".

[KVM]

For details, refer to "[E.6.1 System Configuration](#)".

3.2 Tenant and Resource Pool Design

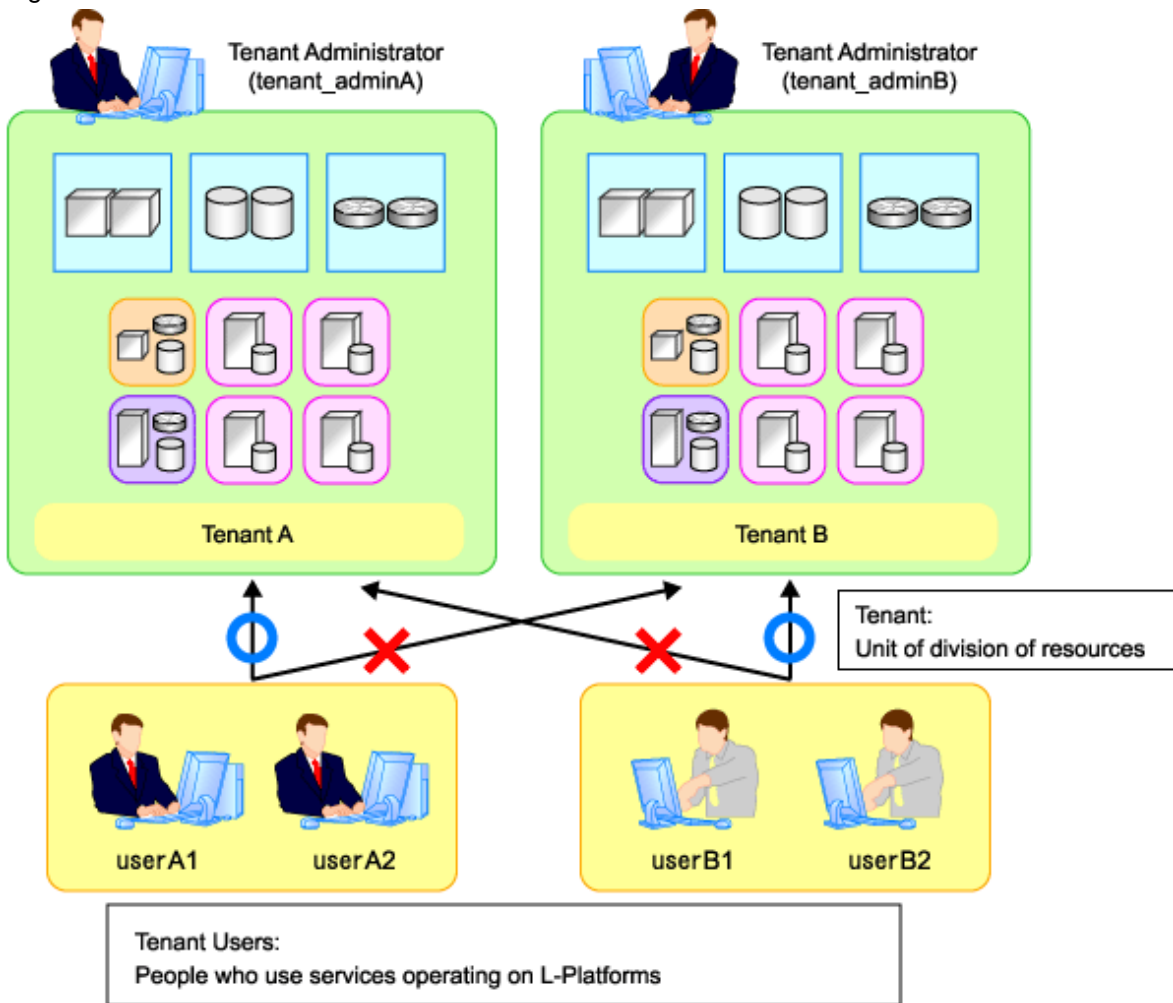
This section explains how to design tenants and resource pools.

3.2.1 Overview of Tenants

This section provides an overview of tenants.

In Resource Orchestrator, the unit for division of management and operation of resources based on organizations or operations is called a tenant.

Figure 3.1 Tenants



An L-Platform, L-Server, and an exclusive resource pool for each tenant are stored in a tenant.

Resource Pool Types

Resource pools are categorized into the following two types:

- Local Pools

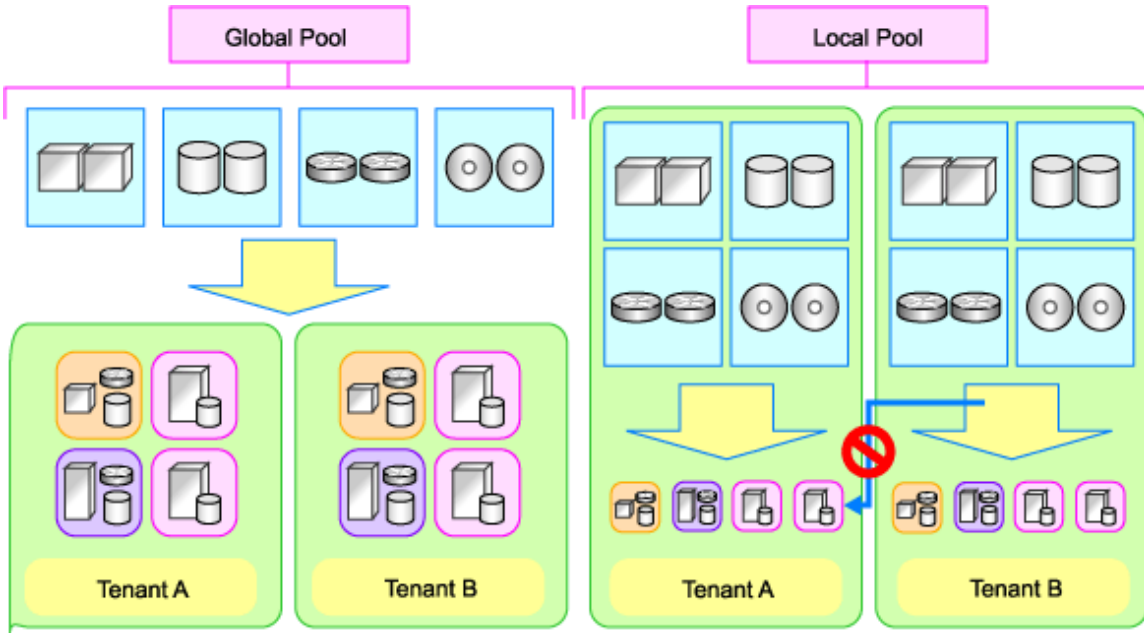
Resource pools for each tenant.

- Global Pools

Resource pools that can be used by multiple tenants.

Resources can be divided and shared by creating a tenant for each organization or department. When creating a tenant, a tenant administrator and local pool can also be created.

Figure 3.2 Global Pools and Local Pools



3.2.2 Tenant Operation

This section explains how to operate tenants.

The following five patterns of tenant operation are available.

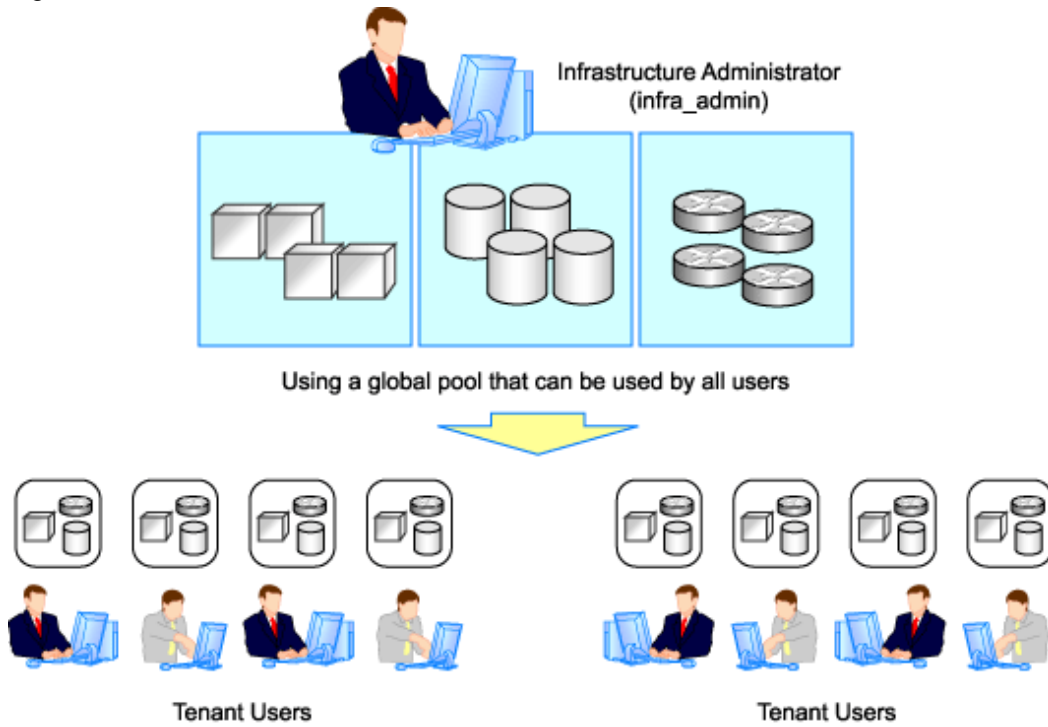
Table 3.1 Tenant Operation

Pattern	Divide Resources in Tenant	Use Global Pools/Local Pools
A	Do not divide in tenant	Use global pools only
B	Divide in tenant	Use global pools only
C	-	Use local pools only
D	-	Use both global pools and local pools Use local pools as a priority
E	-	Use both global pools and local pools Give priority to global pools

(Pattern A) Do not Divide in Tenant

Global pools enable effective use of resources.

Figure 3.3 Pattern A

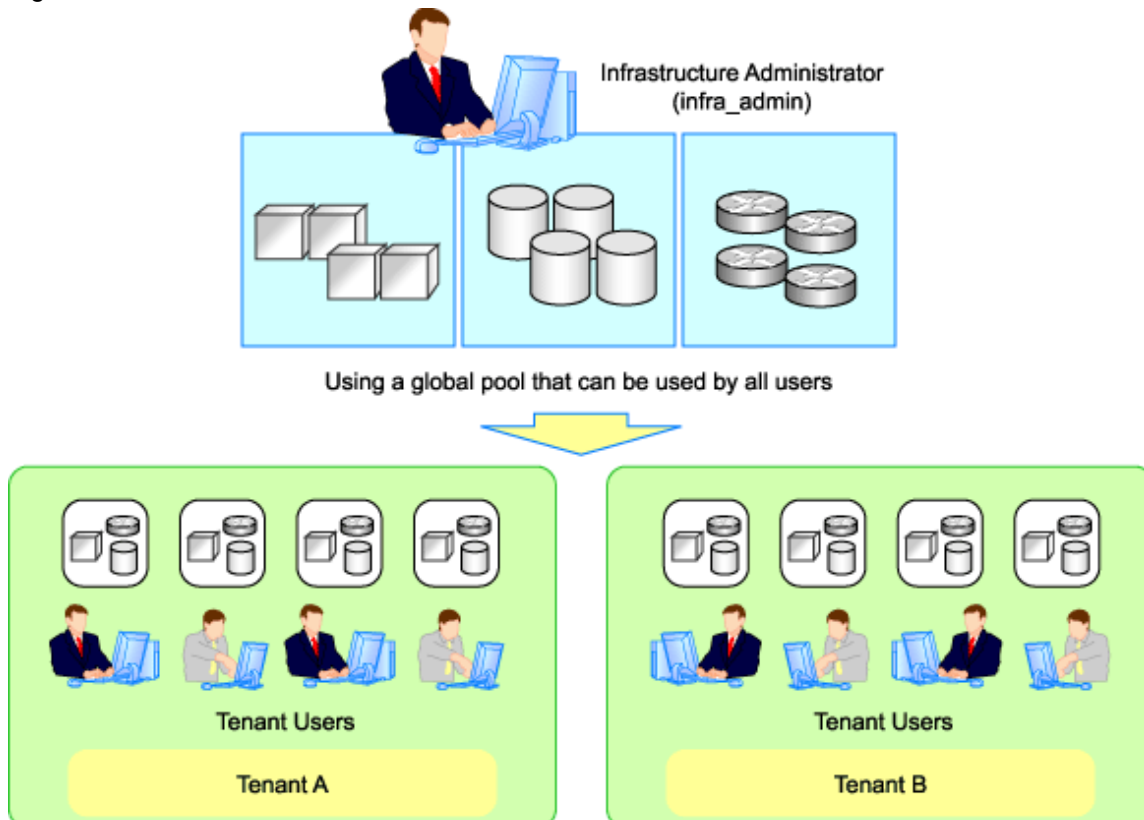


(Pattern B) Divide for Each Tenant (Global Pools Only)

Resources are placed in global pools, and L-Platforms are divided into tenants.

This enables public cloud-conscious tenant operation.

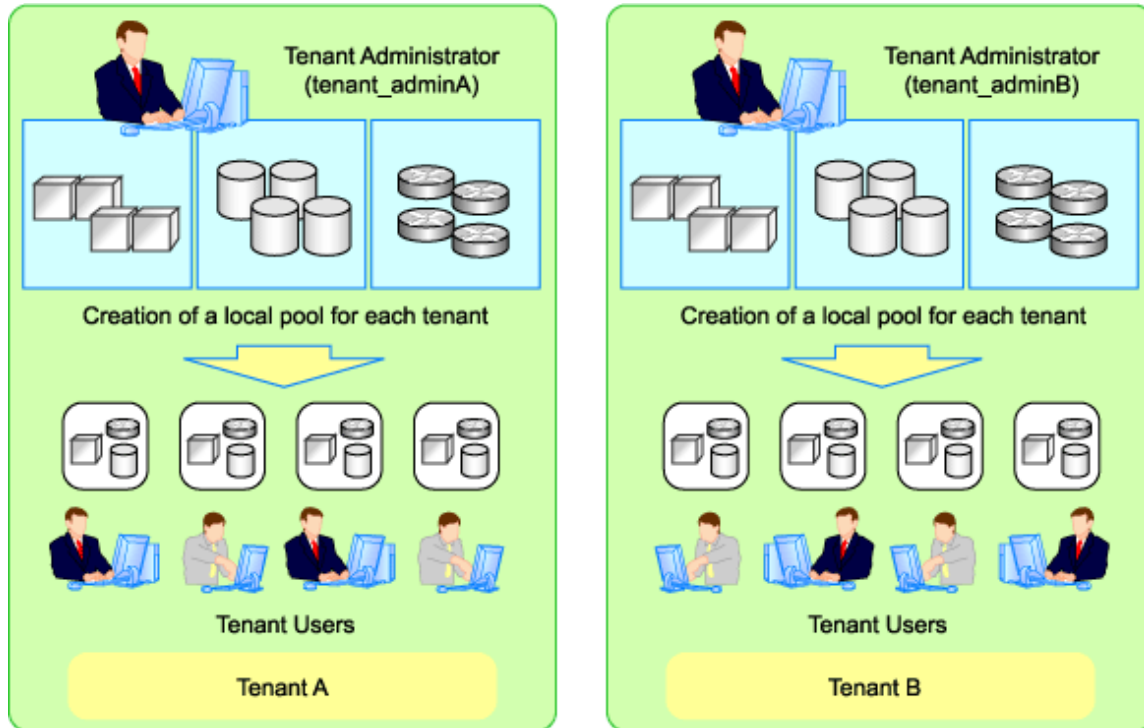
Figure 3.4 Pattern B



(Pattern C) Divide for Each Tenant (Create a Local Pool for Each Tenant)

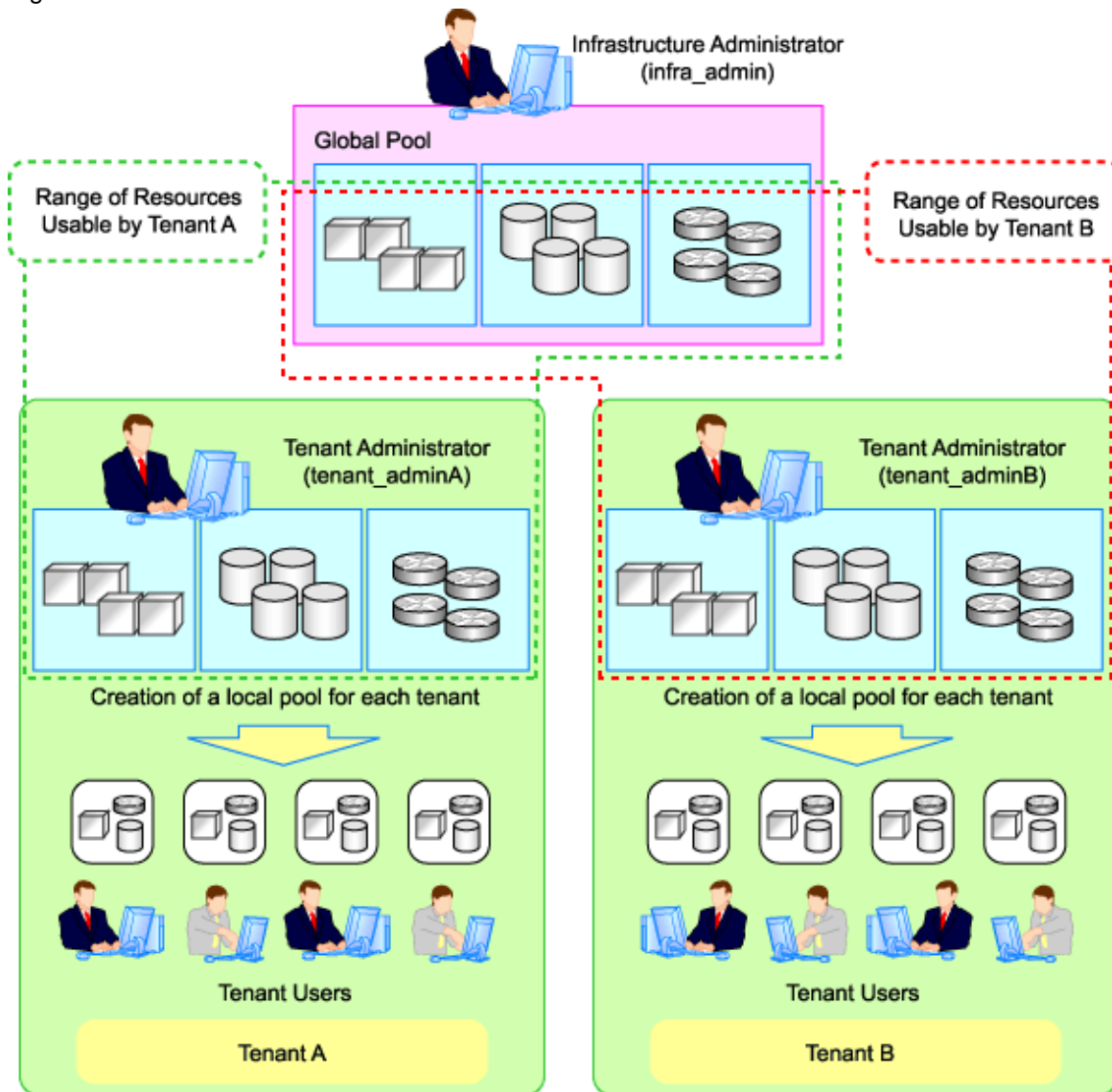
Create a local pool for each tenant. This pattern is a similar operation to allocating resources to each tenant.

Figure 3.5 Pattern C



(Pattern D) Divide for Each Tenant (Both Global and Local Pools, with Local Pools Given Priority)

Figure 3.6 Pattern D

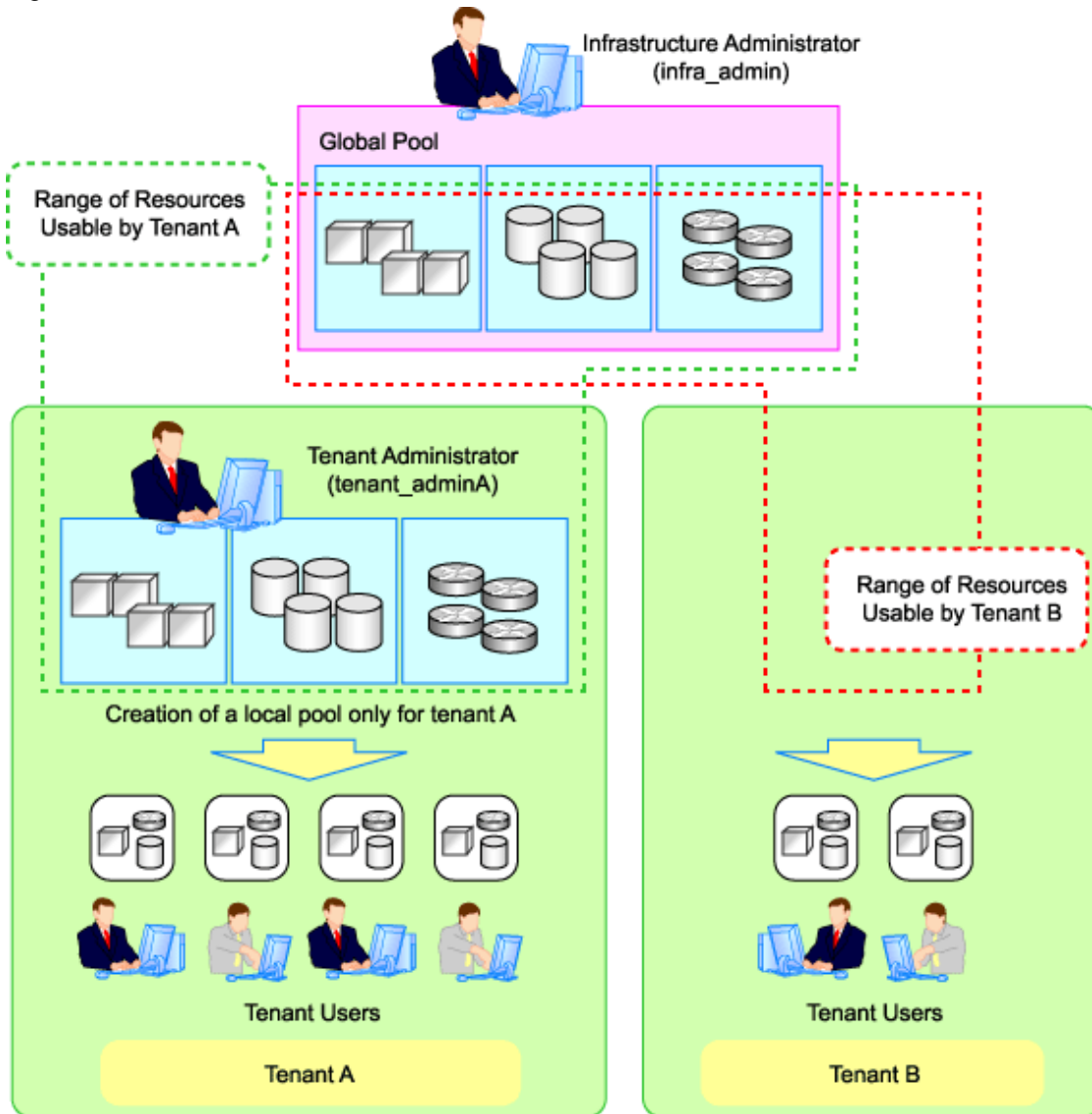


Only spare resources are placed in global pools. These spare resources are used when there is an increased workload.

(Pattern E) Divide for Each Tenant (Both Global and Local Pools, with Global Pools Given Priority)

This enables public cloud-conscious operation; however, tenants with a high service level can create a local pool and use resources exclusively.

Figure 3.7 Pattern E



3.2.3 Global Pool and Local Pool Selection Policy

This section explains the policy for selection of global pools and local pools.

The policy for selection of global pools and local pools from a resource application perspective is as indicated below.

Table 3.2 Global Pool and Local Pool Selection Policy

Resource Pools	Benefits	Disadvantages
Global pools	<p>Resources can be used effectively by placing resources that can be shared over the entire system in global pools.</p> <p>Tenant administrators do not need to be aware of resource availability.</p>	<p>If a specific tenant consumes a large amount of resources, the resources of the entire system may be exhausted.</p> <p>Infrastructure administrators must monitor the space for resources of the entire system.</p>
Local pools	<p>Even if a specific tenant rapidly consumes resources, the system as a whole is not affected.</p>	<p>Even resources that can be shared among tenants must be prepared for each tenant. Consequently, it is necessary to prepare more resources than for global pools.</p> <p>Tenant administrators must monitor resource availability for each tenant.</p>

3.2.4 Resource Pool Types

This section explains the types of resource pools.

Resource pools are categorized as indicated below.

Table 3.3 Resource Pool Types

Resource Pool Name	Description
Server pool	Resource pools containing physical servers.
VM pool	Resource pools containing VM hosts. VM hosts of different server virtualization software can be stored together.
Storage pool	Resource pools containing the following resources: <ul style="list-style-type: none">- Virtual storage resources (RAID groups, aggregates, VM file systems)- Disk resources (LUNs, FlexVol, virtual disks) The following resources can be stored together: <ul style="list-style-type: none">- Virtual storage resources- Disk resources- Resources of differing storage devices
Network pool	Resource pools that define and store network resources (VLAN IDs, uplink ports, etc.).
Address pool	Resource pools containing MAC addresses and WWNs.
Image pool	Resource pools containing the following resources: <ul style="list-style-type: none">- Physical image resources Cloning images collected from physical L-Servers- Virtual image resources Cloning images collected from virtual L-Servers Images using a template used for VM guest creation with VM management software

3.2.5 Subdividing Resource Pools

This section explains how to subdivide resource pools.

For resource pools, global pools and local pools can be divided for the following reasons:

- Resource differences (VM type, storage type, OS type, etc.)
- Performance differences
- Application differences (divide by user, etc.)

It is recommended to name resource pools including divided resources using names that make it clear to resource pool users.

3.2.6 Concept for Separating Tenants by Resource Pool

This section explains the concept for separating tenants (necessity of local pool creation) for each resource pool.

3.2.6.1 Server Pool

This section explains the concept for separating tenants of server pools.

Servers of differing models can be placed in the same server pool.

When performing server redundancy, consider a server pool to use as the work servers and spare server pool to use as backup servers.

- Use the same pool for servers and spare servers

As well as the work server, a spare server must also be considered.

- Separate the server pool and spare server pool

The server pool can be placed in a local pool, and the spare server pool can be placed in a global pool.

3.2.6.2 VM Pool

This section explains the concept for separating tenants of VM pools.

VM hosts of different server virtualization software can be stored in VM pools.

Even if a VM host exists in one VM pool, virtual L-Servers can be placed in a different tenant. Therefore, it is not necessary to separate VM pools.

However, local VM pools must be created for each tenant in the following cases:

- Consolidate VM hosts comprising VMwareDRS or HA in VM pools under the same tenant. A virtual machine may operate beyond tenants by VM management software control, when VM hosts are registered in different tenants.
- Place VM pools separately for each tenant when considering the vulnerabilities and loads of VM hosts.

3.2.6.3 Storage Pool

This section explains the concept for separating tenants of storage pools.

Virtual storage resources or disk resources of differing server virtualization software can be placed in the same storage pool.

Disk resources generated from virtual storage resources and disk resources created in advance can also be stored together.

In the following cases, place storage pools separately for each tenant:

- When separating storage pools according to usage
- When maintaining unique user information for security reasons
- When giving consideration to performance
- When using them as shared disks (from the disk resources created in advance)
- When using thin provisioning
- When using Automatic Storage Layering

3.2.6.4 Network Pool

This section explains the concept for separating tenants of network pools.

Network pools should be separated for each tenant for security reasons.

Network pools can be shared in environments that allow communication between tenants, such as intranets.

3.2.6.5 Address Pool

This section explains the concept for separating tenants of address pools.

MAC addresses and WWNs can be stored together in an address pool. However, they can easily be managed in separate address pools as the required resources differ depending on the server type. Use the same method of separation as for server pools.

Table 3.4 Address Set Resources Required for Each Server Type

	MAC address (Media Access Control address)	WWN
Blade servers (VIOM is required)	Yes	Yes
Rack mount servers (HBA address rename is required)	No	Yes

In the following cases, separate address pools:

- When separating the LAN for each tenant, and registering MAC addresses for firewalls etc.
- When separating the SAN for each tenant, and setting WWNs for fibre channel switch zoning
- When using software that is aware of MAC addresses for license authentication etc.

3.2.6.6 Image Pool

This section explains the concept for separating tenants of image pools.

For images of tenant-independent operating systems, it is not necessary to separate image pools.

It is necessary to separate image pools for each tenant for images that have tenant-unique information.

Specify the settings for tenant-unique applications, and then perform measures such as collecting images.

3.3 Defining User Accounts

This section explains how to define setting values for user accounts.

With Resource Orchestrator, you can restrict the operations that each user account can perform and the resources that operations can be performed on.

- Role

The operations that can be used by each user account.

- Access Scope

The resources that can be operated by each user account.

For details on the resources which can be operated for each role, refer to "Appendix B Access Control by Roles" in the "Operation Guide CE".

User Account Conditions

Configure the following parameters for user accounts and roles to be created on Resource Orchestrator:

User ID

The user ID must start with an alphanumeric character, and can contain between 4 and 31 alphanumeric characters, underscores ("_"), hyphens ("-"), and periods (".").

The number of characters for user ID and usable character types may be limited depending on the directory service used for Single Sign-On. For details on attributes to configure the user ID using the directory service, refer to "Table 4.14 Object Class" in "4.5.4 Registering Administrators". For details on limit values which can be specified as attributes to configure user IDs, refer to the manual for the directory service.

When using OpenDS for the directory service used by Single Sign-On, the user ID (uid attribute) must be unique in the directory service.

Password

The string must be composed of alphanumeric characters and symbols, and can be between 8 and 64 characters long.

The number of characters for passwords and the usable character types may be limited depending on the directory service used for Single Sign-On. For details on limit values of passwords, refer to the manuals of directory service.

Role

Configure the role to set for the user account.

Access Scope

Configure the access scope to set for the user account.

3.4 High Availability and Disaster Recovery Design

Using the following functions of Resource Orchestrator, high availability systems can be provided smoothly.

- L-Server redundancy

L-Server redundancy can be made with Resource Orchestrator.

On physical L-Servers, by specifying a spare server pool, an operating server can be switched to a spare server during server failure.

On virtual L-Servers, settings differ according to the server virtualization software being used.

For details, refer to "14.1.1 L-Server High Availability" in the "Operation Guide CE".

- Server switchover when a chassis fails

If a blade chassis in a configuration where Resource Orchestrator manages multiple blade chassis fails, when starting the physical L-Server on a blade chassis that is not damaged, operations can be re-started.

For details, refer to "14.1.2 Blade Chassis High Availability" in the "Operation Guide CE".

When creating VM hosts on physical L-Servers, server switchover can be performed for VM hosts if chassis failure occurs.

For details, refer to "[Appendix F Installation of VM Hosts on Physical L-Servers](#)".

- Switchover of operating or standby status of storage

For physical L-Servers, realizes the switchover of operating or standby disks (system/data disks) in configurations in which replication of the operating storage volume used by an L-Server to a standby storage volume is configured.

For details on prerequisites, refer to "[3.4.2 Storage Chassis High Availability Design](#)".

For details on operation methods, refer to "14.1.3 Storage Chassis High Availability" in the "Operation Guide CE".

- Admin server redundancy

Managers can be operated in cluster systems with Resource Orchestrator.

When operating the admin server in a Windows or Linux environment, redundancy for managers is also possible using clustering software.

An admin server can be operated on VMware and Hyper-V virtual machines.

Using redundancy for virtual machines, redundancy for managers is also possible.

For details on operation methods, refer to "14.2 Admin Server High Availability" in the "Operation Guide CE".

- Disaster Recovery

A simple and reliable Disaster Recovery environment is provided by exporting and importing the resource configuration information and user definition information (XML files) of Resource Orchestrator.

For details on prerequisites, refer to "[3.4.4 Disaster Recovery Design](#)".

For details on installing and operating Disaster Recovery, refer to "Chapter 15 Disaster Recovery" in the "Operation Guide CE".

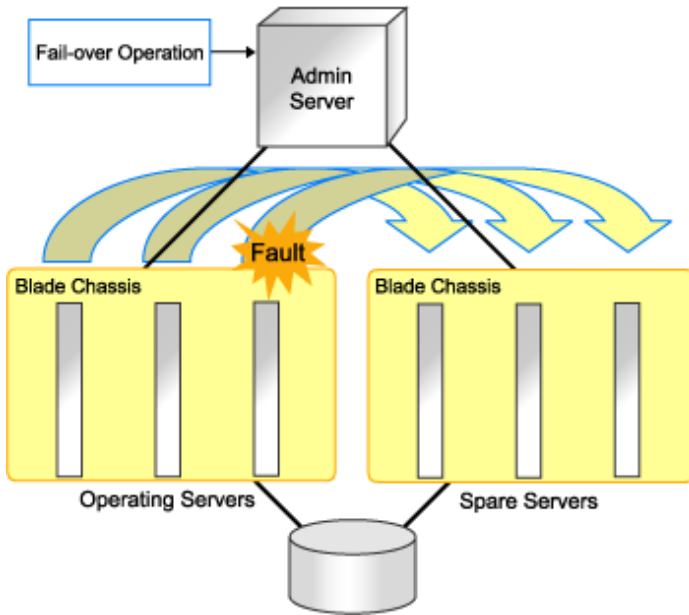
3.4.1 Blade Chassis High Availability Design

To perform server switchover for chassis failures, it is necessary to set the server switchover settings in advance.

By registering VM hosts as physical L-Servers, VM hosts can be switched to spare servers and virtual L-Servers can also be restarted.

For details, refer to "[Appendix F Installation of VM Hosts on Physical L-Servers](#)".

Figure 3.8 Server Switchover when a Chassis Fails



3.4.2 Storage Chassis High Availability Design

This section describes the prerequisites for switchover of operating or standby status of storage.

- The following disk resources are the targets of switchover.
 - Dynamic LUN mirroring
 - The replication is automatically configured.
 - LUN prepared in the storage unit
 - LUN replication settings need to have been made beforehand between the operational storage and backup storage.
- The LUN replication ratio between operating and standby storage states must be 1:1.
- If the operating disk resource is a disk (TPV or FTV for ETERNUS) with Thin Provisioning attributes set, the standby disk resource must also be a disk with Thin Provisioning attributes set. Similarly, if the operating disk resource is a disk with thick provisioning attributes set, the standby disk resource must also be a disk with thick provisioning attributes set.
- Operating disk resources must be connected to physical L-Servers.
 - Disk resources that are not registered in storage pools or are not connected to L-Servers are not processed.
- The switchover of disk resources is processed according to the replication relationship described in the replication definition file created in advance. Disk resources that are not described in the replication definition file are not processed.
 - If LUNs are added or the storage configuration is modified, it is necessary to edit the replication definition file.
- Standby disk resources must be detected by Resource Orchestrator. If LUNs can be accessed from the server, Resource Orchestrator cannot detect them. Do not register detected disk resources in storage pools.
- The storage unit identifier to enter in the replication definition file (IP address for ETERNUS, NetApp, or EMC CLARiON, or SymmID for EMC Symmetrix DMX Storage or EMC Symmetrix VMAX storage) must not be of the same configuration.
 - In this case, storage units with the same IP address or SymmID as an operating storage unit cannot be used as standby storage units.
- For configurations with NetApp storage units using the MetroCluster function for storage replication, switchover cannot be performed with this function.
 - By switching the operating and standby storage using the MetroCluster function, operation of physical L-Servers can be restored.

- To access operating and standby storage units from servers with physical L-Servers running on them, it is necessary to set the fibre channel switch in advance.

If the storage unit is ETERNUS, no settings are required in advance.

- The time required for switchover is relative to the number of L-Servers using operating storage units and the number of disk resources being used by L-Servers.

It is recommended that a test be performed in advance to confirm the time for restoration from storage unit failure.

3.4.3 Admin Server High Availability Design

Redundancy for managers is possible with Resource Orchestrator.

The following two methods of high availability operation for admin servers are available:

- Performing redundancy for managers using clustering software

When operating the admin server in a Windows or Linux environment, redundancy for managers is also possible using clustering software.

- Operating the manager on a virtual machine and using the redundancy function of the virtual machine

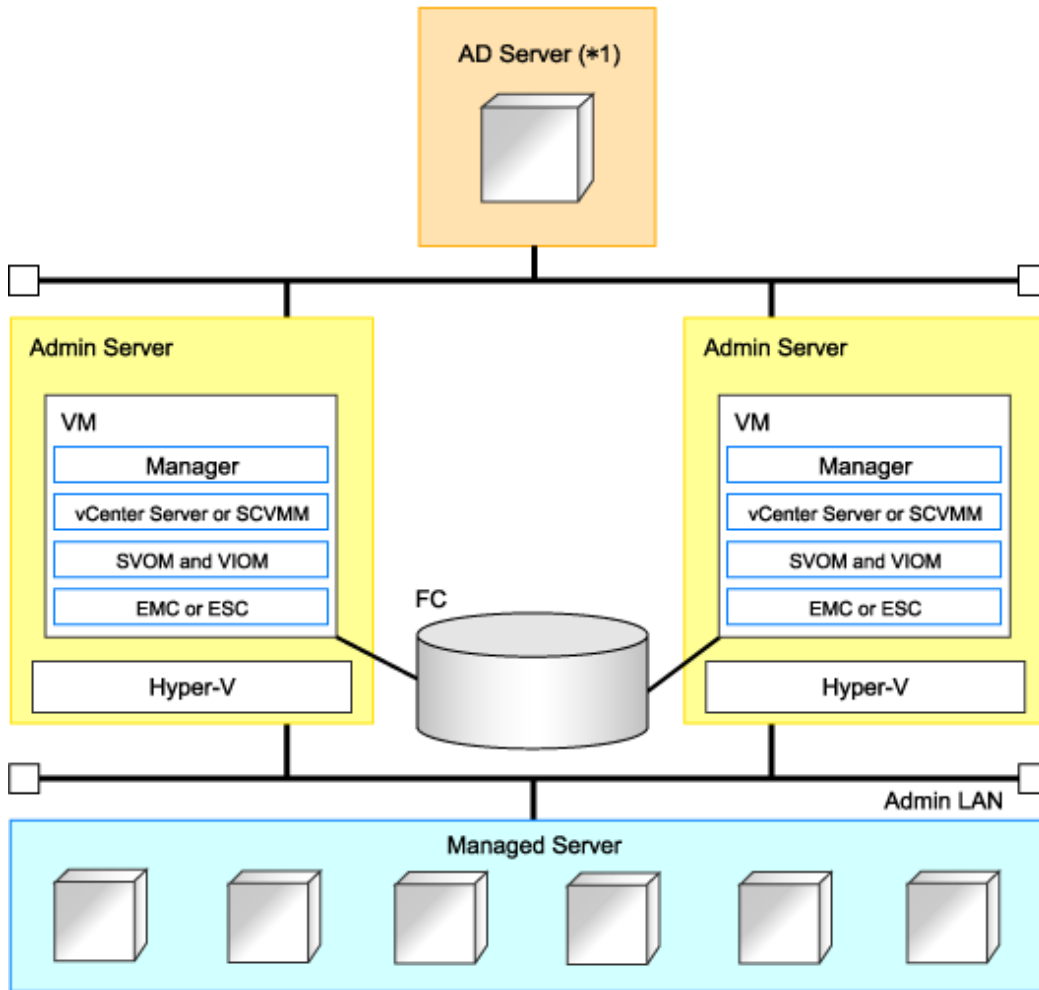
- Managers operate on the Windows guest OS's of Windows, Linux, and Hyper-V environments.
- If Virtual I/O by VIOM is used, create the manager on the Windows guest OS of a Hyper-V environment.

To operate managers in clusters on the Windows guest OS of a Hyper-V environment, use the configuration below.

- Place the manager on the same VM guest as the ServerView Operations Manager and ServerView Virtual-IO Manager.
- Place the manager and VM management software on the same VM guest.
- Place storage management software, excluding the manager and Solutions Enabler, on the same VM guest.
- Place Solutions Enabler on a VM host because it requires a fibre channel connection.

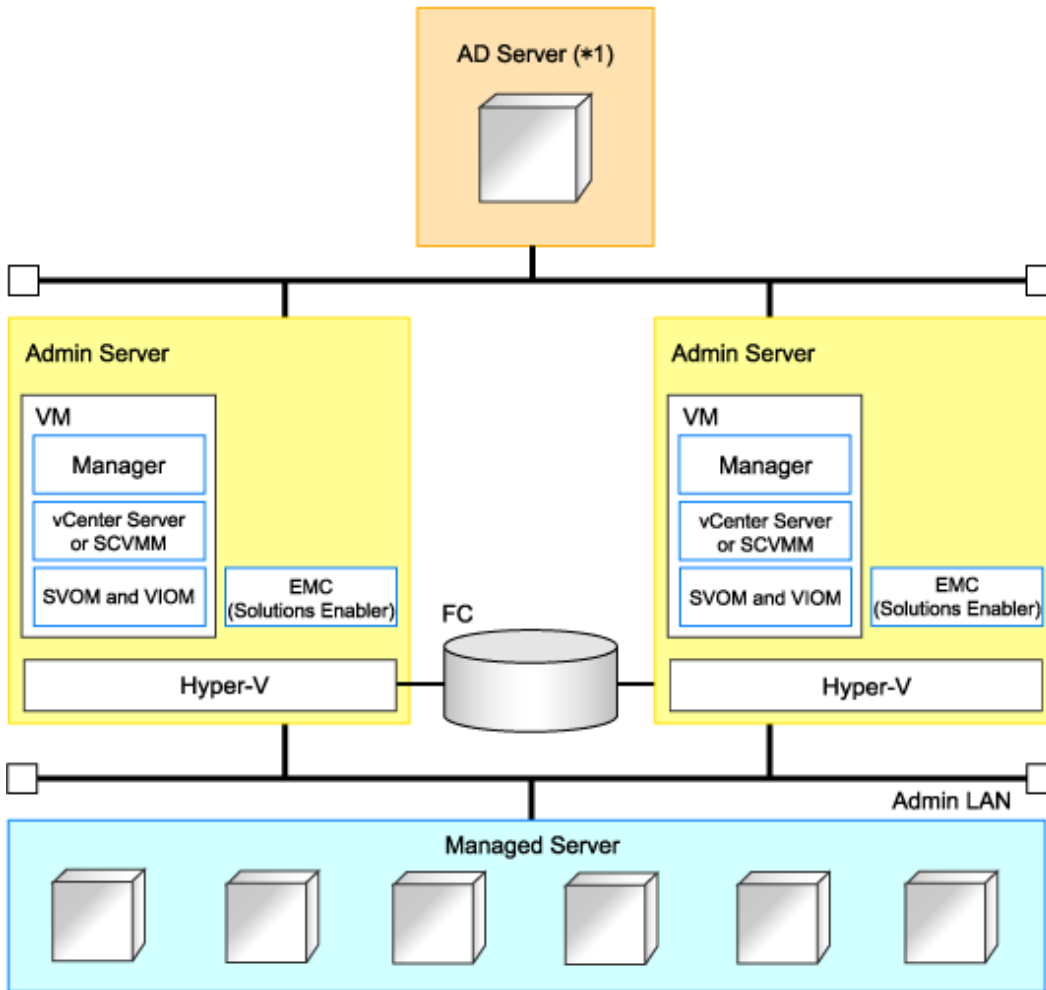
The configurations are shown below.

Figure 3.9 Storage other than EMC (Symmetrix)



*1: AD Server can be placed on each admin server.

Figure 3.10 EMC (Symmetrix) Storage



*1: AD Server can be placed on each admin server.

3.4.4 Disaster Recovery Design

This section explains the prerequisites for Disaster Recovery of L-Platforms and L-Servers.

Prerequisites for Disaster Recovery Environment Configuration

The prerequisites for configuring a Disaster Recovery environment are as follow:

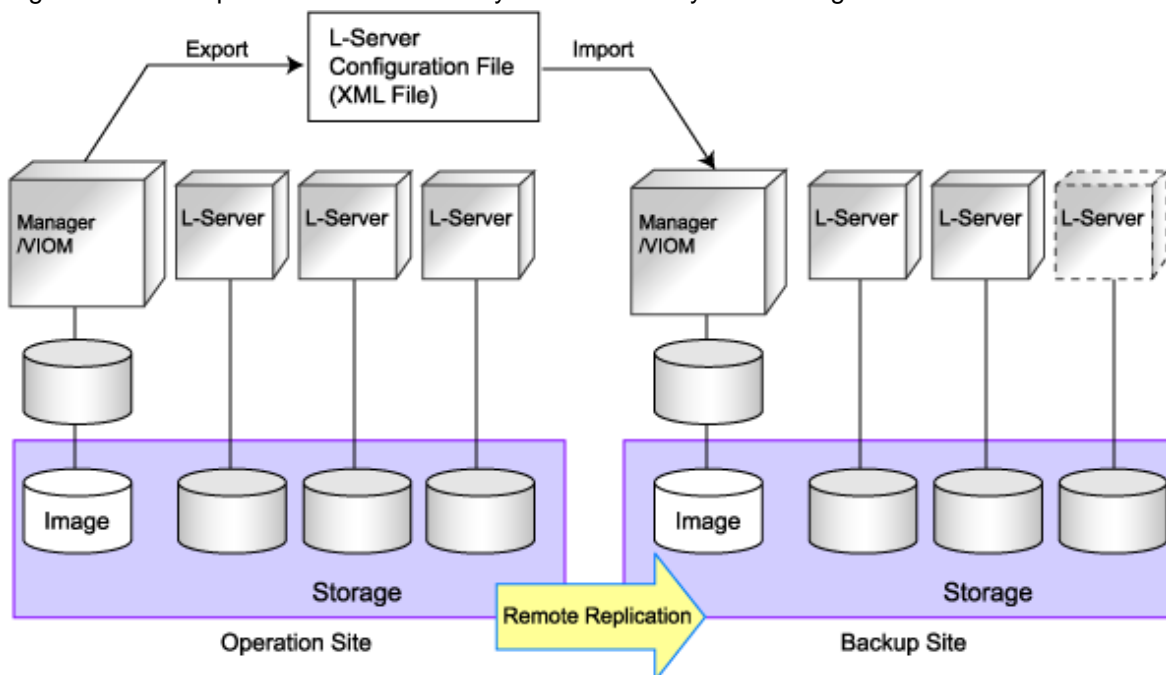
- Supported only when the manager is Windows.
- Primary and backup sites are supported only with ServerView Resource Orchestrator V2.3.0 or later. Use the same version of the primary and backup sites.
- When the managed server includes environments in which virtual L-Servers on RHEL-KVM are located, operations cannot be taken over by Disaster Recovery.
- Multiple primary sites can be set for one backup site, but the backup server cannot inherit the operations of multiple primary sites at the same time.
- When using the network device auto-configuration function, set the same network device configuration (model, links, firmware, account settings) for the primary and backup sites.
- Specify the zoning, VLAN, and CB uplink port settings for external networks and SAN switches. When manually configuring in advance, specify the same settings for the primary and backup sites.

- It is recommended that the same server configuration be used for the primary and backup sites. If the number of servers on backup sites decreases, not all operations running on primary sites can be continued.
- CB (Connection Blade) can be used for switch mode and end-host mode. IBP mode cannot be used.
- For systems using virtual L-Servers, create VM hosts and VM management software on physical L-Servers. Set different host names on primary sites and backup sites.
- L-Servers for which only the configuration definition has been created cannot inherit the operations of primary sites on backup sites.
- Set different IP addresses of storage units on primary sites and backup sites.

Example of Disaster Recovery Environment System Configuration Using Resource Orchestrator

An example Disaster Recovery environment system configuration using Resource Orchestrator is given below.

Figure 3.11 Example of Disaster Recovery Environment System Configuration



Chapter 4 Pre-setup Preparations

This chapter explains how to design and prepare a Resource Orchestrator installation.

4.1 Defining and Configuring the Server Environment

This section explains how to define and configure server environments.

4.1.1 Defining the Server Environment

This section explains how to define setting values for server environments.

4.1.1.1 Preparations for Server Environments

This section explains the preparations for setup of server environments.

Define the Server Environment

Define the following values for the server environment in advance.

- Chassis setting values (settings for blade servers and PRIMEQUEST)
- Settings for rack mount servers and tower servers

For details on how to define server environments, refer to "[4.1.1 Defining the Server Environment](#)".

For the servers not using server management software, refer to "For rack mount or tower servers" in "[4.1.1.3 Settings for Rack Mount or Tower Servers](#)".

For servers other than HP servers, a Baseboard Management Controller (hereinafter BMC) is used for server management.

Configure the Server Environment

Configure the following values for the server environment in advance.

- Chassis settings (settings for blade servers and PRIMEQUEST)
- iRMC settings (remote management controller)
- BIOS settings of managed servers

For details on how to configure server environments, refer to "[4.1.2 Configuring the Server Environment](#)".

For configuration of a server environment not using server management software, refer to "[Remote Management Controller Settings \(for Non-Blade Servers\)](#)" of "[4.1.2 Configuring the Server Environment](#)".

For the servers other than HP servers, replace the remote management controller with a BMC.

Configuration when Creating a Physical L-Server

When creating a physical L-Server, it is necessary to configure VIOM or HBA address rename settings as well as defining and configuring the server environment.

Usage methods of HBA address rename and VIOM differ depending on the hardware of the managed servers used to create a physical L-Server.

- Blade Servers
Use VIOM.

- Rack Mount Servers

Use HBA address rename.

Note

When using iSCSI boot, VIOM is required in the server environment.

For details, refer to "[Appendix D Design and Configuration when Creating a Physical L-Server](#)".

4.1.1.2 Chassis Settings (for Blade Server Environments)

Choose values for the following management blade settings, given the following criteria:

Chassis name

This name is used to identify the chassis on the admin server. Each chassis name must be unique within the system.
The first character must be alphabetic, and the name can contain up to 10 alphanumeric characters and hyphens ("-").

Admin IP address (IP address of the management blade)

These IP addresses can be used to communicate with the admin server.

SNMP community name

This community name can contain up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

SNMP trap destination

This must be the IP address of the admin server.

Note

To enable server switchover and cloning between servers in different chassis, use the same SNMP community for each chassis.

4.1.1.3 Settings for Rack Mount or Tower Servers

Resource Orchestrator supports the following types of remote management controllers to manage servers.

- For PRIMERGY Servers

iRMC2

- For HP Servers

iLO2 (integrated Lights-Out)

- For DELL or IBM Servers

BMC (Baseboard Management Controller)

Choose values for the following remote management controller settings according to the criteria listed below.

Admin IP address (IP address of the IPMI controller)

These IP addresses can be used to communicate with the admin server.

User name

Name of the user account used to log in the remote management controller and gain control over the managed server.

A user account with at least administration privileges within the remote management controller must be specified.

The user name can contain up to 16 alphanumeric characters and symbols (ASCII characters 0x20 to 0x7e).

If a user account with a name of 17 or more characters has already been set up, either create a new user account or rename it with a name of up to 16 characters.

Password

Password used to log in the remote management controller with the above user name.

The user name can contain up to 16 alphanumeric characters and symbols (ASCII characters 0x20 to 0x7e).

If a user account with password of 17 or more characters has already been set up, either create a new user account or change the password with one of up to 16 characters.

SNMP trap destination

The destination for SNMP traps sent by the remote management controller should be set as the admin server's IP address.

For PRIMERGY servers, the server status can be monitored from external server management software (ServerView Agents). In that case, choose a value for the following setting.

SNMP community name

Name of the SNMP community used to communicate with the server management software (ServerView Agents) on the managed server.

This community name can contain up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").



Use the same SNMP community for each server when using server switchover and cloning functions.

4.1.1.4 Chassis Setting Values (For PRIMEQUEST)

Choose values for the following management board settings, given the following criteria:

Chassis name

This name is used to identify the PRIMEQUEST chassis on the admin server. Each chassis name must be unique within the system.

The first character must be alphabetic, and the name can contain up to 10 alphanumeric characters and hyphens ("-").

Admin IP address (Virtual IP address of the management board)

These IP addresses can be used to communicate with the admin server.

User name

Name of the user account used to log into remote server management and gain control over the managed server.

A user account with at least administration privileges within the remote server management must be specified.

This user name must be between 8 and 16 alphanumeric characters long.

Password

Password used to log in the remote management controller with the above user name.

This password must be between 8 and 16 alphanumeric characters long.

SNMP community name

This community name can contain up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

SNMP trap destination

This must be the IP address of the admin server.



To enable server switchover and cloning between servers in different chassis, use the same SNMP community for each chassis.

4.1.2 Configuring the Server Environment

This section describes how to configure servers and chassis for Resource Orchestrator.

Chassis Settings (for Blade Servers)

Refer to the management blade manual to apply the settings chosen in "[4.1.1.2 Chassis Settings \(for Blade Server Environments\)](#)" to the management blade.

Note that the SNMP community must be set to Write (read and write) access.

- Admin IP address (IP address of the management blade)
- SNMP community name
- SNMP trap destination

This must be the IP address of the admin server.

Refer to the management blade manual to set the following SNMP agent settings.

- Set Agent SNMP Enable
Set to "enable".
- Set Agent SNMP Security Enable
Set to "disable".



Note

When powering off a chassis together with its enclosed server blades, servers are shut down using the graceful shutdown option of the management blade. To enable this feature, all servers within the chassis should have a ServerView Agents installed.

Chassis Settings (for PRIMEQUEST)

Refer to the management board manual to apply the settings chosen in "[4.1.1.4 Chassis Setting Values \(For PRIMEQUEST\)](#)" to the management board.

Note that the SNMP community must be set to Write (read and write) access.

- Admin IP address (Virtual IP address of the management board)
- User name
- Password
- SNMP community name
- SNMP trap destination

This must be the IP address of the admin server.

Enable the following function referring the instructions given in the management board's manual.

- SNMP Agent

Remote Management Controller Settings (for Non-Blade Servers)

Refer to the remote management controller manual to configure the following on the IPMI controller.

- IP address
- User name
- Password

- SNMP trap destination

This must be the IP address of the admin server.

BIOS Settings of Managed Servers

The following BIOS configurations must be modified.

System BIOS

This is the system BIOS for a managed server.

Enable or disable the internal SCSI BIOS and FC-HBA BIOS as appropriate, and set up the appropriate boot order.

Note

- The BIOS settings of server blades include an option to automatically start up servers when their enclosing chassis is powered on. For details, refer to the server blade manual.
- For PRIMERGY BX900/BX400, when an LND-PG203 is mounted as the LAN expansion card of the server blade, do not set the NIC of the LAN expansion card as "disable" in the server blade's BIOS settings. The connections between server blades and LAN switch blades are not shown correctly, when "disable" is set. The following functions do not operate correctly.
 - Changing and setting the VLAN for LAN switch blades (internal and external ports)
 - Server switchover (changing network settings while a server is switched over)
- If "UEFI" and "Legacy" are displayed when configuring boot settings from the network interface, select "Legacy".

FC-HBA BIOS

This is a BIOS setting that relates to FC-HBAs that have been installed as an expansion card in the blade server.

Enable or disable SAN boot as well as the connection of a SAN storage environment by means of a Fibre Channel switch.

Configure the following settings depending on the operating environment.

- **When using HBA address rename for SAN boot**

System BIOS

Enable the FC-HBA BIOS.

Set the boot order as follows:

1. Boot from the first admin LAN network interface (NIC1 (Index1))
2. Boot from the network interface used by the admin LAN (NIC2 (Index2))
3. Boot from CD-ROM (when a CD-ROM Drive is Connected)
4. Boot from a storage device

Note

- Do not change the boot order once a managed server has commenced operation. Even when booting from disk, there is no need to change the boot order.
- NICs other than NIC1 and NIC2 can also be used for the admin LAN. In this case, switch the order of step 1. and step 2. When using NICs other than NIC1 and NIC2 for the admin LAN, specify the same NIC configured in this procedure when registering the server. For details, refer to "2.4.2 Registering Blade Servers" and "2.5.1 Registering Rack Mount or Tower Servers" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".
- If "UEFI" and "Legacy" are displayed when configuring boot settings from the network interface, select "Legacy".

FC-HBA BIOS

Enable booting from SAN storage devices.

Refer to the manual of each FC-HBA for details on FC-HBA BIOS settings.

Note

- Restart the server saving BIOS configuration changes.
- HBA address rename may not work properly with older BIOS firmware versions. Please obtain and update the latest BIOS firmware from the following web site.

URL: <http://www.fujitsu.com/global/services/computing/server/ia/> (As of February 2012)

OS Settings for Managed Servers

When using the following functions, configure the OS to respond to ping commands.

- Auto-Recovery (for rack mount or tower servers)
- Configuration of monitoring information (ping monitoring)

Settings for ServerView Operations Manager (VMware ESXi)

When managing VMware ESXi using Resource Orchestrator, register the target VMware ESXi with ServerView Operations Manager.

For details, refer to the ServerView Operations Manager manual.

4.2 Defining and Configuring the Network Environment

This section explains how to define and pre-configure the network environment.

Use the following procedure to define and pre-configure the network environment.

1. Define the Network Environment
Design a network and define the network environment to set up.
2. Define Configuration Settings for Devices
Define the information to use to configure devices for use in the defined network environment.
3. Pre-configure Devices
Pre-configure the devices to be used in the defined network environment.
4. Preparations for Resource Orchestrator Network Environments
Perform the preparations necessary for setting up the Resource Orchestrator network environment.

4.2.1 Defining the Network Environment

When defining a network environment, the physical network device configuration should be designed considering the virtual systems that will actually be provided to the users.

Resource Orchestrator Networks

Resource Orchestrator networks are categorized into the following three types:

- Network for the Admin LAN

The admin LAN is the network used by admin servers to communicate with agents on managed servers and other managed devices (network and storage devices) for performing installation, operation, and maintenance.

- Network for the Public LAN

The public LAN is the network used by managed servers and managed network devices (firewalls and L2 switches) to provide services over internal or external networks (such as intranets or the Internet).

- Network for the iSCSI LAN

The iSCSI LAN is the network designed for communication between managed servers and storage devices.

For keeping operations secure, it is recommended to physically configure each network separately.

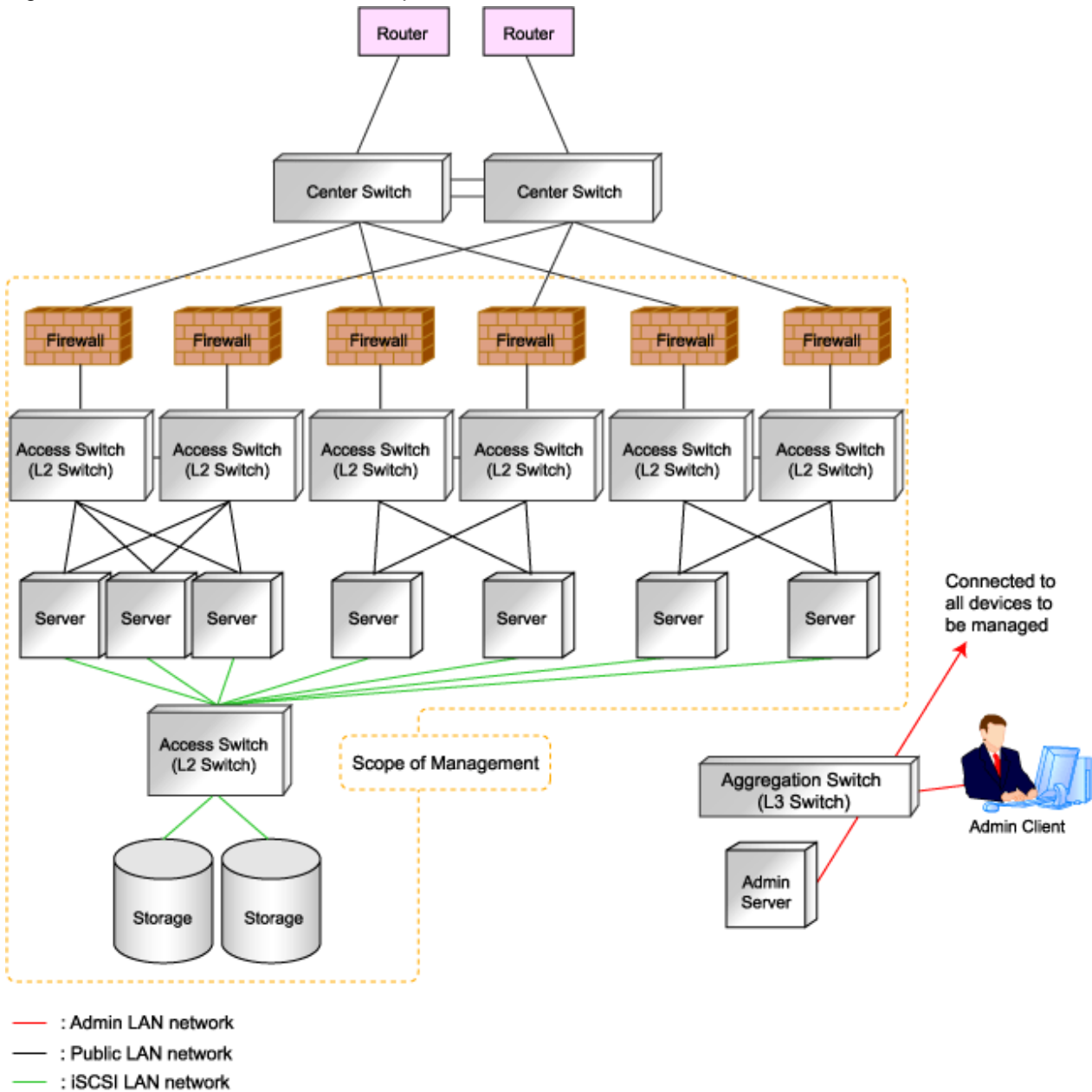
The maximum value of the subnet mask of the network that Resource Orchestrator support is 255.255.255.255(32bit mask). The minimum value is 255.255.0.0(16bit mask). However, 255.255.255.254 is not supported.



Information

.....
The admin LAN and iSCSI LAN are the networks that only infrastructure administrators need to be concerned about in normal operation.
.....

Figure 4.1 Network Environment Example



4.2.1.1 Admin LAN Network Design

Managed devices (servers, storage units, and network devices), the admin server, and the admin client are connected to the admin LAN.

An admin LAN can be divided into multiple admin LANs. Using this function, communication among tenants on physical L-Servers performed through an admin LAN can be prevented.

When using multi-tenant functions, prepare a separate admin LAN for each tenant, and configure the admin LAN for each tenant for network pools.

This improves the security of the network.

Information Necessary for Design

When designing an admin LAN, the following information needs to be defined beforehand:

- Estimate the number of tenants.
- Define the number of VLAN IDs for use on the admin LAN.
As the upper limit of the number of VLAN IDs varies depending on the device, when using devices that connect with both the admin and public LANs, ensure that the number does not exceed the maximum.
- Define the VLAN ID range for use on the admin LAN.
As available VLAN ID range varies depending on the device, when using the devices that connect with both the admin and public LANs, ensure that ranges do not overlap.
- Define the IP address range of the admin LAN.
- Decide whether to configure admin route redundancy.

Admin LAN for Servers

For each server, choose the network interfaces to use for the following purposes.

- Decide the network interfaces assigned to the admin LAN.

The number of network interfaces required for the admin server and managed servers can be determined as follows.

For a non-redundant configuration: one network interface

For a redundant configuration: two network interfaces

If HBA address rename is used, two network interfaces (named NIC1 and NIC2) are required regardless of network redundancy.

For details, refer to "[Required Network Configuration when Using HBA address rename](#)".

For PRIMERGY Managed Servers

- For a non-redundant configuration
NIC1 (Index1)
- For a redundant configuration, or when using HBA address rename
NIC1 (Index1) and NIC2 (Index2)

The NICs above used by managed servers are the default values, and they can be changed when registering managed servers.

For details, refer to "2.4 When using Blade Servers" and "2.5 When using Rack Mount and Tower Servers" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

For PRIMEQUEST Managed Servers

- For a non-redundant configuration
The smallest NIC number of the GSPB allocated to a partition
- For a redundant configuration, or when using HBA address rename
The smallest and the second smallest NIC number of the GSPB allocated to a partition

For Rack Mount or Tower Managed Servers

Check the alignment sequence and number of NICs on the back of rack mount or tower servers, and then decide the numbers of NICs specified for the admin LAN using consecutive numbers starting with 1 (such as 1, 2,...).

- For a non-redundant configuration
NIC 1
- For a redundant configuration
NIC 1 and NIC 2

Choose the following settings to fit the system environment.

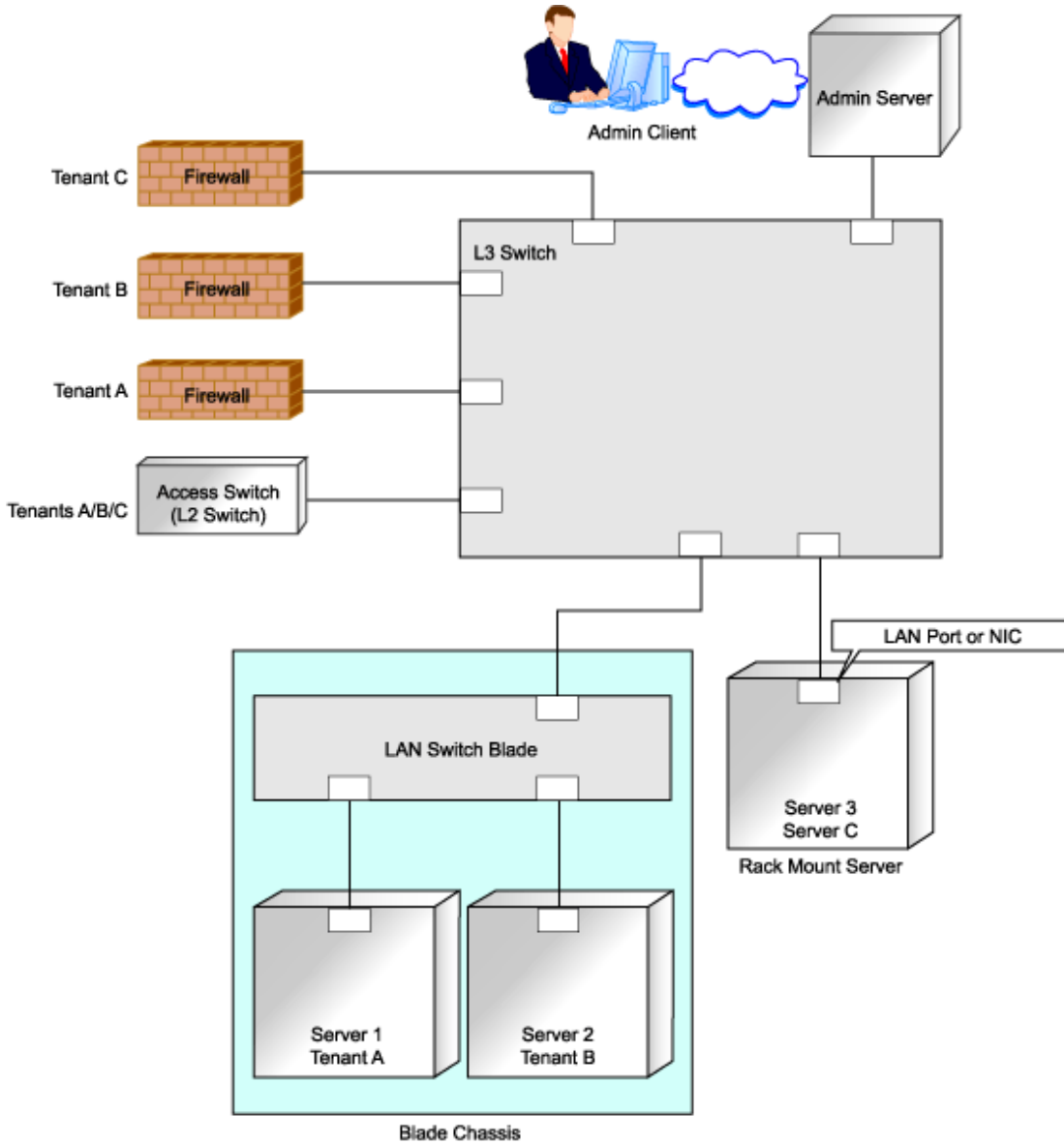
- Decide whether to use Admin LAN redundancy.
Perform the redundancy of the admin LAN as below.

- For physical L-Servers, use Intel PROSet, PRIMECLUSTER GLS, or Linux bonding.
- For VM hosts, perform redundancy according to the server virtualization software used.
- Decide the network configuration for LAN switch blades.

Admin LAN for Network Devices

Choose the LAN ports of the network devices (firewalls, L2 switches, and L3 switches) to be used.

Figure 4.2 Admin LAN Connection Example



 See

When the admin LAN is operated among multiple subnets, install DHCP servers referring to "2.1.2 Installation [Windows]" or "2.1.3 Installation [Linux]" in the "Installation Guide CE".

Note

- Do not place DHCP servers between the manager and managed servers.
 - For the admin server, only a single IP address can be used on the admin LAN.
 - A network address that was set when installing the manager has been registered as an admin LAN network resource.
 - Change the admin LAN network resource specifications, and register the IP address of a device that is not managed by Resource Orchestrator as an IP address to exclude from allocation.
If the IP address is not registered, it may conflict with the IP addresses of devices that are not managed by Resource Orchestrator.
 - When using blade servers, connecting the management blade to a LAN switch blade will make the management blade inaccessible in the event of a LAN switch blade failure. Therefore, it is recommended that the management blade be connected to the admin LAN using a LAN switch outside the chassis.
 - When performing I/O virtualization using HBA address rename, if specifying a 10Gbps expansion card (NIC) for the admin LAN, backup and restore, and cloning cannot be used.
 - Do not place a DHCP server or a PXE server on the admin LAN.
 - Do not configure multiple IP addresses for network interfaces used on the admin LAN.
 - When the same cloning image is deployed to multiple servers, IGMP snooping should be enabled on admin LAN switches. If IGMP snooping is not enabled, transfer performance may deteriorate in the following cases:
 - When ports with different speeds co-exist in the same network
 - When multiple image operations are being executed simultaneously
 - For PRIMERGY BX900/BX400 LAN switch blades operating in IBP mode, the admin LAN should not be included in the ServiceLAN or the ServiceVLAN group configuration.
-

Safer Communication

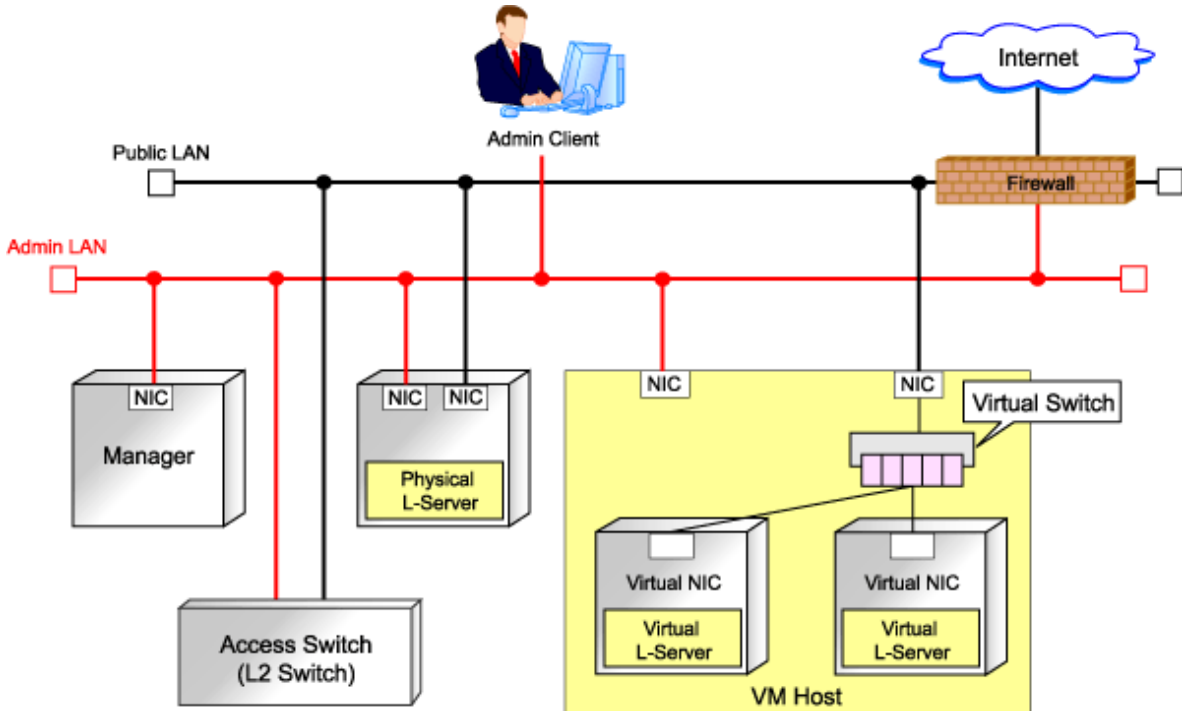
For environments where virtual L-Servers and the admin server (manager) communicate, it is recommended to perform the following configuration to improve security:

- Place a firewall between the public LAN used by the virtual L-Servers and the admin LAN.

Installing firewalls or configuring OS firewalls according to the description in "[Appendix A Port List](#)" enables secure operation of the admin LAN.

In Resource Orchestrator, the manager accesses agents using HTTPS communication.

Figure 4.3 Network Configuration Example



Required Network Configuration when Using HBA address rename

At startup a managed server set with HBA address rename needs to communicate with the Resource Orchestrator manager. To enable startup of managed servers even when the manager is stopped, Resource Orchestrator should be set according to one of the following configurations.

- Manager cluster configuration with admin LAN redundancy using the redundant line control function of PRIMECLUSTER GLS or Intel PROSet

For details, refer to "Appendix B Manager Cluster Operation Settings and Deletion" in the "Installation Guide CE".

- Dedicated HBA address rename server

This section describes the network configuration that is required for an environment with a dedicated HBA address rename server. For details about the HBA address rename setup service, refer to "[8.2.1 Settings for the HBA address rename Setup Service](#)".

- This service must be on the same admin LAN as the admin server. Do not start more than one instance of this service.
- This service uses NIC2 (Index2).

Connect NIC2 of the managed server to the admin LAN.

NIC2 is the default value, and it can be changed when registering managed servers.

For details, refer to "2.4 When using Blade Servers" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- This service periodically obtains information about managed servers from the admin server and operates using this information. For this reason, it should be installed on a server that can be left active all the time.
- There must be two LAN cables between LAN switches (cascade connection) on the admin server and on the managed server.

[Linux]

- Use eth0, for the network interface for this service to communicate with the admin server.

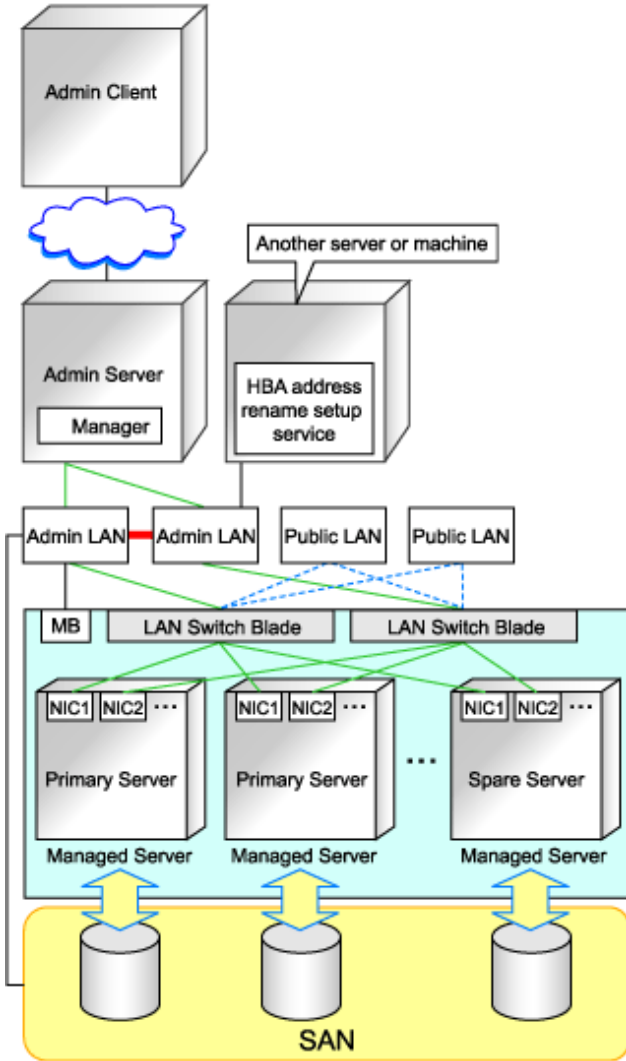
Connect the eth0 NIC to the admin LAN.

Note

The HBA address rename setup service cannot operate on the same server as ServerView Deployment Manager, or on a server where any other DHCP or PXE service is running.

The following diagram shows an example of how the HBA address rename setup service can be configured.

Figure 4.4 Sample Configuration Showing the HBA address rename Setup Service (with PRIMERGY BX600)



MB: Management Blade
—: Redundancy using link aggregation

- Connections between switches on the admin LAN can be made redundant using link aggregation.
- Connect NIC2 (Index2) to the admin LAN (when it is the default).
- Configure the HBA address rename setup service on a server connected to the admin LAN. This server must be different from the admin server.
- Ensure that the server or personal computer that is used to operate the HBA address rename setup service is always on when the managed servers are active.

4.2.1.2 Virtual System Design

Design virtual systems for users.

Information Necessary for Design

When designing virtual systems, the following information needs to be defined beforehand:

- Define the required resources.
 - Decide whether to use firewalls.

If security must be maintained for each virtual system, deploy firewalls.

Firewalls should also be deployed when using a hierarchical configuration that establishes an intranet connected with a DMZ.
 - Choose the server type (physical L-Server or virtual L-Server).
 - Decide whether to use iSCSI. (Storage)
- Define the communication route configuration.

It is normal to use a redundant configuration for communication routes.
- Define the assumed communication performance (throughput).

Define the assumed communication performance for each system.

Figure 4.5 Example of Virtual System Configuration Elements

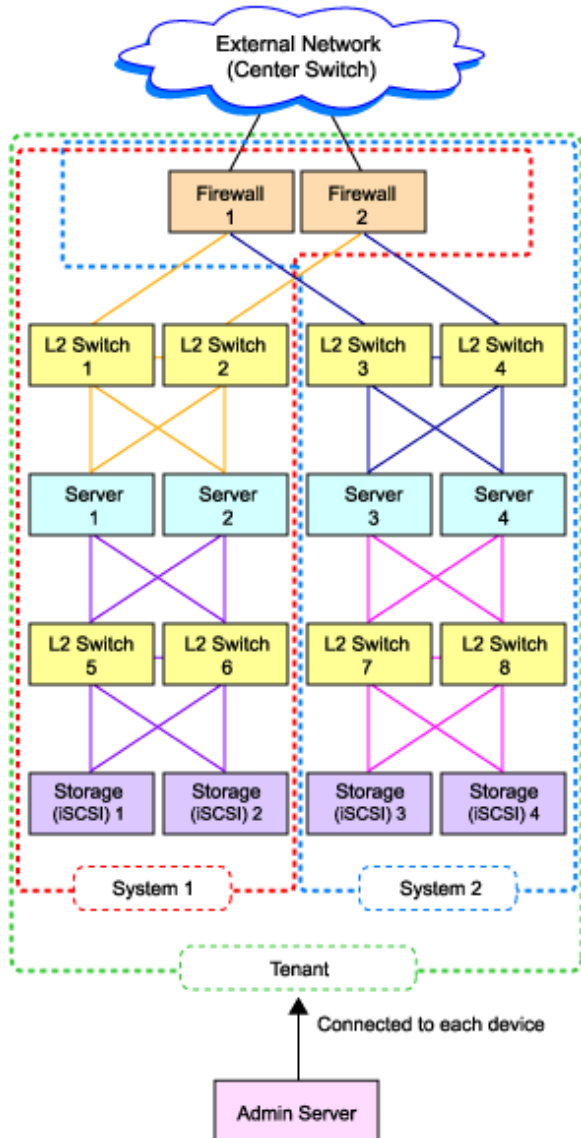
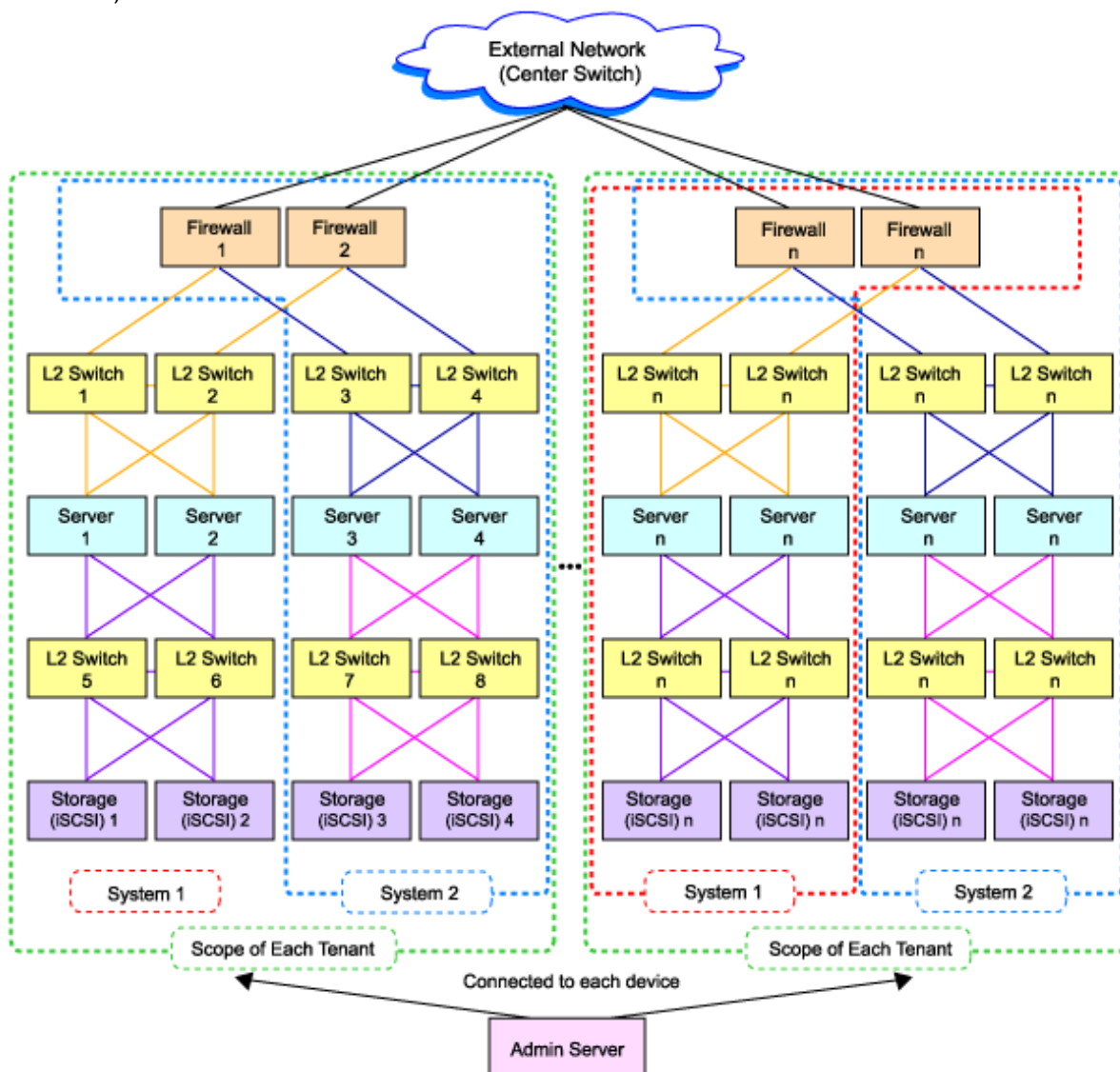


Figure 4.6 Example of Overall Configuration of a Virtual System (A Collective of Virtual System Configuration Elements)



4.2.1.3 Physical Network Design for the Public LAN and iSCSI LAN

Managed devices (server machines and network devices) are connected using the public LAN.

Managed devices (server machines and storage units) are connected using the iSCSI LAN.

Design of an iSCSI LAN is required to connect the iSCSI-enabled storage devices and servers to which physical L-Servers will be deployed.

Information Necessary for Designing a Public LAN

When designing a public LAN, the following information needs to be defined beforehand:

- Estimate the number of required devices (servers and network devices).

Define the required devices based on the designed virtual system.

The number of required devices should be estimated based on the following information:

- Performance requirements assumed during designing of the virtual system
- The number of planned tenants defined during designing of the admin LAN

- Specifications of devices to be used
- Estimate the specifications (including supported functions) required for the devices.
- Define the number of VLAN IDs for use on the public LAN.

As the upper limit of the number of VLAN IDs varies depending on the device, when using devices that connect with both the admin and public LANs, ensure that the number does not exceed the maximum.

- Define the VLAN ID range for use on the public LAN.

As available VLAN ID range varies depending on the device, when using the devices that connect with both the admin and public LANs, ensure that ranges do not overlap.

- Define the IP address range of the public LAN.
- Decide whether to configure communication route redundancy.

Whether to configure communication route redundancy should be decided based on the designed virtual system.

- Define the LAN ports or NICs to use.

Define one of the following:

- For network devices, LAN ports other than the ones assigned to the admin LAN.
- For servers, NIC ports other than the ones assigned to the admin LAN.

When planning to use a rack mount server or tower server as a physical L-Server, define the following information:

- The NIC number of the rack mount server or tower server

Check the alignment sequence and number of NICs on the back of the rack mount or tower servers, and then choose the numbers of NICs to be specified when creating a physical L-Server, by consecutive numbers starting with 1 (such as 1, 2,...).

As the admin LAN uses small NIC numbers ("1" for non-redundant admin LANs or "1-2" for redundant LANs), ensure NICs with larger numbers are used.

Information

For blade servers, depending on the model of LAN switch blade used in the same chassis, certain network interfaces may not be available.

In this case, add expansion NICs and a LAN switch blade, or share the NIC used for the admin LAN.

All network interfaces shared between the admin LAN and the public LAN for managed servers should be configured with tagged VLAN IDs.

The NICs that are unavailable depend on the combination of the mounted LAN switch blade and blade server. For details, refer to the manual of the LAN switch blade and blade server.

Information Necessary for Designing an iSCSI LAN

When designing an iSCSI LAN, the following information needs to be defined beforehand:

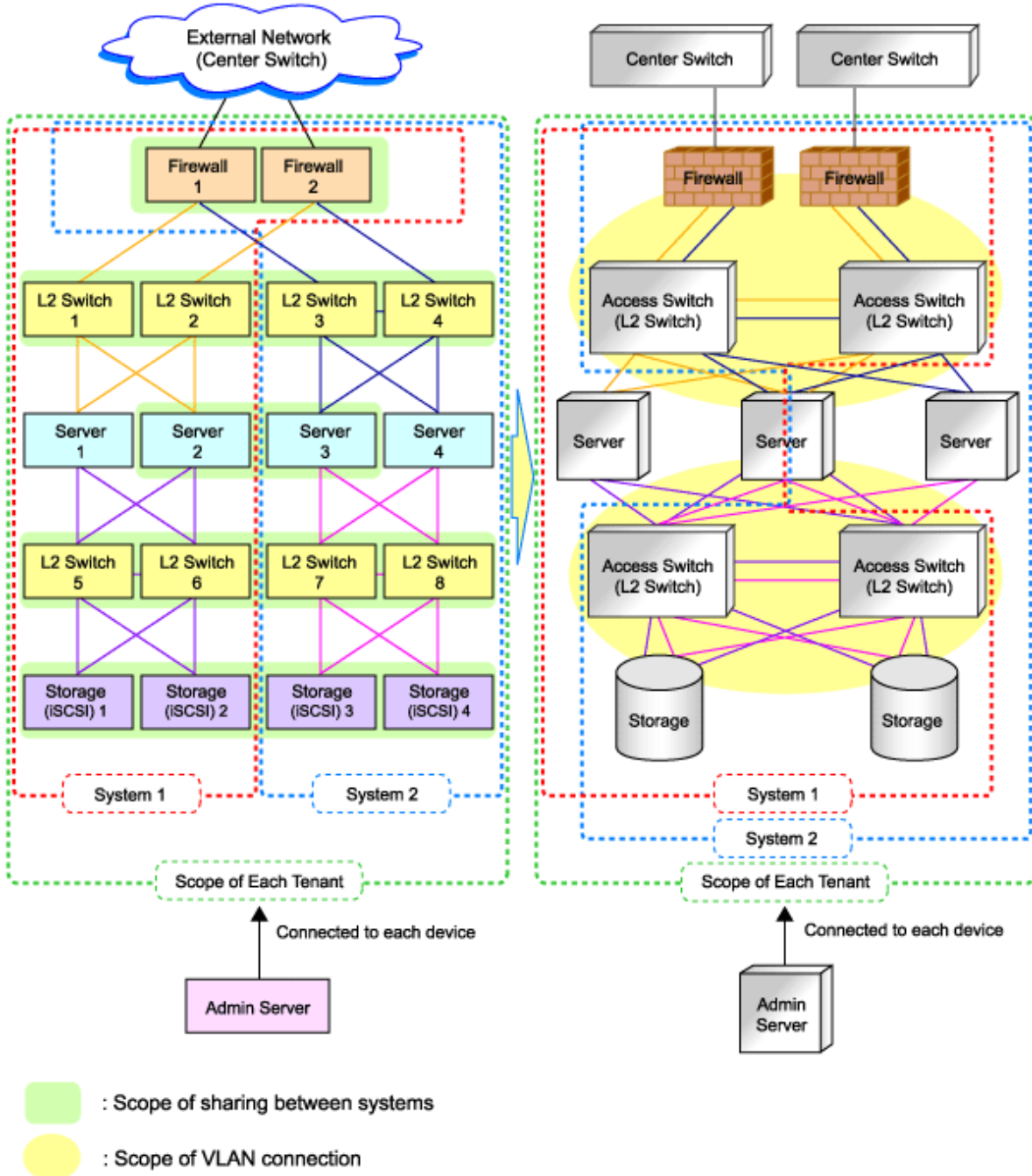
- Define a NIC on the server used for an iSCSI LAN.
Both single and multi-path configurations are available.
- For each tenant, define a network address and a VLAN ID for use on the iSCSI LAN.
- Define whether to connect external switches between ETERNUS storage and LAN Switch Blades, or NetApp storage and LAN switch blades.
- Define whether to use multi-tenant functions on ETERNUS storage or NetApp storage.
- Define an IQN to be used for the NIC of the server.

- Decide a network address to be used for the port of the storage.
- Define an IQN to be used for the port of the storage.
- Define the use of authentication on iSCSI communication. When using authentication, define the authentication information.

Determine the physical network configuration by defining devices necessary for the public LAN and iSCSI LAN that meet the requirements for the designed virtual system.

A sample image of virtual systems and the corresponding physical network configuration is shown below:

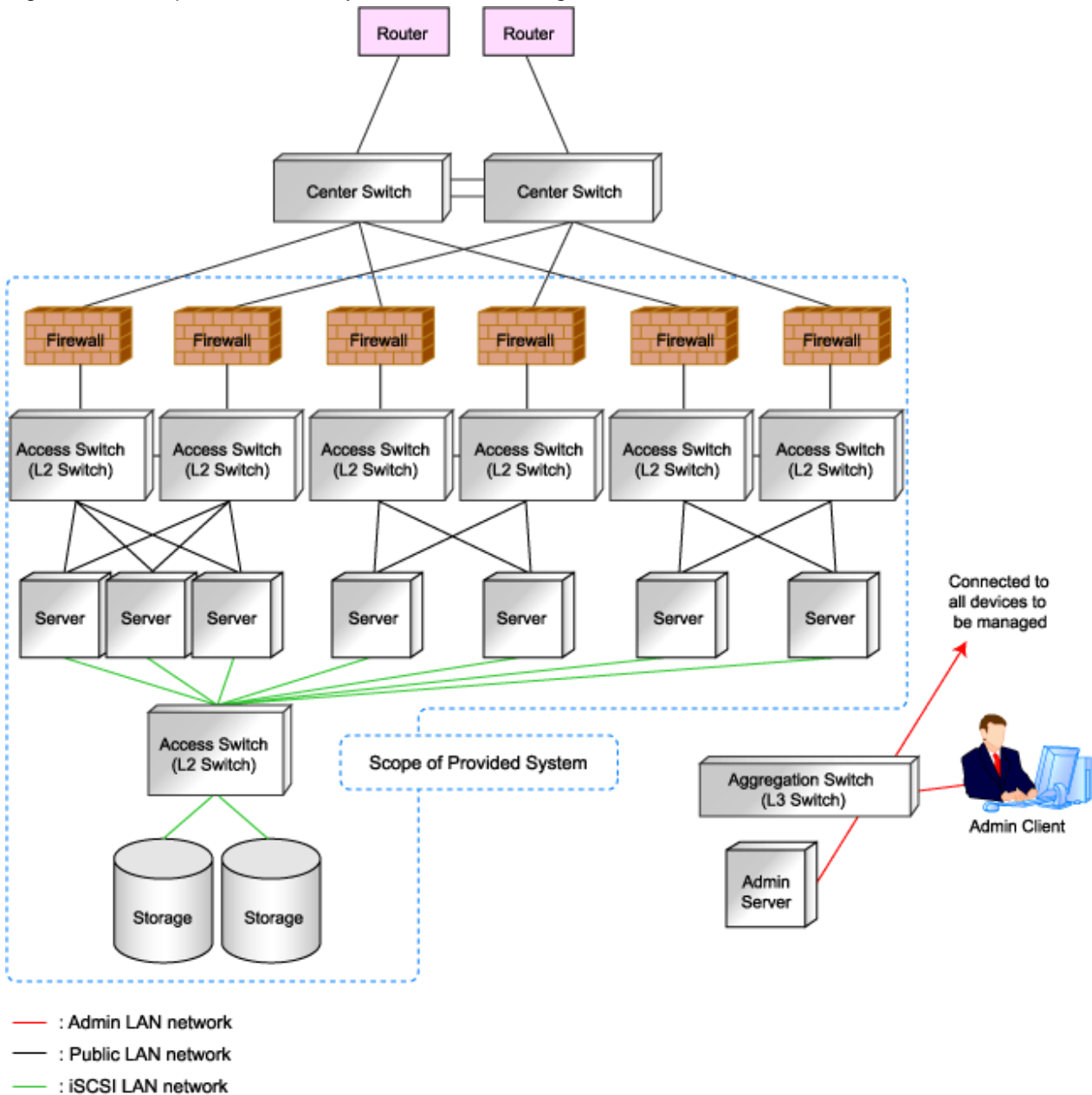
Figure 4.7 Sample Image of Virtual Systems and the Corresponding Physical Network Configuration



By defining how many virtual systems should be configured for each tenant and how many tenants are to be prepared, the required number of devices can be determined, making the overall configuration clear.

An example of the overall configuration of the physical system is shown below:

Figure 4.8 Example of Overall Physical Network Configuration



4.2.1.4 Relationship between Physical Network Configuration and Resources

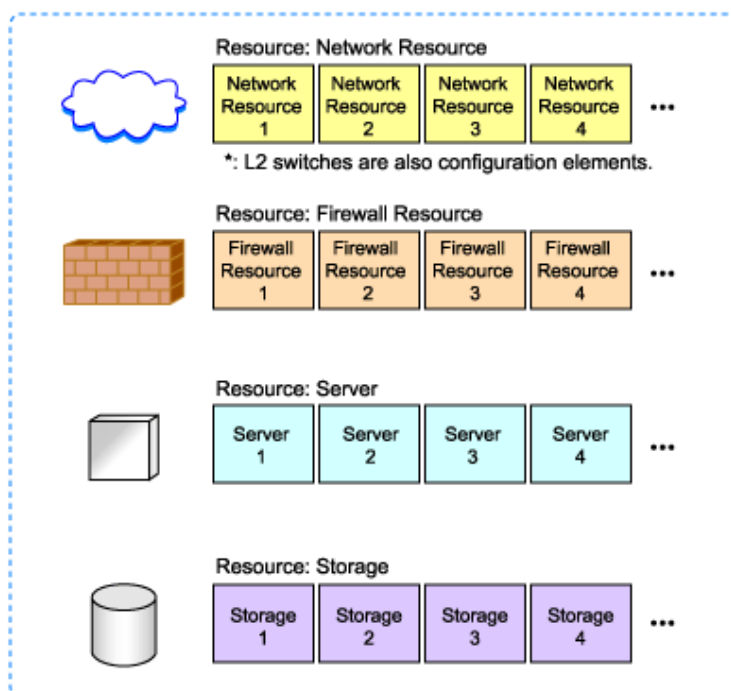
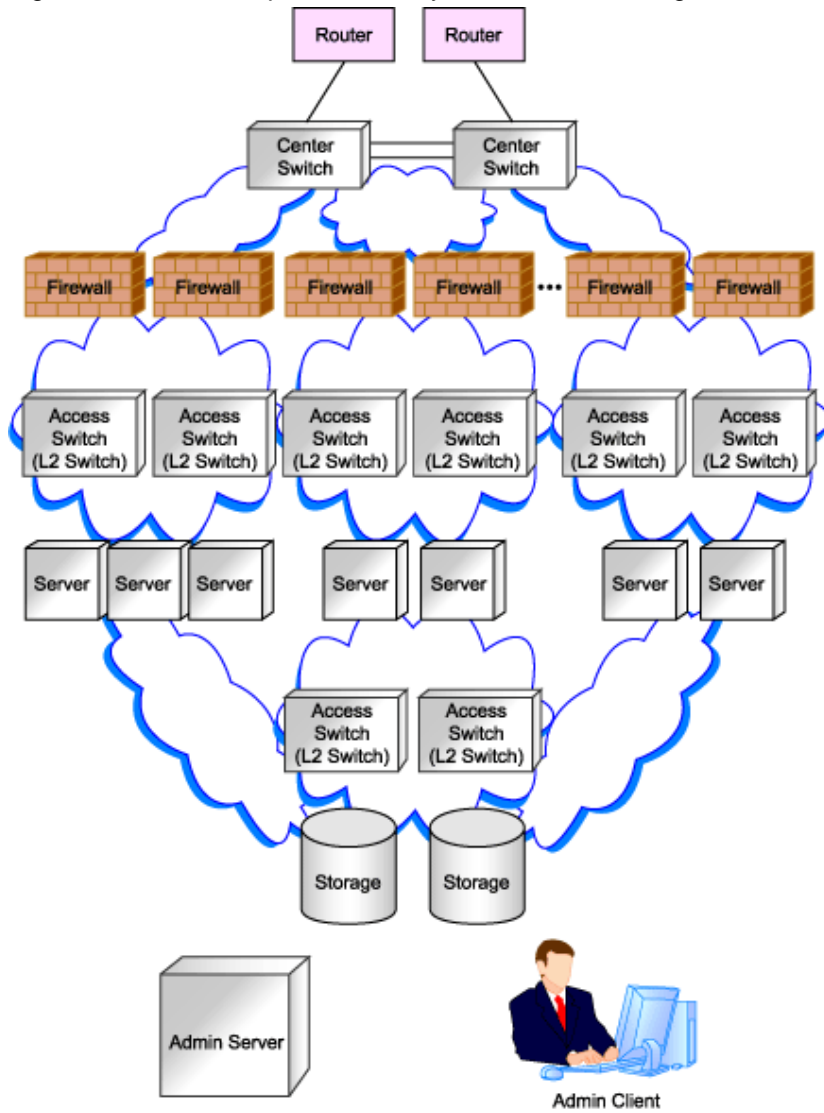
This section explains the relationship between the defined physical system and the resources managed by Resource Orchestrator.

Using Resource Orchestrator, you can provide users with virtual systems and also operate those virtual systems. Therefore, it is necessary to understand the relationship between physical systems and the resources configuring the virtual systems in advance.

Depending on how the physical devices are used in the virtual system, physical devices and resources can be in "one-to-one" or "one-to-*n*" relationships.

The relationship between physical networks and resources is shown below, using "Figure 4.8 Example of Overall Physical Network Configuration" as an example.

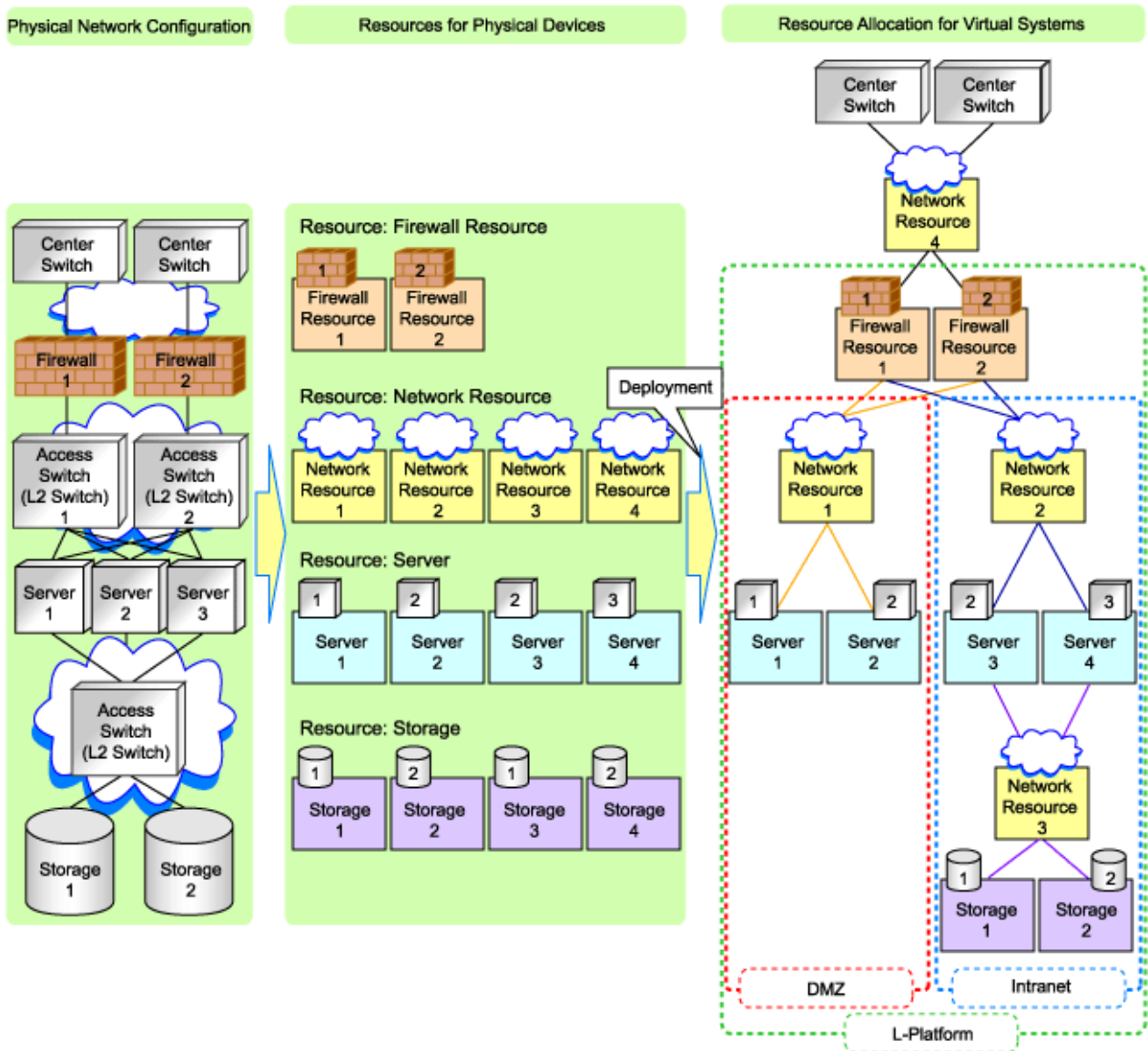
Figure 4.9 Relationship between Physical Network Configuration and Resources



The following figure shows a sample image when physical devices and resources are allocated for a single virtual system (L-Platform). In this sample image, resources are allocated for firewalls and L2 switches on a one-to-one basis, while resources are allocated for servers and storage devices on a one-to-*n* basis.

Resource Orchestrator manages L2 switches as network devices. However, when allocated to a virtual system, L2 switches are not displayed on the virtual system because they are included as network resource components.

Figure 4.10 Virtual System and Resource Allocation Example



4.2.2 Defining Configuration Settings for Devices

Define the configuration settings necessary for management of the defined network environment.

Information

In addition to the information necessary for management by Resource Orchestrator, additional information is required to operate each device.

For example, the following configuration information is necessary:

- Configuration information necessary for saving and referring to the logs output by individual devices
- Configuration information necessary for backing up and restoring the information from individual devices

Refer to the manuals of the devices to be used to check the information necessary for operation.

4.2.2.1 Settings for the Admin Server

Define the following information to be configured on the admin server.

- Device name
- IP address used by the admin server for management purposes

Decide the IP address for the network interface used to communicate with managed servers and network devices.

4.2.2.2 Settings for Admin Clients

Define the following information to be configured on the admin clients.

- Device name
- Routing information

When the admin IP address of the admin client is in a different subnet from that of the admin server, check the network device that works as the gateway, and define the routing information accordingly.

4.2.2.3 Settings for Managed Network Devices

Define the following information to be configured on each of the network devices.

Settings for Management

Define configuration information necessary for management.

- Device name

Define the name of the managed device.

This name can contain up to 32 alphanumeric characters (upper or lower case), underscores ("_"), hyphens ("-"), and periods (".").

- IP addresses used by managed network devices for management purposes

Choose an IP address to be used for communication with the admin server.

- SNMP community name

Define the name of the SNMP community to be used when collecting MIB information using the monitoring function of the network device.

This user name can contain up to 32 alphanumeric characters (upper or lower case), underscores ("_"), and hyphens ("-").

- Administrator information (user name and password)

- Telnet Login User Name

Define the Telnet login user name to be used for logging into the network device.

This user name can contain up to 32 alphanumeric characters (upper or lower case), underscores ("_"), and hyphens ("-").

- Telnet Password

Define the password for the Telnet login user name to be used for directly logging into the network device.

This user name can contain up to 32 alphanumeric characters (upper or lower case), underscores ("_"), and hyphens ("-").

- Administrator Password

Define the login password for the administrator to be used for logging into the network device as an administrator.

This user name can contain up to 32 alphanumeric characters (upper or lower case), underscores ("_"), and hyphens ("-").

- SNMP trap destination

This must be the admin IP address of the admin server.

- Monitoring method (PING, SNMP)

Define the monitoring methods for the network devices (firewalls, L2 switches, and L3 switches).

Choose PING for monitoring active/inactive status, and choose SNMP for status monitoring.

It is possible to monitor using only one method or both methods.

Settings for Pre-configuration

Define settings necessary for pre-configuration.

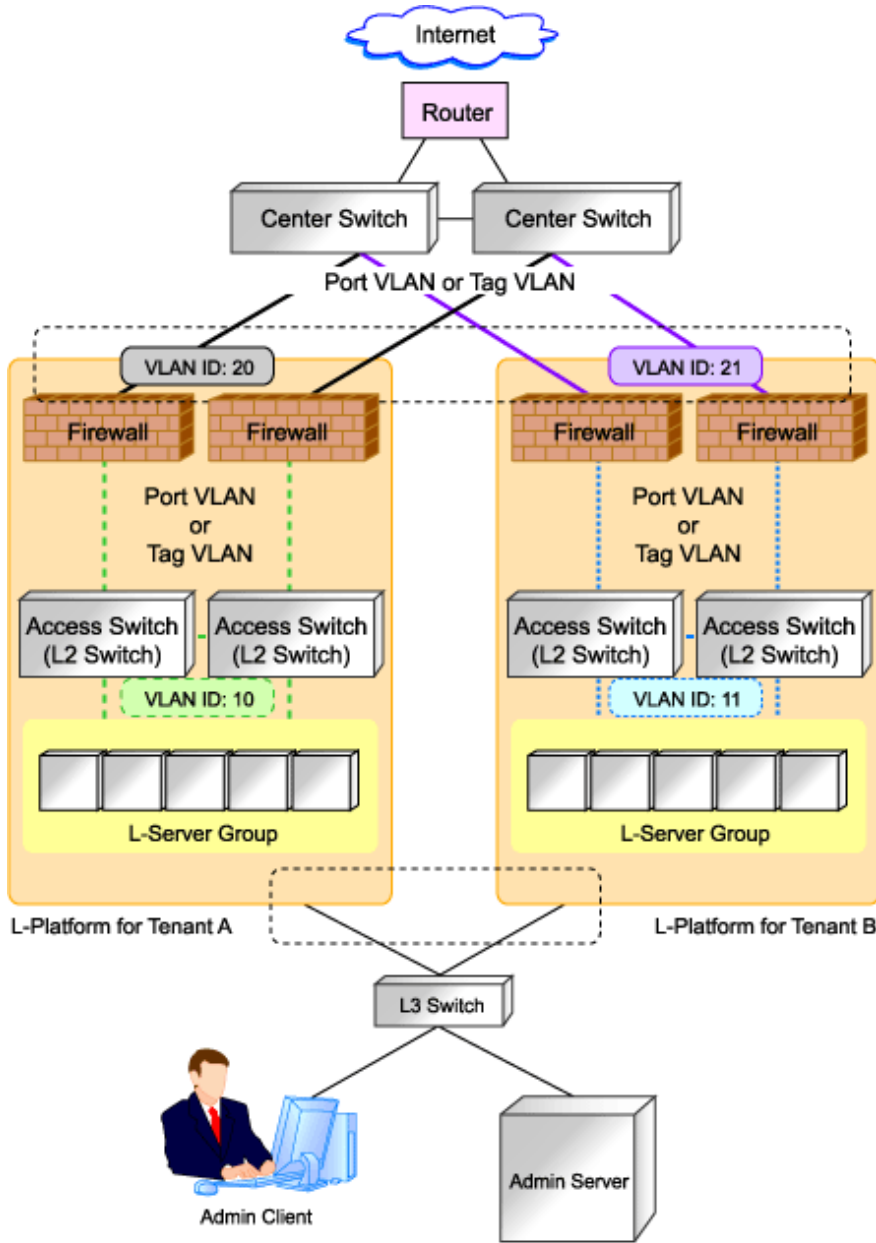
- Public LAN Pre-configuration Settings


Check the connection configuration of the LAN ports to be used for the public LAN to be connected with the center switches, and define the necessary settings accordingly.

- Admin LAN Pre-configuration Settings

Check the connection configuration of the LAN ports to be used for the admin LAN to be connected with the L3 switches, and define the necessary settings accordingly.

Figure 4.11 Managed Device Pre-configuration Scope



 : Range of preparations by the user

 Information

Character limitations vary depending on the network device used.

For specific settings of individual devices, define the settings according to the specifications of the network devices, within the limitations of types and number of characters described above.

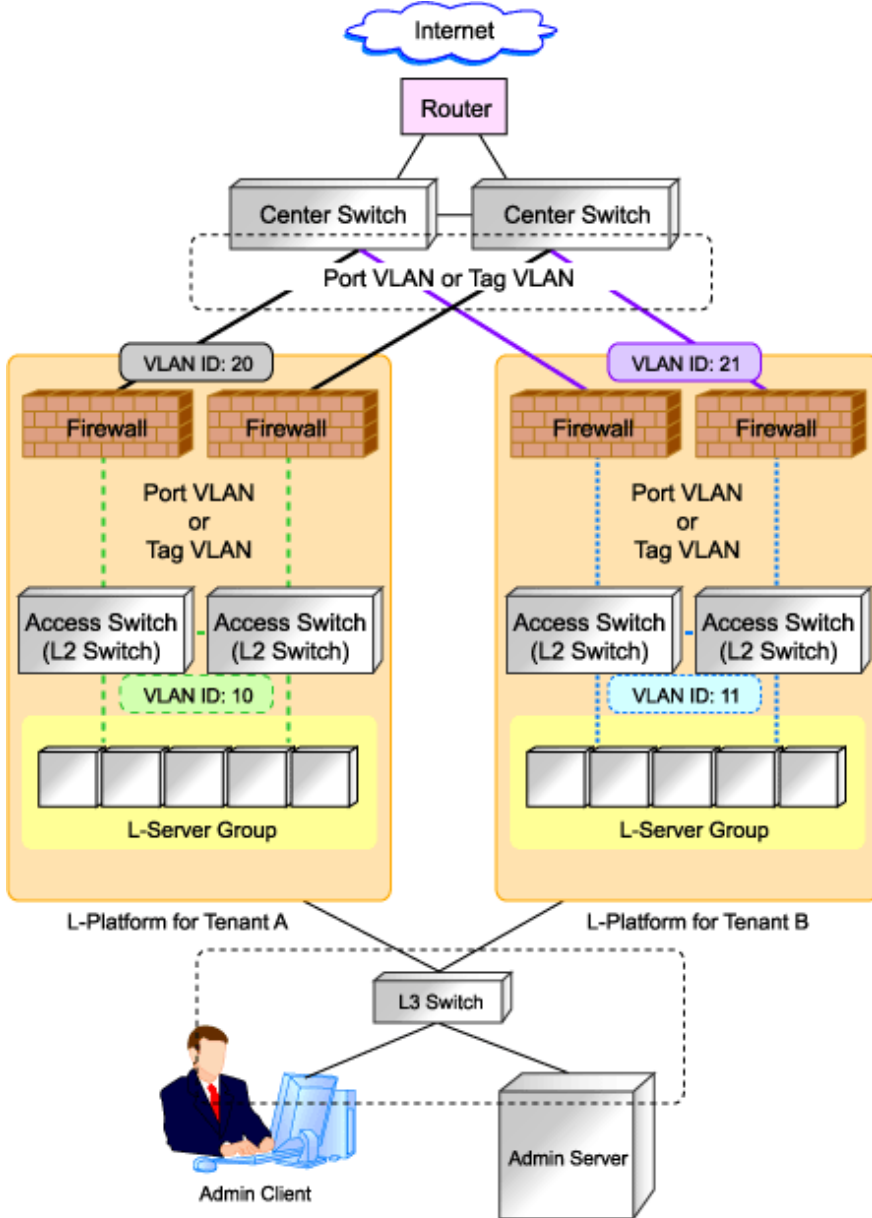
The information necessary to be configured based on the public and admin LAN connection configurations also depends on the specifications of network devices.


For details on the specifications for each network device, refer to the manual for each device.

4.2.2.4 Settings for Unmanaged Network Devices

Define the information to be configured on each unmanaged network device.

Figure 4.12 Example of the Configuration Scope of Unmanaged Network Devices



 : Range of preparations by the user

Public LAN Pre-configuration Settings

Define the public LAN settings that must be pre-configured by users.

- Routing Information

Define the routing method for the routers and center switches to enable communication with the L-Platform network.

- VLAN Information

Check the VLAN information of routers and center switches used within the L-Platform network, and then define the VLAN information necessary for connection and communication with L-Platforms.

- Redundancy Information

Check whether to make network devices and communication routes redundant, and then define any settings necessary for redundant configuration.

Admin LAN Settings

Define the admin LAN settings that must be pre-configured by users.

Figure 4.13 Admin LAN Network Configuration

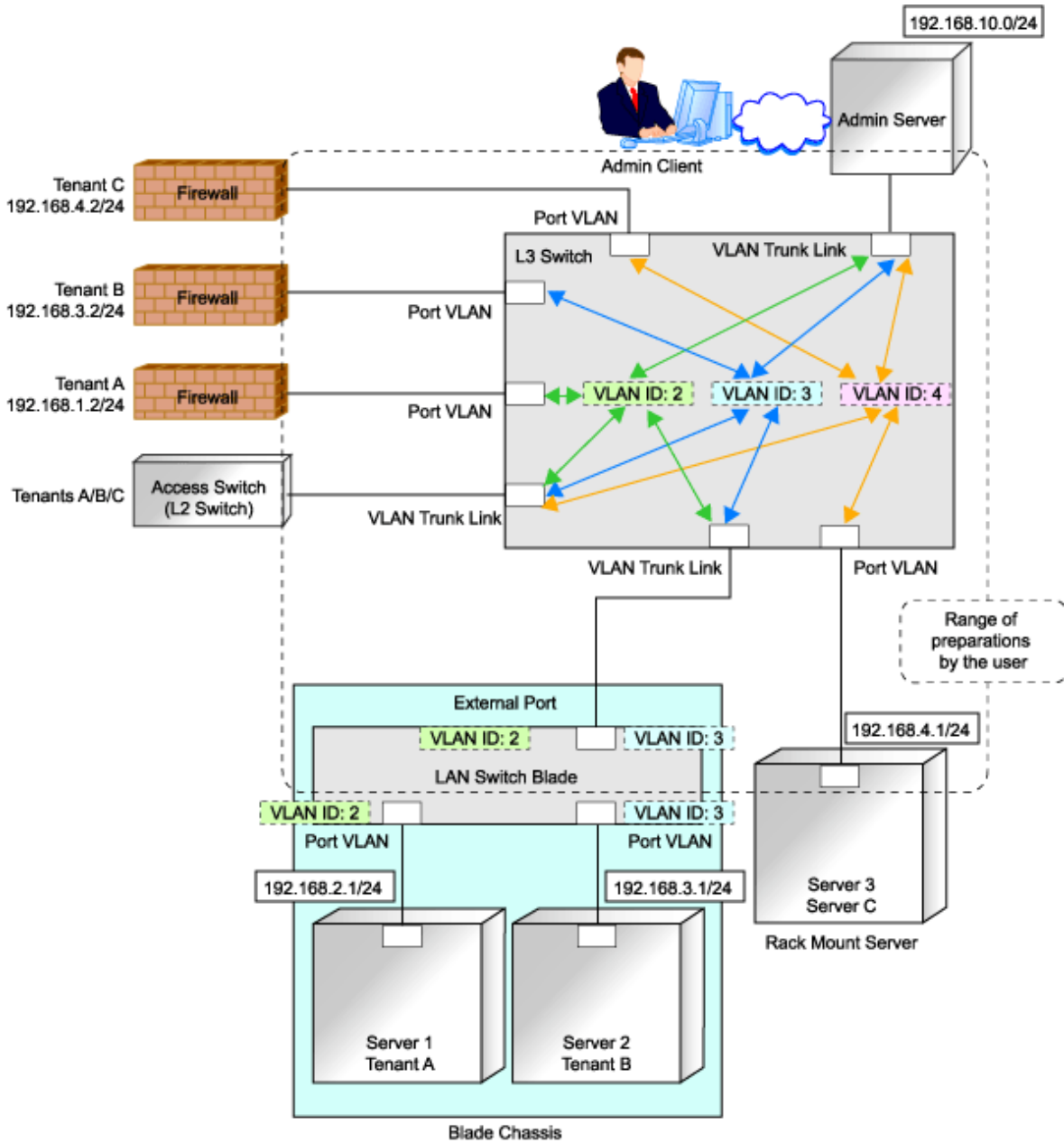
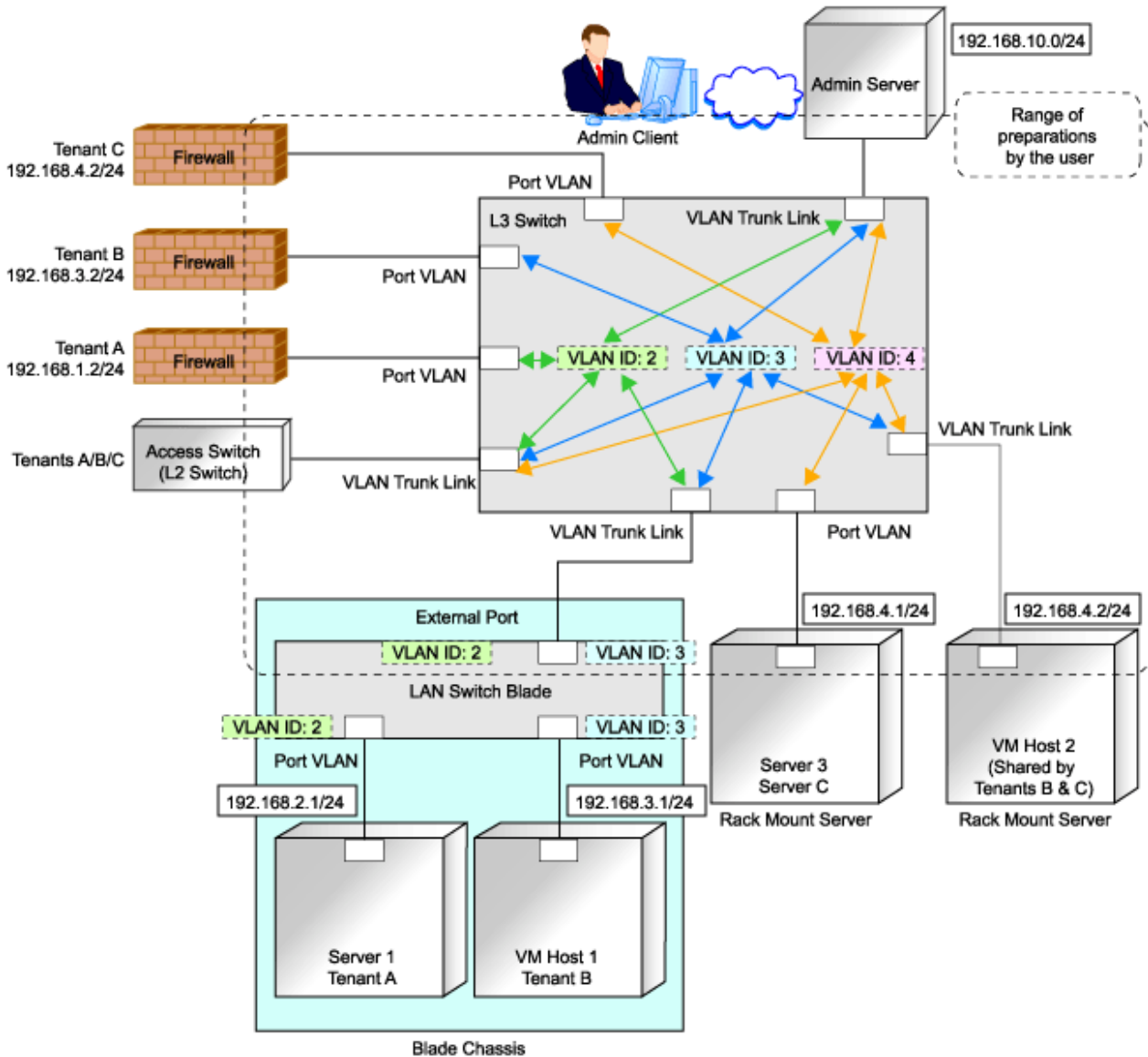


Figure 4.14 Admin LAN Network Configuration (with Both Servers and VM Hosts)



- Routing information

When the admin server and individual devices (servers, storage units, network devices, and admin clients) belong to different subnets, define the routing method on the L3 switch to enable communication between the admin server and individual devices using the admin LAN.

When using routing protocols (such as RIP and OSFP), define the information necessary for configuring dynamic routing. When not using dynamic routing, define the settings for the routing information table.

In addition, it is necessary to configure the following multicast routing for managed resources from the admin server.

225.1.0.1 - 225.1.0.8

- VLAN information

Check the VLAN information of external ports of LAN switch blades and L3 switches used in the admin LAN network, and define the settings (VLAN IDs). Set the ports to be used as trunk links when necessary.

- Redundancy information

Check whether to make network devices and communication routes redundant, and then define any settings necessary for redundant configuration.

- Access control information

When configuring access control on L3 switches, define the ports that allow connection, because it is necessary to allow connection with the ports used by Resource Orchestrator.

Refer to "[Appendix A Port List](#)", for details on the ports used by Resource Orchestrator.

Define whether to allow or block communication when the routing is operating in order to define the access control.

- When using the following functions, it is necessary to configure DHCP relay agents to enable the manager to receive DHCP requests from managed servers belonging to different subnets.
 - Backup and restoration of managed servers
 - Collection and deployment of cloning images
 - SAN boot using HBA address rename
- When using the HBA address rename setup service, it is necessary to configure DHCP relay agents to enable the HBA address rename setup service to receive DHCP requests from managed servers belonging to different subnets.
- For information about multicast routing setting and DHCP relay agents, refer to the router manual.

4.2.2.5 Settings for Managed Servers

Define the following information to be configured on the servers to be managed.

- Device name
- IP addresses used by managed servers for management purposes

Choose an IP address to be used for communication with the admin server.

- IP Address of iSCSI Initiator

Choose an IP address for the network interface to use for communication with managed servers.

This is not necessary for servers for which iSCSI is not enabled.



Note

- IP addresses chosen for iSCSI should be static and do not use DHCP.
- When using a multi-path configuration using iSCSI, separate the networks using different ports.
Interface segments and virtual switches also need to be separated.
- Ensure that all of the IP addresses configured here are on the same subnet.

4.2.2.6 Settings for LAN Switch Blades on Managed Blade Systems

For blade servers, also define the following information to be configured on LAN switch blades.

- VLAN IDs for the admin LAN ports used to communicate with the admin server
- IP addresses used by managed network devices for management purposes
Choose an IP address to be used for communication with the admin server.
- SNMP community name

Define the name of the SNMP community to be used when collecting MIB information from the LAN switch blade.

This user name can contain up to 32 alphanumeric characters (upper or lower case), underscores ("_"), and hyphens ("-").

- Administrator information (user name and password)
 - Telnet Login User Name

Define the Telnet login user name to be used for directly logging into the LAN switch blade.
This user name can contain up to 64 alphanumeric characters (upper or lower case), underscores ("_"), and hyphens ("-").
 - Telnet Password

Define the password of the Telnet login user name to be used for directly logging into the LAN switch blade.
This password can contain up to 80 alphanumeric characters (upper or lower case) and symbols (ASCII characters 0x20, 0x21, and 0x23 to 0x7e) with the exception of double quotation marks (").
 - Administrator Password

Define the login password for the administrator to be used for directly logging into the LAN switch blade as an administrator.
This password can contain up to 80 alphanumeric characters (upper or lower case) and symbols (ASCII characters 0x20, 0x21, and 0x23 to 0x7e) with the exception of double quotation marks (").
- SNMP trap destination

This must be the admin IP address of the admin server.

4.2.2.7 Settings for Managed Storage Units

Define the following information to be configured on storage units.

- Device name
- IP address used by managed storage for management purposes

Choose an IP address to be used for communication with the admin server.
- IP address of iSCSI target

Define the IP address of the storage unit with which the iSCSI initiator will communicate.
This is not necessary for storage units for which iSCSI is not enabled.

Note

- IP addresses chosen for iSCSI should be static and do not used DHCP.
- When using a multi-path configuration, separate the networks using different ports.
- Ensure that all of the IP addresses configured here are on the same subnet.

4.2.2.8 Settings for Other Managed Hardware

Define the following information to be configured on each of the other hardware devices.

Other hardware devices include "server management units", "power monitoring devices", etc.

- Device name
- IP addresses used by other hardware devices for management purposes

Choose an IP address to be used for communication with the admin server.

4.2.3 Pre-configuring Devices

Configure defined setting information.

4.2.3.1 Pre-configuring Admin Servers

Configure the information defined in "[4.2.2.1 Settings for the Admin Server](#)" on the admin server.

The admin IP address should be specified when installing the manager on the admin server.

For details on how to configure the other information on the admin server, refer to the manual of the admin server.

4.2.3.2 Pre-configuring Admin Clients

Configure the information defined in "[4.2.2.2 Settings for Admin Clients](#)" on admin clients.

For details on how to configure information on admin clients, refer to the manual of the admin client.

4.2.3.3 Pre-configuring Managed Network Devices

Configure the information defined in "[4.2.2.3 Settings for Managed Network Devices](#)" on network devices.

In order to track the network connections between managed servers (PRIMERGY BX series) and adjacent network devices (L2 switches, etc.), and display them in the Network Map, the following protocols should be first enabled on each LAN switch blade and network device.

- LLDP (Link layer Discovery Protocol)
- CDP (Cisco Discovery Protocol)



Note

- The same protocol needs to be set on the LAN switch blade and the network devices it is connected to.
- It is not possible to automatically detect the connection relationship between LAN switch blades set in the IBP mode and network devices.
- Network connections may not be displayed properly if two or more network devices are set with a conflicting system name (sysName).

For details on how to configure information on network devices, refer to the manual for each device.

4.2.3.4 Pre-configuring Unmanaged Network Devices

Configure the information defined in "[4.2.2.4 Settings for Unmanaged Network Devices](#)" on the network devices.

For details on how to configure information on network devices, refer to the manual for each device.

4.2.3.5 Pre-configuring Managed Servers

Configure the information defined in "[4.2.2.5 Settings for Managed Servers](#)" on managed servers.

When the managed servers are rack mount or tower servers, configure the admin IP address on the network interfaces defined in the "[Admin LAN for Servers](#)" of "[4.2.1.1 Admin LAN Network Design](#)".

For details on how to configure information on managed servers, refer to the manual for the server.

4.2.3.6 Pre-configuring LAN Switch Blades on Managed Blade Systems

Configure LAN switch blades on the managed blade systems using the information defined in "[4.2.2.6 Settings for LAN Switch Blades on Managed Blade Systems](#)".

For details on how to configure LAN switch blades on managed blade systems, refer to the manual of the LAN switch blade.

Information

VLAN settings for switch blade ports not used for the admin LAN can also be set from the [Resource] tab on the ROR console. For details, refer to "2.4.4 Configuring VLANs on LAN Switch Blades" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Note

- After setting up a LAN switch blade, perform a backup of the LAN switch blade's configuration definition information. For details how to backup the configuration definition information of a switch blade, refer to the manual of the LAN switch blade.
- Resource Orchestrator uses telnet to log into LAN switch blades and automate settings.

When telnet connection is disabled, enable it.

Refer to the manual of the relevant product.

Some models of LAN switch blades may restrict the number of simultaneous connections. In this case, log out from other telnet connections.

- If telnet is unavailable, the following features are also unavailable.
 - Registration of LAN switch blades
 - Changing of LAN switch blade settings
 - Changing and setting the VLAN for LAN switch blades (internal and external connection ports)
 - Restoration of LAN switch blades
 - Server switchover (changing network settings while a server is switched over)
- For PY CB Eth Switch/IBP 10Gb 18/8, the maximum unregistered VLAN ID is used for the "oob" port in the LAN switch blade. When the maximum VLAN ID, "4094", is set in the LAN switch blade and the "oob" port is used to connect the telnet, the following functions cannot be used.
 - Changing and setting the VLAN for LAN switch blades (internal and external connection ports)
 - Restoration of LAN switch blades
 - Server switchover (changing network settings while a server is switched over)
- When using end host mode, use the default pin-group and do not create new pin-groups. Also, disable the Auto VLAN Uplink Synchronization (AVS) setting.
- If the VLAN settings are to be performed on the ports with link aggregation set on the following LAN switch blades, set the apparatuses as follows. Also, disable the Auto VLAN Uplink Synchronization (AVS) setting.

LAN switch blades

- PY CB Eth Switch/IBP 10Gb 18/8+

Configuration

- LLDP (Link layer Discovery Protocol)
When setting LLDP, make the setting for "VLAN name information" invalid.
Make the other settings valid.

However, settings other than VLAN settings should be made directly on the LAN switch blade.

Network Configuration of LAN Switch Blades (when using PRIMERGY BX Servers)

In a blade system environment, multiple subnets can be consolidated onto LAN switch blades by using VLANs.

For PRIMERGY BX900/BX400 LAN switch blades operating in IBP mode, the above can also be achieved by using port group settings for IBP instead of VLAN settings.

Each port of a LAN switch blade can be set with VLAN IDs.

Only those ports set with a same VLAN ID can communicate with each other.

Setting up different VLAN IDs then results in multiple subnets (one per VLAN ID) co-existing within the same switch.

Define the VLANs to set on both the internal (server blade side) and external connection ports of each LAN switch blade.

- Internal Connection Ports

Ensure that port VLANs are configured for the ports corresponding to the NICs connected to the admin LAN.

If NICs connected to the admin LAN are used for public LANs as well, configure tagged VLANs.

For the ports corresponding to the NICs connected to the public LAN, assign a VLAN ID (port or tagged VLAN) other than VLAN ID1 (the default VLAN ID) for each subnet.

Using tagged VLANs on LAN switch ports also requires configuring the network interfaces of managed servers with tagged VLANs. As Resource Orchestrator cannot set tagged VLANs to network interfaces on managed servers, this must be done manually.

- External Connection Ports

Choose the LAN switch blade ports to connect to external LAN switches, and the VLAN IDs to use for both the admin and public LANs.

When choosing a tagged VLAN configuration, the VLAN ID chosen for a LAN switch blade's external port must be the same as that used on its adjacent port on an external LAN switch.

When using VLAN auto-configuration on the external ports of the LAN switch blades that compose the link aggregation, configure the link aggregation beforehand and enable the LLDP.

Refer to the manual for the LAN switch blade for information on how to configure link aggregation and to enable LLDP.



Note

- To change the VLAN ID for the admin LAN, perform the following.

1. Enable communications between the admin server and the LAN switch blade.

Manually change the following two settings.

- Change the VLAN ID of the external connection port(s) used for the admin LAN.
- Change the VLAN ID used by the admin IP address of the LAN switch blade.

2. Change the VLAN ID used by the managed server on the admin LAN.

- VLAN settings for LAN switch blades are not included in cloning images. Configure VLAN settings for the target servers before deploying a cloning image.

- In the following cases, VLANs cannot be configured using the ROR console.

Configuring VLANs on external connection ports

- Link state group
- Port backup function

Configuring VLANs on external and internal connection ports

- Link aggregation (excluding LAN switch blades PY CB Eth Switch/IBP 10Gb 18/8+)
- Deactivated (depends on LAN switch blade model)

Choose VLAN IDs and VLAN types for the ports on the switches connected to NICs on the physical servers.

- Physical server name
- NIC index

- VLAN ID
- VLAN type (port or tagged VLAN)

Note

On servers, operating systems associate each physical network interface with a connection name (Local area connection *X* in windows and *eth.X* in Linux).

If more than one network interface is installed, depending on the OS type and the order of LAN driver installation, the index numbers (*X*) displayed in their connection name may differ from their physically-bound index (defined by each interface's physical mount order).

The relations between physically-bound indexes and displayed connection names can be confirmed using OS-provided commands or tools.

For details, refer to network interface manuals.

Also, note that Resource Orchestrator uses the physical index of a network interface (based on physical mount order).

If the connection relationship (topology) between the managed server (PRIMERGY BX series) and neighboring network devices (L2 switches, etc.) is to be displayed in the network map, the following settings are required in the LAN switch blade and network device so that the topology can be automatically detected.

- LLDP (Link layer Discovery Protocol)
- CDP (Cisco Discovery Protocol)

Note

- The same protocol needs to be set on the LAN switch blade and the network devices it is connected to.
- It is not possible to automatically detect the connection relationship between LAN switch blades set in the IBP mode and network devices.
- For the following LAN switch blades, the settings described below should be set to the same values in order to enable proper detection of network links.

LAN Switch Blades:

- PY CB Eth Switch/IBP 1Gb 36/12
- PY CB Eth Switch/IBP 1Gb 36/8+2
- PY CB Eth Switch/IBP 1Gb 18/6

Expected Values:

- hostname set from the hostname command
- system name set from the snmp-server sysname command

Example

When setting both the hostname and system name to "swb1".

```
# hostname swb1
# snmp-server sysname swb1
```

- For the following LAN switch blade, the settings described below should be set to the same value to enable proper detection of network links.

LAN Switch Blades

- PY CB Eth Switch/IBP 10Gb 18/8

Configuration

- Using the snmp agent address command, set the admin IP address of the LAN switch blade for the agent address.
- Network connections may not be displayed properly if two or more network devices are set with a conflicting system name (sysName).

[Windows/Hyper-V]

When using the backup, restore, or cloning functions, enable the managed server's NetBIOS over TCP/IP.

Note that the managed server should be restarted after enabling NetBIOS over TCP/IP.

Example of VLAN Network Configuration (with PRIMERGY BX600)

Figure 4.15 With Port VLANs

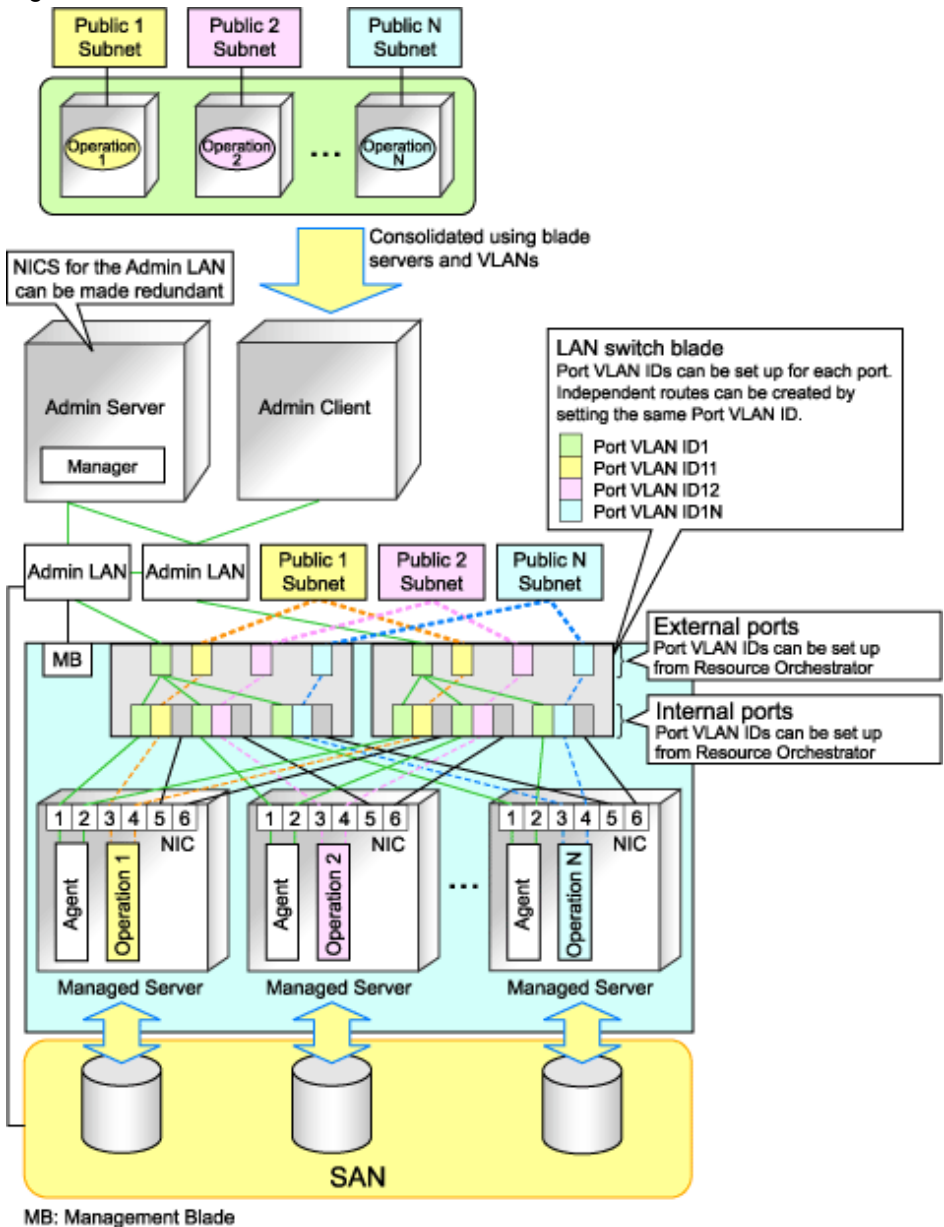
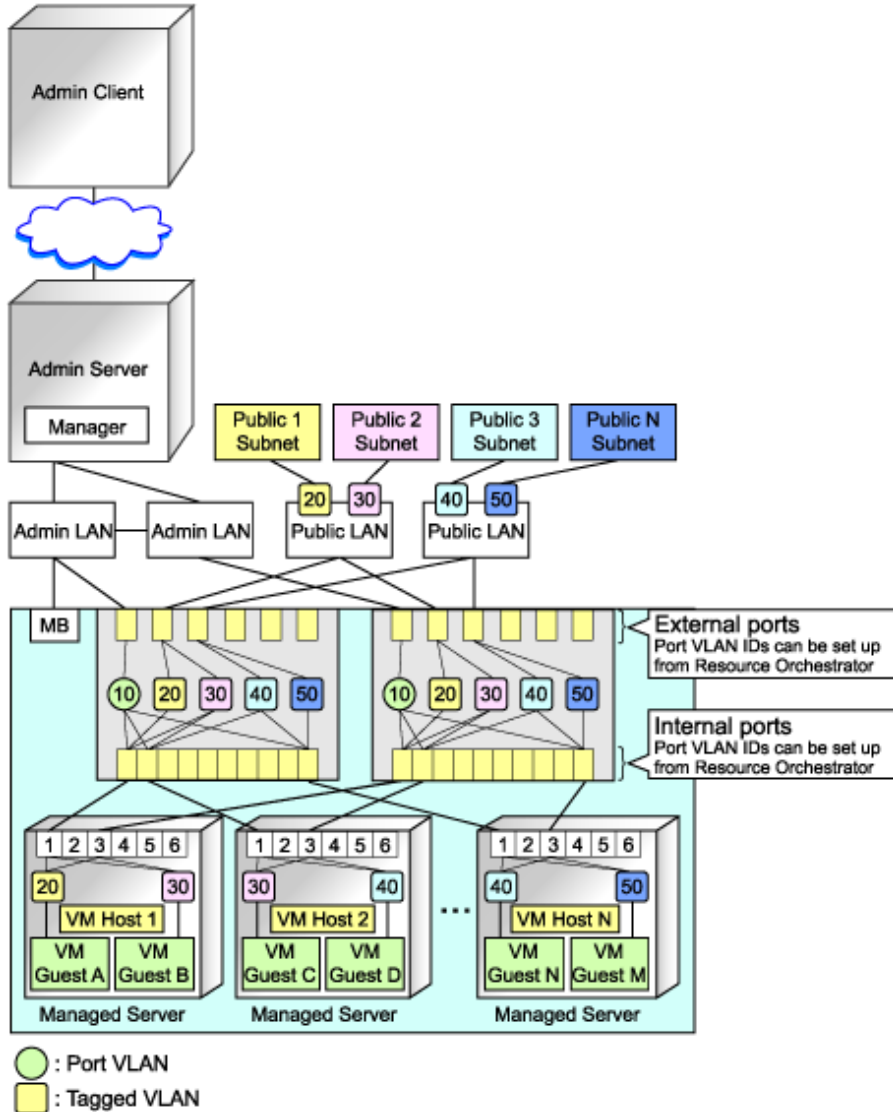


Figure 4.16 With Tagged VLANs



Information

It is recommended that a dedicated admin LAN be installed as shown in "Example of VLAN network configuration (with PRIMERGY BX600)".

If you need to use the following functions, a dedicated admin LAN is required in order to allocate admin IP addresses to the managed servers using the DHCP server included with Resource Orchestrator.

- Backup and restore
- Collection and deployment of cloning images
- HBA address rename

In a configuration using a LAN switch blade, a VLAN has to be configured if the LAN switch blade is shared by an admin and public LANs where a dedicated admin LAN is required.

4.2.3.7 Pre-configuring Managed Storage Units

Configure the information defined in "4.2.2.7 Settings for Managed Storage Units" on the managed storage.

For details on how to configure information on managed storage units, refer to the manuals for the storage units.

4.2.3.8 Pre-configuring Other Managed Hardware

Configure the information defined in "4.2.2.8 Settings for Other Managed Hardware" on the managed hardware.

For details on how to configure information on the managed hardware, refer to the manual for each hardware.

4.2.3.9 Pre-configuration for Making iSCSI LAN Usable

Specify the following settings to make an iSCSI LAN usable.

- Configurations for LAN Switch Blades
 - Configure a VLAN ID for a LAN switch blade external port. Set trunk links when necessary.
- LAN Switch Settings
 - Configure a VLAN ID for the port on the switch connected with the LAN switch blade. Set trunk links when necessary.
- Storage Configurations
 - Set the following items for the port for iSCSI connection.
 - IP address
 - Subnet mask
 - Default gateway
 - CHAP authentication
 - Mutual CHAP authentication
 - Information of hosts that can communicate with the port for iSCSI connection

4.2.4 Preparations for Resource Orchestrator Network Environments

This section explains the preparations for setting up the network environment.

Conditions	Necessary Preparations
When automatically configuring the network	Create network resources
When using IBP	Create an IBP uplink set
When using an iSCSI LAN for iSCSI boot	Create a network definition file for iSCSI boot
When using Link Aggregation	Pre-configure link aggregation for LAN switch blades and L2 switches
When using NICs other than those in the default configuration of the automatic network configuration used when using blade servers	Create a server NIC definition
When using VMware on rack mount or tower servers to use automatic virtual switch configuration	Create a server NIC definition
When deploying L-Servers even if the service console and port group is the same, when VMware is being used for server virtualization software	Create the VMware excluded port group definition file
When registering network devices as resources	Create network resources
When using the automatic configuration function for network devices registered as network device resources	Create model definitions for the network devices
	Create a folder for registering rulesets

Conditions	Necessary Preparations
	Register sample scripts

4.2.4.1 When Automatically Configuring the Network

By connecting the NIC for an L-Server to a network resource, the following settings are automatically configured.

- Automatic configuration for LAN switch blades (physical/virtual L-Servers)
- Network configuration for blade servers (physical/virtual L-Servers)
- Configuration for rack mount or tower servers (physical/virtual L-Servers)
- IP address auto-configuration (virtual L-Servers)
- Automatic configuration for L2 switches

Automatic VLAN Configuration for LAN Switch Blades (Physical/Virtual L-Servers)

VLANs are automatically configured on LAN switch blades.

There are the following three types of firmware for LAN switch blades:

- Switch Firmware
Provides layer 2 switch functions.
- End-Host Firmware
This provides the layer 2 switch functionality and pin connection functionality.
- IBP Firmware
Delivers virtualization.

In Resource Orchestrator, operation of a LAN switch blade using Switch firmware is called Switch mode, operation using end-host firmware is called end-host mode, and operation using IBP firmware is called IBP mode.

For details, refer to the manual of the LAN switch blade.

- Switch Mode/End-Host Mode
VLANs are automatically configured for a LAN switch blade port.
 - Automatic configuration for an internal connection port
Automatic configuration of tagged VLANs and port VLANs for server blade internal connection ports is performed.
 - Automatic configuration for an uplink port
Automatic configuration of tagged VLANs that connect to network devices, such as access switches out of chassis, is performed.

Information

Automatic configuration of tagged VLANs for uplink ports is triggered by the creation or modification of network resources. Modifying network resources here means the addition of uplink ports.

Note

- When automatically configuring tagged VLANs for uplink ports, the following functions must be enabled:
 - Automatic network configuration
 - Automatic configuration for uplink ports

Set the link aggregation in advance if the VLAN auto-configuration of the external ports making up the link aggregation is to be enabled.

- When configuring the port VLAN for an uplink port, manually configure the settings from the server resource tree on the ROR console.
- Creating the following network resources may generate network loops.
 - Automatically configuring VLAN for an uplink port
 - Specifying multiple uplink ports on a single LAN switch blade

In these cases, take actions to prevent network loops, such as disconnecting the cables for uplink ports, and then create network resources.

- Untagged VLAN 1 cannot be used as an external port that is the target of VLAN auto-configuration. If untagged VLAN 1 is to be used, disable VLAN auto-configuration and set the VLAN manually.
- The VLAN set for external ports by VLAN auto-configuration will not be automatically deleted even if the relevant network resource is deleted. The infrastructure administrator should check the network configuration, and if the VLAN settings of the external ports are deemed unnecessary, then they should be deleted from the VLAN settings for LAN switch blades in the ROR console.
- VLAN auto-configuration for external ports that compose link aggregations can be used for LAN switch blades in the following blade servers where the mode is switch or end host.

Blade Servers

- PRIMERGY BX400
- PRIMERGY BX900

Switch blade

- PY CB Eth switch/IBP 10Gb 18/8



See

For details on how to create network resources which automatically configure VLANs for LAN switch blade uplink ports, refer to "3.5.2 Changing VLANs Set for External Connection Ports of LAN Switch Blades" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- IBP Mode

Connect to the port group that was created beforehand. Automatic configuration of VLANs is not supported.

Network Configuration for Blade Servers (Physical/Virtual L-Servers)

- Automatic Network Configuration

When the NIC for an L-Server and a network resource are connected, the network is automatically configured.

The explanation given here is for a non-redundant configuration of a LAN switch blade. For automatic configuration items including redundant configuration, refer to "[Table 4.1 Network Configurations for Blade Servers](#)".

For details on the timing of automatic configuration, refer to "[Table 1.5 Timing of Automatic Network Settings Execution](#)".

For the configurations that support automatic configuration, refer to the following:

- For Physical L-Servers

Refer to "[Physical Server \(Blade Server\) Configuration to Support Automation of Network Configuration in Resource Orchestrator](#)" in "[D.6.1 Automatic Network Configuration](#)".

- For Virtual L-Servers

[VMware]

Refer to "Default Blade Server Configuration to Support Automation of Network Configuration in Resource Orchestrator" in "E.2.5 Setup".

[Hyper-V]

Refer to "Default Blade Server Configuration to Support Automation of Network Configuration in Resource Orchestrator" in "E.3.4 Setup".



- For details on the `rcxadm nicdefctl` command, refer to "1.7.16 rcxadm nicdefctl" in the "Reference Guide (Resource Management) CE".
- For details on the server NIC definitions, refer to "2.11 Server NIC Definition" of the "Reference Guide (Resource Management) CE".

Figure 4.17 Automatic Network Configuration for Blade Servers

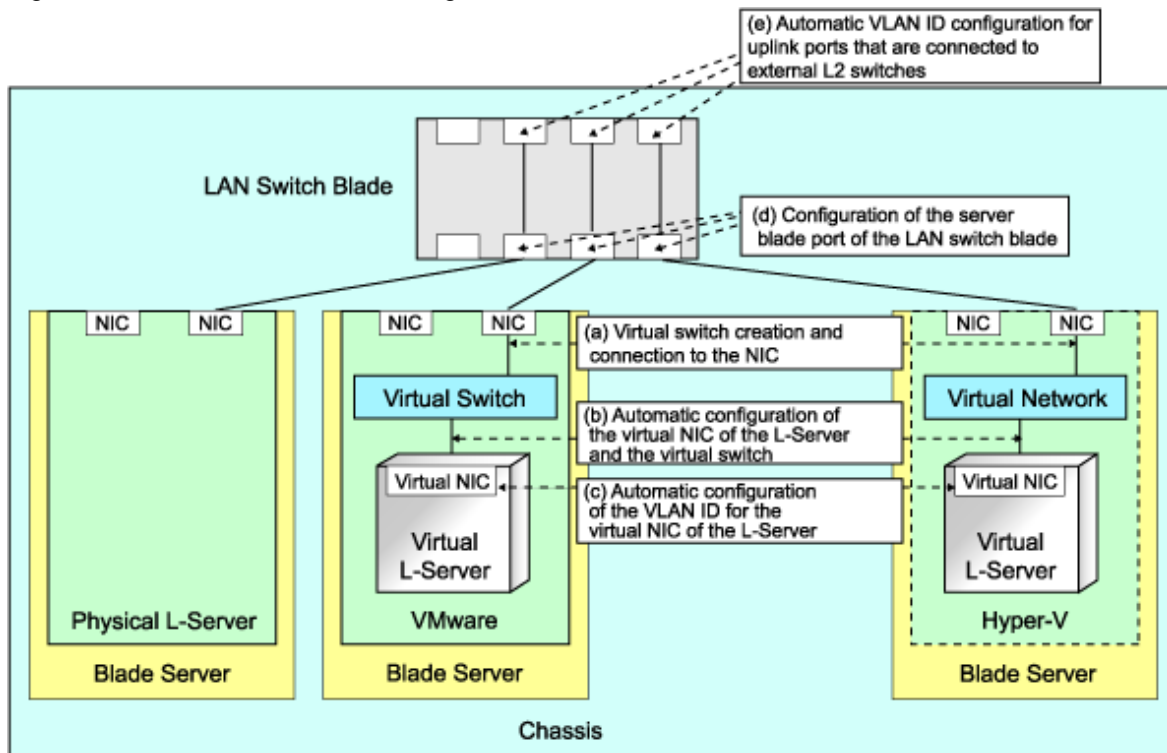


Table 4.1 Network Configurations for Blade Servers

		Physical L-Server		Virtual L-Server									
				VMware		Hyper-V		RHEL5-Xen		RHEL-KVM		Oracle VM	
		Redundancy (*1)		Redundancy (*1)		Redundancy (*1)		Redundancy (*1)		Redundancy (*1)		Redundancy (*1)	
		Witho ut	With	Witho ut	With	Witho ut	With	Witho ut	With	Witho ut	With	Witho ut	With
A	Creating virtual switches and connecting to NICs (*2)	-	-	Yes (*3)	Yes	Yes (*3)	Yes (*4)	No	No	No	No	No	No

		Physical L-Server		Virtual L-Server									
				VMware		Hyper-V		RHEL5-Xen		RHEL-KVM		Oracle VM	
		Redundancy (*1)		Redundancy (*1)		Redundancy (*1)		Redundancy (*1)		Redundancy (*1)		Redundancy (*1)	
		Without	With	Without	With	Without	With	Without	With	Without	With	Without	With
B	Automatic connection between L-Server virtual NICs and virtual switches (*5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
C	Automatic VLAN ID configuration for L-Server virtual NICs	-	-	Yes	Yes	Yes	Yes	No	No	No	No	No	No
D	Configurations for the server blade ports of LAN switch blades	Yes (*6)	Yes	Yes (*3, *7)	Yes (*7)	Yes (*3, *7)	Yes (*4, *7)	No	No	No	No	No	No
E	Automatic VLAN ID configuration for uplink ports that are connected to external L2 switches (*7)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Yes: Configured in Resource Orchestrator

No: Not configured in Resource Orchestrator

-: None

*1: LAN redundancy.

For physical L-Servers, the NIC of the physical L-Server is the target of LAN redundancy.

For virtual L-Servers, the NIC connected to the virtual switch is the target of LAN redundancy.

*2: Replace as follows for each server virtualization software.

Table 4.2 Correspondence Table for Server Virtualization Software

VMware	Creating virtual switches and port groups
Hyper-V	Creating a virtual network
RHEL5-Xen RHEL-KVM Oracle VM	Creating a virtual bridge

Information

- When using VMware as server virtualization software, the following configurations are automatically performed:
 - Virtual switch creation
 - VLAN configuration for virtual switches
 - Teaming connection of virtual switches and NICs

- When using Hyper-V as server virtualization software, the following configurations are automatically performed:
 - Virtual network creation
 - VLAN configuration for virtual networks

Teaming connections of virtual networks and NICs are automatic if teaming settings are configured for NICs in advance.

*3: In order to configure the network automatically, it is necessary to create a server NIC definition suitable for the server to be configured, and then reflect the definition on the manager using the `rcxadm nicdefctl commit` command in advance. For details on the server NIC definitions, refer to "2.11 Server NIC Definition" of the "Reference Guide (Resource Management) CE". For details on the `rcxadm nicdefctl` command, refer to "1.7.16 rcxadm nicdefctl" of the "Reference Guide (Resource Management) CE". When not using server NIC definitions, manually configure the network.

*4: Automatic configuration is possible for redundancy configurations with Intel PROSet or PRIMECLUSTER GLS.

*5: Replace as follows for each server virtualization software.

Table 4.3 Correspondence Table for Server Virtualization Software

VMware	Connections Virtual NICs of L-Servers and Port Groups of Virtual Switches
Hyper-V	Connections Virtual NICs of L-Servers and Virtual Networks
RHEL5-Xen RHEL-KVM Oracle VM	VLAN ID configuration for the L-Server virtual network interface and connection with virtual bridges which have been created manually in advance

Information

If VMware is used as the server virtualization software and the same VLAN ID is used for the service console and port group, the port group and L-Server can be connected by creating a VMware excluded port group definition file.

For details on VMware excluded port group definition files, refer to "2.12 VMware Excluded Port Group Definition File" in the "Reference Guide (Resource Management) CE".

*6: Configure a port VLAN or a tagged VLAN. For details on how to configure VLANs, refer to "2.4.6 Configuring VLANs on Internal Connection Ports" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

*7: Configure a tagged VLAN.

In Resource Orchestrator, when a virtual L-Server is connected to the admin LAN that has the same subnet address as the admin server, to preserve security, virtual switches are not automatically created.

Ensure the network security of the communication route between the admin server and the virtual L-Server, and then create virtual switches.

- Manual Network Configuration

For configurations other than the default blade server configuration that supports automatic network configuration, manually configure the network, referring to the following:

- For Physical L-Servers
 - Refer to "[D.6.2 Manual Network Configuration](#)".
- For Virtual L-Servers
 - [VMware]
Refer to "[Manual Network Configuration](#)" in "[E.2.5 Setup](#)".
 - [Hyper-V]
Refer to "[Manual Network Configuration](#)" in "[E.3.4 Setup](#)".

Network Configuration for Rack Mount or Tower Servers (Physical/Virtual L-Servers)

For rack mount or tower servers, make connections between L-Server virtual NICs and virtual switches.

Figure 4.18 Network Configuration for Rack Mount or Tower Servers

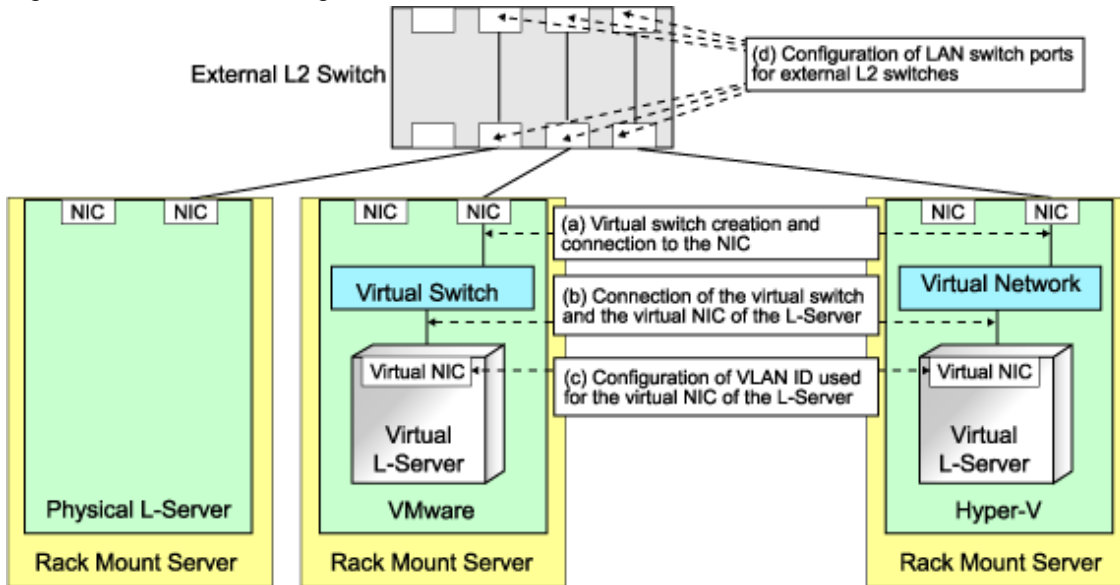


Table 4.4 Network Configurations for Rack Mount or Tower Servers

		Physical L-Server		Virtual L-Server									
				VMware		Hyper-V		RHEL5-Xen		RHEL-KVM		Oracle VM	
		Redundancy (*1)		Redundancy (*1)		Redundancy (*1)		Redundancy (*1)		Redundancy (*1)		Redundancy (*1)	
		Witho ut	With	Witho ut	With	Witho ut	With	Witho ut	With	Witho ut	With	Witho ut	With
A	Creating virtual switches and connecting to NICs (*2)	-	-	Yes	Yes	No	No	No	No	No	No	No	No
B	Connection between L-Server virtual NICs and virtual switches (*3)	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
C	Configuration of VLAN IDs used by L-Server virtual NICs	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
D	Configuration of LAN switch ports for external L2 switches (*4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Yes: Configured in Resource Orchestrator

No: Not configured in Resource Orchestrator

*1: LAN redundancy.

For physical L-Servers, the NIC of the physical L-Server is the target of LAN redundancy.

For virtual L-Servers, the NIC connected to the virtual switch is the target of LAN redundancy.

*2: In order to configure the network automatically, it is necessary to create a server NIC definition suitable for the server to be configured, and then reflect the definition on the manager using the `rxadm nicdefctl commit` command in advance.

For details on the server NIC definitions, refer to "2.11 Server NIC Definition" of the "Reference Guide (Resource Management) CE".

For details on the `rxadm nicdefctl` command, refer to "1.7.16 rxadm nicdefctl" of the "Reference Guide (Resource Management) CE".

Replace as follows for each server virtualization software.

Table 4.5 Correspondence Table for Server Virtualization Software

VMware	Creating virtual switches and port groups
Hyper-V	Creating a virtual network
RHEL5-Xen RHEL-KVM Oracle VM	Creating a virtual bridge

 Information

When using VMware as server virtualization software, the following configurations are automatically performed:

- Virtual switch creation
- VLAN configuration for virtual switches
- Teaming connection of virtual switches and NICs

The model names of rack mount or tower servers that can perform virtual switch creation, VLAN configuration, and teaming connection are as follows:

- RX100 S5/S6
- RX200 S4/S5/S6
- RX300 S4/S5/S6
- RX600 S4/S5
- RX900 S1
- TX150 S6/S7
- TX200 S5/S6
- TX300 S4/S5/S6

*3: Replace as follows for each server virtualization software.

Table 4.6 Correspondence Table for Server Virtualization Software

VMware	Connections Virtual NICs of L-Servers and Port Groups of Virtual Switches
Hyper-V	Connections Virtual NICs of L-Servers and Virtual Networks
RHEL5-Xen RHEL-KVM Oracle VM	VLAN ID configuration for the L-Server virtual network interface and connection with virtual bridges which have been created manually in advance

 Information

If VMware is used as the server virtualization software and the same VLAN ID is used for the service console and port group, the port group and L-Server can be connected by creating a VMware excluded port group definition file.

 See

For details on VMware excluded port group definition files, refer to "2.12 VMware Excluded Port Group Definition File" in the "Reference Guide (Resource Management) CE".

*4: Configured by network device automatic configuration.

IP Address Auto-Configuration (Virtual L-Servers)

[Windows/Linux] [VMware] [Hyper-V] [KVM]

If a subnet address has been set for the network resource, the IP address can be automatically set when deploying an image to an L-Server. The settings for the IP address, subnet mask and default gateway are configured according to DHCP settings.

[Hyper-V]

IP addresses can be automatically configured, on the following guest OS's on which the integrated services are installed.

- Microsoft(R) Windows Server(R) 2008 R2
- Microsoft(R) Windows Server(R) 2008
- Microsoft(R) Windows Server(R) 2003 R2
- Microsoft(R) Windows Server(R) 2003
- Microsoft(R) Windows(R) 7
- Microsoft(R) Windows Vista(R)
- Microsoft(R) Windows(R) XP

[KVM]

When the guest OS type is Linux, IP addresses can be automatically configured.

[Xen] [Oracle VM]

Automatic configuration of IP addresses is not supported.

If a subnet address is set for a network resource, set an IP address manually after deploying an image to an L-Server (Also set an IP address manually on the DNS server).

For details on how to check IP addresses, refer to the Note of "10.3.4 [Network] Tab" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

If no subnet address has been set, manually set a subnet address for operation on the DHCP server after deploying an image to an L-Server.

Automatic Configuration for L2 Switches

When an L-Server or a firewall resource is deployed on an L-Platform, definitions such as interfaces can be automatically configured on the L2 switch on the communication route, using a script created in advance.

Available Network Configurations

Available network configurations and configuration methods in Resource Orchestrator are given below.

PRIMERGY Blade Servers

- Non-Redundant Configuration

- For Physical L-Servers

Refer to "[D.6.2 Manual Network Configuration](#)".

- For Virtual L-Servers

Settings differ according to the server virtualization software being used.

[VMware]

Refer to "[Manual Network Configuration](#)" in "[E.2.5 Setup](#)".

[Hyper-V]

Refer to "[Manual Network Configuration](#)" in "[E.3.4 Setup](#)".

[Xen]

Refer to "[Manual Network Configuration](#)" in "[E.4.4 Setup](#)".

[KVM]

Refer to "[Manual Network Configuration](#)" in "[E.6.4 Setup](#)".

[Oracle VM]

Refer to "[Manual Network Configuration](#)" in "[E.5.4 Setup](#)".

- Redundant Configuration

- For Physical L-Servers

Refer to "[D.6.1 Automatic Network Configuration](#)" and "[D.7.4 Network Redundancy and VLAN Settings of L-Servers](#)".

- For Virtual L-Servers

Settings differ according to the server virtualization software being used.

[VMware]

Refer to "[Automatic Network Configuration](#)" in "[E.2.5 Setup](#)".

[Hyper-V]

Refer to "[Automatic Network Configuration for Blade Servers](#)" in "[E.3.4 Setup](#)".

[Xen]

Refer to "[Manual Network Configuration](#)" in "[E.4.4 Setup](#)".

[KVM]

Refer to "[Manual Network Configuration](#)" in "[E.6.4 Setup](#)".

[Oracle VM]

Refer to "[Manual Network Configuration](#)" in "[E.5.4 Setup](#)".

PRIMERGY Rack Mount Servers, PRIMERGY Tower Servers, or PRIMEQUEST Servers

- Non-Redundant Configuration

- For Physical L-Servers

Refer to "[D.6.2 Manual Network Configuration](#)".

- For Virtual L-Servers

Settings differ according to the server virtualization software being used.

[VMware]

Refer to "[Manual Network Configuration](#)" in "[E.2.5 Setup](#)".

[Hyper-V]

Refer to "[Manual Network Configuration](#)" in "[E.3.4 Setup](#)".

[Xen]

Refer to "[Manual Network Configuration](#)" in "[E.4.4 Setup](#)".

[KVM]

Refer to "[Manual Network Configuration](#)" in "[E.6.4 Setup](#)".

[Oracle VM]

Refer to "[Manual Network Configuration](#)" in "[E.5.4 Setup](#)".

- Redundant Configuration

- For Physical L-Servers

Refer to "[D.6.1 Automatic Network Configuration](#)".

- For Virtual L-Servers

Settings differ according to the server virtualization software being used.

[VMware]

Refer to "[Automatic Network Configuration](#)" in "[E.2.5 Setup](#)".

[Hyper-V]

Refer to "[Manual Network Configuration](#)" in "[E.3.4 Setup](#)".

[Xen]

Refer to "[Manual Network Configuration](#)" in "[E.4.4 Setup](#)".

[KVM]

Refer to "[Manual Network Configuration](#)" in "[E.6.4 Setup](#)".

[Oracle VM]

Refer to "[Manual Network Configuration](#)" in "[E.5.4 Setup](#)".

Point

- When Creating Physical L-Servers

For details on the network configuration example, refer to "[Appendix D Design and Configuration when Creating a Physical L-Server](#)".

- When Creating Virtual L-Servers

For details on the network configuration example, refer to "[Appendix E Design and Configuration for Creating Virtual L-Servers](#)".

Network Settings for Physical L-Servers

When configuring NIC redundancy and tagged VLANs, or specifying a Red Hat Enterprise Linux image, the network on the OS is not automatically configured.

Collect an image with the preset script that configures the network at initial OS startup, and then create an L-Server using that image.

Physical L-Server network information (such as IP address, NIC redundancy, and tagged VLAN settings) is transferred to the OS as a network information file when the image is deployed to the OS.

For details on how to configure a network using a network information file, refer to "[D.7.4 Network Redundancy and VLAN Settings of L-Servers](#)".

When network configuration is not performed on the OS, create the L-Server then connect to it via the admin LAN or using the console, and configure the network on the OS on the L-Server.

Note

Depending on operating conditions of the network configuration script, a communication error may occur on the business application that is installed on the server.

Since this error cannot be detected by Resource Orchestrator, please check any network errors that occur on user applications to detect it.

When those errors occur, the server or the application must be restarted.

Restart the server using the network configuration script.

Modifying Network Resource Specifications

The following network resource specifications can be modified.

- Basic information (network resource names, etc.)
- Connection information (LAN segments, etc.)
- Subnet information (subnet addresses, etc.)

For details on how to modify network specifications, refer to "[3.6 Changing Network Resource Settings](#)" in the "[User's Guide for Infrastructure Administrators \(Resource Management\) CE](#)", and "[2.5.2 Modification](#)" in the "[Reference Guide \(Resource Management\) CE](#)".

4.2.4.2 When Using IBP

When using IBP, it is necessary to create an IBP uplink set for the public LAN and the admin LAN in advance.

- For Physical L-Servers

Refer to "D.4 Pre-setup Preparations (Network)".

- For Virtual L-Servers

When using virtual L-Servers, connect the IBP uplink sets used for the public LAN and admin LAN to the VM host regardless of VIOM, after creating each IBP uplink set.

It is not necessary to combine the name of the uplink set and the name of the network resource.

4.2.4.3 When Using an iSCSI LAN for iSCSI Boot

[Windows/Linux]

Create the following file in advance to define the network information used for iSCSI boot.

The network information is linked with the iSCSI boot information that is registered using the iSCSI boot operation command (rcxadm iscsictl). Refer to "2.4.2 iSCSI Boot Information" in the "Reference Guide (Resource Management) CE" beforehand.

Storage Location of the Definition File

[Windows]

Installation_folder\Manager\etc\customize_data

[Linux]

/etc/opt/FJSVrcvnr/customize_data

Definition File Name

- User Groups

iscsi_user_group_name.rcxprop

- Common on System

iscsi.rcxprop

Definition File Format

In the definition file, an item to define is entered on each line. Enter the items in the following format.

<i>Variable = Value</i>

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

Definition File Items

Table 4.7 Network Definition File Items for iSCSI Boot

Variable	Meaning	Value
<i>server_model.model_name.boot_nic</i>	<p>Specify the server model name and NIC to be booted using iSCSI. Multiple NICs can be specified.</p> <p>The following models can be specified:</p> <ul style="list-style-type: none"> - BX620 - BX920 - BX922 - BX924 - BX960 <p>When setting the default, specify an asterisk ("*").</p>	<p>Specify the items in the following format.</p> <p><i>NIC[index]</i></p> <p><i>index</i> is an integer starting from 1.</p>



Example

```
#Server Section
server_model.BX922.boot_nic = NIC1
server_model.BX924.boot_nic = NIC1,NIC2
server_model.*.boot_nic = NIC1,NIC2
```

- The entries are evaluated in the order they are added. When the same entry is found, the evaluation will be performed on the first one.
- When setting the default, specify an asterisk ("*").

4.2.4.4 When Using Link Aggregation

When using link aggregation, configure link aggregation on the LAN switch blade and L2 switch in advance. For details on configuration of link aggregation, refer to the manual of the LAN switch blade and L2 switch.

When creating a network resource, specify the link aggregation group name as the external connection port of the network resource.

For details, refer to "[C.3 Using Link Aggregation](#)".

4.2.4.5 When Using NICs other than Those in the Default Configuration of the Automatic Network Configuration

When using blade servers, NICs other than those in the default configuration of automatic network configuration can be used by creating and registering a server NIC definition with the manager in advance.

The created server NIC definition can be enabled by executing the `rcxadm nicdefctl commit` command. In the server NIC definition, define the relationship between the NICs of the managed blade servers and a physical LAN segment. By specifying this physical LAN segment from the network resource, it is possible to specify the NIC used by the network resource.

For details on the server NIC definitions, refer to "2.11 Server NIC Definition" of the "Reference Guide (Resource Management) CE". For details on the `rcxadm nicdefctl commit` command, refer to "1.7.16 rcxadm nicdefctl" in the "Reference Guide (Resource Management) CE".

4.2.4.6 When Using Automatic Virtual Switch Configuration on Rack Mount or Tower Servers

When using VMware on managed rack mount or tower servers, virtual switches and port groups can be automatically configured. In this case, it is necessary to create a server NIC definition and register it with the manager.

Use the `rcxadm nicdefctl commit` command to register the server NIC definition with the manager.

For details on the server NIC definitions, refer to "2.11 Server NIC Definition" of the "Reference Guide (Resource Management) CE". For details on the `rcxadm nicdefctl commit` command, refer to "1.7.16 rcxadm nicdefctl" in the "Reference Guide (Resource Management) CE".

4.2.4.7 When Deploying L-Servers even if the Service Console and Port Group are the Same

When using VMware as the server virtualization software, in order to deploy L-Servers even if the service console and port group is the same, it is necessary to create a VMware excluded port group definition file.

For details on VMware excluded port group definition files, refer to "2.12 VMware Excluded Port Group Definition File" in the "Reference Guide (Resource Management) CE".

4.2.4.8 When Registering Network Devices as Resources

The infrastructure administrator creates network configuration information (XML definition files) for registering network devices based on the network device information (admin IP address, account information, connection information) obtained from the network device administrator.

- About the information to be confirmed beforehand
 - When specifying the ifName for a network device as the "unit connection port name" of link information

Check the ifname of a network device using the snmpwalk command.



Example

```
snmpwalk -v 1 -c [SNMP_community_name] [IP_address] ifName
```

If the information is available from the manual or vendor of the destination device, obtain it from there.

- Necessary definitions based on the number of devices to be registered.

- When registering each network device individually

The Netdevice element must be the first.

- When registering all network devices at once

Starting with the Netconfig element, define the settings for each network device under the Netdevices element. When registering multiple network devices at once, connection information can be also defined under the Links element.

When connection information has been registered, and the connection information (in the Links element) has been specified in the network configuration information used for registering multiple network devices at the same time, all registered connection information is deleted and then the specified connection information is registered, regardless of whether registration mode (the Mode element) is specified.

- When Adding Connection Information

Specify it including already registered connection information.

- When not Changing Connection Information

Do not specify connection information.

Already registered connection information can be retrieved using the rcxadm netconfig export command.

- When registering network devices as network devices before installing them

When a network device is registered as a network device, the monitoring function starts monitoring that device. To avoid unnecessary monitoring, specify "true" for the Maintenance element when registering devices.

This setting enables the maintenance mode, excluding that device from monitored devices. After installing a network device and making it a monitoring target, release the maintenance mode.

The Maintenance element can be specified on individual network devices (individual Netdevice elements) to be registered.

- When checking account information on registration or modification of a network device as a network device

When performing network device automatic configuration, Resource Orchestrator logs in to the network device using the registered account information. For this reason, if incorrect account information is specified, automatic configuration of the network device cannot be performed.

To check in advance whether the specified account information is correct, specify "check=true" for the LoginInfo element. This allows the login process to be performed using the specified account to check that login is possible.

The LoginInfo element can be specified on individual network devices (individual Netdevice tags) to be registered.

Only account information for network devices satisfying the following conditions can be confirmed.

Vendor	Unit Name	Prompt Type	Prompt Character
Fujitsu	SR-X IPCOM EX	Login prompt	Login:
		Password prompt	Password:
		Command prompt (*1)	<i>Arbitrary string</i> #
<i>Arbitrary string</i> >			
Cisco	Catalyst ASA	Login prompt	Username:
		Password prompt	Password:
		Command prompt (*1)	<i>Arbitrary string</i> #
<i>Arbitrary string</i> >			

*1: The "#" or ">" following *arbitrary string* is used as a prompt character for the command prompt.

- When registering a network device that provides a Web interface for management

When a problem occurs on the system, sometimes investigation may be performed using the Web interface provided by the network device. In such cases, it was necessary to start the web interface of the network device from another Web browser. However, specifying a URL for opening the web interface of the network device for the MgmtURL element when registering the network device makes it be possible to quickly open the web interface of the network device from the ROR console.

The MgmtURL element can be specified on individual network devices (individual Netdevice tags) to be registered.

- When registering redundant network devices as network devices

Network devices that have the same "vendor name" and "device name" can be registered for redundant configurations. When registering a network device that has the same vendor name and device name, specify the same value as the registered network device for "Group_ID" of the Redundancy group_id element to treat that device as being in a redundant configuration.

For the "vendor name" and "device name" of a network device, collect MIB information from the network device when registering it, and confirm that the "vendor name" and "device name" are same as the ones of the registered device.

- When registering information about connections with rack mount servers

When using a rack mount server with Resource Orchestrator, it is necessary to align the NIC number of the rack mount server with the subscript of the interface name of the server OS in advance. Also, use NIC1 and NIC2 for the admin LAN.

As NIC numbers used for the public LAN are 3 or a higher number, be careful when specifying connection information.

Example

[Windows]

NIC number = the subscript of the OS interface name

The first NIC: Local Area Connection 1

The second NIC: Local Area Connection 2

[Linux]

NIC number -1 = the subscript of the OS interface name

The first NIC: eth0

The second NIC: eth1

- When registering an L2 switch

When registering an L2 switch as a network device, omit the Tenant element.

- When registering models other than those with model definitions for network devices

Add the model of the network device to be registered to the model definition for network devices, and register the network device after updating the model definition file.

- When regularly monitoring network devices registered as network device resources

When the workload of the network or network devices is temporarily increased, the response to the communication of regular monitoring may be delayed. When this delay exceeds the time-out period, the communication for regular monitoring will be executed again.

Therefore, if the monitoring interval (Interval element) or timeout period (Timeout element) specified during registration is short, the number of communications for regular monitoring may increase. It is recommended to use the default values in order to avoid increasing the load on the network and network devices.



See

- For details on network configuration information (XML definitions), refer to "2.6 Network Configuration Information" in the "Reference Guide (Resource Management) CE".
- For details on the rxadm netconfig command, refer to "1.3.7 rxadm netconfig" in the "Reference Guide (Resource Management) CE".
- For details on releasing maintenance mode, refer to "14.1 Switchover of Maintenance Mode" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".
- For details on model definitions for network devices, refer to "2.13 Network Device Model Definition" in the "Reference Guide (Resource Management) CE".

4.2.4.9 When Automatically Configuring Network Devices

This section explains how to prepare to use the function for automatically configuring network devices.



Information

Automatic configuration of firewalls is not possible if they are not registered in a network pool.

Creating Model Definitions for Network Devices

Rulesets used for the function that automatically configures network devices are registered by network device model. Therefore, it is necessary to create model definitions for determining the models of network devices.

The created model definitions are enabled by registering the following XML definition file:

[Windows]

Installation_folder\Manager\etc\customize_data\network_device_model.xml

[Linux]

/etc/opt/FJSVrcvnr/customize_data/network_device_model.xml

Newly-added models can be supported by editing the model definitions.

The network device model definitions provided with sample scripts for automatic configuration of network devices are registered in the above folder when Resource Orchestrator is installed.



Information

When editing a model definition, check the sysObjectID of the network device using the snmpwalk command.

Example

```
snmpwalk -v 1 -c [SNMP_community_name] [IP_address] sysObjectID
```

If the information is available from the manual or vendor of the destination device, obtain it from there.

See

For details on model definitions for network devices, refer to "2.13 Network Device Model Definition" in the "Reference Guide (Resource Management) CE".

Note

Use the specified OID string as the SysObjectId element in the Model element to specify the model name of the network device.

- The model definition file of network devices is searched from the start, and the first sysObjectID that matches will be used as the model name of the name attribute of the Model element.
- When there is no matching OID string in the model definition file, the model name is not specified.

Creating a Folder for Registering Rulesets

The function for automatically configuring network devices is used by executing the scripts prepared by the infrastructure administrator for each network device.

When it is necessary to specify settings that differ according to the provided service, register these patterns as separate rules to manage them. This management is performed by the ruleset.

Create a folder for registering scripts, etc. for each ruleset.

There are two types of folders for registering rulesets; folders for L-Platform templates and folders for network resources.

Folders for L-Platform Templates

Create the folders for registering rulesets for L-Platform templates with the following name:

[Windows]

Installation_folder\Manager\etc\scripts*vendor_name**unit_name or model_name*\rulesets*ruleset_name*\

[Linux]

/etc/opt/FJSVrcvmr/scripts/ vendor_name/unit_name or model_name/rulesets/ruleset_name/

Folders for Network Resources

Create the folders for registering rulesets for network resources with the following name:

[Windows]

Installation_folder\Manager\etc\scripts*network_resource**ruleset_name*\

[Linux]

/etc/opt/FJSVrcvmr/scripts/network_resource/ruleset_name/

Information

- For "*vendor_name*", "*unit_name*", and "*model_name*", specify the "*vendor name*", "*unit name*", and "*model name*" of the target network device for script execution, respectively.
The "*Vendor name*", "*unit name*", and "*model name*" of a network device can be confirmed by checking the model definition (XML file) for that device.

For details on model definitions for network devices, refer to "2.13 Network Device Model Definition" in the "Reference Guide (Resource Management) CE".

- Specify the folder name of "*ruleset name*" using up to 32 characters, including alphanumeric characters, underscores ("_"), and hyphens ("-"). This name should start with an alphabetical character.

Set a unique name for the folder name of "*ruleset name*", excluding the following folders in which sample scripts are registered.

[Windows]

Installation_folder\Manager\etc\scripts\

[Linux]

/etc/opt/FJSVrcvmr/scripts/



Sample Scripts

Sample scripts to be used for automatic configuration of network devices are registered in the following folder when Resource Orchestrator is installed.

[Windows]

Installation_folder\Manager\etc\scripts\original*vendor_name**unit_name*\rulesets*ruleset_name*\

Installation_folder\Manager\etc\scripts\original\network_resource*ruleset_name*\

[Linux]

/etc/opt/FJSVrcvmr/scripts/original/*vendor_name*/*unit_name*/rulesets/*ruleset_name*/

/etc/opt/FJSVrcvmr/scripts/original/network_resource/*ruleset_name*/

The following table lists the unit names supported by the sample scripts provided by Resource Orchestrator:

Table 4.8 Units for which Sample Scripts are Provided

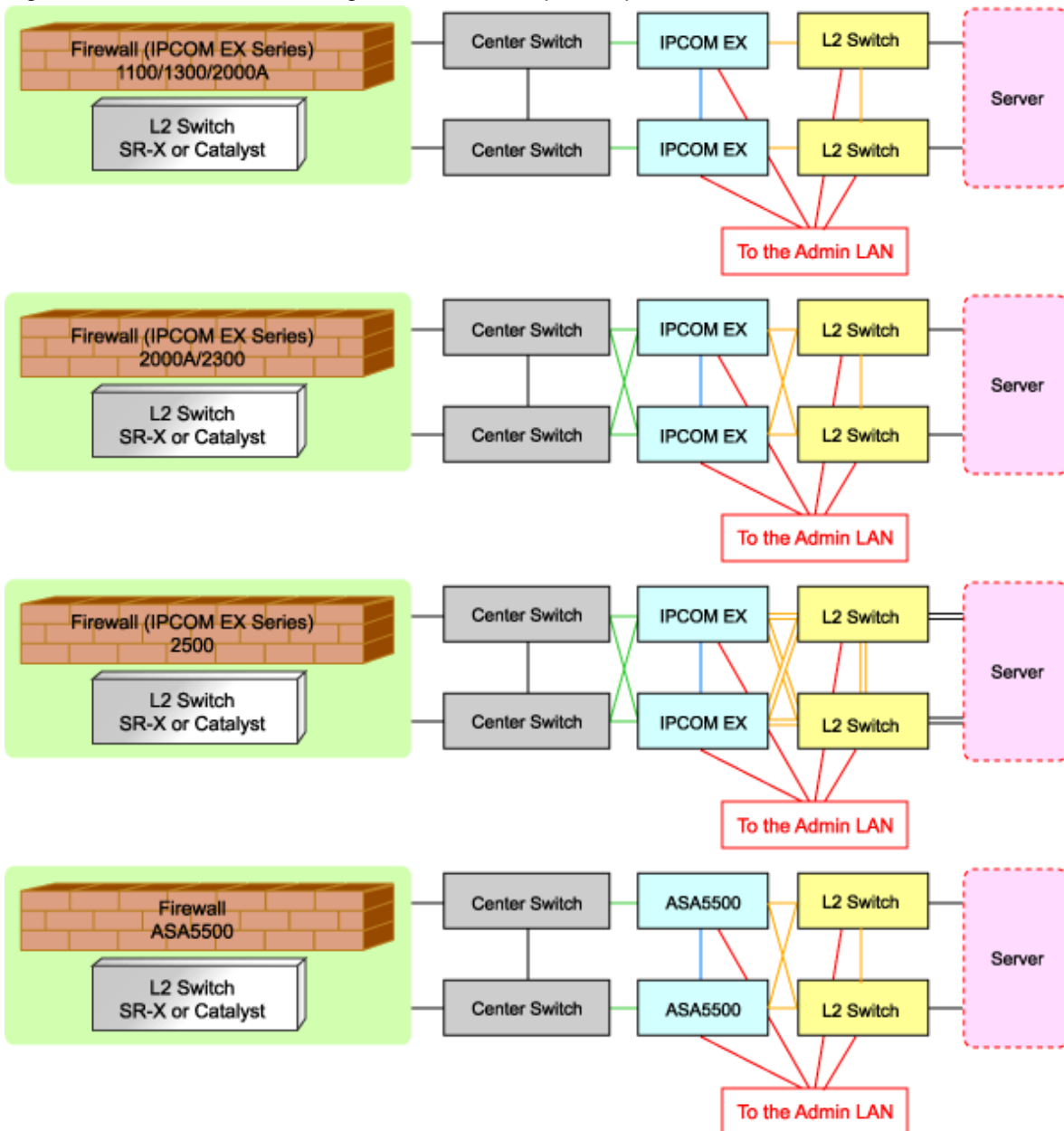
Vendor	Unit Name	Type	Setting Details
Fujitsu	SR-X500	L2 switch	- Add VLAN (tagged VLAN, port VLAN)
	SR-X300		- Delete VLAN (tagged VLAN, port VLAN)
	IPCOMEXSC	Firewall (*1)	- Add VLAN to LAG interface (tagged VLAN, port VLAN)
	IPCOMEXIN		- Delete VLAN of LAG interface (tagged VLAN, port VLAN)
Cisco	Catalyst	L2 switch	- External interface (center switch side)
			- Add or delete Firewall rules
	ASA5500	Firewall (*1)	- Add or delete dstNAT rules
			- Add or delete srcNAT rules
			- Internal interface (L2 switches)
			- Add or delete VLAN interface
			- Add or delete Firewall rules
			- Add VLAN (tagged VLAN, port VLAN)
			- Delete VLAN (tagged VLAN, port VLAN)
			- Add VLAN to LAG interface (tagged VLAN, port VLAN)
			- Delete VLAN of LAG interface (tagged VLAN, port VLAN)

Vendor	Unit Name	Type	Setting Details
			<ul style="list-style-type: none"> - Add or delete Firewall rules - Add or delete dstNAT rules - Add or delete srcNAT rules - Internal interface (L2 switches) - Add or delete VLAN interface - Add or delete Firewall rules

*1: Configure Firewall rules for the VLAN interfaces of LAN ports to use as public LANs.

The default model configuration assumed by a sample script is given below:

Figure 4.19 Default Model Configuration for a Sample Script



Listed below are sample ruleset names provided by Resource Orchestrator:

For SR-X300

tag_vlan_port--SR-X300
tag_vlan_port--SR-X300_n

For the systems that configure tagged VLANs on the LAN ports connected with firewalls and servers

untag_vlan_port--SR-X300
untag_vlan_port--SR-X300_n

For the systems that configure port VLANs on the LAN ports connected with firewalls and servers

tag_vlan_net--SR-X300
tag_vlan_net--SR-X300_n

For the systems that configure tagged VLAN networks

untag_vlan_net--SR-X300
untag_vlan_net--SR-X300_n

For the systems that configure untagged VLAN networks

n: Number of "2" or larger

For SR-X500

tag_vlan_port--SR-X500
tag_vlan_port--SR-X500_n

For the systems that configure tagged VLANs on the LAN ports connected with firewalls and servers

untag_vlan_port--SR-X500
untag_vlan_port--SR-X500_n

For the systems that configure port VLANs on the LAN ports connected with firewalls and servers

tag_vlan_net--SR-X500
tag_vlan_net--SR-X500_n

For the systems that configure tagged VLAN networks

untag_vlan_net--SR-X500
untag_vlan_net--SR-X500_n

For the systems that configure untagged VLAN networks

n: Number of "2" or larger

For IPCOM EX SC

3Tier_system_firewall--IPCOMSC1

For the systems that use IPCOMEX1100_SC/1300_SC/2000A_SC as an IPCOM EX SC series model for three-tier models

LAN Ports to be Used

- For Public LANs (Center Switch Side)

LAN0.0

- For Public LANs (L2 Switch Side)

LAN0.1

- For the Admin LAN

LAN0.3

- For Unit Synchronization

LAN0.2

3Tier_system_firewall--IPCOMSC2

For the systems that use IPCOMEX2000A_SC/2300_SC as an IPCOM EX SC series model for three-tier models

LAN Ports to be Used

- For Public LANs (Center Switch Side)

bnd0: Redundant LAN Channels

LAN0.0
LAN1.0

- For Public LANs (L2 Switch Side)

bnd1: Redundant LAN Channels

LAN0.1
LAN1.1

- For the Admin LAN

LAN0.3

- For Unit Synchronization

LAN1.3

3Tier_system_firewall--IPCOMSC3

For the systems that use IPCOMEX2500_SC as an IPCOM EX SC series model for three-tier models

LAN Ports to be Used

- For Public LANs (Center Switch Side)

bnd0: Redundant LAN Channels

LAN0.0
LAN1.0

- For Public LANs (L2 Switch Side)

bnd1: Redundant LAN Channels

LAN0.1 and LAN0.2
LAN1.1 and LAN1.2

Connection using Link aggregation

- For the Admin LAN

LAN0.3

- For Unit Synchronization

LAN1.3

For IPCOM EX IN

3Tier_system_firewall--IPCOMIN2

For the systems that use IPCOMEX2000A_IN/2300_IN as an IPCOM EX IN series model for three-tier models

LAN Ports to be Used

- For Public LANs (Center Switch Side)

bnd0: Redundant LAN Channels

LAN0.0
LAN1.0

- For Public LANs (L2 Switch Side)

bnd1: Redundant LAN Channels

LAN0.1
LAN1.1

- For the Admin LAN
LAN0.3
- For Unit Synchronization
LAN1.3

3Tier_system_firewall--IPCOMIN3

For the systems that use IPCOMEX2500_IN as an IPCOM EX IN series model for three-tier models

LAN Ports to be Used

- For Public LANs (Center Switch Side)

bnd0: Redundant LAN Channels

LAN0.0
LAN1.0

- For Public LANs (L2 Switch Side)

bnd1: Redundant LAN Channels

LAN0.1 and LAN0.2
LAN1.1 and LAN1.2

Connection using Link aggregation

- For the Admin LAN
LAN0.3
- For Unit Synchronization
LAN1.3

For Catalyst

tag_vlan_port--Catalyst
tag_vlan_port--Catalystn

For the systems that configure tagged VLANs on the LAN ports connected with firewalls and servers

untag_vlan_port--Catalyst
untag_vlan_port--Catalystn

For the systems that configure port VLANs on the LAN ports connected with firewalls and servers

tag_vlan_net--Catalyst
tag_vlan_net--Catalystn

For the systems that configure tagged VLAN networks

untag_vlan_net--Catalyst
untag_vlan_net--Catalystn

For the systems that configure untagged VLAN networks

n: Number of "2" or larger

For ASA5500

3Tier_system_firewall--ASA1

For the systems that use ASA5510 as an ASA5500 series model for three-tier models

LAN Ports to be Used

- For Public LANs (Center Switch Side)
redundant1: Redundant LAN Channels
ethernet0/0
ethernet0/1

- For Public LANs (L2 Switch Side)

redundant2: Redundant LAN Channels

ethernet0/2
ethernet0/3

- For the Admin LAN

management0/0

3Tier_system_firewall--ASA2

For the systems that use ASA5520/5540/5550 as an ASA5500 series model for three-tier models

LAN Ports to be Used

- For Public LANs (Center Switch Side)

redundant1: Redundant LAN Channels

gigabitethernet0/0
gigabitethernet0/1

- For Public LANs (L2 Switch Side)

redundant2: Redundant LAN Channels

gigabitethernet0/2
gigabitethernet0/3

- For the Admin LAN

management0/0

3Tier_system_firewall--ASA3

For the systems that use ASA5580 as an ASA5500 series model for three-tier models

LAN Ports to be Used

- For Public LANs (Center Switch Side)

redundant1: Redundant LAN Channels

gigabitethernet3/0
gigabitethernet3/1

- For Public LANs (L2 Switch Side)

redundant2: Redundant LAN Channels

gigabitethernet3/2
gigabitethernet3/3

- For the Admin LAN

management0/0

The following script lists are also provided as samples for each ruleset:

- create.lst

Sample script list for additional configuration

- modify.lst

Sample script list for configuration modification

- delete.lst

Sample script list for configuration deletion

- create_recovery.lst

Sample script list for recovery from errors detected during addition of settings

- modify_recovery.lst
Sample script list for recovery from errors detected during modification of settings
- connect.lst
Sample script list for configuration of interfaces adjacent to servers (only for L2 switches)
- disconnect.lst
Sample script list for deletion of interfaces adjacent to servers (only for L2 switches)
- connect_recovery.lst
Sample script list for recovery from errors detected during configuration of adjacent servers (only for L2 switches)

Note

The sample scripts provided by Resource Orchestrator may be added or deleted when the software is updated.

When using the sample scripts, confirm the directory on the admin server in which the sample scripts are registered beforehand.

Copy Destination of Sample Script Rulesets

Rulesets in which sample scripts are registered are copied to the folder for ruleset registration during installation and made available for use.

For example, when using an SR-X300 as an L2 switch, and an IPCOM EX1300 SC, rulesets are copied as follows:

- For SR-X300

When an admin server operates on Windows

- For Port Configuration
 - Source Folder:
Installation_folder\Manager\etc\scripts\original\Fujitsu\SR-X300\rulesets\xxx_vlan_port--SR-X300
 - Destination Folder
Installation_folder\Manager\etc\scripts\Fujitsu\SR-X300\rulesets\xxx_vlan_port--SR-X300
- For Network Configuration
 - Source Folder:
Installation_folder\Manager\etc\scripts\original\network_resource\xxx_vlan_net--SR-X300
 - Destination Folder
Installation_folder\Manager\etc\scripts\network_resource\xxx_vlan_net--SR-X300

xxx: "tag" or "untag"

When an admin server operates on Linux

- For Port Configuration
 - Source directory
/etc/opt/FJSVrcvmr/scripts/original/Fujitsu/SR-X300/rulesets/xxx_vlan_port--SR-X300
 - Destination directory
/etc/opt/FJSVrcvmr/scripts/Fujitsu/SR-X300/rulesets/xxx_vlan_port--SR-X300
- For Network Configuration
 - Source directory
/etc/opt/FJSVrcvmr/scripts/original/network_resource/xxx_vlan_net--SR-X300

- Destination directory

/etc/opt/FJSVrcvmr/scripts/network_resource/xxx_vlan_net--SR-X300

xxx: "tag" or "untag"

- For IPCOM EX1300 SC

When an admin server operates on Windows

- Source Folder

Installation_folder\Manager\etc\scripts\original\Fujitsu\IPCOMEXSC\rulesets\3Tier_system_firewall--IPCOMSC1

- Destination Folder

Installation_folder\Manager\etc\scripts\Fujitsu\IPCOMEXSC\rulesets\3Tier_system_firewall--IPCOMSC1

When an admin server operates on Linux

- Source Folder

/etc/opt/FJSVrcvmr/scripts/original/Fujitsu/PCOMEXSC/rulesets/3Tier_system_firewall--IPCOMSC1

- Destination Folder

/etc/opt/FJSVrcvmr/scripts/Fujitsu/PCOMEXSC/rulesets/3Tier_system_firewall--IPCOMSC1

4.2.5 When Providing IPv6 Network for Public LANs

When building an IPv6 network on a public LAN, the required network devices and settings vary depending on the desired operations.



Note

- Resource Orchestrator does not provide IPv6 address management.

Address management should be performed by the infrastructure administrator and tenant administrator.

- Network configurations that allow IPv6 packets on a public LAN to pass through the admin LAN to reach the admin server and managed server or units are not supported.

Table 4.9 Network Devices Required for an IPv6 network on a Public LAN

Operation	Required Network Device	Required Configuration
Use of a static IP address to allow access from other servers.	None	Configure an IPv6 address for the server OS.
Connects with the other servers as a client. IP addresses are configured by the server's automatic configuration function.	IPv6 routers	Set a prefix and the RA M/O flag on the IPv6 router.
Use of the name published using DNS to allow access from the other servers. IP addresses are configured by the server's automatic configuration function.	IPv6 routers	Set a prefix and the RA M/O flag on the IPv6 router.
	DHCPv6 server	Register the DNS address on the DHCPv6 server.
	DNS server	Configure the DNS server to enable connection with the IPv6 network. Configure the IPv6 address assigned to the server and domain name to be published on the DNS server.
Use of the name published using DNS to allow access from the other servers. Static IP addresses are assigned using a DHCPv6 server.	IPv6 routers	Set a prefix and the RA M/O flag on the IPv6 router.
	DHCPv6 server	Register the DNS address on the DHCPv6 server. Add an entry for the server identifier (DUID) and entries including the pair of the NIC identifier (IAID) and the IPv6 address to the DHCPv6 server.

Operation	Required Network Device	Required Configuration
	DNS server	<p>Configure the DNS server to enable connection with the IPv6 network.</p> <p>Configure the IPv6 address assigned to the server and domain name to be published on the DNS server.</p>

*1: When the IP address changes because of automatic IP address configuration performed by the server, the server may be temporarily inaccessible until updating processes for DNS cache, etc. complete. To avoid such a problem, use an automatic IP address configuration method that would not change IP addresses over time (such as EUI-64 or the OS specific method).

Information

- In order to use IPv6 immediately after image deployment, perform the following on the collection target OS before collecting the image:
 - Enable IPv6
 - When there are manually configured IPv6 addresses, delete them
- In Resource Orchestrator, an IPv6 network can be used for the public LAN only when using the following L-Servers:
 - Physical L-Servers
 - Virtual L-Servers (only for VMware)

For details on required configurations for individual devices, refer to the manual of each device.

Design of IPv6 Prefixes to be Allocated to Public LANs

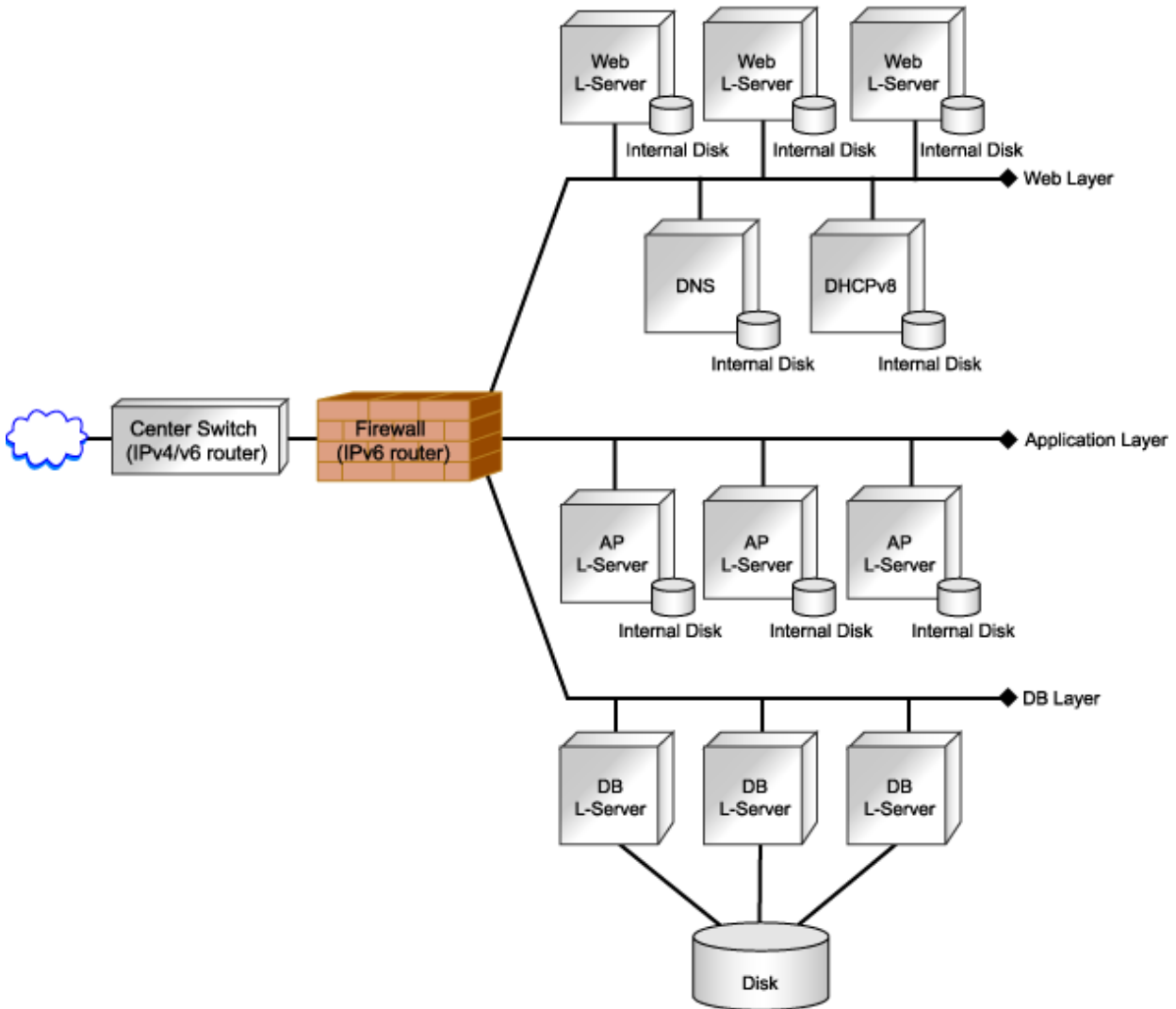
An example of designing the IPv6 address range (prefix and network ID) to be allocated to each public LAN based on the assigned GUA is given below:

Assign prefixes in the unit of /64 for each network t so that automatic server configuration can be selected.

For three-tier models, assign /62 for the prefix length of each L-Platform, as this model requires four networks (three "public LAN networks" and one "network connecting IPv4/v6 routers and firewalls").

When performing static routing, configure routing settings on the IPv6 router. For details on how to configure routing on the IPv6 router, refer to the manual for the IPv6 router being used.

Figure 4.20 Example of Public LAN Configuration Using an IPv6 Network



4.3 Deciding and Configuring the Storage Environment

This section explains how to decide and configure the storage environment.

4.3.1 Deciding the Storage Environment

This section explains how to define the storage environment settings required for a Resource Orchestrator setup.

4.3.1.1 Storage Environment Preparation

This section explains the preparations for setting up storage.

When creating physical servers and virtual machines, it was difficult to smoothly provide servers as configuration of storage units and the storage network was necessary.

Using the following functions of Resource Orchestrator, servers can be provided smoothly.

Allocating Storage to a Virtual L-Server

There are two ways to allocate storage to a virtual L-Server:

- Allocate disk resources (virtual disks) automatically created from virtual storage resources (datastores)
 1. Through coordination with VM management software, virtual storage resources (such as the file systems of VM guests) that were created in advance are automatically detected by Resource Orchestrator. From the detected virtual storage resources, virtual storage resources meeting virtual L-Server specifications are automatically selected by Resource Orchestrator.
 2. From the automatically selected virtual storage resources, disk resources (such as virtual disks) of the specified size are automatically created and allocated to the virtual L-Server.
 - [Xen]
 - GDS single disks can be used as virtual storage.
- Allocate disk resources (raw devices or partitions) that were created in advance [KVM]
 1. Create LUNs for the storage units.
 - LUNs are used for virtual L-Server disks. Create the same number of LUNs as that of necessary disks. The size of each LUN must be larger than the size of each disk.
 2. Make the VM host recognize the LUNs created in 1. as raw devices.
 - When migrating VM guests for virtual L-Servers, configure zoning and affinity to set LUNs as shared disks.
 - Partitions are also used for virtual L-Server disks. Create the same number of partitions as that of necessary disks. The size of each partition must be larger than the size of each disk.
 3. Use the rcxadm disk command to register the raw devices or the partitions with Resource Orchestrator as disk resources.
 - When migrating VM guests for virtual L-Servers, register the raw devices or the partitions shared between multiple VM hosts as disk resources defined to be shared.
 4. From the registered disk resources, disk resources meeting the virtual L-Server specifications are automatically selected and allocated to the L-Server by Resource Orchestrator.

Definition File Required when Using a Virtual L-Server

The definition file required when using a virtual L-Server is indicated below.

- When configuring Thin Provisioning attributes on a storage pool
 - Refer to "Configuring Thin Provisioning Attributes for Storage Pools" in "12.2 Resource Pool Operations" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".
- When using priority for resource selection on Thin Provisioning
 - Refer to "[Configuration of Priority for Resource Selection on Thin Provisioning](#)" of "[E.1.1 Definition Files](#)".

Allocating Storage to a Physical L-Server

There are two ways to allocate storage to a physical L-Server:

- Allocate disk resources (LUNs) automatically created from virtual storage resources (RAID groups)
 1. Through coordination with storage products, Resource Orchestrator automatically detects virtual storage resources that were created in advance.
 2. From the detected virtual storage resources, Resource Orchestrator automatically selects virtual storage resources meeting physical L-Server specifications.
 3. From the automatically selected virtual storage resources, create disk resources of the specified size and allocate them to the physical L-Server.
- Allocate disk resources (LUNs) that were created in advance
 1. Through coordination with storage products, Resource Orchestrator automatically detects disk resources that were created in advance.

2. From the detected disk resources, Resource Orchestrator automatically selects disk resources meeting physical L-Server specifications and allocates them to the L-Server.

Storage Allocation Methods and Storage Types

The storage allocation method varies depending on the storage units being used.

For the storage allocation methods and storage types, refer to "[Table 4.10 Storage Allocation Methods and Storage Types for Physical L-Servers](#)" in "[4.3.1.2 Storage Configuration](#)".

Storage Units that can be Connected with Physical L-Servers

For the storage units that can be connected with physical L-Servers, refer to "[Table 1.61 Storage Units that can be Connected with L-Servers on Physical Servers](#)" in "[1.5 Hardware Environment](#)".

Effective Utilization of Storage Using Thin Provisioning

Thin provisioning is technology for virtualizing storage capacities.

It enables efficient utilization of storage.

The function does not require the necessary storage capacity to be secured in advance, and can secure and extend the storage capacity according to how much is actually being used.

Thin provisioning can be achieved using the following two methods:

- Method for using the thin provisioning of a storage unit
Resource Orchestrator can be coordinated with the thin provisioning of ETERNUS storage.
- Method for using the thin provisioning of server virtualization software
Resource Orchestrator can be coordinated with VMware vStorage Thin Provisioning.

For details on linking with thin provisioning, refer to "[4.3.1.2 Storage Configuration](#)".

Effective Utilization of Storage Using Automatic Storage Layering

Automatic Storage Layering is a feature that monitors data access frequency in mixed environments that contain different storage classes and disk types. It then automatically relocates data to the most appropriate storage devices based on set data usage policies.

Resource Orchestrator can be coordinated with Automatic Storage Layering for ETERNUS storage. For details on coordination with Automatic Storage Layering, refer to "[4.3.1.2 Storage Configuration](#)".

Prerequisites when Creating a Physical L-Server

For details on the prerequisites when creating a physical L-Server, refer to "[Prerequisites when Creating a Physical L-Server](#)" in "[4.3.1.2 Storage Configuration](#)".

Storage Configuration when Using a Physical Server as an L-Server

For details on the storage configuration when using a physical server as an L-Server, refer to "[Storage Configuration when Creating a Physical L-Server](#)" in "[4.3.1.2 Storage Configuration](#)".

Storage resources are categorized into the following two types.

The resource registration method differs depending on the type of storage resource.

- Virtual Storage Resources

When storage management software is registered to Resource Orchestrator, the storage information controlled by the storage management software is automatically obtained and detected as a virtual storage resource. Therefore, it is not necessary to register virtual storage resources individually.

- Disk Resources

For disk resources created in advance such as LUNs, storage information is automatically obtained when storage management software is registered, and they are detected as disk resources. Therefore, it is not necessary to register disk resources individually.

Disks created in advance using storage management software can be managed as disk resources.

Detected virtual storage resources and disk resources must be registered to the storage pool.

For details on registering to a storage pool, refer to "7.5 Storage Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Automatic Detection of Storage Resources

When addition or modification of storage is performed using storage management software or VM management software, periodic queries are made to the storage management software or VM management software to detect changes to the configuration/status of storage. The interval between regular updates varies according to the number of storage resources.

By right-clicking a storage resource on the ROR console orchestration tree and selecting [Update] on the displayed menu, the configuration/status of the storage management software and VM management software is refreshed without waiting for the regular update.

After that, perform registration in the storage pool.

Definition File Required when Using a Physical L-Server

The definition file required when using a physical L-Server is indicated below.

- When using the following storage

- ETERNUS Storage
- EMC CLARiiON Storage
- EMC Symmetrix DMX Storage
- EMC Symmetrix VMAX Storage

Refer to "[6.1.1 Creating Definition Files Combining Ports of SAN Storage](#)".

- When using ESC as storage management software

Refer to "[Format Selection for the Names of Virtual Storage Resources and Disk Resources Managed by ESC](#)" of "[D.5.1 Definition Files](#)".

- When using EMC Navisphere Manager or EMC Solutions Enabler as storage management software

For details, refer to "[Definition File for EMC Storage](#)" of "[D.5.1 Definition Files](#)".

- When configuring Thin Provisioning attributes on a storage pool

Refer to "Configuring Thin Provisioning Attributes for Storage Pools" in "12.2 Resource Pool Operations" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- When using priority for resource selection on Thin Provisioning and Automatic Storage Layering

Refer to "[Configuration of Priority for Resource Selection on Thin Provisioning on Thin Provisioning and Automatic Storage Layering](#)" of "[D.5.1 Definition Files](#)".

- When using dynamic LUN mirroring

For details, refer to "[Creating Mirroring Definition Files for Dynamic LUN Mirroring](#)" of "[D.5.1 Definition Files](#)".

4.3.1.2 Storage Configuration

This section explains how to configure a storage environment and define the settings required for Resource Orchestrator installation.

Storage Allocation Methods and Storage Types

The storage allocation method varies depending on the storage units being used.

The following storage allocation methods and storage types are available for physical L-Servers.

Table 4.10 Storage Allocation Methods and Storage Types for Physical L-Servers

Allocation Method	Storage Type
Allocate disk resources automatically created from virtual storage resources	<ul style="list-style-type: none"> - ETERNUS Storage - NetApp FAS Storage
Allocate disk resources that were created in advance	<ul style="list-style-type: none"> - ETERNUS Storage - NetApp FAS Storage - EMC CLARiON Storage - EMC Symmetrix DMX Storage - EMC Symmetrix VMAX Storage

Storage Configuration

Decide the storage configuration necessary for the system.

The storage configurations supported by Resource Orchestrator are as follow:

Table 4.11 Supported Storage Configurations

Server (VM host) Type	L-Server System Disk	L-Server Data Disk
Physical	SAN storage	SAN storage
	iSCSI storage (*1, *2)	iSCSI storage (*1, *3)
VMware	Storage configured for datastores of ESX/ESXi (VMFS Version 3 or later, or NFS mount)	
Hyper-V	Storage configured for Cluster Shared Volumes (CSV) of MSFC	

*1: Available when ETERNUS storage and NetApp storage are used.

*2: When using Linux for a physical L-Server, and iSCSI storage for a system disk, it is not possible to create an L-Server using a cloning image.

*3: When creating an L-Server, iSCSI storage is not allocated to the L-Server as a data disk. Manually allocate the iSCSI storage to the L-Server, after starting the L-Server. Attaching or detaching iSCSI storage to or from an L-Server cannot be performed using Resource Orchestrator. Perform those operations manually. For details on data disk allocation for iSCSI storage, refer to "Information- Physical L-Server Data Disk for iSCSI Boot".

Information

Physical L-Server Data Disk for iSCSI Boot

- When Using ETERNUS Storage

Using storage management software, the data disk can be accessed from managed servers by defining LUNs of the iSCSI boot disk and of the data disk in the same Affinity group.

- When Using NetApp Storage

Using storage management software, the data disk can be accessed from managed servers by defining LUNs of iSCSI boot disk and of the data disk in the same igroup.

Linking with Thin Provisioning

Resource Orchestrator can be linked with the thin provisioning of storage units and server virtualization software.

- Linking with the thin provisioning of ETERNUS storage

With ETERNUS storage, a virtual resource pool comprised of one or more RAID groups is called a Thin Provisioning Pool (hereinafter TPP).

Also, a virtual volume that shows a volume with a greater capacity than the physical disk capacity of the server is called a Thin Provisioning Volume (hereinafter TPV).

Capacity is allocated to TPVs from TPPs.

With Resource Orchestrator, TPPs can be managed as virtual storage resources.

The virtual storage resource of a TPP is called a virtual storage resource with thin provisioning attributes set.

The virtual storage resource of a RAID group is called a virtual storage resource with thick provisioning attributes set.

With Resource Orchestrator, ESC can be used to create a TPV in advance and manage that TPV as a disk resource.

The disk resource of a TPV is called a disk with thin provisioning attributes set.

The disk resource of an LUN is called a disk with thick provisioning attributes set.

- Coordination with VMware vStorage Thin Provisioning

In VMware, a virtual disk with a thin provisioning configuration is called a thin format virtual disk.

With Resource Orchestrator, thin format virtual disks can be managed as disk resources.

A thin format virtual disk is called a disk with thin provisioning attributes set.

A thick format disk resource is called a disk with thick provisioning attributes set.

- Storage resource management

With Resource Orchestrator, storage resources (virtual storage resources and disk resources) can be managed in a storage pool. Storage pools must take into account the existence of thin provisioning attributes.

The following resources can be registered in a storage pool with thin provisioning attributes set:

- Virtual storage resources with thin provisioning attributes set
- Disk resources with thin provisioning attributes set

The following resources can be registered in a storage pool without thin provisioning attributes set:

- Virtual storage resources with thick provisioning attributes set
- Disk resources with thick provisioning attributes set

[VMware]

Thin provisioning cannot be set for VMware datastores. Therefore, the following settings must be specified in Resource Orchestrator.

- When creating disk resources from virtual storage resources registered in a storage pool with thin provisioning attributes set, set the thin format and allocate the disk resources to an L-Server.
- When creating disk resources from virtual storage resources registered in a storage pool without thin provisioning attributes set, set the thick format and allocate the disk resources to an L-Server.

For the method to set thin provisioning for a storage pool, refer to "Configuring Thin Provisioning Attributes for Storage Pools" in "12.2 Resource Pool Operations" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".



Note

[VMware]

When creating a virtual L-Server with a cloning image specified, the provisioning attribute of the cloning image takes preference over the provisioning attribute of the storage pool.

Coordination with Automatic Storage Layering

In Resource Orchestrator, coordination with Automatic Storage Layering for storage units is available.

- Coordination with Automatic Storage Layering for ETERNUS Storage

In ETERNUS storage, the physical disk pool created using Automatic Storage Layering is called a Flexible TieR Pool (hereafter FTRP). The virtual volume created using Automatic Storage Layering is called a Flexible Tier Volume (hereafter FTV). FTV is allocated from FTRP.

In Resource Orchestrator, an FTRP can be managed as a virtual storage resource. The virtual storage resource for FTRP, similar to a TPP, is called a virtual storage resource for which the Thin Provisioning attribute has been configured.

In Resource Orchestrator, after creating an FTV using ESC, that FTV can be managed as a disk resource. The disk resource for FTV, similar to a TPV, is called a disk for which the Thin Provisioning attribute has been configured.

- Management of FTRP and FTV

In Resource Orchestrator, FTRP and FTV can be managed as storage resources in storage pools.

FTRP and FTV are considered the same as TPP and TPV for Thin Provisioning. For details, refer to "[Linking with Thin Provisioning](#)".



Users are recommended to operate the storage pool used for registering FTRP and FTV separately from the storage pool used for registering TPP and TPV.

When operating the storage in the same storage pool, the storage may not be operated by taking advantage of the properties, since the virtual storage to be selected will change depending on the amount of free space when allocating disks.

Storage Configuration when Creating a Physical L-Server

The storage configuration when creating a physical L-Server is indicated below.

- When using a Fibre Channel connection, multiple storage units can be connected to a single L-Server (when VIOM connections are not supported, only one storage unit can be connected). When using an iSCSI connection, one storage unit can be connected to a single L-Server.
- Sharing of storage between multiple L-Servers is supported.



Local disks are not supported. Do not connect local disks.

For details on required VM management software and storage management software, refer to "[1.4.2.2 Required Software](#)".

For details on supported storage units and Fibre Channel switches, refer to "[1.5 Hardware Environment](#)".

Prerequisites when Creating a Physical L-Server

- L-Servers support SAN boot and iSCSI boot configurations.
- When using a physical server as an L-Server, it is necessary that connection using VIOM or HBA address rename is supported. For details on connection using VIOM or HBA address rename, refer to "[4.3.1 Deciding the Storage Environment](#)" and "[4.3.2 Configuring the Storage Environment](#)".
- Usage methods of VIOM and HBA address rename differ depending on the hardware of managed servers used to configure a physical L-Server.
 - Blade Servers
 - Use VIOM.
 - Rack Mount Servers
 - Use HBA address rename.

- For L-Server SAN storage paths and iSCSI storage paths, multipaths (two paths) are supported.
- Configurations with two or less HBA ports on managed servers are supported.
- When using the MMB firmware for which Fibre Channel card information cannot be obtained by blade servers, only configurations where Fibre Channel cards are mounted in expansion slot 2 are supported. The servers for which the information of Fibre Channel cards can be obtained are as follows:
 - PRIMERGY BX900 series servers
4.70 or later
 - PRIMERGY BX400 series servers
6.22 or later
- In the case of blade servers, please do not set the following parameters during setup of VIOM.
 - WWN Address Range
 - MAC Address Range

HBA and Storage Unit Configuration

When designing systems, define the relationships of physical servers and HBA WWNs on servers, and the relationships of storage volumes and HBA WWNs on storage.

Configure SAN Storage Environments

SAN storage environment configurations differ according to the L-Server type in use, "Physical" or "Virtual".

When using a physical server as an L-Server, refer to "[Appendix D Design and Configuration when Creating a Physical L-Server](#)".

When using server virtualization software, refer to the information for the software being used in "[Appendix E Design and Configuration for Creating Virtual L-Servers](#)".

Configure iSCSI Storage Environments

When using iSCSI boot on physical L-Servers, create LUNs that can be connected to L-Servers in advance.

For details, refer to "[D.3.1 When Using ETERNUS Storage](#)" and "[D.3.2 When Using NetApp FAS Storage](#)".

Dynamic LUN Mirroring Settings

If dynamic LUN mirroring is to be used on the physical L-Server, make settings so that copying between ETERNUS storage machines is made possible.

For details on the configuration method, refer to the "ETERNUS SF AdvancedCopy Manager Operator's Guide for Copy Control Module".

4.3.1.3 HBA and Storage Device Settings

System configuration requires that the relationship between physical servers and HBA WWNs from the perspective of the server, and the relationship between storage volumes and HBA WWNs from the perspective of storage devices be defined clearly.

An example where blades connect to storage devices via multiple paths using two HBA ports is shown below.

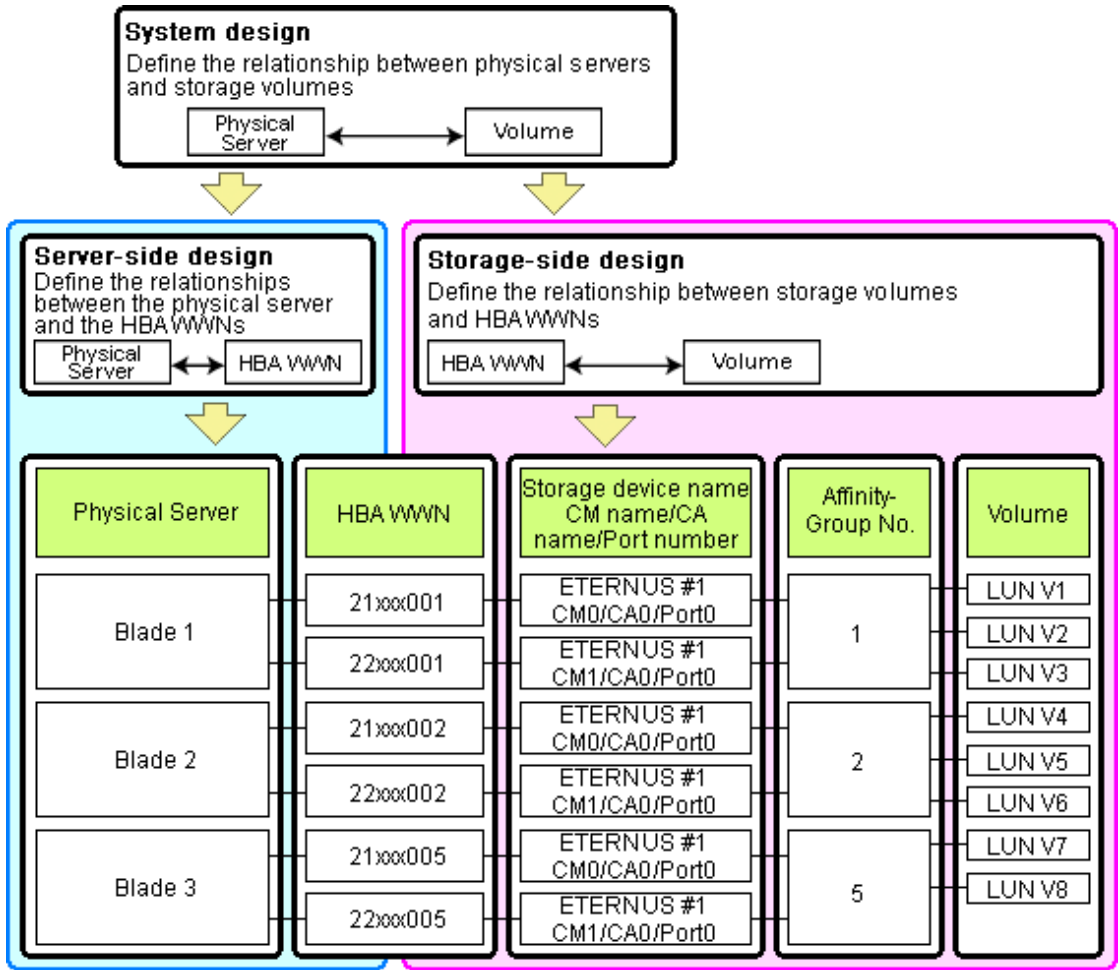
Refer to the storage device manual of each storage device for details.



Note

Resource Orchestrator does not support configurations where managed servers are mounted with three or more HBA ports.

Figure 4.21 WWN System Design



Choosing WWNs

Choose the WWNs to use with the HBA address rename or VIOM function.

After WWNs have been chosen, associate them with their corresponding operating systems (applications) and physical servers (on the server side), and with corresponding volume(s) (on the storage side).

Using HBA address rename or VIOM, storage-side settings can be defined without prior knowledge of the actual WWN values of a server's HBAs. This makes it possible to design a server and storage system without having the involved physical servers on hand.

When HBA address rename is used, the value provided by the "I/O virtualization option" is used as the WWN.

When VIOM is used, set the WWN value with either one of the following values:

- The value provided by the "I/O virtualization option"
- The value selected automatically from the address range at VIOM installation

To prevent data damage by WWN conflict, you are advised to use the value provided by "I/O virtualization option".

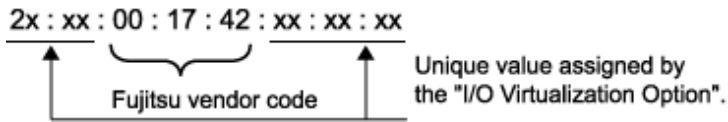
Information

Specify the unique WWN value provided by the "I/O virtualization option". This can prevent unpredictable conflicts of WWNs.

Note

Do not use the same WWN for both HBA address rename and VIOM. If the same WWN is used, there is a chance data will be damaged.

The WWN format used by the HBA address rename and VIOM functions are as follows:



The "2x" part at the start of the provided WWN can define either a WWNN or a WWP. Define and use each of them as follows.

- 20: Use as a WWNN
- 2x: Use as a WWP

With HBA address rename, x will be allocated to the I/O addresses of HBA adapters in descending order. I/O addresses of HBA adapters can be confirmed using the HBA BIOS or other tools provided by HBA vendors.

Note

With HBA address rename, as WWNs are allocated to the I/O addresses of HBAs in descending order, the order may not match the port order listed in the HBA.

For details, refer to "[C.2 WWN Allocation Order during HBA address rename Configuration](#)".

The WWN chosen here would be used for the system design of the servers and storage.

- Server-side Design

WWNs are used in server-side design by assigning one unique to each server.

- Storage-side Design

One or more volumes are chosen for each server, and the corresponding WWN assigned to each server in the server-side design is configured on the storage-side for those volumes.

Defining WWN settings for VIOM

VIOM should be configured first. Then, storage devices should also be configured in accordance with the WWN settings that were defined within VIOM.

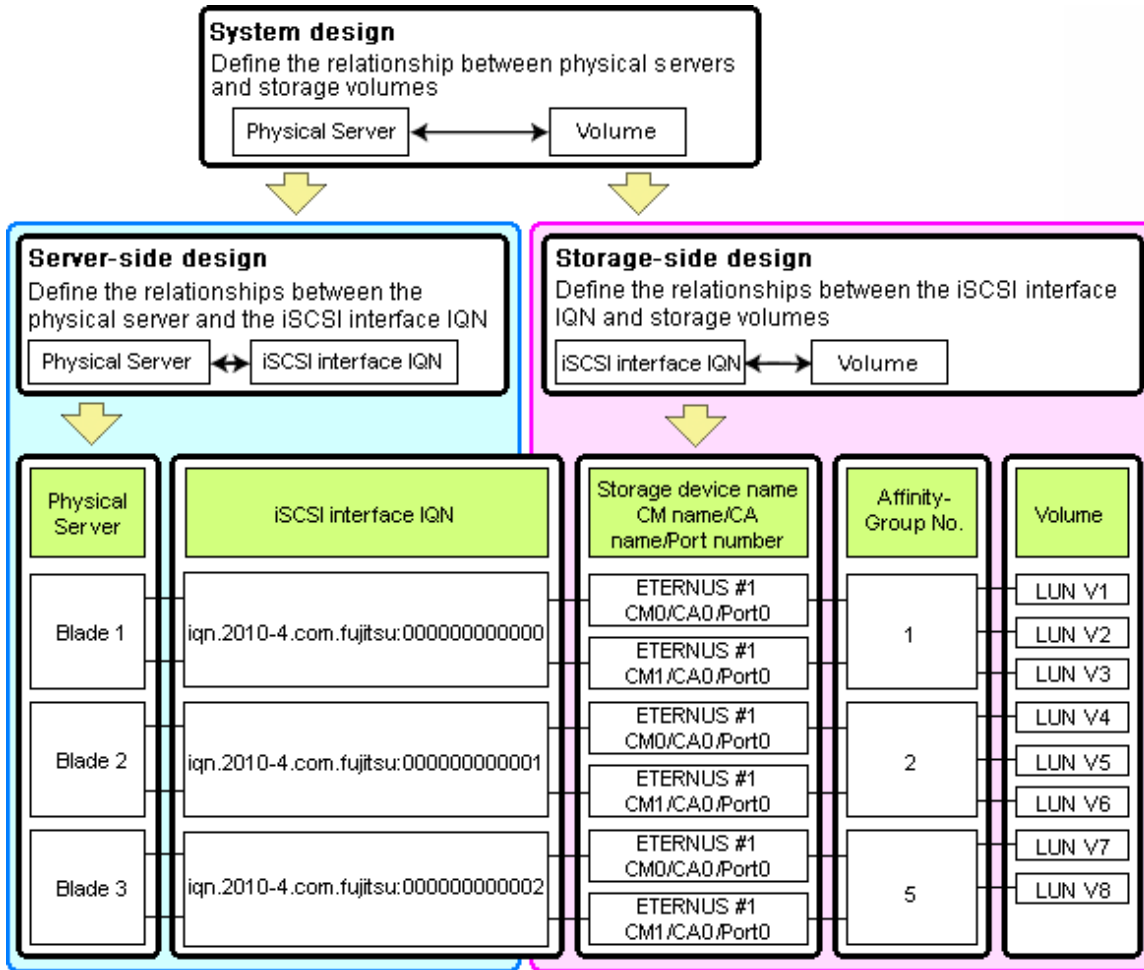
4.3.1.4 iSCSI Interface and Storage Device Settings (iSCSI)

System configuration requires that the relationship between physical servers and the IQN of the iSCSI adapter from the perspective of the server, and the relationship between storage volumes and the IQN of iSCSI from the perspective of storage devices, be defined clearly.

An example where blades connect to storage devices via multiple paths using two iSCSI interface ports is shown below.

Refer to the storage device manual of each storage device for details.

Figure 4.22 IQN System Design



Choosing IQNs

Choose the IQNs to use with the iSCSI.

After IQNs have been chosen, associate them with their corresponding operating systems (applications) and physical servers (on the server side), and with corresponding volume(s) (on the storage side).

IQNs are made up of the following:

- Type identifier "iqn."
- Domain acquisition date
- Domain name
- Character string assigned by domain acquirer

IQNs must be unique.

Create a unique IQN by using the server name, or the MAC address provided by the "I/O virtualization option" that is to be allocated to the network interface of the server, as part of the IQN.

If IQNs overlap, there is a chance that data will be damaged when accessed simultaneously.

An example of using the virtual MAC address allocated by the "I/O virtualization option" is given below.

Example

When the MAC address is 00:00:00:00:00:FF

IQN iqn.2010-04.com.fujitsu:0000000000ff

The IQN chosen here would be used for the system design of the servers and storage.

- Server-side Design

IQNs are used in server-side design by assigning one unique to each server.

- Storage-side Design

One or more volumes are chosen for each server, and the corresponding IQN assigned to each server in the server-side design is configured on the storage-side for those volumes.

4.3.2 Configuring the Storage Environment

This section describes how to configure storage devices for Resource Orchestrator.

The settings differ depending on whether the L-Server is physical or virtual.

When Using Physical L-Servers

- Configure SAN Storage Environments

- Configure HBA address rename or VIOM coordination

Configure the HBA address rename function or VIOM coordination in advance.

- Configure the storage and fibre channel switch, install and set up storage management software

With physical L-Servers, virtual storage resources and disk resources are controlled via storage management software.

When allocating disk resources automatically created from virtual storage to physical L-Servers, create the virtual storage resources such as RAID groups or aggregates in advance.

When allocating disk resources to physical L-Servers, create the disk resources such as LUNs in advance.

- When using ETERNUS storage

Refer to "[D.3.1 When Using ETERNUS Storage](#)".

- When using NetApp FAS storage

Refer to "[D.3.2 When Using NetApp FAS Storage](#)".

- When using EMC CLARiiON storage

Refer to "[D.3.3 When Using EMC CLARiiON Storage](#)".

- When using EMC Symmetrix DMX storage or EMC Symmetrix VMAX storage

Refer to "[D.3.4 When Using EMC Symmetrix DMX Storage or EMC Symmetrix VMAX Storage](#)".

- Configure iSCSI Storage Environments

- Configure the storage and fibre channel switch, install and set up storage management software

When using iSCSI boot on physical L-Servers, create LUNs that can be connected to L-Servers in advance.

- When using ETERNUS storage

Refer to "[D.3.1 When Using ETERNUS Storage](#)".

- When using NetApp FAS storage

Refer to "[D.3.2 When Using NetApp FAS Storage](#)".

When Using Virtual L-Servers

- Configure the storage and fibre channel switch, install and set up VM management software

Virtual L-Servers are controlled via VM management software.

Create the virtual storage resources such as datastores and the disk resources such as raw devices in advance.

- When Using VMware
Refer to "[Storage Preparations](#)" in "[E.2.2 Preparations](#)".
- When Using Hyper-V
Refer to "[Storage Preparations](#)" in "[E.3.2 Preparations](#)".
- When Using RHEL5-Xen
Refer to "[Storage Preparations](#)" in "[E.4.2 Preparations](#)".
- When Using Oracle VM
Refer to "[Storage Preparations](#)" in "[E.5.2 Preparations](#)".
- When Using RHEL-KVM
Refer to "[Storage Preparations](#)" in "[E.6.2 Preparations](#)".

4.4 Deciding and Configuring Server Virtualization Software

This section explains how to decide and configure server virtualization software.

4.4.1 Deciding Server Virtualization Software

This section explains how to decide the settings for server virtualization software.

- Select the server virtualization software to use

Select the server virtualization software.

Resource Orchestrator can perform resource management using the server virtualization software indicated below.

- VMware
- Hyper-V
- RHEL5-Xen
- KVM
- Oracle VM

Settings differ according to the server virtualization software being used.

When using server virtualization software, refer to "[Appendix E Design and Configuration for Creating Virtual L-Servers](#)".



[VMware] [Hyper-V] [RHEL-KVM] [Oracle VM]

When registering managed servers to the manager, the password for the administrative privilege user of the managed server is required. Configure the password for the administrator account of managed server in advance.

Resource Orchestrator Functions Enabled with the Functions of Each Server Virtualization Software

The Resource Orchestrator functions enabled by using the functions of each server virtualization software are indicated below.

Table 4.12 List of Resource Orchestrator Functions Enabled by Using Each Server Virtualization Function

Resource Orchestrator Function	VMware Function	Hyper-V Function	RHEL-Xen Function	RHEL-KVM Function	Oracle VM Function	Reference
L-Server power operations	VM guest power operations					Refer to "11.1 Power Operations" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".
L-Server cloning image	Template		-	-	Template	Refer to the setup section for the server virtualization software to use " Appendix E Design and Configuration for Creating Virtual L-Servers ".
L-Server snapshots	Snapshot	Checkpoints	-	-	-	Refer to "11.6 Snapshots, and Backup and Restoration of L-Servers" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".
VM host maintenance mode	Maintenance mode		-	-	Maintenance mode	VM host maintenance mode
Moving an L-Server between VM hosts (migration)	Migration	Migration using clusters	Migration			Refer to "11.7 Migration of VM Hosts between Servers" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Functions of Each Server Virtualization Software That Must Not Be Directly Used/Operated

The functions of each server virtualization software that must not be directly used/operated are indicated below.

Table 4.13 List of Functions of Each Server Virtualization Software That Must Not Be Directly Used/Operated

Server Virtualization Software	Functions with no Support of Combined Use
VMware vSphere (R) 4 VMware vSphere (R) 4.1 VMware vSphere (R) 5.0	Cisco Nexus 1000V virtual switch
Microsoft(R) System Center Virtual Machine Manager 2008 R2 Microsoft(R) System Center 2012 Virtual Machine Manager	<ul style="list-style-type: none"> - Movement of storage areas - Movement changing the virtual machine storage destination - Saving in the virtual machine library

[Hyper-V]

VMware(R) ESX and Citrix(R) XenServer(TM) can be managed by SCVMM, but only VM hosts for Hyper-V can be managed when using SCVMM in Resource Orchestrator.

4.4.2 Configuring Server Virtualization Software

This section explains how to configure server virtualization software.

The settings indicated below are required when using server virtualization software.

- Install and configure the VM management software
- Install and configure the VM management software.

Required when using VMware, Hyper-V, or Oracle VM.

For details, refer to the manual of server virtualization software.

- Install and configure the VM hosts

Install and configure the VM hosts.

The settings required in advance are indicated below.

[VMware]

- Volumes have been created
- Zoning and host affinity have been set
- VM hosts have been configured to recognize a datastore
- Datastores have been used to specify dynamic allocation

For details, refer to "[E.2.2 Preparations](#)".

[Hyper-V]

The configuration enables use of SAN environments on VM hosts

- Volumes have been created
- Zoning and host affinity have been set
- MSFC has been added to VM hosts
- A SAN volume has been configured as a cluster disk
- A cluster disk has been added as a shared cluster volume

All created L-Servers are located on a cluster as high availability virtual machines.

For details, refer to "[E.3.2 Preparations](#)".

[RHEL5-Xen]

- Volumes (LUNs) to assign to the admin OS have already been created
- Zoning and host affinity have been set
- The LUN has already been set as the shared class of PRIMECLUSTER GDS

For details, refer to "[E.4.2 Preparations](#)".

[Oracle VM]

- Volumes have been created
- Zoning and host affinity have been set
- A storage and a repository have been added as a shared cluster volume
- A server pool has been created
- The VM hosts have been registered in the server pool
- A storage repository has been registered in the server pool
- VM guests can be created in the server pool
- A cloning image exists in the server pool

For details, refer to "[E.5.2 Preparations](#)".

[KVM]

For details, refer to "[E.6.2 Preparations](#)".

4.5 Installing and Configuring Single Sign-On

When installing Resource Orchestrator, a Single Sign-On environment can be configured. This section explains the necessary preparations. When upgrading Resource Orchestrator from earlier versions, configure the Single Sign-On environment, referring to "[4.5.6 Updating from Earlier Versions](#)".

Note

- Resource Orchestrator and ServerView Operations Manager must be installed on the same server.
 - If you cannot log in to the ROR console after installation, the environment setup may have failed.
For details, refer to "[4.5.5 When Reconfiguring Single Sign-On](#)"
 - Do not modify the LDAP port number of OpenDS.
-

4.5.1 Deciding the Directory Service to Use

Decide a directory service to use for performing Single Sign-On.

- OpenDS provided with ServerView Operations Manager
- Individually configured directory services
 - OpenDS
 - Active Directory

Note

The directory server which can be used by Resource Orchestrator is only one that was specified during installation.

4.5.2 Setting up ServerView Operations Manager and Directory Service Environments

Set up ServerView Operations Manager and the Directory Service Environment.

The following settings can be made for coordination of Resource Orchestrator and a directory service.

- [Coordination with the User Registration Directory Service](#)
- [To Use a User already Registered with Active Directory as a Resource Orchestrator User](#)
- [Single Sign-On When Using the ServerView Operations Manager Console](#)
- [When Installing ServerView Operations Manager Again](#)

4.5.2.1 Coordination with the User Registration Directory Service

Whether user operations performed from Resource Orchestrator are reflected on the directory service or not is determined by the settings in the directory service operation definition file (`ldap_attr.rcxprop`).

For details, refer to "6.6.1 Settings for Tenant Management and Account Management" in the "Operation Guide CE". By default, the operation content is reflected on the directory service.

User information of Resource Orchestrator is created in the following location.

- When Using Active Directory
`cn=Users,Base_DN`

- When Using OpenDS

cn=Users,*Base_DN*

When using a user account of the existing directory service as the user of Resource Orchestrator, edit the directory service operation definition file so that the operation content will not be reflected.

Note

If the directory service operation file defines the setting which reflects the operation content, when the user is deleted from Resource Orchestrator, corresponding user account of the directory service is deleted as well. Be careful when using an existing directory service for user management on the other system.

4.5.2.2 To Use a User already Registered with Active Directory as a Resource Orchestrator User

When installing ServerView Operations Manager, specify the following items related to the directory service.

- Select Directory Server

Select "Other directory server".

- Directory Service Settings

- Host

The fully-qualified name of the server on which Active Directory is running.

- Port

The port number used for access to Active Directory. Specify the port number for SSL communication.

- SSL

Select "Yes".

- SVS Base DN

Set the highest level of the Active Directory tree.

Example

DC=fujitsu,DC=com

- User Search Base

The starting point for the user search in Active Directory.

Example

CN=Users,DC=fujitsu,DC=com

- User Search Filter

The filter for user searches.

Specify the sAMAccountName attribute or cn attribute. Specify the same value as the value of the attribute specified for the User Search Filter as the value of the User ID of all the users of Resource Orchestrator.

When using the application process, set the sAMAccountName attributes.

sAMAccountName=%u

- User

Specify a user account with write privileges for Active Directory.

Example


```
CN=Administrator,CN=Users,DC=fujitsu,DC=com
```

- Password / Confirm password

Specify the password of the user who specified it as the "User".

For more details, refer to the following manual.

- "Menu-Driven Installation of the Operations Manager Software" in the "ServerView Suite ServerView Operations Manager Installation Guide"

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

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

When setting up Resource Orchestrator, it is necessary to establish communication beforehand, since communication between the manager and the directory service requires LDAP (Lightweight Directory Access Protocol) of the TCP/IP protocol protected by SSL. Use tools or commands to check communications.

For details, refer to the Microsoft web site below.

How to enable LDAP over SSL with a third-party certification authority

```
URL: http://support.microsoft.com/kb/321051/en/
```

4.5.2.3 Single Sign-On When Using the ServerView Operations Manager Console

In the "Resource" tab of the ROR console, you can open the screen of ServerView Operations Manager using the function to open the server management screen. This section explains how to set up Single Sign-on. You can use it access the server management screen of ServerView Operations Manager without being prompted to log in.

Assign roles to users on ServerView Operations Manager.

Assign roles to users in the following procedure.

When Using OpenDS Provided with ServerView Operations Manager

- **ServerView Operations Manager V5.5 or later**

1. Execute the rcxadm user command and register a user.
2. The user is registered in the directory service
3. Start the "User Management Wizard" of ServerView Operations Manager.
4. The user registered in 2. is displayed in the list. Assign a suitable role to the user.

For details on the "User Management Wizard", refer to the following manual.

- "ServerView user management with OpenDS" in "ServerView Suite User Management in ServerView"

- **Versions Earlier Than ServerView Operations Manager V5.5**

1. Execute the rcxadm user command and register a user.
2. The user is registered in the directory service
3. Create an ldif file.

An example of how to assign the Administrator role to the "rormanager" user account is indicated below.

```
dn: cn=Administrator,OU=AuthorizationRoles,OU=CMS,OU=Departments,OU=SVS,dc=fujitsu,dc=com
changetype: modify
add: member
member: cn=rormanager,ou=users,dc=fujitsu,dc=com

dn:
cn=Administrator,OU=AuthorizationRoles,OU=DEFAULT,OU=Departments,OU=SVS,dc=fujitsu,dc=com
```

```
changetype: modify
add: member
member: cn=rormanager,ou=users,dc=fujitsu,dc=com
```

4. Execute the OpenDS ldapmodify command to register the ldif file created in 3. with the directory service.

Set the Java SE 6 path for the environment variable JAVA_HOME, before executing the ldapmodify command of OpenDS.
Example:

[Windows]

```
>"C:\Program Files\Fujitsu\ServerView Suite\opens\bat\ldapmodify.bat" -p 1473 -f user.ldif -D
"cn=Directory Manager" -w admin -c <RETURN>
```

[Linux]

```
# /opt/fujitsu/ServerViewSuite/opens/bin/ldapmodify -p 1473 -f user.ldif -D "cn=Directory Manager" -w
admin -c <RETURN>
```

The meanings of the options of the ldapmodify command are as follow.

- p: the port number when not using SSL communications in the OpenDS (the default value is 1473).
- f: the ldif file
- D: the OpenDS administrator user DN("cn=Directory Manager")
- w: the password of the OpenDS administrator user DN.

When Using Active Directory

Refer to the following manual.

- "Integrating ServerView user management into Microsoft Active Directory" of the "ServerView Suite User Management in ServerView"

4.5.2.4 When Installing ServerView Operations Manager Again

When using the OpenDS bundled with ServerView Operations Manager, back up the user information before uninstalling ServerView Operations Manager, if it becomes necessary to install ServerView Operations Manager again.

Restore the user information in OpenDS, after installing ServerView Operations Manager again.

For details on the backup and restore of OpenDS, refer to the ServerView Operations Manager manual.

4.5.3 Preparing Certificates

Copy the CA certificates of both ServerView Operations Manager and the directory service to use, and store them in an arbitrary folder. Only store the CA certificates in the destination folder.

Stored CA certificates will be used when installing Resource Orchestrator.

CA Certificates of ServerView Operations Manager

Copy the CA certificate (keystore) of ServerView Operations Manager to an arbitrary folder.

The CA certificate (keystore) of ServerView Operations Manager is stored in the following location:

[Windows]

```
ServerView Suite_installation_folder\jboss\server\serverview\conf\pki\keystore
```

[Linux]

```
/opt/fujitsu/ServerViewSuite/jboss/server/serverview/conf/pki/keystore
```

CA Certificate of Individually Configured OpenDS

Copy the CA certificate (keystore) of OpenDS and store it in an arbitrary folder.
The CA certificate (keystore) of OpenDS is stored in the following location:

[Windows]

OpenDS_installation_folder\config\keystore

[Linux]

OpenDS_installation_folder\config\keystore

CA Certificate of Individually Configured Active Directory

Copy the CA certificate of Active Directory and store it in an arbitrary folder. Change the extension of the copied CA certificate to "cer" or "crt".

For details on how to obtain the CA certificate of Active Directory, refer to the Active Directory manual.

4.5.4 Registering Administrators

Register a privileged user (an administrator) to be specified when installing Resource Orchestrator to the directory service.

Use the following object classes.

Table 4.14 Object Class

Directory Service	Object Class	Attribute used for the Login user ID
OpenDS	inetOrgPerson	uid or cn
Active Directory	user	sAMAccountName or cn (*)

* Note: Specify these either as the User Search Filter in the Directory Service Settings of ServerView Operations Manager. Specify the same value as the value of the attribute specified as the User Search Filter as the value of the User ID of all the users including the privileged user (an administrator) of Resource Orchestrator.

When using OpenDS, the user ID (uid attribute) must be unique in the directory service.

When using the OpenDS provided with ServerView Operations Manager, a predefined user exists when installing ServerView Operations Manager.

For details on predefined user information, refer to the following ServerView Operations Manager manual.

- "ServerView user management with OpenDS" in "ServerView Suite User Management in ServerView"

An example of how to register a privileged user of Resource Orchestrator in OpenDS is indicated below.

1. Create an ldif file.

```
dn: cn=manager,ou=users,dc=fujitsu,dc=com
changetype: add
objectclass: inetOrgPerson
cn: manager
sn: manager
uid: manager
userPassword: mypassword
```

2. Use the OpenDS client function to register the ldif file created in 1. with the directory service.

Set the Java SE 6 path for the environment variable JAVA_HOME, before executing the ldapmodify command of OpenDS.

For details on the command, refer to the OpenDS documentation.

[Windows]

```
>"OpenDS_installation_folder\bat\ldapmodify.bat" -p Port_number -f Idif_file -D OpenDS_administrator_user_DN -w Password <RETURN>
```

[Linux]

```
# "OpenDS_installation_folder/bin/ldapmodify" -p Port_number -f Idif_file -D OpenDS_administrator_user_DN -w Password  
<RETURN>
```

SSL communications are not required when registering a user in OpenDS. The default value of the port number when not using SSL communications is "1473" in the OpenDS provided with ServerView Operations Manager.

For details on how to configure connection settings of the OpenDS provided with ServerView Operations Manager, refer to README and the manuals of "ServerView Suite User Management in ServerView".

Example

```
>"C:\Program Files\Fujitsu\ServerView Suite\opens\bat\ldapmodify.bat" -p 1473 -f manager.ldif -D "cn=Directory  
Manager" -w admin <RETURN>
```

4.5.5 When Reconfiguring Single Sign-On

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

4.5.5.1 Confirming Certificates

Execute the keytool command, and check if the CA certificate has been correctly imported. For the -alias option, specify "svs_cms". When using individually configured OpenDS or ActiveDirectory, specify `ror_ldap_1` for the -alias option.

Example

[Windows]

```
>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -list -alias Another_name -keystore "C:\Fujitsu\ROR\SVROR\Manager  
\runtime\jre6\lib\security\cacerts" <RETURN>  
Enter keystore password: changeit  
svs_cms, 2010/10/05, PrivateKeyEntry,  
Certificate fingerprints (MD5): C9:3C:8B:8B:C6:BA:67:92:89:70:D1:00:55:A3:CD:6  
  
>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -list -alias Another_name -keystore "C:\Fujitsu\ROR\IAPS\JDK5\jre\lib  
\security\cacerts" <RETURN>  
Enter keystore password: changeit  
svs_cms, 2010/10/05, PrivateKeyEntry,  
Certificate fingerprints (MD5): C9:3C:8B:8B:C6:BA:67:92:89:70:D1:00:55:A3:CD:6
```

[Linux]

```
# /opt/FJSVrcvmr/runtime/jre6/bin/keytool -list -alias Another_name -keystore /opt/FJSVrcvmr/runtime/jre6/lib/security/cacerts  
<RETURN>  
Enter keystore password: changeit  
svs_cms, 2010/10/05, PrivateKeyEntry,  
Certificate fingerprints (MD5): C9:3C:8B:8B:C6:BA:67:92:89:70:D1:00:55:A3:CD:6  
  
# /opt/FJSVrcvmr/runtime/jre6/bin/keytool -list -alias Another_name -keystore /opt/FJSVawjbc/jdk5/jre/lib/security/cacerts <RETURN>  
Enter keystore password: changeit  
svs_cms, 2010/10/05, PrivateKeyEntry,  
Certificate fingerprints (MD5): C9:3C:8B:8B:C6:BA:67:92:89:70:D1:00:55:A3:CD:6
```

When the information on the CA certificate is not displayed, that means that registration of the CA certificate has failed. In this case, register the CA certificate referring to "[4.5.5.2 Registering Certificates](#)".

4.5.5.2 Registering Certificates

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

1. Copy the keystore of Resource Orchestrator.

[Windows]

- Files to Copy

Installation_folder\SVROR\Manager\runtime\jre6\lib\security\cacerts

- Copy Destination

Installation_folder\SVROR\Manager\runtime\jre6\lib\security\cacerts.org

- Files to Copy

Installation_folder\IAPS\JDK5\jre\lib\security\cacerts

- Copy Destination

Installation_folder\IAPS\JDK5\jre\lib\security\cacerts.org

[Linux]

- Files to Copy

/opt/FJSVrcvnr/runtime/jre6/lib/security/cacerts

- Copy Destination

/opt/FJSVrcvnr/runtime/jre6/lib/security/cacerts.org

- Files to Copy

/opt/FJSVawjkb/jdk5/jre/lib/security/cacerts

- Copy Destination

/opt/FJSVawjkb/jdk5/jre/lib/security/cacerts.org



Ensure that the keystore of Resource Orchestrator is copied, as it will be necessary when changing the directory service.

2. Import the CA certificate (keystore) of ServerView Operations Manager to the keystore of Resource Orchestrator.

The CA certificate (keystore) of ServerView Operations Manager is stored in the following location:

[Windows]

ServerView Suite_installation_folder\jboss\server\serverview\conf\pki\keystore

[Linux]

/opt/fujitsu/ServerViewSuite/jboss/server/serverview/conf/pki/keystore



[Windows]

```
>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -importkeystore -srckeystore " C:\Program Files\Fujitsu
\ServerView Suite \jboss\server\serverview\conf\pki\keystore" -destkeystore "C:\Fujitsu\ROR\SVROR\Manager\runtime
\jre6\lib\security\cacerts" <RETURN>

>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -importkeystore -srckeystore " C:\Program Files\Fujitsu
\ServerView Suite \jboss\server\serverview\conf\pki\keystore" -destkeystore "C:\Fujitsu\ROR\IAPS\JDK5\jre\lib\security
\cacerts"<RETURN>
```

[Linux]

```
# /opt/FJSVrcvmr/runtime/jre6/bin/keytool -importkeystore -srckeystore /opt/fujitsu/ServerViewSuite/jboss/server/serverview/
conf/pki/keystore -destkeystore /opt/FJSVrcvmr/runtime/jre6/lib/security/cacerts <RETURN>

# /opt/FJSVrcvmr/runtime/jre6/bin/keytool -importkeystore -srckeystore /opt/fujitsu/ServerViewSuite/jboss/server/serverview/
conf/pki/keystore -destkeystore /opt/FJSVawjkb/jdk5/jre/lib/security/cacerts <RETURN>
```

After executing the command, enter the password.

The password for the keystore of Resource Orchestrator is set to "changeit" by default.

3. The following messages will be displayed when import is successfully completed.

Check the "*Another name*" section.

```
Enter destination keystore password: changeit
Enter source keystore password: changeit
Entry for Another name sv_s_cm successfully imported.
Import command completed: 1 entries successfully imported. 0 entries failed or cancelled.
```

4. Execute the keytool command, and check if the CA certificate has been correctly imported.

For the -alias option, specify the "*another name*" checked in 3.



Example

[Windows]

```
>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -list -alias Another_name -keystore " C:
\Fujitsu\ROR\Manager\runtime\jre6\lib\security\cacerts" <RETURN>
Enter keystore password: changeit
sv_s_cm, 2010/10/05, PrivateKeyEntry,
Certificate fingerprints (MD5): C9:3C:8B:8B:C6:BA:67:92:89:70:D1:00:55:A3:CD:6

>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -list -alias Another_name -keystore " C:
\Fujitsu\ROR\IAPS\JDK5\jre\lib\security\cacerts"<RETURN>
Enter keystore password: changeit
sv_s_cm, 2010/10/05, PrivateKeyEntry,
Certificate fingerprints (MD5): C9:3C:8B:8B:C6:BA:67:92:89:70:D1:00:55:A3:CD:6
```

[Linux]

```
# /opt/FJSVrcvmr/runtime/jre6/bin/keytool -list -alias Another_name -keystore /opt/FJSVrcvmr/runtime/jre6/lib/security/
cacerts <RETURN>
Enter keystore password: changeit
sv_s_cm, 2010/10/05, PrivateKeyEntry,
Certificate fingerprints (MD5): C9:3C:8B:8B:C6:BA:67:92:89:70:D1:00:55:A3:CD:6

# /opt/FJSVrcvmr/runtime/jre6/bin/keytool -list -alias Another_name -keystore /opt/FJSVawjkb/jdk5/jre/lib/security/cacerts
<RETURN>
Enter keystore password: changeit
```

```
svs_cms, 2010/10/05, PrivateKeyEntry,  
Certificate fingerprints (MD5): C9:3C:8B:8B:C6:BA:67:92:89:70:D1:00:55:A3:CD:6
```

5. Import the CA certificate of the individually configured directory service to the keystore of Resource Orchestrator.

When using a directory service other than OpenDS that comes with ServerView Operations Manager, import the CA certificate of the directory service to the keystore of Resource Orchestrator.

The CA certificate format is the DER encoded binary X.509 (CER) format.

Example

- When Using Active Directory

```
>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -importcert -alias rcve_ldap -trustcacerts -file c:  
\myserver.serverview.local_svsca.crt -keystore "C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\lib\security\cacerts"  
Enter keystore password: changeit  
Owner: CN=svsca, DC=serverview, DC=local  
Issuer: CN=svsca, DC=serverview, DC=local  
Serial number: 22646549ec7ac1994cc3a2b8eff66e27  
Valid from: Mon Oct 04 11:19:47 JST 2010 until: Sun Oct 04 11:26:54 JST 2015  
Certificate fingerprints:  
MD5: 70:E3:CB:23:6F:D1:17:00:56:CA:E2:0D:30:73:14:A8  
SHA1: 01:3C:06:81:2D:3F:6D:D9:C3:A6:D4:AA:7B:D5:5E:D5:5F:43:90:E5  
Signature algorithm name: SHA1withRSA  
Version: 3  
...  
Trust this certificate? [no]: yes  
  
>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -importcert -alias rcve_ldap -trustcacerts -file c:  
\myserver.serverview.local_svsca.crt -keystore "C:\Fujitsu\ROR\IAPS\JDK5\jre\lib\security\cacerts"  
Enter keystore password: changeit  
Owner: CN=svsca, DC=serverview, DC=local  
Issuer: CN=svsca, DC=serverview, DC=local  
Serial number: 22646549ec7ac1994cc3a2b8eff66e27  
Valid from: Mon Oct 04 11:19:47 JST 2010 until: Sun Oct 04 11:26:54 JST 2015  
Certificate fingerprints:  
MD5: 70:E3:CB:23:6F:D1:17:00:56:CA:E2:0D:30:73:14:A8  
SHA1: 01:3C:06:81:2D:3F:6D:D9:C3:A6:D4:AA:7B:D5:5E:D5:5F:43:90:E5  
Signature algorithm name: SHA1withRSA  
Version: 3  
...  
Trust this certificate? [no]: yes
```

- When Using OpenDS

```
>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -importkeystore -srckeystore "C:\win32app  
\OpenDS-2.2.0\config\keystore" -destkeystore C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\lib\security\cacerts  
Enter destination keystore password: changeit  
Enter source keystore password: changeit  
Entry for Another name server-cert successfully imported.  
Import command completed: 1 entries successfully imported. 0 entries failed or cancelled.  
  
>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -importkeystore -srckeystore "C:\win32app  
\OpenDS-2.2.0\config\keystore" -destkeystore C:\Fujitsu\ROR\IAPS\JDK5\jre\lib\security\cacerts  
Enter destination keystore password: changeit  
Enter source keystore password: changeit  
Entry for Another name server-cert successfully imported.  
Import command completed: 1 entries successfully imported. 0 entries failed or cancelled.
```

6. Import the server certificate to ServerView Operations Manager. For details, refer to "[6.3.5 Importing a Certificate to ServerView SSO Authentication Server](#)".

4.5.5.3 Checking Directory Service Connection Information

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

1. Execute the following command:

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

The connection information registered in Resource Orchestrator is displayed.

2. Check the displayed connection information.

The information is displayed as follows:

```
ip address: 127.0.0.1
port: 1474
base: dc=fujitsu,dc=com
bind: cn=Directory Manager
method: SSL
auth: serverview
```

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

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

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

For details on how to check the connection settings of the OpenDS provided with ServerView Operations Manager, refer to the following manuals.

- "Configuring directory service access" and "ServerView user management with OpenDS" in "ServerView Suite User Management in ServerView"

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

For details on the `rcxadm authctl` command, refer to "1.7.10 `rcxadm authctl`" of the "Reference Guide (Resource Management) CE".

4.5.5.4 Modifying Directory Service Connection Information

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

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

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

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

2. Refer to "[4.5.5.1 Confirming Certificates](#)" and check whether the CA certificate of ServerView Operations Manager has been imported correctly to the Resource Orchestrator keystore .

3. When the certificate has not been imported to the keystore, refer to "[4.5.5.2 Registering Certificates](#)" and register a certificate.
4. Change the directory service connection information.

Execute the rxcadm authctl modify command and change the directory service connection information.



Example

```
>rxcadm authctl modify -bind "cn=Directory Manager" -passwd admin
```

Specify the password for directory server administrator as a passwd option. The OpenDS Directory Manager's predefined password is "admin".

For details on the rxcadm authctl command, refer to "5.4 rxcadm authctl" in the "Reference Guide (Command/XML) CE".

If the password of the user with the directory service administrator rights has been changed, perform the following procedure.

1. Stop the manager.

Refer to "[7.2 Starting and Stopping the Manager](#)" for information on how to stop the manager.

2. Issue the command shown below.

Following the message requesting the user to modify is displayed, specify "3. LDAP administrator DN" and register the password.

[Windows Manager]

```
Installation_folder\SWRBAM\bin\swrba_regist_password
```

[Linux Manager]

```
/opt/FJSVswrbam/bin/swrba_regist_password
```

3. Start the manager.

Refer to "[7.2 Starting and Stopping the Manager](#)" for information on how to start the manager.

4.5.5.5 When Certificates Have Expired

When the CA certificate of ServerView Operations Manager or the directory server has expired, re-register the CA certificates after obtaining new certificates. For details on how to register the CA certificates, refer to "[4.5.5.2 Registering Certificates](#)".

4.5.6 Updating from Earlier Versions

This section explains the procedure to configure Single Sign-On environments, when upgrading from earlier versions to this version.

The procedure for configuration differs according to the authentication method used for the earlier version. Refer to the following list:

Authentication methods for earlier versions

- a. Internal authentication in ServerView Resource Coordinator VE (hereinafter RCVE)
(Authentication is not executed using Single Sign-On)
- b. Authentication using Single Sign-On in RCVE
- c. Internal authentication in ROR
- d. Authentication using directory service in ROR
- e. Authentication using Single Sign-On in ROR
- f. Internal authentication in ROR VE
- g. Authentication using Single Sign-On in ROR VE

Table 4.15 Procedure to Configure Single Sign-On Environments from Earlier Versions

Number	Configuration Procedure	A	B	C	D	E	F	G
1	Installing Resource Orchestrator	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2	Registering CA Certificates of ServerView Operations Manager 1	Yes	-	Yes	Yes (*1)	-	Yes	-
3	Registering CA Certificates of ServerView Operations Manager 2	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4	Registering CA Certificate of Individually Configured OpenDS or Active Directory 1 (*1)	Yes	-	Yes	-	-	Yes	-
5	Registering CA Certificate of Individually Configured OpenDS or Active Directory 2 (*1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6	Registering Administrators (Privileged Users)	Yes	-	Yes	-	-	Yes	-
7	Setup	Yes	Yes	Yes	Yes	Yes	Yes	Yes
8	Login on the ROR Console	Yes	Yes	Yes	Yes	Yes	Yes	Yes
9	License Setup	Yes	Yes	Yes	Yes	Yes	Yes	Yes
10	Moving Information in the Directory Service Used in Earlier Versions	-	Yes	-	Yes	Yes	-	-
11	Registering Users in the Directory Service	Yes	-	Yes	-	-	Yes	-
12	Registering Directory Service Connection Information in Resource Orchestrator	Yes	-	Yes	-	-	Yes	-
13	Changing Already Registered Directory Service Connection Information	-	-	-	Yes	-	-	-
14	Role Allocation to Tenant Administrator	-	-	Yes	Yes	Yes	Yes	-
15	Configuration after Installation	Yes	Yes	Yes	Yes	Yes	Yes	Yes
16	Importing a Certificate to a Browser	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Yes: Required, - : Not Required

*1: This procedure is necessary when using OpenDS or an Active Directory that was configured individually.

1. Installing Resource Orchestrator

Refer to "Chapter 4 Upgrading from Earlier Versions" in the "Installation Guide VE".

2. Registering CA Certificates of ServerView Operations Manager 1

Refer to "[4.5.6.1 Registering CA Certificates of ServerView Operations Manager 1](#)".

3. Registering CA Certificates of ServerView Operations Manager 2

Refer to "[4.5.6.2 Registering CA Certificates of ServerView Operations Manager 2](#)".

4. Registering CA Certificate of Individually Configured OpenDS or Active Directory 1

Refer to "[4.5.6.3 Registering CA Certificate of Individually Configured OpenDS or Active Directory 1](#)".

5. Registering CA Certificate of Individually Configured OpenDS or Active Directory 2

Refer to "[4.5.6.4 Registering CA Certificate of Individually Configured OpenDS or Active Directory 2](#)".

6. Registering Administrators (Privileged Users)

For details, refer to "[4.5.4 Registering Administrators](#)".

7. Setup

Set up the manager. Refer to "2.1.4 Setup" in the "Installation Guide CE".

8. Login on the ROR Console

Refer to "[7.1 Login](#)".

9. License Setup

Refer to "[License Setup](#)" in "[7.1 Login](#)".

10. Moving Information in the Directory Service Used in Earlier Versions

Refer to "[4.5.6.5 Moving Information in the Directory Service Used in Earlier Versions](#)".

11. Registering Users in the Directory Service

Refer to "[4.5.6.6 Registering Users in the Directory Service](#)".

12. Registering Directory Service Connection Information in Resource Orchestrator

Refer to "[4.5.6.7 Registering Directory Service Connection Information in Resource Orchestrator](#)".

13. Changing Already Registered Directory Service Connection Information

Refer to "[4.5.6.8 Changing Already Registered Directory Service Connection Information](#)".

14. Allocating Roles to Tenant Administrator

For details, refer to "[4.5.6.9 Allocating Roles to Tenant Administrator](#)".

15. Configuration after Installation

Refer to "[Chapter 6 Configuration after Installation](#)".

16. Importing a Certificate to a Browser

Refer to "[7.4 Importing a Certificate to a Browser](#)".

4.5.6.1 Registering CA Certificates of ServerView Operations Manager 1

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

1. Copy the keystore of Resource Orchestrator.

[Windows]

- Files to Copy

Installation_folder\SVROR\Manager\runtime\jre6\lib\security\cacerts

- Copy Destination

Installation_folder\SVROR\Manager\runtime\jre6\lib\security\cacerts.org

[Linux]

- Files to Copy

/opt/FJSVrcvmt/runtime/jre6/lib/security/cacerts

- Copy Destination

/opt/FJSVrcvmt/runtime/jre6/lib/security/cacerts.org



Ensure that the keystore of Resource Orchestrator is copied, as it will be necessary when changing the directory service.

2. Import the CA certificate (keystore) of ServerView Operations Manager to the keystore of Resource Orchestrator.

The CA certificate (keystore) of ServerView Operations Manager is stored in the following location:

[Windows]

```
ServerView Suite_installation_folder\jboss\server\serverview\conf\pki\keystore
```

[Linux]

```
/opt/fujitsu/ServerViewSuite/jboss/server/serverview/conf/pki/keystore
```

Example

[Windows]

```
>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -importkeystore -srckeystore " C:
\Program Files\Fujitsu\ServerView Suite \jboss\server\serverview\conf\pki\keystore" -destkeystore "C:
\Fujitsu\ROR\SVROR\Manager\runtime\jre6\lib\security\cacerts" <RETURN>
```

[Linux]

```
# /opt/FJSVrcvmr/runtime/jre6/bin/keytool -importkeystore -srckeystore /opt/fujitsu/ServerViewSuite/
jboss/server/serverview/conf/pki/keystore -destkeystore /opt/FJSVrcvmr/runtime/jre6/lib/security/cacerts
<RETURN>
```

After executing the command, enter the password.

The password for the keystore of Resource Orchestrator is set to "changeit" by default.

3. The following messages will be displayed when import is successfully completed.

Check the "*Another name*" section.

```
Enter destination keystore password: changeit
Enter source keystore password: changeit
Entry for Another name svv_cms successfully imported.
Import command completed: 1 entries successfully imported. 0 entries failed or cancelled.
```

4. Execute the keytool command, and check if the CA certificate has been correctly imported.

For the -alias option, specify the "*another name*" checked in 3.

Example

[Windows]

```
>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -list -alias Another_name -keystore " C:
\Fujitsu\ROR\Manager\runtime\jre6\lib\security\cacerts" <RETURN>
Enter keystore password: changeit
svv_cms, 2010/10/05, PrivateKeyEntry,
Certificate fingerprints (MD5): C9:3C:8B:8B:C6:BA:67:92:89:70:D1:00:55:A3:CD:6
```

[Linux]

```
# /opt/FJSVrcvmr/runtime/jre6/bin/keytool -list -alias Another_name -keystore /opt/FJSVrcvmr/runtime/
jre6/lib/security/cacerts <RETURN>
Enter keystore password: changeit
svv_cms, 2010/10/05, PrivateKeyEntry,
Certificate fingerprints (MD5): C9:3C:8B:8B:C6:BA:67:92:89:70:D1:00:55:A3:CD:6
```

4.5.6.2 Registering CA Certificates of ServerView Operations Manager 2

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

1. Copy the keystore of Resource Orchestrator.

[Windows]

- Files to Copy

Installation_folder\IAPS\JDK5\jre\lib\security\cacerts

- Copy Destination

Installation_folder\IAPS\JDK5\jre\lib\security\cacerts.org

[Linux]

- Files to Copy

/opt/FJSVawjkb/jdk5/jre/lib/security/cacerts

- Copy Destination

/opt/FJSVawjkb/jdk5/jre/lib/security/cacerts.org



Ensure that the keystore of Resource Orchestrator is copied, as it will be necessary when changing the directory service.

2. Import the CA certificate (keystore) of ServerView Operations Manager to the keystore of Resource Orchestrator.

The CA certificate (keystore) of ServerView Operations Manager is stored in the following location:

[Windows]

ServerView Suite_installation_folder\jboss\server\serverview\conf\pki\keystore

[Linux]

/opt/fujitsu/ServerViewSuite/jboss/server/serverview/conf/pki/keystore



[Windows]

```
>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -importkeystore -srckeystore " C:  
\Program Files\Fujitsu\ServerView Suite \jboss\server\serverview\conf\pki\keystore" -destkeystore "C:  
\Fujitsu\ROR\IAPS\JDK5\jre\lib\security\cacerts"<RETURN>
```

[Linux]

```
# /opt/FJSVrcvnr/runtime/jre6/bin/keytool -importkeystore -srckeystore /opt/fujitsu/ServerViewSuite/  
jboss/server/serverview/conf/pki/keystore -destkeystore /opt/FJSVawjkb/jdk5/jre/lib/security/cacerts  
<RETURN>
```

After executing the command, enter the password.

The password for the keystore of Resource Orchestrator is set to "changeit" by default.

3. The following messages will be displayed when import is successfully completed.

Check the "*Another name*" section.

```
Enter destination keystore password: changeit  
Enter source keystore password: changeit
```

```
Entry for Another name sv_scms successfully imported.  
Import command completed: 1 entries successfully imported. 0 entries failed or cancelled.
```

- Execute the keytool command, and check if the CA certificate has been correctly imported.

For the `-alias` option, specify the "*another name*" checked in 3.

Example

[Windows]

```
>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -list -alias Another_name -keystore " C:  
\Fujitsu\ROR\IAPS\JDK5\jre\lib\security\cacerts" <RETURN>  
Enter keystore password: changeit  
svs_cms, 2010/10/05, PrivateKeyEntry,  
Certificate fingerprints (MD5): C9:3C:8B:8B:C6:BA:67:92:89:70:D1:00:55:A3:CD:6
```

[Linux]

```
# /opt/FJSVrcvmr/runtime/jre6/bin/keytool -list -alias Another_name -keystore /opt/FJSVawjkb/  
jdk5/jre/lib/security/cacerts <RETURN>  
Enter keystore password: changeit  
svs_cms, 2010/10/05, PrivateKeyEntry,  
Certificate fingerprints (MD5): C9:3C:8B:8B:C6:BA:67:92:89:70:D1:00:55:A3:CD:6
```

- Import the server certificate to ServerView Operations Manager. For details, refer to "[6.3.5 Importing a Certificate to ServerView SSO Authentication Server](#)".

4.5.6.3 Registering CA Certificate of Individually Configured OpenDS or Active Directory

1

When using a directory service that was individually configured, import the CA certificate of the directory service to the keystore of Resource Orchestrator.

When using a directory service other than OpenDS that comes with ServerView Operations Manager, import the CA certificate of the directory service to the keystore of Resource Orchestrator.

The CA certificate format is the DER encoded binary X.509 (CER) format.

Example

- When Using Active Directory

```
>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -importcert -alias rcve_ldap -  
trustcacerts -file c:\myserver.serverview.local_svsc.crt -keystore "C:\Fujitsu\ROR\SVROR\Manager  
\runtime\jre6\lib\security\cacerts"  
Enter keystore password: changeit  
Owner: CN=svsca, DC=serverview, DC=local  
Issuer: CN=svsca, DC=serverview, DC=local  
Serial number: 22646549ec7ac1994cc3a2b8eff66e27  
Valid from: Mon Oct 04 11:19:47 JST 2010 until: Sun Oct 04 11:26:54 JST 2015  
Certificate fingerprints:  
MD5: 70:E3:CB:23:6F:D1:17:00:56:CA:E2:0D:30:73:14:A8  
SHA1: 01:3C:06:81:2D:3F:6D:D9:C3:A6:D4:AA:7B:D5:5E:D5:5F:43:90:E5  
Signature algorithm name: SHA1withRSA  
Version: 3
```

```
...  
Trust this certificate? [no]: yes
```

- When Using OpenDS

```
>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -importkeystore -srckeystore "C:  
\win32app\OpenDS-2.2.0\config\keystore" -destkeystore C:\Fujitsu\ROR\SVROR\Manager\runtime  
\jre6\lib\security\cacerts  
Enter destination keystore password: changeit  
Enter source keystore password: changeit  
Entry for Another name server-cert successfully imported.  
Import command completed: 1 entries successfully imported. 0 entries failed or cancelled.
```

4.5.6.4 Registering CA Certificate of Individually Configured OpenDS or Active Directory 2

When using a directory service that was individually configured, import the CA certificate of the directory service to the keystore of Resource Orchestrator.

When using a directory service other than OpenDS that comes with ServerView Operations Manager, import the CA certificate of the directory service to the keystore of Resource Orchestrator.

The CA certificate format is the DER encoded binary X.509 (CER) format.



Example

- When Using Active Directory

```
>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -importcert -alias rcve_ldap -  
trustcacerts -file c:\myserver.serverview.local_svsca.crt -keystore "C:\Fujitsu\ROR\IAPS\JDK5\jre\lib  
\security\cacerts"  
Enter keystore password: changeit  
Owner: CN=svsca, DC=serverview, DC=local  
Issuer: CN=svsca, DC=serverview, DC=local  
Serial number: 22646549ec7ac1994cc3a2b8eff66e27  
Valid from: Mon Oct 04 11:19:47 JST 2010 until: Sun Oct 04 11:26:54 JST 2015  
Certificate fingerprints:  
MD5: 70:E3:CB:23:6F:D1:17:00:56:CA:E2:0D:30:73:14:A8  
SHA1: 01:3C:06:81:2D:3F:6D:D9:C3:A6:D4:AA:7B:D5:5E:D5:5F:43:90:E5  
Signature algorithm name: SHA1withRSA  
Version: 3  
...  
Trust this certificate? [no]: yes
```

- When Using OpenDS

```
>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -importkeystore -srckeystore "C:  
\win32app\OpenDS-2.2.0\config\keystore" -destkeystore C:\Fujitsu\ROR\IAPS\JDK5\jre\lib\security  
\cacerts  
Enter destination keystore password: changeit  
Enter source keystore password: changeit  
Entry for Another name server-cert successfully imported.  
Import command completed: 1 entries successfully imported. 0 entries failed or cancelled.
```

4.5.6.5 Moving Information in the Directory Service Used in Earlier Versions

When performing user management using a directory service in ServerView Resource Orchestrator V2.3.0, move the resource information in the directory server to the management information in Resource Orchestrator.

Move the following information:

- User group information and belonging users

For the user information, the same user name must be registered in both the directory server and the management information in Resource Orchestrator. Single Sign-On is used for authentication to log on to Resource Orchestrator. Manage the user passwords using the directory service used for Single Sign-On.

- Role definitions
- Access scope and roles

Execute the `rcxadm authctl export` command to move the information. Move the information as an OS administrator. For details on the `rcxadm authctl export` command, refer to "1.7.10 `rcxadm authctl`" in the "Reference Guide (Resource Management) CE".

4.5.6.6 Registering Users in the Directory Service

Register a user to the directory service.

When Using Active Directory

1. Export the user information which is registered in Resource Orchestrator as files in the LDIF format.

Example

```
>rcxadm user list -format ldif > myusers.ldif <RETURN>
```

2. Modify the user information exported as the ldif file in 1. for the actual environment.
Modify the base names of entries based on the base name of the Active Directory.
3. Execute the `ldifde` command to register the ldif file modified in 2. with Active Directory.

Example

```
>ldifde -i -e -k -t 636 -f myusers.ldif <RETURN>
```

For details on the `ldifde` command, refer to the Active Directory documentation.

Registered user passwords are reset as follows.

```
rcxuser@123
```

4. Change the user passwords registered in 3. to appropriate values. Use the Active Directory functions, and change the password.
5. When performing Single Sign-On operations with ServerView Operations Manager, user definitions are necessary for ServerView Operations Manager. For details on how to add user definitions for ServerView Operations Manager, perform settings for Single Sign-On referring to the following manual:
 - "Integrating ServerView User Management into Microsoft Active Directory" of the "ServerView Suite User Management in ServerView"

When Using OpenDS

1. Export the user and user group information which are registered in Resource Orchestrator as files in the LDIF format.



Example

```
>rcxadm user list -format ldif > myusers.ldif <RETURN>
```

The ldif file for the Active Directory is output.

2. Modify the user information exported as the ldif file in 1. for OpenDS.
 - a. Modify the base names of entries based on the base name of the directory service.
 - b. Delete the following attributes.
 - samAccountName
 - userAccountControl
 - unicodePwd
 - c. Add the following attributes to user entries.
 - sn
 - uid (same value as the cn attribute)
 - userPassword
 - d. Modify the values of the objectclass attribute.
 - Change "user" to "inetOrgPerson".
 - e. Change "cn=Users" in the "cn=*User_name*,cn=Users,dc=fujitsu,dc=com" to "ou=Users".



Example

- Before editing (ldif file for Active Directory)

```
# User
dn: cn=user01,cn=Users,dc=example,dc=local          # Change cn=Users to
ou=Users.
changetype: add
objectclass: user                                # Change to objectclass:
inetOrgPerson.
cn: user01
samAccountName: user01                          # Delete this line.
userAccountControl: 512                          # Delete this line.
unicodePwd:: IgByAGMAeAB1AHMAZQByAEAAMQAYADMAIga= # Delete this line.
                                                    # Add sn,uid, and
userPassword attributes.
```

- After editing (ldif file for OpenDS)

```
# User
dn: cn=user01,ou=Users,dc=fujitsu,dc=com
changetype: add
objectclass: inetOrgPerson
cn: user01
sn: user01
```

```
uid: user01
userPassword: mypassword
```

- Use the directory service client function to register the ldif file modified in 3. with the directory service.

Set the Java SE 6 path for the environment variables JAVA_HOME, before executing the ldapmodify command of OpenDS.

For details on the command, refer to each directory service manual.

[Windows]

```
>"OpenDS_installation_folder\bat\ldapmodify.bat" -p Port_number -f ldif_file -D Administrator_user_DN
-w Password <RETURN>
```

[Linux]

```
# "OpenDS_installation_folder/bin/ldapmodify" -p Port_number -f ldif_file -D Administrator_user_DN -w
Password <RETURN>
```

SSL communications are not required when registering a user in OpenDS. The default value of the port number when not using SSL communications is "1473" in the OpenDS provided with ServerView Operations Manager.

For details on how to configure connection settings of the OpenDS provided with ServerView Operations Manager, refer to README and the manuals of "ServerView Suite User Management in ServerView".



Example

```
>"C:\Program Files\Fujitsu\ServerView Suite\opends\bat\ldapmodify.bat" -p 1473 -f myusers.ldif -D
"cn=Directory Manager" -w admin -c <RETURN>
```

- When performing Single Sign-On operations with ServerView Operations Manager, specify users who are defined in ServerView Operations Manager as the user information of Resource Orchestrator.

For details on how to register the user information, refer to "Appendix C User Management Using Directory Service" of the "Operation Guide CE".

- When users of Resource Orchestrator log in to ServerView Operations Manager, user definitions are necessary for ServerView Operations Manager. For details refer to "4.5.2.3 Single Sign-On When Using the ServerView Operations Manager Console".

4.5.6.7 Registering Directory Service Connection Information in Resource Orchestrator

Register the directory service connection information for performing Single Sign-On in Resource Orchestrator.

Check directory service connection information.

Table 4.16 Directory Service Connection Information

Connection Information	Description
IP address	IP address for the directory server to connect to.
Port number	Port number for SSL communication with the directory server to connect to. When using the OpenDS provided with ServerView Operations Manager, the default value is 1474.
Base name (DN)	Base name (DN) for the directory server to connect to. When using the OpenDS provided with ServerView Operations Manager, the default value is "dc=fujitsu,dc=com".
Directory server administrator name (DN)	Directory server administrator name (DN) for the directory server to connect to.

Connection Information	Description
	When using the OpenDS provided with ServerView Operations Manager, the default value is "cn=Directory Manager".
Directory server administrator password	Password for the directory server to connect to. When using the OpenDS provided with ServerView Operations Manager, refer to the following manual. ServerView Operations Manager manuals "ServerView user management with OpenDS" in "ServerView Suite User Management in ServerView"

Use the following procedure to register the directory service connection information in Resource Orchestrator.

1. Stop the manager.

For information on stopping managers, refer to ["7.2 Starting and Stopping the Manager"](#).

2. Register the directory service connection information for performing Single Sign-On.

Execute the rcxadm authctl command and register the directory service connection information.

For details on the rcxadm authctl command, refer to "1.7.10 rcxadm authctl" of the "Reference Guide (Resource Management) CE".

Example

Example when using Active Directory

```
>rcxadm authctl register -ip 192.168.1.1 -port 636 -base dc=example,dc=local -bind
cn=Administrator,cn=Users,dc=example,dc=local -method SSL -passwd mypasswd <RETURN>
```

Example when using the OpenDS Provided with ServerView Operations Manager

```
>rcxadm authctl register -ip 192.168.1.1 -port 1474 -base dc=fujitsu,dc=com -bind "cn=Directory
Manager" -method SSL -passwd admin <RETURN>
```

3. Start the manager.

For information on starting managers, refer to ["7.2 Starting and Stopping the Manager"](#).

4.5.6.8 Changing Already Registered Directory Service Connection Information

Change the already registered directory service connection information from authentication by the directory service to Single Sign-On operations.

1. Stop the manager.

For information on stopping managers, refer to ["7.2 Starting and Stopping the Manager"](#).

2. Change the directory service connection information to Single Sign-On operations.

Execute the rcxadm authctl command and change the directory service connection information.

For details on the rcxadm authctl command, refer to "1.7.10 rcxadm authctl" of the "Reference Guide (Resource Management) CE".

```
>rcxadm authctl modify -auth serverview
```

3. Start the manager.

For information on starting managers, refer to ["7.2 Starting and Stopping the Manager"](#).

4.5.6.9 Allocating Roles to Tenant Administrator

Allocate appropriate roles to the users operating as tenant administrators, tenant operators, or tenant monitors among users operating on the earlier versions.

Use the following procedure to allocate roles to users.

1. Output the user information in files in the XML format.

```
>rcxadm user list -format xml > myusers.xml
```

For details on the rcxadm user command, refer to "1.6.1 rcxadm user" of the "Reference Guide (Resource Management) CE".

2. Edit the XML files.

Delete the information of other users from the XML file, so that only users operating as tenant administrators, tenant operators, and tenant monitors remain.

Define the tenant administrator roles to allocate to.

Add the following information:

- Mail address
- First name
- Family name

For details on the XML definition of tenant administrators, refer to "2.8.1 Tenant Management Roles and Tenant User Role" in the "Reference Guide (Resource Management) CE".



Example

Example of the XML definition in which the tenant administrator role of "tenantA" is allocated to the user "john"

```
<?xml version="1.0" encoding="utf-8"?>
<Users>
  <User name="john">
    <Roles>
      <Role name="tenant_admin">
        <Scopes>
          <Scope>tenantA</Scope>
        </Scopes>
      </Role>
    </Roles>
    <MailAddress>john@mail.example.com</MailAddress>
    <ActualName>
      <FirstName>john</FirstName>
      <LastName>fujitsu</LastName>
    </ActualName>
  </User>
</Users>
```

3. Allocate the tenant administrator roles to the user by specifying the XML file edited in the rcxadm user command.

```
>rcxadm user modify -file my_tenantadmins.xml
```

Chapter 5 Installation/Uninstallation

Installation of Resource Orchestrator requires the preparations described in "[Chapter 3 Resource Orchestrator Setup Design](#)" to be performed first. For details on how to install Resource Orchestrator, refer to the "Installation Guide CE".

For details on how to uninstall Resource Orchestrator, refer to the "Installation Guide CE".

Chapter 6 Configuration after Installation

This chapter explains configuration after installing Resource Orchestrator.

6.1 Creating Definition Files

This section explains how to use Resource Orchestrator to create the definition files required to manage (monitor and automatically configure, etc.) network devices.

Definition File Required for Creating a Physical L-Server

When creating a physical L-Server, it is necessary to create a definition file combining ports of SAN storage first.

For details, refer to ["6.1.1 Creating Definition Files Combining Ports of SAN Storage"](#).

When not specifying a model name in the L-Server template, it is necessary to create a file that defines the configuration information of the server.

For details, refer to ["Configuration when Creating a Physical L-Server without Specifying a Model Name in the L-Server Template"](#) of ["D.5.1 Definition Files"](#).

Definition File Required for Network Device Management (such as Monitoring and Auto-Configuration)

For details, refer to ["6.1.2 Creating Definition Files for Registering Network Devices"](#) and ["6.1.3 Creating Model Definition Files for Network Devices"](#).

6.1.1 Creating Definition Files Combining Ports of SAN Storage

Create the following definition file in advance, then define the combination of the ports of storage units used when accessing the L-Server disk.

In Resource Orchestrator, LUN masking on the ports of storage units is configured using the definition file combining ports for SAN storage. For ETERNUS storage units, zoning of fibre channel switches is also configured using the port combination definition file of the SAN storage.

When adding a storage unit and then adding it to a resource pool as a storage resource, define the following file:

Storage Location of the Definition File

[Windows]
Installation_folder\Manager\etc\customize_data

[Linux]
/etc/opt/FJSVrcvmr/customize_data

Definition File Name

storage_portset.rcxprop

Definition File Format

Describe the storage information. Each storage information must be described using a single line, and be in the following format starting from the start of the line. Use of line breaks is not allowed.

```
storage_unit_ipaddr,"port X:port Y","port X:port Y",...
```

Definition File Items

- When using ETERNUS storage

storage_unit_ipaddr

Specify IP addresses of operation management LAN ports of ETERNUS storage that are managed by ESC.

When the same IP address is specified in multiple lines, the first defined line is valid.

Portset

A pair of FC-CA ports of ETERNUS storage used when accessing an L-Server disk, represented using the WWPN of the FC-CA ports.

Specify a pair of FC-CA ports using two WWPNs (16 digit hexadecimal numbers) separated with colons (":"). Up to 64 combination can be specified.

If there is trouble with the ETERNUS storage controller, in order to avoid blocking both of the FC-CA ports used for L-Server, do not use combinations of ports on the same controller.

WWPNs of FC-CA ports that are not connected using Fibre Channel cable cannot be specified.

WWPNs that are already defined cannot be specified for different portsets.

LUN masking and zoning are configured by the following pairs of HBA and storage unit port. Check that Fibre Channel cables are connected between the ports of HBAs and storage units.

- HBA Port1 and the first defined storage unit port
- HBA Port2 and the second defined storage unit port

Note

In Resource Orchestrator, access paths are defined in the following order.

- Storage unit port defined in portX and HBA Port1
- Storage unit port defined in portX and HBA Port2

- When using EMC CLARiiON storage

storage_unit_ipaddr

Specify the IP address of SP of EMC CLARiiON storage.

When the same IP address is specified in multiple lines, the first defined line is valid.

Portset

A pair of SP ports of EMC CLARiiON storage used when accessing an L-Server disk, represented using an SP port name.

Specify a pair of SP ports using two SP port names separated with colons (":"). Up to 64 combination can be specified.

If the number of FCs to be used on one L-Server is 1 or 4, use the definition file described in "[Setting the Number of FCs Fitted and their Position for Each Physical Server](#)" in "[D.5.1 Definition Files](#)" rather than the file described here.

The two ports specified here should be selected from the SP ports of different SPs. When using SP ports on the same SP of EMC CLARiiON storage, if there is trouble with the SP, the SP ports used by L-Servers may not be available.

SP ports that are not connected using Fibre Channel cables cannot be specified.

SP ports that are already defined cannot be specified for different portsets.

- When using EMC Symmetrix DMX storage or EMC Symmetrix VMAX storage

storage_unit_ipaddr

Specify the Symmetrix ID of EMC Symmetrix DMX Storage or EMC Symmetrix VMAX Storage.

When the same Symmetrix ID is specified in multiple lines, the first defined line is valid.

Portset

A pair of ports of EMC Symmetrix DMX storage or EMC Symmetrix VMAX storage used when accessing an L-Server disk, represented using director numbers and port numbers.

Specify a pair of ports using two port names separated with colons (":"). Up to 1 combination can be specified.

The two ports specified here should be selected from the ports of different directors. When using ports on the same director of EMC Symmetrix DMX storage or EMC Symmetrix VMAX storage, if there is trouble with the director, the ports used by L-Servers may not be available.

The ports not connected using Fibre Channel cables cannot be specified.

Director numbers and port numbers that are already defined cannot be specified for different portsets.

In the following cases, use the definition file described in "[Setting the Number of FCs Fitted and their Position for Each Physical Server](#)" in "[D.5.1 Definition Files](#)" rather than the file described here.

- When using 2 or more groups of director ports from an L-Server
- If the number of FCs to be used on one L-Server is 1 or 4
- When there is a large number of L-Servers using the storage

Example

An example definition file is indicated below.

- When using ETERNUS storage

```
192.168.1.24,"500000E0D00C7006:500000E0D00C7086","500000E0D00C7086:500000E0D00C7087"
```

- When using EMC CLARiiON storage

```
192.168.1.24,"SPAPort0:SPBPort0"
```

- When using EMC Symmetrix DMX storage or EMC Symmetrix VMAX storage

```
000192601264,"07GPort1:08GPort1"
```

6.1.2 Creating Definition Files for Registering Network Devices

The infrastructure administrator creates XML definition files for registering network devices based on the network device information (admin IP address, account information, connection information) obtained from the network device administrator.

For details, refer to "[4.2.4.8 When Registering Network Devices as Resources](#)".

6.1.3 Creating Model Definition Files for Network Devices

Create an XML definition file to be used for identifying network device models to be configured using the network device automatic configuration function.

For details, refer to "[Creating Model Definitions for Network Devices](#)" of "[4.2.4.9 When Automatically Configuring Network Devices](#)".

6.2 Preparations for the Network Device Automatic Configuration Function

This section explains how to prepare to use the function for automatically configuring network devices.

6.2.1 Creating a Folder for Registering Rulesets

Create folders for registering rulesets (scripts) to be used by the auto-configuration function.

For details, refer to "[Creating a Folder for Registering Rulesets](#)" of "[4.2.4.9 When Automatically Configuring Network Devices](#)".

6.2.2 Registering Sample Scripts

Register the sample script provided by Resource Orchestrator.

For details, refer to "[Sample Scripts](#)" and "[Copy Destination of Sample Script Rulesets](#)" in "[4.2.4.9 When Automatically Configuring Network Devices](#)".

6.3 SSL Communication Environment Settings

SSL communication is used for access to the ROR Console.

This section explains the environment settings required for SSL communication.



- "Certification" explains in this chapter indicates "Server Certification".
- In these procedures, a certification environment is created after installation. If an operation such as restarting the operating system is performed before these procedures are implemented, a message indicating Web server start failure might be output to the operating system log, but you may continue with processing.
- When uninstalling this product in order to use the same certificate environment, and if you do not:
 - SMEE Uninstallation [Linux] (Section 3.1.5.2 (*1))
 - Securecrypto Library RunTime Uninstallation [Linux] (Section 3.1.5.3 (*1))
 - or delete the installation directory

the "SSL Communication Environment Settings" may not need to be defined as they may already exist.

*1: Refer to the *Installation Guide CE*.

6.3.1 Stop Web Server

Stop Web server

Stop Interstage Application Server's Web server.

The shutdown procedure of the Web server is as follows.

1. Start the Interstage Management Console.

The start procedure of the Interstage Management Console is as follows.

[Windows]

From **start** menu, select **All programs >> Interstage >> Application Server >> Interstage Management Console**.

[Linux]

1. Start a Web browser
2. Specify URL of the Interstage Management Console.

URL is as follows.

(If you do not use SSL encrypted communication)

http://[host name]:[port number]/IsAdmin/

(If you use SSL encrypted communication)

https://[host name]:[port number]/IsAdmin/

3. Log in the Interstage Management Console.

2. Stop Web server

Select **Interstage Management Console >> Interstage Application Server >> System >> Service >> Web server >> list**

Stop the following Web servers if they have been started:

- RCXCF-API
- RCXCT-ext
- RCXCT-ext2

6.3.2 Setting the Interstage Certificate Environment Access Permissions [Linux]

Create an owner group that has permissions to access the Interstage certificate environment.

An example of creating the owner group using the command is shown below:

1. Create the Interstage certificate environment owner group.

In the following example, the owner group is created as "iscertg".

```
# groupadd iscertg
```

Note

The owner group that was created at the time of the Interstage certificate environment build must be specified in the -g option of the Certificate Signing Request (CSR) creation command (scsmakeenv). Refer to "[Creating the Interstage Certificate Environment and the Application to Obtain the Certificate that is used for SSL Communication](#)" for information on the CSR creation command.

2. Register the executing user in the "iscertg" group.

In the following example, the executing user is created as "nobody".

```
# usermod -G iscertg nobody
```

Note

The executing user that is registered in the Interstage certificate environment owner group must have been set in the User directive of the Interstage HTTP Server environment configuration file (httpd.conf). The user "nobody" has been set if you installed Interstage Application Server bundled with Systemwalker Service Catalog Manager.

6.3.3 Getting and Registering a Certificate

Execute either one of the following procedures to suit the environment.

- [Getting a Certificate from the Certificate Authority](#)
- [Creating Test Site Certificates](#)

6.3.3.1 Getting a Certificate from the Certificate Authority

The following procedures are required for getting a certificate from the Certificate Authority:

- [Creating the Interstage Certificate Environment and the Application to Obtain the Certificate that is used for SSL Communication](#)
- [Registering Certificates used in SSL Communication](#)

This section explains how to get a certificate from the Certificate Authority.

Creating the Interstage Certificate Environment and the Application to Obtain the Certificate that is used for SSL Communication

The CSR creation command (from now on, this is referred to as the "scsmakeenv command") is used to create the CSR that will create the Interstage certificate environment and apply for the certificate that is used for SSL communication.

The creation procedure and execution example are shown below:

Creation procedure

1. Set the JDK or JRE installation path in the JAVA_HOME environment variable. This procedure is only required for Linux. Setting of the environment variable JAVA_HOME is unnecessary for Windows.

2. Execute the scsmakeenv command.

[Windows]

```
scsmakeenv -n <private key nickname> -f <output destination file name for the CSR>
```

[Linux]

```
scsmakeenv -n <private key nickname> -f <output destination file name for the CSR> -g <Group that has permissions to access the Interstage certificate environment>
```

Change the CSR output destination file name if necessary.

Note

The private key nickname specified in the scsmakeenv command will be required when the site certificate obtained from the CA is registered.

Information

Refer to "Chapter 16 SSL Environment Setting Commands" in the *Interstage Application Server Reference Manual (Command Edition)* for information on the scsmakeenv command.

3. Enter a password to access the Interstage certificate environment.

The password will be required to access the Interstage certificate environment.

4. Enter an identifier.

When the "What is your first and last name?" enquiry is made, specify the FQDN of the server used to apply for the certificate as the Web server host name.

5. As with step 4, enter the following items:

- Name of organizational unit
- Name of organization
- Name of City or Locality
- Name of State or Province
- Two-letter country code

6. Check the values that were entered.

To create the CSR using the values that were entered, enter **yes**. To change the values that were entered, enter **no**.

7. Send the CSR to the CA to request that a certificate be issued.

If the scsmakeenv command has terminated normally, the CSR will be output to the certificate output destination file name that was specified in the -f option of the scsmakeenv command. Send that file to the CA and request that a certificate be issued. Follow the request method used by the CA.

Execution example [Windows]

The command execution examples shown below use the following values:

```
- Site certificate nickname: SERVERCERT  
- Applicant output destination file name: C:\temp\ssocert.txt  
- First and last name: rormanager.example.com  
- Name of organizational unit: FUJITSU TOKYO  
- Name of organization: FUJITSU  
- Name of City or Locality: Shinjuku
```

```
- Name of State or Province: Tokyo
- Two-letter country code for this unit:jp
```

```
C:\>scsmakeenv -n SERVERCERT -f C:\temp\ssocert.txt
New Password:
Retype:

Input X.500 distinguished names.
What is your first and last name?
  [Unknown]: rormanager.example.com
What is the name of your organizational unit?
  [Unknown]: FUJITSU TOKYO
What is the name of your organization?
  [Unknown]: FUJITSU
What is the name of your City or Locality?
  [Unknown]: Shinjuku
What is the name of your State or Province?
  [Unknown]: Tokyo
What is the two-letter country code for this unit?
  [Un]: jp

Is <CN=rormanager.example.com, OU=FUJITSU TOKYO, O=FUJITSU, L=Shinjuku, ST=Tokyo,C=jp> correct?
  [no]: yes
C:\>
```

Execution example [Linux]

The command execution examples shown below use the following values:

```
- Site certificate nickname: SERVERCERT
- Applicant output destination file name: /tmp/ssocert.txt
- Group that has permissions to access the Interstage certificate environment:iscertg
- First and last name: rormanager.example.com
- Name of organizational unit: FUJITSU TOKYO
- Name of organization: FUJITSU
- Name of City or Locality: Shinjuku
- Name of State or Province: Tokyo
- Two-letter country code for this unit:jp
```

In the execution example, a new Interstage certificate environment is created for which "iscertg" access permissions are set, and the CSR is also created. If an Interstage certificate environment has already been created, then set access permissions to it if necessary.

The Bourne shell has been used in the execution example.

```
# JAVA_HOME=/opt/FJJSVawjbbk/jdk5;export JAVA_HOME
# scsmakeenv -n SERVERCERT -f /tmp/ssocert.txt -g iscertg
New Password:
Retype:

Input X.500 distinguished names.
What is your first and last name?
  [Unknown]: rormanager.example.com
What is the name of your organizational unit?
  [Unknown]: FUJITSU TOKYO
What is the name of your organization?
  [Unknown]: FUJITSU
What is the name of your City or Locality?
  [Unknown]: Shinjuku
What is the name of your State or Province?
  [Unknown]: Tokyo
What is the two-letter country code for this unit?
  [Un]: jp
```

```
Is <CN=rormanager.example.com, OU=FUJITSU TOKYO, O=FUJITSU, L=Shinjuku, ST=Tokyo,C=jp> correct?
[no]: yes
UX:SCS: INFO: scs0180: The owners group of Interstage certificate environment was set.
#
```

Note

You will be prompted to input password for Interstage certificate environment if Interstage certificate environment is already configured. In this case, input the password that was set when you configured Interstage certificate environment.

Registering Certificates used in SSL Communication

Obtain the site certificate that was issued by the CA, and the CA certificate of the issuer of that certificate, and register them using the certificate/CRL registration command (from now on, this is referred to as the "scscenter command").

Information

Depending on the CA, it might be necessary to register an intermediate CA certificate. Refer to "Registering Certificates and CRL" in "Chapter 9 Setting and Use of the Interstage Certificate Environment" in the *Interstage Application Server Security System Guide* for details.

This work is unnecessary if you created a test site certificate.

Creation procedure

1. Set the JDK or JRE installation path in the JAVA_HOME environment variable.
2. Register the CA certificate using the scscenter command.

```
scscenter -n <CA certificate nickname> -f <CA certificate>
```

Information

Refer to "SSL Environment Setting Commands" in the *Interstage Application Server Reference Manual (Command Edition)* for information on the scscenter command.

3. Enter a password to access the Interstage certificate environment.

Enter the password that was specified in the scsmakeenv command to access the Interstage certificate environment.

4. Register the site certificate using the scscenter command.

```
scscenter -n <Site certificate nickname> -f <Site certificate> -o
```

To register the site certificate that was obtained from the CA, specify the nickname that was specified in the private key in the scsmakeenv command. Note that the -o option must be specified to register the site certificate.

5. Enter a password to access the Interstage certificate environment.

Enter the password that was specified in the scsmakeenv command to access the Interstage certificate environment.

Execution example [Windows]

The command execution examples shown below use the following values:

```
- CA certificate: C:\temp\ca-cert.cer
- CA certificate nickname: CACERT
- Site certificate: C:\temp\server-cert.cer
- Site certificate nickname: SERVERCERT
```

Change the file names of the CA and site certificates that were obtained if necessary.

```
C:\>scsenter -n CACERT -f C:\temp\ca-cert.cer
Password:
SCS: INFO: scs0104: Certificate was imported.
C:\>scsenter -n SERVERCERT -f C:\temp\server-cert.cer -o
Password:
SCS: INFO: scs0104: Certificate was imported.
C:\>
```

Execution example [Linux]

The command execution examples shown below use the following values:

```
- CA certificate: /tmp/ca-cert.cer
- CA certificate nickname: CACERT
- Site certificate: /tmp/server-cert.cer
- Site certificate nickname: SERVERCERT
```

Change the file names of the CA and site certificates that were obtained if necessary.
The Bourne shell has been used in the execution example.

```
# JAVA_HOME=/opt/FJJSvawjbc/jdk5;export JAVA_HOME
# scsenter -n CACERT -f /tmp/ca-cert.cer
Password:
UX:SCS: INFO: scs0104: Certificate was imported.
# scsenter -n SERVERCERT -f /tmp/server-cert.cer -o
Password:
UX:SCS: INFO: scs0104: Certificate was imported.
#
```

6.3.3.2 Creating Test Site Certificates

The test site certificate can only be used for testing before the site certificate issued by the CA is used. Examples of how to create the test site certificate are shown below:

An example of creating a test site certificate when the server FQDN is "rormanager.example.com" is shown below.

Note

The test site certificate can only be used in a test environment.
Do not use the test site certificate in actual operations.

The command execution examples shown below use the following values:

```
- Test site certificate nickname: testCert
- First and last name:rormanager.example.com
- Name of organizational unit: FUJITSU TOKYO
- Name of organization: FUJITSU
- Name of City or Locality: Shinjuku
- Name of State or Province: Tokyo
- Two-letter country code for this unit:jp
```

The password that was entered will not be displayed. The password will be registered the first time it is entered. To create the certificate using the information displayed for the confirmation of the password that was entered, enter "yes". To enter a different password, enter "no".

[Windows]

```
scsmakeenv -n testCert
New Password:
Retype:

Input X.500 distinguished names.
What is your first and last name?
[Unknown]: rormanager.example.com
```

```

What is the name of your organizational unit?
  [Unknown]: FUJITSU TOKYO
What is the name of your organization?
  [Unknown]: FUJITSU
What is the name of your City or Locality?
  [Unknown]: Shinjuku
What is the name of your State or Province?
  [Unknown]: Tokyo
What is the two-letter country code for this unit?
  [Un]: jp

Is <CN=ssoserver.fujitsu.com, OU=FUJITSU TOKYO, O=FUJITSU, L=Shinjuku, ST=Tokyo,C=jp> correct?
  [no]: yes
SCS: INFO: scs0102: Self-sign certificate was issued

```

[Linux]

The Bourne shell has been used in the execution example.

```

# JAVA_HOME=/opt/FJSVawjkb/jdk5;export JAVA_HOME
# scsmakeenv -n testCert
New Password:
Retype:

Input X.500 distinguished names.
What is your first and last name?
  [Unknown]: rormanager.example.com
What is the name of your organizational unit?
  [Unknown]: FUJITSU TOKYO
What is the name of your organization?
  [Unknown]: FUJITSU
What is the name of your City or Locality?
  [Unknown]: Shinjuku
What is the name of your State or Province?
  [Unknown]: Tokyo
What is the two-letter country code for this unit?
  [Un]: jp

Is <CN=rormanager.example.com, OU=FUJITSU TOKYO, O=FUJITSU, L=Shinjuku, ST=Tokyo,C=jp> correct?
  [no]: yes
UX:SCS: INFO: scs0102: Self-sign certificate was issued
#

```



Note

You will be prompted to input password for Interstage certificate environment if Interstage certificate environment is already configured. In this case, input the password that was set when you configured Interstage certificate environment.

6.3.4 Creating SSL Definitions

Create SSL definitions based on the registered certificate.

1. Start the Interstage Management Console.
 1. Start the Web browser.
 2. Specify the URL of the Interstage Management Console.

The URL format is as follows:
(If SSL encrypted communication is not used)

http://[<host name>]:[<port number>]/lsAdmin/

(If SSL encrypted communication is used)

https://[<host name>]:[<port number>]/IsAdmin/

3. Log in to the Interstage Management Console.

2. Create the SSL definitions.

Select **System >> Security >> SSL >> Create a new SSL Configuration** tabs to show General Settings. Select the nickname of the registered site certificate and create the SSL definitions.

Set the following items, and then click the **Create** button:

Setting item	Setting value
Configuration name	Set a name that identifies the SSL definitions. Set "RCX-SSL" (fixed).
Site Certificate Nickname	Select the nickname that was specified when the site certificate was registered in the Interstage certificate environment as described in "6.3.3 Getting and Registering a Certificate". Registered site certificates can be viewed at the Interstage Management Console at System >> Security >> Certificates >> Site Certificates window.
Protocol Version	Select "SSL 3.0" and "TLS 1.0".
Verify Client Certificate?	Select "No".
Encryption Method	Refer to the Interstage Management Console Help, and change if required.
CA Certificate Nickname	Refer to the Interstage Management Console Help, and change if required.

6.3.5 Importing a Certificate to ServerView SSO Authentication Server

This section explains how to import a certificate to the ServerView SSO authentication server.

1. Export the registered certificate information.

Use the following command to export the registered certificate information:

```
scsexppfx -n <certificate nickname> -f <export file name>
```

The parameters to specify in the command are shown below.

Setting item	Setting value
Certificate nickname	Select the nickname that was specified when the site certificate was registered in the Interstage certificate environment as described in "6.3.3 Getting and Registering a Certificate". Registered site certificates can be viewed at the Interstage Management Console at System >> Security >> Certificates >> Site Certificates window.
Export file name	Specify the temporary file name used for import in Step 2.

2. Import the certificate information to the authentication server.

Use the commands shown below to import the certificate information to the authentication server.

[Windows]

```
<JDK6 installation directory>\bin\keytool.exe -importkeystore -srckeystore <export file name> -  
destkeystore "<ServerView Suite installation folder>\jboss\server\serverview\conf\pki\cacerts" -  
srcstoretype PKCS12
```

[Linux]


```
<JDK6 installation directory>/bin/keytool -importkeystore -srckeystore <export file name> -
destkeystore /opt/fujitsu/ServerViewSuite/jboss/server/serverview/conf/pki/cacerts -
srcstoretype PKCS12
```

3. Delete the export file.

Delete the export file specified in Step 2.

Example

[Windows]

Use screen input for the following commands:

```
- Certificate nickname: testCert
- Export file name: c:\work\isas.p12
```

```
C:\>scsexppfx -n testCert -f c:\work\isas.p12
Password:<Interstage certificate environment password>
PKCS#12 Password:<Password of the certificate being exported> <- Used by the command parameters shown
below.
Retype:<Password of the certificate being exported>

C:\>cd C:\Program Files (x86)\Java\jre6\bin
C:\Program Files (x86)\Java\jre6\bin>keytool.exe -importkeystore -srckeystore c:\work\isas.p12 -
destkeystore "C:\Program Files (x86)\Fujitsu\ServerView Suite\jboss\server\serverview\conf\pki
\cacerts" -srcstoretype PKCS12

Enter destination keystore password:<jboss certificate creation environment password: The default is
changeit.>
Enter source keystore password:<Password at time of export> <- Specify the password that was specified
for the above command.

del c:\work\isas.p12
```

[Linux]

Use screen input for the following commands:

```
- Certificate nickname:testCert
- Export file name: /tmp/isas.p12
```

```
# scsexppfx -n testCert -f /tmp/isas.p12
Password:<Interstage certificate environment password>
PKCS#12 Password:<Password of the certificate being exported><- Used by the command parameters shown
below.
Retype:<Password of the certificate being exported>
# cd /usr/java/jre1.6.0_02/bin
# ./keytool -importkeystore -srckeystore /tmp/isas.p12 -destkeystore /opt/fujitsu/ServerViewSuite/
jboss/server/serverview/conf/pki/cacerts -srcstoretype PKCS12

Enter destination keystore password:<jboss certificate creation environment password: The default is
changeit.>
Enter source keystore password:<Password at time of export> <- Specify the password that was specified
for the above command.

# rm /tmp/isas.p12
#
```

6.3.6 Start the Web server

Start the FJapache Web server for Interstage Application Server if it is stopped.
The procedure for starting the Web server is as follows:

1. Start the Interstage Management Console.

Use the following procedure to start the Interstage Management Console:

[Windows]

From the **Start** menu, select **All Programs >> Interstage, Application Server >> Interstage Management Console**.

[Linux]

1. Start a Web browser.
2. Specify the URL of the Interstage Management Console.

The format of the URL is shown below:

(For communications without SSL encryption)

http://[<host name>]:[<port number>]/IsAdmin/

(For communications with SSL encryption)

https://[<host name>]:[<port number>]/IsAdmin/

3. Log in to the Interstage Management Console.

2. Start a Web browser

Select **Interstage Management Console >> Interstage Application Server >> System >> Services >> Web Server >> List**.

Start the following Web servers if they have been stopped:

- RCXCF-API
- RCXCT-ext
- RCXCT-ext2

6.4 Settings for Sending E-mail

This section explains how to change settings for sending e-mail.

This product sends the following three types of email:

- Email sent from the tenant management

Email sent from the tenant management will be enabled only if the tenant has set the performing tenant management setting.

When an operation such as registering a tenant or adding or changing a user has been performed, notification to that effect is sent to the tenant administrators, tenant users, and tenant email addresses within that same tenant.

- Email sent from the L-Platform Management window

Email sent from the L-Platform management window notifies the end or failure of processing to the tenant administrators and the tenant users when the tenant users have used the ROR Console to perform an application to use L-Platform, an L-Platform modification, or an application to cancel L-Platform.

- Email sent via the application process

An email will be sent via the application process when changes or requests have been made.

The following notification will be sent for an application to use L-Platform, an L-Platform modification, or an application to cancel L-Platform from the L-Platform management window:

- Notification of acceptance of application, rejection of application, and dismissal of application to the tenant users
- Notification of request for approval and dismissal of application to the tenant administrators
- Notification of request for assessment to the infrastructure administrators

- Email sent from the dashboard

Email can be sent from the dashboard if the dashboard alert function is being used.

A notification is sent to the email address specified in the dashboard email send settings when the resource pool use rate threshold value is exceeded.

6.4.1 Stopping the Manager

Stop the manager before settings for sending e-mail.

Refer to "[7.2 Starting and Stopping the Manager](#)" for information on how to stop the manager.

6.4.2 Settings for Email Sent from Tenant Management

Modify the operating environment file so that the tenant administrator (within the same tenant), the tenant users, and the tenant email addresses are notified when operations such as adding or modifying users are performed.

portal.properties settings

Follow the steps below to modify the email settings:

1. Open the following file.

[Windows]

```
<Installation directory for this product >\RCXCTMG\SecurityManagement\conf\portal.properties
```

[Linux]

```
/etc/opt/FJSVctsec/conf/portal.properties
```

2. The following information must be modified:

Setting item	Description
sendmail.smtp	Host name or IP address of the SMTP server
sendmail.smtp.port	Port number of the SMTP server "25" is set during installation.
sendmail.fromAddress	Sender's email address

An example is shown below.

```
...
# sendmail
sendmail.smtp = smtp.example.com
sendmail.smtp.port = 25
sendmail.fromAddress = cloud-master@example.com
...
```



Note

- When editing the portal.properties file, do not change any settings items other than sendmail.smtp, sendmail.smtp.port, and sendmail.fromAddress.
- Save the portal.properties file before editing it. If any settings items other than sendmail.smtp, sendmail.smtp.port, and sendmail.fromAddress have been changed, restore the saved file.

6.4.3 Settings for Email Sent from the L-Platform Management Window

Modify the operating environment file so that users are notified of processes completion or failure by email when tenant administrators and tenant users have used the L-Platform Management window for L-Platform subscription, L-Platform modification, or L-Platform cancellation operations.

mail_config.xml settings

Follow the steps below to modify the email settings:

1. Open the following file.

[Windows]

```
<Installation directory for this product >\RCXCFMG\config\mail_config.xml
```

[Linux]

```
/etc/opt/FJSVcfmg/config/mail_config.xml
```

2. The following information must be modified:

Setting item	Description
enable-email	Set true. Set true in order to enable the email sending function.
smtp-host	Host name or IP address of the SMTP server
smtp-port	Port number of the SMTP server "25" is set during installation.
from-email	Sender's email address
from-name	Set the sending source name. Set "System Administrator" to match the name of email sent from the tenant administrator.
show-password	Configure the settings according to whether the default password for the deployed server will be displayed in the email. Set to "true" if the password will be displayed, or "false" if not. At the time of installation, this is set to "true". Add the item if it has not been.

An example is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
  <entry key="enable-email">true</entry>
  ...
  <entry key="smtp-host">smtp.example.com</entry>
  <entry key="smtp-port">25</entry>
  ...
  <entry key="from-email">cloud-master@example.com</entry>
  <entry key="from-name">system administrator</entry>
  ...
  <entry key="show-password">true</entry>
</properties>
```



Note

- When editing the mail_config.xml file, do not change any settings items other than enable-email, smtp-host, smtp-port, from-email, from-name, and show-password.

- Save the mail_config.xml file before editing it. If any settings items other than enable-email, smtp-host, smtp-port, from-email, from-name, and show-password have been changed, restore the saved file.

6.4.4 Starting the Manager

Start the manager in order to enable the email settings set in "6.4.2 Settings for Email Sent from Tenant Management" and "6.4.3 Settings for Email Sent from the L-Platform Management Window".

Refer to "7.2 Starting and Stopping the Manager" for information on how to stop the manager.

6.4.5 Settings for Email Sent via the Application Process

In order to send email via the application process, the information about the mail server and the mail sender information must be registered in admin Server.

Registering the mail server and sender

Login as the system administrator, and register the mail server and the mail sender information to admin server using the procedure shown below.

1. Check whether admin server has started by using the swrba_status command. If it has not, then start it by using the swrba_start command. Refer to the procedure 6 on the command.

[Windows]

```
<Installation directory for this product>\SWRBAM\bin\swrba_status
```

[Linux]

```
/opt/FJSVswrbam/bin/swrba_status
```

2. If SMTP server authentication will be used when the mail is sent, then encrypt the password. This procedure is not necessary if SMTP server authentication will not be used when the mail is sent.

[Windows]

```
> <Installation directory for this product>\IBPM\server\deployment\bin\EncryptPassword.bat -e
"password"
-----ENCRYPTED PASSWORD-----
encrypted password
```

[Linux]

```
# /opt/FJSVibpm/client/samples/configuration/EncryptPassword.sh -e "password"
-----ENCRYPTED PASSWORD-----
encrypted password
```

3. Prepare the mail server and mail sender definition files (they can be created in any location).

1. SMTP server settings file (smtpserver.conf)

Set the following items:

Setting item	Description	Default value
SMTPServerHost	Host name or IP address of the SMTP server that will be used to send mail.	localhost
SMTPServerPort	Port number of the SMTP server that will be used to send mail.	25
SMTPUserName	User name that will be used in SMTP server authentication when the mail is sent. Specify a backslash followed by a space (" ") if SMTP server authentication will not be used when the mail is sent.	None

Setting item	Description	Default value
SMTPPassword	Password that will be used in SMTP server authentication when the mail is sent. Specify a backslash followed by a space (" ") if SMTP server authentication will not be used when the mail is sent.	None

Example: showing how to define the settings file so that SMTP server authentication is used when the mail is sent.

```
SMTPServerHost=swrba.mail.server
SMTPServerPort=25
SMTPUserName=swrbamailuser
SMTPPassword=encrypted password
```

Example: SMTP server authentication will not be used when the mail is sent.

```
SMTPServerHost=swrba.mail.server
SMTPServerPort=25
SMTPUserName=\ (*)
SMTPPassword=\ (*)
```

*: A space must be specified after the backslash.

2. Mail sender settings file (emailaddress.conf)

Set the following items:

Setting item	Description	Default value
ServerEmailAddress	Mail sender ('from' address) that will be assigned to the mail in mail address format.	postmaster@example.com

An example is shown below.

```
ServerEmailAddress=swrbamailuser@swrba.mail.server
```

4. Register the mail server information.

[Windows]

```
<Installation directory for this product >\IBPM\server\deployment\bin\importProperties.bat
smtpserver.conf [Process Management Database user] [Process Management Database password]
```

*: "swrbadb" as Process Management Database user and Process Management Database password is set during installation.

[Linux]

```
/opt/FJSVibpm/server/deployment/bin/importProperties.sh mtpserver.conf [Process Management
Database user] [Process Management Database password]
```

*: "swrbadb" as Process Management Database user and Process Management Database password is set during installation.

5. Register the mail sender information.

[Windows]

```
<Installation directory for this product >\IBPM\server\deployment\bin\importProperties.bat
emailaddress.conf [Process Management Database user] [Process Management Database password]
Default
```

*: "swrbadb" as Process Management Database user and Process Management Database password is set during installation.

[Linux]

```
/opt/FJSVibpm/server/deployment/bin/importProperties.sh emailaddress.conf [Process Management
Database user] [Process Management Database password] Default
```

*: "swrbadb" as Process Management Database user and Process Management Database password is set during installation.

The "Default" option must be specified at the end.

6. Restart admin server

To reflect the information that was set, stop Systemwalker Runbook Automation by issuing the swrba_stop command, then restart it by issuing the swrba_start command.

1. Stop admin server

[Windows]

```
<Installation directory for this product >\SWRBAM\bin\swrba_stop
```

[Linux]

```
/opt/FJSVswrbam/bin/swrba_stop
```

2. Start admin server

[Windows]

```
<Installation directory for this product >\SWRBAM\bin\swrba_start
```

[Linux]

```
/opt/FJSVswrbam/bin/swrba_start
```

6.4.6 Settings for Email Sent from the Dashboard

If the dashboard alert function is to be used, use the operation management console of Interstage Business Process Manager Analytics to set the mail settings to be used by the dashboard alert function.

Note that the dashboard email send settings must be set if the dashboard alert function is used. Refer to "[Appendix K To Customize Dashboard](#)" for information on setting dashboard email send settings.

SMTP server information settings

Follow the steps below to modify the email settings:

1. Connect to the operation management console and log in. (The initial password is bpm).

From a Web browser at the dashboard development environment, access the following URL and start the operation management console of Interstage Business Process Manager Analytics:

```
http://<admin Server FQDN>/ibpmm/BPMAdminTool.do
```

2. In the left pane, click **IBPM Analytics >> System >> Mail**.
3. Change the displayed SMTP Server settings to suit the environment. After setting the following items click **Modify**:

Setting item	Description
SMTP Server Address	Host name or IP address of the SMTP server
SMTP Port Number	Port number of the SMTP server "25" is set during installation.
Sender Address	Sender's email address

4. Select **BPM Analytics >> Server Management** and then **BPM Analytics Server** on the left hand side pane. Click **Stop** on the right hand side pane. After confirming **Status** has changed to **Stopped**, click **Start**.
5. Confirm **Status** has changed to **Running**.



Note

The initial password must be changed. Use the operation management console of Interstage Business Process Manager Analytics to change the password. Refer to "Change Administrator Password" under section "1.1.1 After the first installation" in Chapter 1, "Interstage BPM Analytics Management Console" in the Interstage Business Process Manager Analytics V11.1 Management Console Guide for details.

Do not perform any operations from the operation management console other than changing password settings, changing SMTP server information, and restarting the Interstage Business Process Manager Analytics server.

6.5 Application Process Settings

This section explains how to set application process setting.

To use application process, perform the following procedure.

- [Registering an Application Process Assessor](#)
- [Setting Application process settings](#)
- [Setting Application process to be used](#)

6.5.1 Registering an Application Process Assessor

This section explains how to register an infrastructure administrator or dual-role administrator as an application process assessor.

Add all infrastructure administrators and dual-role administrators to the directory service IflowUsers group in order to use application processes. Use the LDIF file to register an application process assessor at the directory server. Follow the procedure below to register as application process assessor.

1. Create an infrastructure administrator or dual-role administrator.
2. Add the infrastructure administrator or dual-role administrator as a member of the IflowUsers group.



Note

- Infrastructure administrators and dual-role administrators who have not been registered in the "IflowUsers" group cannot conduct assessment in application processes. Also, if infrastructure administrators and dual-role administrators not registered in the "IflowUsers" group select the **Request** tab in the ROR Console, the following error message appears:

```
Error message : Failed to authenticate the user.
```

- Administrators (dual-role administrators) created during installation are not registered in the "IflowUsers" group. Add them to the "IflowUsers" group.
- If an email address is not set, assessment request emails are not sent, and reservation notification emails are not sent when an error occurs.
- If no infrastructure administrators or dual-role administrators are registered in the IflowUsers group, the following message is displayed after the application is forwarded from the **Forward screen** window when the user subscribes to the service:

```
PCS1002  
An error occurred while processing application.  
Please contact the infrastructure administrator.
```

6.5.1.1 Creating an infrastructure administrator/dual-role administrator

Refer to "Appendix C User Management Using Directory Service" in the *Setup Guide CE* for information on how to create infrastructure administrators and dual-role administrators.

6.5.1.2 Adding an infrastructure administrator/dual-role administrator to IflowUsers Group

Follow the procedure below to add an infrastructure administrator or dual-role administrator as a member of the IflowUsers group.

For OpenDS

1. Create an LDIF file.

Edit a sample LDIF file to create the file. An example of an LDIF file is shown below.

```
# Add manager to IflowUsers
dn: cn=IflowUsers,ou=group,dc=fujitsu,dc=com
changetype: modify
add: member
member: cn=manager,ou=users,dc=fujitsu,dc=com
```

2. Execute the ldapmodify command.

Before executing the ldapmodify command of OpenDS, set JAVA_HOME as the path of Java SE 6.

[Windows]

Specify the created LDIF file, and then execute the ldapmodify command.

```
<OpenDS installation directory>\bat\ldapmodify.bat" -p <port number> -f <ldif file> -D <
administrator user DN> -w <password>
```

An execution example is shown below.

```
c:\> c:\Program Files (x86)\Fujitsu\ServerView Suite\opens\bat\ldapmodify -p 1473 -f c:\ldif
\adduser2group.ldif -D "cn=Directory Manager" -w admin
Processing MODIFY request for cn=IflowUsers,ou=group,dc=fujitsu,dc=com
MODIFY operation successful for DN cn=IflowUsers,ou=group,dc=fujitsu,dc=com
```

[Linux]

Specify the created LDIF file, and then execute the ldapmodify command.

```
# <OpenDS installation directory>/bin/ldapmodify" -p <port number> -f <ldif file> -D
<administrator user DN> -w <password>
```

An execution example is shown below.

```
# /opt/fujitsu/ServerViewSuite/opens/bin/ldapmodify -p 1473 -D "cn=Directory Manager" -f /tmp/
ldif/adduser2group.ldif -w admin
Processing MODIFY request for cn=IflowUsers,ou=group,dc=fujitsu,dc=com
MODIFY operation successful for DN cn=IflowUsers,ou=group,dc=fujitsu,dc=com
```

Note

- In the command input line, enter the command as one line without entering any line feeds.
- For the directory service port number, administrator DN, and administrator DN password, enter the values that were set during installation.

For Active Directory

1. From the Start menu, open [Control Panel]-[Administrative Tools]-[Active Directory Users and Computers].
2. Select the name of a domain that is managed by Active Directory.
3. Right-click "IflowUsers" of the organizational unit "Group", and select [Property].
4. Select the [Members] tab, and click the [Add] button.

- The [Select Users, Contacts, Computers, Or Groups] window will be displayed. Input the member list of the above table in the [Enter the object names to select] field, and click the [OK] button. If there is more than one member, separate them with semicolons.
- After returning to the property window of the group, confirm that the members have been added correctly, and click the [OK] button.

6.5.2 Stopping the Manager

Stop the manager before settings for sending e-mail.

Refer to ["7.2 Starting and Stopping the Manager"](#) for information on how to stop the manager.

6.5.3 Setting Application process settings

This section explains how to modify the application process settings.



Note

The setting to "use" application process cannot be modified to "not use" once the operation has started.

To change Application process settings

The procedure for changing the setting whether to use the application process is as follows.

- Open the following file.

[Windows]

```
<Installation directory for this product >\RCXCTMG\MyPortal\config\custom_config.xml
```

[Linux]

```
/etc/opt/FJSVctmvp/config/custom_config.xml
```

- Set the following items:

Setting item	Description
enable-create-workflow	Specify true if you want to use the application process for L-Platform subscriptions. Specify false to not use it. "false" is set during installation.
enable-reconfigure-workflow	Specify true if you want to use the application process for L-Platform modifications. Specify false to not use it. "false" is set during installation.
enable-return-workflow	Specify true if you want to use the application process for L-Platform cancellations. Specify false to not use it. "false" is set during installation.



Note

If the values of the setting items are all "false", the **Request** tab is not displayed in the ROR Console.

An example is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<properties>
<entry key="approver-selection-url">http://aaa.example.com/CTMGApproverSelection/
SelectionRequestServlet</entry>
  <entry key="show-estimation">>false</entry>
  <entry key="enable-create-workflow">>true</entry>
```

```

<entry key="enable-reconfigure-workflow">true</entry>
<entry key="enable-return-workflow">true</entry>
...
<entry key="immediate-deployment">true</entry>
</properties>

```

6.5.4 Setting Application process to be used

This section explains how to modify the application process to be used.

To change the application process to be used

The modification procedure of the application process to be used is as follows.

1. Open the following file.

[Windows]

```

<Installation directory for this product >\RCXCTMG\MyPortal\config
\application_process.properties

```

[Linux]

```

/etc/opt/FJSVctmyp/config/application_process.properties

```

2. Set the following items:

Setting item	Setting value
ServiceCreate_processName	When applying to use L-Platform, enter "Default" if approval and assessment are to be performed, enter "ApproverOnly" if approval only is to be performed, and enter "JudgeOnly" if assessment only is to be performed. "Default" is set during installation.
ServiceChange_processName	When modifying L-Platform, enter "Default" if approval and assessment are to be performed, enter "ApproverOnly" if approval only is to be performed, and enter "JudgeOnly" if assessment only is to be performed. "Default" is set during installation.
ServiceReturn_processName	When canceling L-Platform, enter "Default" if approval and assessment are to be performed, enter "ApproverOnly" if approval only is to be performed, and enter "JudgeOnly" if assessment only is to be performed. "Default" is set during installation.

Note

The above three setting values must be identical.

An example is shown below:

```

...
ServiceCreate_applicationId=ctmgApplication
ServiceCreate_processName=Default
ServiceChange_applicationId=ctmgApplication
ServiceChange_processName=Default
ServiceReturn_applicationId=ctmgApplication
ServiceReturn_processName=Default
...

```

6.5.5 Starting the Manager

Start the manager in order to enable the email settings set in "[6.5.3 Setting Application process settings](#)" and "[6.5.4 Setting Application process to be used](#)".

Refer to "[7.2 Starting and Stopping the Manager](#)" for information on how to stop the manager.

6.6 Customizing the Dashboard

Refer to "[Appendix K To Customize Dashboard](#)", for information on customizing the dashboard.

Chapter 7 Logging in to Resource Orchestrator

This chapter explains how to start and stop the Resource Orchestrator manager and agent services, how to check their running state, and how to open and close the ROR console.

Managers and agents start automatically when their respective servers are powered on. Normally no special operation is required to start them.

Note

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

Managed servers will not boot up properly if they are started before the manager. Check that the manager is running before turning on the managed servers.

Additionally, when using the HBA address rename function, the HBA address rename setup service should be started on a server and left running all the time. For details on starting, stopping, and checking the state of the HBA address rename setup service, refer to "[8.2.1 Settings for the HBA address rename Setup Service](#)".

7.1 Login

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

Note

- When accessing the ROR console from Internet Explorer 8 or 9, be sure to enable the Compatibility View in Internet Explorer.
- When downloading files using the ROR console, it is necessary to disable [Do not save encrypted pages to disk] in the Advanced Settings of the browser.
- The ROR console uses the Web browser's standard fonts and is best viewed in a window size of 1024 by 768 pixels. If the Web browser is resized a significant amount, the display quality may deteriorate.
- The ROR console uses JavaScript, Cookies, and IFRAMES. These must be enabled in the Web browser settings before using the ROR console.

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 the ROR console is connected, the login window is displayed.

When Single Sign-On authentication has already been performed, the ROR console can be started without displaying the login window.

Refer to "[4.5 Installing and Configuring Single Sign-On](#)" for details on Single Sign-On.

```
URL: https://Admin_server_FQDN:23461/
```

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

Note

- If the login screen is not displayed, check that the following settings are correct.
 - URL entered in address bar of the Web browser.
 - Proxy settings of the Web browser.
 - Firewall settings on the admin server.
- When opening the ROR console right after launching a Web browser, a warning window concerning the site's security certificate will be displayed.

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

Resource Orchestrator generates unique, self-signed certificates for each admin server when the manager is installed.

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

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

A login window with a URL differing from the address bar's URL in which the IP address or host name (FQDN) may be displayed depending on the OS configuration. There are no problems with using the displayed window.

For details, refer to "[Appendix B HTTPS Communications](#)".
- If already logged in from another Web browser window, login may be performed automatically (without displaying the login screen).

Login

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

- User ID
- Password

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

The [Register License] dialog is displayed.
2. In the [Register License] dialog, enter the license key to register.
3. Click <OK>.

The license will be registered.



Note

After applying the Cloud Edition license, restart the manager.

Confirming the License

Use the following procedure to confirm the registered license:

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

The [Licenses] dialog is displayed.



Note

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

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 or BladeViewer has been opened simultaneously in several Web browser windows, those login sessions may be terminated.

Exit

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

7.2 Starting and Stopping the Manager

The Resource Orchestrator manager starts automatically on the admin server.

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

[Windows]

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

- Manager Services

Resource Coordinator Manager

Resource Coordinator Task Manager

Resource Coordinator Web Server (Apache)

Resource Coordinator Sub Web Server (Mongrel)

Resource Coordinator Sub Web Server (Mongrel2)

Resource Coordinator Sub Web Server (Mongrel3)

Resource Coordinator Sub Web Server (Mongrel4)

Resource Coordinator Sub Web Server (Mongrel5)

Resource Coordinator DB Server (PostgreSQL)

ServerView Resource Orchestrator Service Catalog Manager DB Service (Dashboard)

ServerView Resource Orchestrator Service Catalog Manager DB Service (Charging)
ServerView Resource Orchestrator Service Catalog Manager REST Service (Charging)

- Related Services

Deployment Service
TFTP Service
PXE Services
DHCP Server (*1)
Systemwalker SQC DCM
Interstage BPM Analytics eRule Engine (EFServer)
Systemwalker MpJobsch9
Systemwalker Mpmjes
Systemwalker Mpmjes9
Systemwalker Runbook Automation DB Service
Shunsaku Conductor cmdbc
Shunsaku Sorter cmdbo01

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

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

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

As this command collectively controls both manager and related services, use the command to start and stop services.

For details on the rcxadm network command, refer to "1.7.17 rcxmgrctl" in the "Reference Guide (Resource Management) CE".

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

[Linux]

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

- Manager Services

rcvmr

Manager services also include the following daemons.

rcxmanager
rcxtaskmgr
rcxmongrel1
rcxmongrel2
rcxmongrel3
rcxmongrel4
rcxmongrel5
rcxhttpd

- Database (PostgreSQL)

rcxdb

- Related Services

scwdepsvd
scwpxesvd
scwftpd
dhcpcd (*1)

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

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

```
# service rcvmr status <RETURN>
# service scwdepsvd status <RETURN>
```



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

Services are started and stopped using the `rcxmgrctl` command (start and stop subcommands).

As this command collectively controls both manager and related services, use the command to start and stop services.

For details on the `rcxadm network` command, refer to "1.7.17 `rcxmgrctl`" in the "Reference Guide (Resource Management) CE".

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

For details, refer to the PRIMECLUSTER manual.

Note

- When using ServerView Deployment Manager on an admin LAN, all services related to Resource Orchestrator will be automatically disabled. To prevent conflicts with ServerView Deployment Manager, do not start these services in order. For details, refer to "[Appendix L Co-Existence with ServerView Deployment Manager](#)".
- Resource Orchestrator cannot operate if any of the manager services are stopped. Ensure that all services are running when Resource Orchestrator is running.
- If the manager is unable to communicate on the admin LAN when started up (because of LAN cable disconnections or any other causes), PXE Services may not start automatically. If PXE Services are stopped, investigate the network interface used for the admin LAN and confirm whether it can communicate with other nodes on the admin LAN.

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

- If the manager fails to start, check if the admin server has multiple IP addresses. If it has, refer to "2.1.4 Setup" in the "Installation Guide CE", and perform the procedure of the note "When configuring an environment on the admin server with multiple IP addresses, use the following procedure before initiating setup."
- In Basic mode, the following manager services are started.

In Basic mode, the procedure to start and stop the services and the procedure to check their statuses are same as those in standard mode.

[Windows]

- Manager Services

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

[Linux]

- Manager Services

- `rcvmr`

Manager services also include the following daemons.

- `rcxmanager`
- `rcxtaskmgr`
- `rcxmongrel1`
- `rcxmongrel2`
- `rcxhttpd`

7.3 Starting and Stopping the Agent

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

Note

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

[Windows/Hyper-V]

The agent consists of the following two Windows services:

- Agent Service
 - Resource Orchestrator Agent
- Related Services
 - Deployment Agent
 - Systemwalker SQC DCM

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

- Agent Service
 - Agents can be started and stopped using the start and stop subcommands of the `rcxadm agtctl` command. For details on these commands, refer to "5.1 `rcxadm agtctl`" of the "Command Reference".

- Related Services

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

- Deployment Agent
- Systemwalker SQC DCM

[Linux/VMware/Xen/KVM]

The agent consists of the following services.

- Agent Service
- Related Services
 - Deployment Agent

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

[Linux]

- Systemwalker SQC DCM

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

- Agent Service

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

- Related Services

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

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

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

The following explains how to start and stop each service.

- Agent Service

Agents can be started and stopped using the start and stop subcommands of the rxcadm agtctl command.
For details on these commands, refer to "5.1 rxcadm agtctl" of the "Command Reference".

- Related Services

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

Start

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

Stop

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

7.4 Importing a Certificate to a Browser

In order to use a test site certificate, the certificate must be installed to the Web browser.

Log in to the ROR Console, and perform the operations below while the [Account] dialog is open.

If these operations are not performed, the [Forward screen] dialog used by the ROR Console L-Platform application process cannot be displayed.

"Certificates" stated in this section refer to "server certificates".



- The license settings must be completed, before starting operations in Resource Orchestrator. For details on how to configure licenses, refer to "[License Setup](#)" in "7.1 Login".
- If multiple admin clients are used, perform this operation on each admin client.

1. Open the [Certificate] dialog.

For Internet Explorer 8 and 9, open the "Certificate is invalid dialog" by clicking the "Certificate Error" displayed in the address bar. This will open an "Untrusted Certificate" or "Certificate Expired" message.
Click the "View certificates" link displayed at the bottom of this dialog.

2. Confirm that the "Issued to" and "Issued by" displayed in the [Certificate] dialog are both set to the IP address or host name (FQDN) used to generate the certificate.

3. In the [Certificate] dialog, click <Install Certificate>.

4. The [Certificate Import Wizard] dialog is displayed.

Click <Next>.

5. Select "Place all certificates in the following store" and click <Browse>.

6. The [Select Certificate Store] dialog is displayed.

Select the "Trusted Root Certification Authorities" and click <OK>.

7. Click <Next>.

8. Check that "Trusted Root Certification Authorities" is selected and click <Finish>.
9. Restart the Web browser.

Note

- When the OS is Windows 7 or later version, there may be cases where the URL of the ROR console must be registered in the "Trusted sites", depending on the details of OS security policies.
- Enter the IP address or host name (FQDN) used to generate the certificate in the Web browser's URL bar. If the entered URL differs from that of the certificate, a certificate warning is displayed.

An example of how to display a warning is given below.

- The entered URL uses an IP address while the certificate was created using a host name (FQDN)
 - The admin server is set with multiple IP addresses, and the entered URL uses an IP address different from that used to generate the certificate
-

Chapter 8 Setup

This chapter explains how to set up Resource Orchestrator after installation.

The items to set up after installation are indicated below.

- Register the resources to manage with Resource Orchestrator

Register the resources to manage with Resource Orchestrator.

For details on registering the resources to manage with Resource Orchestrator, refer to ["8.1 Registering Resources with Resource Orchestrator"](#).

- Register Infrastructure Administrators

The administrator role, which is the role that combines infrastructure administrator and tenant administrator roles, is assigned to the user created when installing Resource Orchestrator. Resource Orchestrator can be configured and operated by this user or another user registered with the infrastructure administrator role, in order to prevent the operation of an L-Platform from being stopped by erroneous operations.

For details on how to register network resources, refer to "9.1 Registering User Accounts" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- Create Cloning Images

A cloning image is a system disk collected from a server with an OS installed that is saved for deployment to another server. By deploying a cloning image when creating an L-Server, there is no need to install an OS or software. A cloning image is required to use the L-Platform function.

Cloning images used in common throughout the entire system are created by the infrastructure administrator. Collect cloning images after creating an L-Server or from an existing server.

The tenant administrator can create L-Platforms using the cloning images created by the infrastructure administrator, and can collect cloning images by editing the included L-Server system images. This enables tenant-unique cloning images to be created.

For details, refer to ["8.6 Collecting and Registering Cloning Images"](#).

- Create an L-Server Template

An L-Server template comprises pre-defined specifications (number of CPUs, memory capacity, disk capacity, number of NICs, etc.) for an L-Server.

L-Server templates are created by the infrastructure administrator.

For details, refer to ["8.5 Creating L-Server Templates"](#).

- Create an L-Platform Template

An L-Platform template defines systems of various levels in advance.

L-Platform templates used in common throughout the entire system are created by the infrastructure administrator.

The tenant administrator can edit the L-Platform templates created by the infrastructure administrator to create tenant-unique L-Platform templates.

For details, refer to ["8.7 Creating L-Platform Templates"](#).

8.1 Registering Resources with Resource Orchestrator

This section explains how to register, change, and delete resources used by Resource Orchestrator.

The Resource Orchestrator manager must be completely installed beforehand.

For details on the resources to manage with Resource Orchestrator, refer to ["8.1.1 Managed Resources and Registration Order"](#).

The resources that must be registered differ depending on the type of L-Server and the type of servers to use.

For details on the required resources, refer to ["8.1.1.2 Necessity of Resource Registration"](#).

For details on the registration method and registration order for each type of L-Server, refer to ["8.1.1.3 Registration Order and Registration Method for Resources"](#).

Information

- User Accounts

When creating new user accounts, changing passwords, or modifying permission levels during setup, refer to "Chapter 2 Managing User Accounts" of the "Operation Guide CE".

- 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 "8.2 Backup" in the "Operation Guide VE".

8.1.1 Managed Resources and Registration Order

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

8.1.1.1 Managed Resources

This section explains managed resources.

The following resources can be managed with Resource Orchestrator.

- VIOM
- Storage Management Software
- VM Management Software
- Chassis
- Managed Servers
- LAN Switch Blades
- Power Monitoring Devices
- Virtual Storage Resources
- Disk Resources
- Network Device Resources
- Network Resources
- Address Set Resources
- Virtual Image Resources
- Physical Image Resources

8.1.1.2 Necessity of Resource Registration

This section explains the necessity of resource registration.

The resources that must be registered differ depending on the type of L-Server and the type of servers to use.

Table 8.1 List of Resources that Require Registration

Resources that can be Registered	Necessity of Registration Based on Server Type	
	Physical L-Server	Virtual L-Server
VIOM	Yes (*1)	No

Resources that can be Registered	Necessity of Registration Based on Server Type	
	Physical L-Server	Virtual L-Server
VM management software	No	Yes
Storage management software	Yes	Yes (*2)
Chassis	Yes (*1)	
Managed servers	Yes	
LAN switch blades	Yes (*1)	
Virtual storage resources	Yes (*3)	Yes (*4)
Disk resources	Yes (*5)	Yes (*6)
Network device resources	Yes (*7)	
Network resources	Yes	
Address set resources	Yes	Yes (*2, *6)
Image resources	Yes (*8)	
Power monitoring devices	Yes (*9)	

Yes: Required

No: Not required

*1: Register when using blade servers.

*2: Register when using RHEL5-Xen servers.

*3: Register when using virtual storage resources such as RAID groups and aggregates.

*4: Register when using virtual storage resources such as datastores.

*5: Register when using disk resources created in advance such as LUNs.

*6: Register when using RHEL-KVM servers.

*7: Register when using firewalls and L2 switches.

*8: Register when using images created in advance.

*9: Register when monitoring power consumption.

8.1.1.3 Registration Order and Registration Method for Resources

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

Use the following procedure to register resources:

When Installing Physical L-Servers

- When using a blade server

1. Register VIOM

Refer to "2.1 Registering VIOM Coordination" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

2. Register Storage Management Software

Execute the `rcxadm storagemgr register` command.

For details on the `rcxadm storagemgr register` command, refer to "1.7.1 `rcxadm storagemgr`" in the "Reference Guide (Resource Management) CE".

When storage management software is registered, virtual storage resources and disk resources created in advance are automatically recognized.

3. Register Chassis

Refer to "2.4.1 Registering Chassis" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

4. Register Managed Servers (within Chassis)

Refer to "2.4.2 Registering Blade Servers" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

When performing admin LAN NIC redundancy and registering a physical server, check the "Use Admin LAN redundancy" checkbox in the "Register Server" dialog when registering the server.

When directly specifying an IP address during physical L-Server creation, do not configure the same IP address on a managed server.

An error will occur during the following operations, if there are managed servers configured with the same IP addresses as those allocated to physical L-Servers, in other than physical servers.

- Creation of physical L-Servers
- Starting of a physical L-Server for which only the configuration definition has been created

5. Register LAN Switch Blades

Refer to "2.4.3 Registering LAN Switch Blades" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

To register a network device resource, network resource, or address set resource, specify a resource pool when creating the resource.

- Register Network Device Resources

For details on how to register network device resources, refer to "2.7.2 Registering Network Devices" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- Register Network Resources

For details on how to register network resources, refer to "2.6 Registering Network Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- Register Address Set Resources

Register the MAC address and WWN address set resources to use for I/O virtualization with VIOM.

Execute the `rcxadm addrset create` command to register address set resources.

For details on the `rcxadm addrset create` command, refer to "1.3.10 rcxadm addrset" in the "Reference Guide (Resource Management) CE".

- When using something other than a blade server

1. HBA address rename Settings

Refer to "8.2 HBA address rename Settings".

2. Register Storage Management Software

Execute the `rcxadm storagemgr register` command.

For details on the `rcxadm storagemgr register` command, refer to "1.7.1 rcxadm storagemgr" in the "Reference Guide (Resource Management) CE".

When storage management software is registered, virtual storage resources and disk resources created in advance are automatically recognized.

3. Register Managed Servers

Refer to "2.5.1 Registering Rack Mount or Tower Servers" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

When performing admin LAN NIC redundancy and registering a physical server, check the "Use Admin LAN redundancy" checkbox in the "Register Server" dialog when registering the server.

When directly specifying an IP address during physical L-Server creation, do not configure the same IP address on a managed server.

An error will occur during the following operations, if there are managed servers configured with the same IP addresses as those allocated to physical L-Servers, in other than physical servers.

- Creation of physical L-Servers
- Starting of a physical L-Server for which only the configuration definition has been created

To register a network device resource, network resource, or address set resource, specify a resource pool when creating the resource.

- Register Network Device Resources

For details on how to register network device resources, refer to "2.7.2 Registering Network Devices" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- Register Network Resources

For details on how to register network resources, refer to "2.6 Registering Network Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- Register Address Set Resources

Register the WWN address set resources to use for I/O virtualization with HBA address rename.

Execute the `rcxadm addrset create` command to register address set resources.

For details on the `rcxadm addrset create` command, refer to "1.3.10 rcxadm addrset" in the "Reference Guide (Resource Management) CE".

When Using Virtual L-Servers

- When using a blade server

1. Register VM Management Software

Refer to "2.2 Registering VM Management Software" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

When VM management software is registered, virtual storage resources are automatically recognized.

2. Register Chassis

Refer to "2.4.1 Registering Chassis" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

3. Register Managed Servers (within Chassis)

Refer to "2.4.2 Registering Blade Servers" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

4. Register LAN Switch Blades

Refer to "2.4.3 Registering LAN Switch Blades" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

5. Register Disk Resources (when using RHEL-KVM)

Register the raw devices or partitions recognized by VM hosts as disk resources.

Disk resources can be registered by executing the `rcxadm disk register` command.

When migrating VM guests for virtual L-Servers, register the raw devices or the partitions shared between multiple VM hosts as disk resources defined to be shared.

For details on the `rcxadm disk register` command, refer to "1.3.4 rcxadm disk" in the "Reference Guide (Resource Management) CE".

To register a network device resource, network resource, or address set resource, specify a resource pool when creating the resource.

- Register Network Device Resources

For details on how to register network device resources, refer to "2.7.2 Registering Network Devices" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- Register Network Resources

For details on how to register network resources, refer to "2.6 Registering Network Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- Register Address Set Resources (when using RHEL5-Xen or RHEL-KVM)

Execute the `rcxadm addrset create` command to register address set resources.

For details on the `rcxadm addrset create` command, refer to "1.3.10 rcxadm addrset" in the "Reference Guide (Resource Management) CE".

- When using something other than a blade server

1. Register VM Management Software

Refer to "2.2 Registering VM Management Software" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

When VM management software is registered, virtual storage resources are automatically recognized.

2. Register Managed Servers

Refer to "2.5.1 Registering Rack Mount or Tower Servers" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

3. Register Disk Resources (when Using RHEL-KVM)

Register the raw devices or partitions recognized by VM hosts as disk resources.

Disk resources can be registered by executing the `rcxadm disk register` command.

When migrating VM guests for virtual L-Servers, register the raw devices or the partitions shared between multiple VM hosts as disk resources defined to be shared.

For details on the `rcxadm disk register` command, refer to "1.3.4 `rcxadm disk`" in the "Reference Guide (Resource Management) CE".

To register a network device resource, network resource, or address set resource, specify a resource pool when creating the resource.

- Register Network Device Resources

For details on how to register network device resources, refer to "2.7.2 Registering Network Devices" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- Register Network Resources

For details on how to register network resources, refer to "2.6 Registering Network Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- Register Address Set Resources (when using RHEL5-Xen or RHEL-KVM)

Execute the `rcxadm addrset create` command to register address set resources.

For details on the `rcxadm addrset create` command, refer to "1.3.10 `rcxadm addrset`" in the "Reference Guide (Resource Management) CE".

8.2 HBA address rename Settings

Use the following procedure to configure HBA address rename settings.

The HBA address rename function allows the admin server to control the WWNs set on a managed server's HBAs. Since the admin server carries over these settings when performing maintenance on or switching managed servers, it is not necessary to set the storage side configuration again.

Use of the HBA address rename function requires registering specific settings for each managed server in advance.



Note

- The HBA address rename function is not available if ServerView Deployment Manager is used on the admin LAN. For details, refer to "[Appendix L Co-Existence with ServerView Deployment Manager](#)".
- For servers which already have server switchover configured, when configuring or changing HBA address rename, the following conditions must be met:
 - Primary servers with HBA address rename configured
 - Spare servers with the server switchover method HBA address rename configured

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

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

- When using PRIMEQUEST, FC cards set with HBA address rename cannot use the PHP function.
Restarting of a server is required after replacing the FC card.
-

1. Storage Settings

Refer to "[4.3.2 Configuring the Storage Environment](#)" to configure the storage.

When altering the configuration of a storage device already used by active servers, ensure those servers are powered off before performing any configuration changes.

2. Settings for the HBA address rename Function

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

The [HBA Address Rename Settings] dialog is displayed.

2. Define the following settings:

WWNN

Specify the WWNN value provided by the "I/O virtualization Option".

The admin server generates WWPNs automatically from the values that are input into the WWNN and the number of HBA ports.

HBA ports

Specify the following values according to the system configuration.

- To create a single-path configuration, specify "1".
For details, refer to "[Figure 8.1 Procedures for Single-path Configurations](#)".
- To create a multi-path configuration, specify "2".

However, it is necessary to specify "1" during installation of the operating system. Specify "2" and reconfigure HBA address rename settings after setting up the multi-path driver.

For details, refer to "[Figure 8.2 Procedures for Multi-path Configurations](#)".

Figure 8.1 Procedures for Single-path Configurations

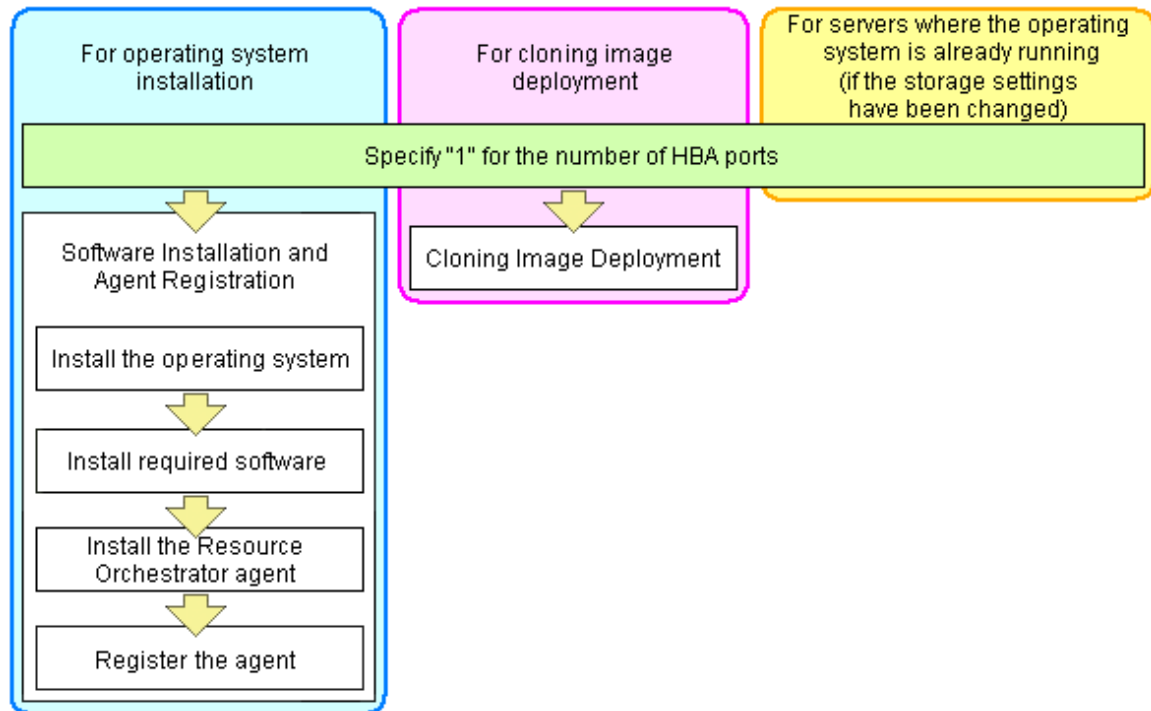
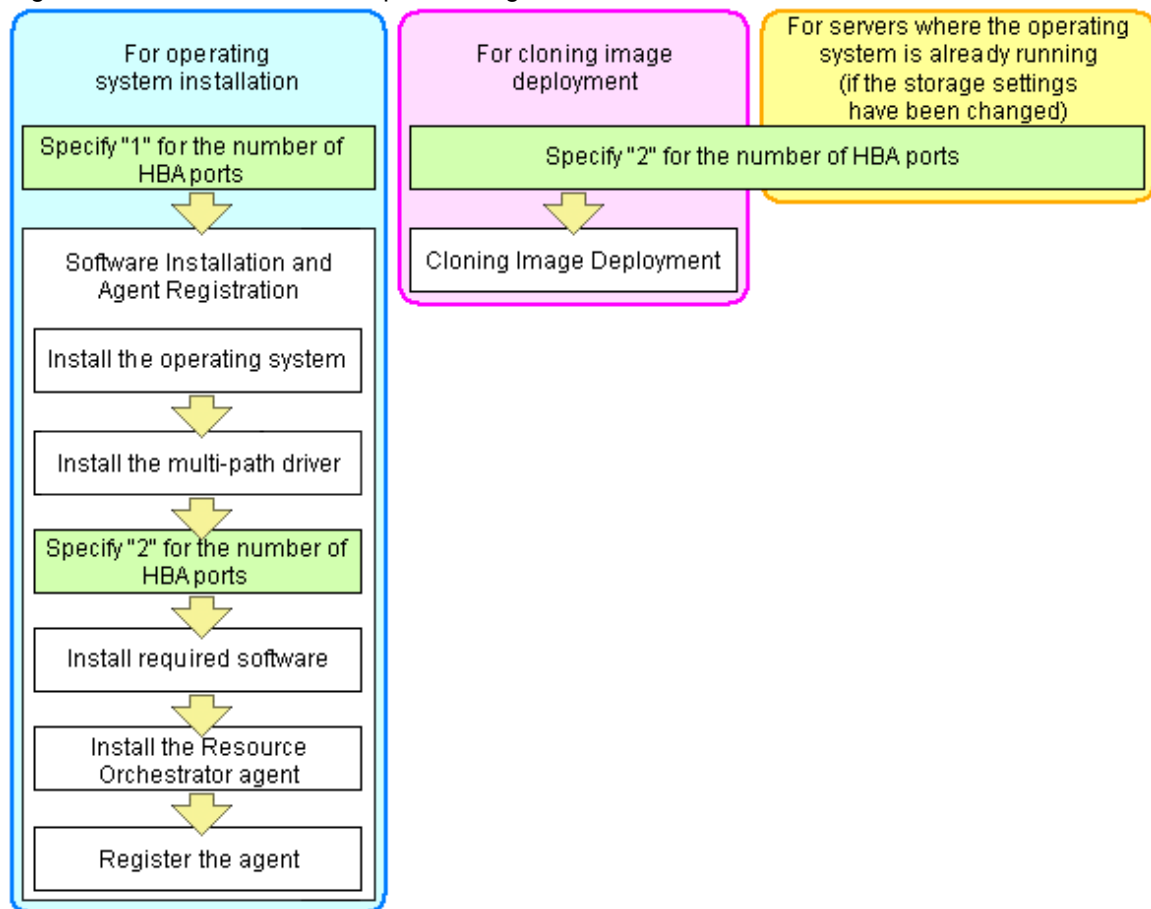


Figure 8.2 Procedures for Multi-path Configurations



Example

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

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

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

"WWNN" value 20:00:00:17:42:51:00:00

"HBA port number" on board: 2

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

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

Information

WWN settings are applied to managed servers during server startup.

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

Information

Select server restart in the following cases.

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

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

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

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

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

4. Click <OK>.
5. Restart the HBA address rename setup service.

The HBA address rename setup service must be running to use the HBA address rename function.

For details, refer to "[8.2.1 Settings for the HBA address rename Setup Service](#)".

8.2.1 Settings for the HBA address rename Setup Service

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 managed servers HBAs WWNs in the same way the admin server does.

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]-[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. Define the following settings:

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.



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 B Manager Cluster Operation Settings and Deletion" in the "Installation Guide CE".

[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 B Manager Cluster Operation Settings and Deletion" in the "Installation Guide CE".

8.3 Software Installation and Agent Registration

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

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 up the admin IP address, the related network mask, and the default gateway for the managed servers defined in "[4.2.2.5 Settings for Managed Servers](#)".

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 "[8.2 HBA address rename Settings](#)" 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, follow the procedure described in "2.1.1 Registering VIOM Server Profiles" in the "User's Guide for Infrastructure Administrators (Resource Management) CE" to configure server profiles on the Web interface of ServerView Virtual-IO 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 "4.1 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.



After configuration of agents, the server name (computer name for [Windows/Hyper-V] or a system node name for [Linux/VMware/Xen/KVM]) 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]

Specify up to 64 characters, including alphanumeric characters as well as the following symbols.

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

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 OS's, VM hosts and VM guests. If duplicated names are used, those resources cannot be managed from the command-line.

2. Install Required Software

Install the software packages that are required for a managed server.
For details on required software, refer to "[1.4.2.2 Required Software](#)".

3. Install the Agent

Refer to "2.2 Agent Installation" in the "Installation Guide CE".

4. Register the Agent

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

- 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 a Physical OS

Select "Windows/Linux".

- For a VM Host

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

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

User name

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

Password

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

- c. Click <OK>.

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 "15.3 "unknown" Server Status" in the "Operation Guide VE" 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 "E.3 Functional Differences between Products" in the "Setup Guide VE".

- When using system image backups or cloning image collection, restart the managed server after registration is complete, or restart the related services indicated in "[7.3 Starting and Stopping the Agent](#)".
For details on restarting the agent, refer to "[7.3 Starting and Stopping the Agent](#)".

- A server running a VM host can still be registered as a physical OS if its selected Server OS category is set to "Windows/Linux". A VM host server that was mistakenly registered as a physical OS should be deleted and re-registered as a VM host.

8.4 Registering Resources to the Global Pool

This section explains the registration of resources to resource pools.

When creating a cloning image common to tenants, an L-Server for the infrastructure administrator must be created.

To create an L-Server for the infrastructure administrator, resources must be registered to the global pool.

The resources that are required to be registered to the resource pool differ depending on the type of L-Server.

Table 8.2 Registering Resources to Resource Pools Based on Resource Type

Resource Pool Types	Type of Resources Stored in the Resource Pool	Method of Registration to the Resource Pool	Necessity of Registration Based on Server Type	
			Physical L-Server	Virtual L-Server
VM pool	VM host resources	Refer to "7.1 VM Host Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".	No	Yes
Server pool	Physical server resources	Refer to "7.2 Physical Server Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".	Yes	No
Storage pool	Virtual storage resources or disk resources	Refer to "7.5 Storage Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".	Yes	Yes
Network pool	Network resources or network devices (firewalls)	For details on how to register network device resources, refer to "7.3 Network Resources" or "7.4 Network Devices" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".	Yes	Yes
Address pool	Address set resources	Refer to "7.6 Address Set Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".	Yes	Yes (*1)

Yes: Required

No: Not required

*1: When using RHEL5-Xen or RHEL-KVM, it is necessary to register MAC addresses.

Information

For details on changing the settings for, canceling registration, and deleting resources registered in a resource pool, refer to "12.3 Resource Operations" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Physical L-Server

Use the following procedure to register resources to the global pool.

1. Register Resources to a Server Pool

Register physical servers to the server pool.

Refer to "7.2 Physical Server Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

2. Register Resources to a Storage Pool

The procedure differs depending on the storage resources to use.

- When using virtual storage resources or disk resources created in advance

Refer to "7.5 Storage Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- When using iSCSI boot

Execute the operation command for iSCSI boot (rcxadm iscsictl register) to register the resources.

For details on the rcxadm iscsictl register command, refer to "1.7.12 rcxadm iscsictl" in the "Reference Guide (Resource Management) CE".

3. Register Resources to a Network Pool

Create network resources and register them to the network pool.

Refer to "7.3 Network Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Create network devices and register the ones whose type is Firewall to the network pool.

Refer to "7.4 Network Devices" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

4. Register Resources to an Address Pool

- For blade servers

For WWNs and MAC addresses, address set resources must be created and registered to the address pool.

Execute the rcxadm addrset create command to register WWNs and MAC addresses to the address pool.

For details on the rcxadm addrset create command, refer to "1.3.10 rcxadm addrset" in the "Reference Guide (Resource Management) CE".

- For rack mount servers

For WWNs, it is necessary to create address set resources and register them in the address pool.

Since MAC addresses use the MAC address assigned to the physical network adapter, it is not necessary to create and register address set resources.

Execute the rcxadm addrset create command to register WWNs to the address pool.

For details on the rcxadm addrset create command, refer to "1.3.10 rcxadm addrset" in the "Reference Guide (Resource Management) CE".

Virtual L-Server

Use the following procedure to register resources to the global pool.

1. Register Resources to a VM Pool

Register a VM host in a VM pool.

Refer to "7.1 VM Host Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

2. Register Resources to a Storage Pool

Procedures differ depending on the server virtualization software being used.

Refer to "Virtual Storage Resources and Disk Resources for Physical L-Servers" in "7.5 Storage Resources" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

[KVM]

Refer to "For Virtual L-Servers" in "7.5 Storage Resources" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

3. Register Resources to a Network Pool

Create network resources and register them to the network pool.

Refer to "7.3 Network Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Create network devices and register the ones whose type is Firewall to the network pool.
Refer to "7.4 Network Devices" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

4. Register resources to the address pool [Xen] [KVM]

For MAC addresses, it is necessary to create address set resources and register them in the address pool.

Execute the `rcxadm addrset create` command to register MAC addresses to the address pool.

For details on the `rcxadm addrset create` command, refer to "1.3.10 `rcxadm addrset`" in the "Reference Guide (Resource Management) CE".

8.5 Creating L-Server Templates

This section explains how to create an L-Server template.

An L-Server template comprises pre-defined specifications (number of CPUs, memory capacity, disk capacity, number of NICs, etc.) for an L-Server.

L-Server templates can be created using the following methods.

- Using the Wizard GUI

L-Server templates can be created using a GUI in the wizard format.

For details on the GUI in the wizard format, refer to "8.1 Operations Using the Wizard GUI" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- Manually

Use the following procedure to create an L-Server template:

1. Export an L-Server Template

The sample L-Server templates provided with Resource Orchestrator can be exported.

For details on how to export L-Server templates, refer to "8.2.1 Exporting a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

2. Edit with an Editor

The L-Server template output in 1. can be edited with an editor, etc.

The format of the L-Server template differs depending on whether the L-Server is physical or virtual.

For details on the L-Server templates for physical L-Servers, refer to "2.2.1 Physical L-Server Templates" in the "Reference Guide (Resource Management) CE".

For details on the L-Server templates for virtual L-Servers, refer to "2.2.2 Virtual L-Server Templates" in the "Reference Guide (Resource Management) CE".

3. Import an L-Server Template

The L-Server template edited in 2. can be imported.

For details on how to import L-Server templates, refer to "8.2.3 Importing a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

8.6 Collecting and Registering Cloning Images

This chapter explains how to collect and register cloning images used for the entire system.

When Collecting from an L-Server

Use the following procedure to collect cloning images:

1. Create an L-Server for the Infrastructure Administrator

The L-Server for the infrastructure administrator is the L-Server to collect cloning images used for the entire system.

Create an L-Server for the infrastructure administrator using the L-Server template created in "8.5 Creating L-Server Templates".

- a. Select the orchestration tree in the [Resource] tab of the ROR console.

- b. Select the L-Server template in the [Template List] tab of the main panel, and click the <Create> button.

Select "None" for images.

- c. In the [General] tab of the [Create an L-Server] dialog, set the required items.

An L-Server without an OS installed can be created.

For details on creating an L-Server for the infrastructure administrator using an L-Server template, refer to "10.1 Creation Using an L-Server Template" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

2. Manually Install an OS

Install an OS to the L-Server for the infrastructure administrator created in step 1.

For physical L-Servers, install agents of Resource Orchestrator after installing the OS.

3. Collect a Cloning Image from the L-Server after the OS is Installed

Cloning images can be collected from the L-Server after an OS is installed.

- a. In the orchestration tree of the [Resource] tab of the ROR console, right-click the L-Server created in step 1. and select [Cloning] - [Collect] from the popup menu.

The [Collect a Cloning Image] dialog is displayed.

- b. Configure the necessary items.

The cloning image is stored in the specified image pool.

For details on collecting cloning images, refer to "11.5.1 Collecting and Registering Cloning Images" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

When Registering a Cloning Image Created from a Physical Server in Advance to the Image Pool

Refer to "7.7.2 Physical Image Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

When Registering an Image (Template) Created with VM Management Software in Advance to the Image Pool

Refer to "7.7.1 Virtual Image Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".



In the following cases, Sysprep is executed and included in the count:

- Customizing a guest OS using a template in VMware
- Template creation in SCVMM

For details on operation, refer to "Note Operation Methods for Cloning Image Collection" in "8.6.2 When Collecting Cloning Images from Virtual L-Servers".

8.6.1 When Collecting Cloning Images from Physical L-Servers

Use the following procedure to collect cloning images:

1. Create a Physical L-Server for the Infrastructure Administrator

Refer to "[Create an L-Server for the Infrastructure Administrator](#)".

2. Manually Install an OS

Install an OS on the physical L-Server for the infrastructure administrator created in 1.

Refer to "[Manual OS Installation](#)".

3. Install a Multipath Driver (when using a Multipath for the Path to the SAN)

Install a multipath driver to the L-Server.

Refer to the manual of the multipath driver for details on installing multipath drivers.

4. Stop the L-Server

For details on stopping L-Servers, refer to "11.1.2 Stopping an L-Server" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

5. Change the SAN Path Status of the L-Server

Follow the procedure below to change the SAN path status of the L-Server.

- a. Right-click the target L-Server in the orchestration tree, and select [Change Settings]-[Modify Specification] from the popup menu. The [Modify an L-Server] dialog is displayed.
- b. Uncheck the "Single path mode" checkbox for FC path.
- c. Click <OK>.

6. Install the Agent

Install the Resource Orchestrator agent to the physical L-Server for the infrastructure administrator.

For details on installing agents, refer to "2.2 Agent Installation" in the "Installation Guide CE".

7. Register the Agent

It is also necessary to install an agent after installing an OS, and then register the server used by an L-Server for an agent.

Use the following procedure to register agents.

- a. Right-click the target L-Server in the orchestration tree, and select [Register]-[Agent] from the popup menu. The [Register Agent] dialog is displayed.
- b. Click <OK>.

8. Start the L-Server

For details on starting L-Servers, refer to "11.1.1 Starting an L-Server" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

9. Stop the L-Server

For details on stopping L-Servers, refer to "11.1.2 Stopping an L-Server" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

10. Collect a Cloning Image from the L-Server after the OS is Installed

Refer to "[Collect a Cloning Image from the L-Server after the OS is Installed](#)".

 Note

- This function is not available if ServerView Deployment Manager is used on the admin LAN. Use the cloning function of ServerView Deployment Manager. For details, refer to "[Appendix L Co-Existence with ServerView Deployment Manager](#)".

- When cloning, only the content of the first disk recognized in the BIOS (the boot disk) of the managed server is collected.

Data disk content (second disk onwards) cannot be cloned. Use other backup software and the copy functions of storage units to collect and deploy the data.

If multiple storage areas (Windows drives or Linux partitions) are set in the first disk, all the partitions are cloned.

Table 8.3 Cloning Target Examples

Disk	Windows Drive	Cloning Target
First disk	C:	Yes
	E:	Yes

Disk	Windows Drive	Cloning Target
Second disk	D:	No
	F:	No

- When collecting a cloning image, work must be stopped because the managed server is restarted.
- The first partition must be a primary partition.
- Cloning images can be collected with the following file systems. Note that LVM (Logical Volume Manager) partitions are not supported.
 - NTFS
 - EXT3
 - EXT4
 - LinuxSwap

- The following conditions must be met for the managed server to collect the cloning image from and the managed server to deploy the cloning image to.
 - The model names are the same
 - The hardware configurations are the same, such as the optional cards and expansion cards, and their locations
 - The same BIOS settings have specified in accordance with "[BIOS Settings of Managed Servers](#)" in "[4.1.2 Configuring the Server Environment](#)" of the "ServerView Resource Orchestrator Setup Guide"
 - The LAN and SAN connections have the same redundancy methods and the same number of redundancy paths, and can access the same network devices and storage units

Note that LAN or fibre channel switches connected in a cascade configuration are viewed as a single device.

- Some applications may require manual adjustments to function properly after cloning. If necessary, manually perform such adjustments before or after the cloning process.
- Up to four system image backup, restoration, and cloning image collection processes can be executed at the same time. If five or more processes are requested, the extra processes wait until the processes being executed are complete.

Restore operations executed by the backup/restore method during server switchover and failback also wait. When using auto-recovery and manual switchover operations with the backup/restore method, execute a maximum of three system image backup/restore or cloning image collection/deployment operations at the same time.

- After collecting or deploying a cloning image, software required for connecting to external servers, etc. when the OS is started may not start correctly.

In this case, restart the OS after it is collected.

- If the Watchdog (function that automatically resets or turns off the OS when a hang is detected because the OS does not respond for a certain period) function of the managed server is enabled, the OS may be automatically reset or turned off during cloning.

It is therefore highly recommended to disable the Watchdog function before a cloning operation.

For details, refer to the manual of the managed server.

- When using MAK license authentication for the activation of Windows Server 2008, Sysprep can be executed a maximum of three times.

Since Sysprep is executed when deploying a cloning image, cloning image collection and deployment cannot be executed four or more times.

Therefore, it is recommended not to collect cloning images from managed servers that have had cloning images deployed, but to collect them from a dedicated master server.

- As there is a chance that data will be damaged, do not perform collection or deployment of a cloning image while performing an iSCSI connection using a software initiator.

When using data disks, use the hardware initiator.

Create an L-Server for the Infrastructure Administrator

The L-Server for the infrastructure administrator is the L-Server to collect cloning images used for the entire system.

Create an L-Server for the infrastructure administrator using the L-Server template created in ["8.5 Creating L-Server Templates"](#).

In this case, perform the following configuration:

- Select "None" for images.
- Check the "Single path mode" checkbox for FC path.

For details on creating an L-Server for the infrastructure administrator using an L-Server template, refer to "10.1 Creation Using an L-Server Template" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Manual OS Installation

Install the OS and applications required for deployment.

For manual OS installation, installation by remote console is recommended after starting the MB (Management Blade) or iRMC (Remote Management Controller) screen.

Additionally, apply any required patches and other necessary settings.

Make sure that the source server operates properly after those steps.

- Check whether the DHCP client is enabled on the managed server to collect the cloning image from.
- Cloning images with the same name can be saved up until the maximum number of image versions.

When collecting a new cloning image when the maximum number of image versions has already been reached, select the cloning image to delete.

The maximum number of image versions is three by default.

For details of how to change the maximum number of image versions, refer to "3.1.4 Changing the Maximum Number of Cloning Image Versions (Physical Servers)" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- When the target of operation is a PRIMEQUEST server, confirm that boot option settings on the target server and the boot option set in BIOS are set to Legacy boot.
If either setting is UEFI, change the settings to Legacy boot.

For details on changing the boot options, refer to "3.2.10 Changing Boot Options" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

[Windows]

- Enable NetBIOS over TCP/IP
- A volume license is required for cloning, and must be entered during the installation of Resource Orchestrator Agent.

For details, refer to "2.2.1.2 Collecting and Checking Required Information" and "2.2.2 Installation [Windows/Hyper-V]" in the "Installation Guide CE".

If no volume license is entered during the agent installation, or if this information is changed after installation, edit the following license configuration file on the source server. Note that the structure and location of this file depend on the version of Windows that is being used.

- For Windows Server 2003

Installation_folder\Agent\scw\SeparateSetting\sysprep\sysprep.inf

Edit the following line to enter a valid product ID.

ProductID= *Windows product key* (*1)

*1: 5-digit values separated by hyphens

 **Example**

ProductID=11111-22222-33333-44444-55555

 **Note**

If there is a mistake in the product ID value or format, an error occurs when the collected cloning image is deployed. Make sure to enter a valid product ID when editing the definition file.

- For Windows Server 2008

Installation_folder\Agent\scw\SeparateSetting\ipadj\activation.dat

Specify the parameters in the format "parameter=value" in each line of the [ActivationInfo] section of the definition file.

Refer to the following table for details on each parameter.

Table 8.4 Structure of the Definition File

Format	Parameter	Value
KMS	.cmd.remotescript. 1.params.kmscheck (Mandatory)	KMS host search type. Select one of the following: - AUTO Automatically searches KMS hosts. - MANUAL Specify the KMS host. When "MANUAL" is selected, make sure to set .cmd.remotescript.1.params.kmsname.
	.cmd.remotescript. 1.params.kmsname	Host name (FQDN), computer name or IP address of the KMS host.
	.cmd.remotescript. 1.params.kmsport	KMS host port number. If omitted, "1688" will be set.
MAK	.cmd.remotescript. 1.params.makkey (Mandatory)	MAK key.
Common	.cmd.remotescript. 1.params.ieproxy	Host name (FQDN) and the port number of the proxy server. The host name and port number are separated by a colon (":").
	.cmd.remotescript. 1.params.password	Administrator password. An existing password setting will be displayed as an encrypted character string. To edit the password, overwrite it with plain text, delete the "encrypted=yes" line, and perform the encryption procedure indicated in the example. If this parameter is not set, the password will be re-initialized.
	encrypted	The encryption status of the Administrator password. Encryption is performed when "yes" is specified.

Format	Parameter	Value
		If this line exists, the rcxadm deployctl command does not operate.

Example

- With KMS (Automatic Search)

```
[ActivationInfo]
.cmd.remotescript.1.params.kmscheck=AUTO
.cmd.remotescript.1.params.ieproxy=proxy.activation.com:8080
.cmd.remotescript.1.params.password=PASSWORD
```

- With KMS (Manual Settings)

```
[ActivationInfo]
.cmd.remotescript.1.params.kmscheck=MANUAL
.cmd.remotescript.1.params.kmsname=fujitsu.activation.com
.cmd.remotescript.1.params.kmsport=4971
.cmd.remotescript.1.params.ieproxy=proxy.activation.com:8080
.cmd.remotescript.1.params.password=PASSWORD
```

- With MAK

```
[ActivationInfo]
.cmd.remotescript.1.params.makkey=11111-22222-33333-44444-55555
.cmd.remotescript.1.params.ieproxy=proxy.activation.com:8080
.cmd.remotescript.1.params.password=PASSWORD
```

If the Administrator password has been changed, execute the following command. The password specified in the `.cmd.remotescript.1.params.password` parameter of the definition file is changed to the encrypted string, and the line "encrypted=yes" is added to indicate that the password is encrypted.

For details, refer to "5.4 rcxadm deployctl" in the "Command Reference".

```
>"Installation_folder\Agent\bin\rcxadm" deployctl passwd -encrypt <RETURN>
```

- With MAK (Already Encrypted Password)

```
[ActivationInfo]
.cmd.remotescript.1.params.makkey=11111-22222-33333-44444-55555
.cmd.remotescript.1.params.ieproxy=proxy.activation.com:8080
.cmd.remotescript.1.params.password=xyz123456
encrypted=yes
```

[Windows]

- For physical L-Servers, specify the NIC number defined for the rack mount or tower servers decided in "[4.2.1.1 Admin LAN Network Design](#)" and "[4.2.1.3 Physical Network Design for the Public LAN and iSCSI LAN](#)" as the subscript.

Example

If the NIC number of the leftmost NIC on the back of a rack mount server is defined as "1", specify "Local area connection 1" here.

[Linux]

- For physical L-Servers, specify the number with 1 subtracted from NIC number defined for the rack mount or tower servers decided in ["4.2.1.1 Admin LAN Network Design"](#) and ["4.2.1.3 Physical Network Design for the Public LAN and iSCSI LAN"](#) as the subscript.



Example

.....
If the NIC number of the leftmost NIC on the back of a rack mount server is defined as "1", specify "eth0" here.
.....



Information

.....
The following are examples of the methods for aligning the subscript of a network interface name and NIC number of the NIC at back of the rack mount server.

For details, refer to the OS manual.

- Red Hat Enterprise Linux

Configure the MAC address of the NIC at the back of the rack mount server for HWADDR in the following file: `/etc/sysconfig/network-scripts/ifcfg-ethX`

- SLES

Use udev.
.....

Collect a Cloning Image from the L-Server after the OS is Installed

Cloning images can be collected from the L-Server after an OS is installed.

1. In the orchestration tree on the [Resource] tab of the ROR console, right-click the L-Server created in "1. Create a physical L-Server for the infrastructure administrator", and select [Cloning] - [Collect] from the popup menu.

The [Collect a Cloning Image] dialog is displayed.

2. Configure the necessary items.

The cloning image is stored in the specified image pool.

For details on collecting cloning images, refer to "11.5.1 Collecting and Registering Cloning Images" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

8.6.2 When Collecting Cloning Images from Virtual L-Servers

Use the following procedure to collect cloning images:

1. Create an L-Server for the Infrastructure Administrator

The L-Server for the infrastructure administrator is the L-Server to collect cloning images used for the entire system.

Create an L-Server for the infrastructure administrator using the L-Server template created in ["8.5 Creating L-Server Templates"](#).

- a. Select the orchestration tree in the [Resource] tab of the ROR console.
- b. Select the L-Server template in the [Template List] tab of the main panel.
- c. Click <Create>.

Select "None" for images.

- d. In the [General] tab of the [Create an L-Server] dialog, set the required items.

An L-Server without an OS installed can be created.

For details on creating an L-Server for the infrastructure administrator using an L-Server template, refer to "10.1 Creation Using an L-Server Template" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

2. Manually Install an OS

Install an OS to the L-Server for the infrastructure administrator created in step 1.

3. Collect a Cloning Image from the L-Server after the OS is Installed

Use the following procedure to collect cloning images from the L-Server after an OS is installed:

- In the orchestration tree of the [Resource] tab of the ROR console, right-click the L-Server created in step 1. and select [Cloning] - [Collect] from the popup menu.

The [Collect a Cloning Image] dialog is displayed.

- Configure the necessary items.

The cloning image is stored in the specified image pool.

For details on collecting cloning images, refer to "11.5.1 Collecting and Registering Cloning Images" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Note

Resource Orchestrator collects cloning images for virtual L-Servers using Sysprep.

When using MAK license authentication for activation of Windows Server 2008 image, Sysprep can be executed a maximum of three times.

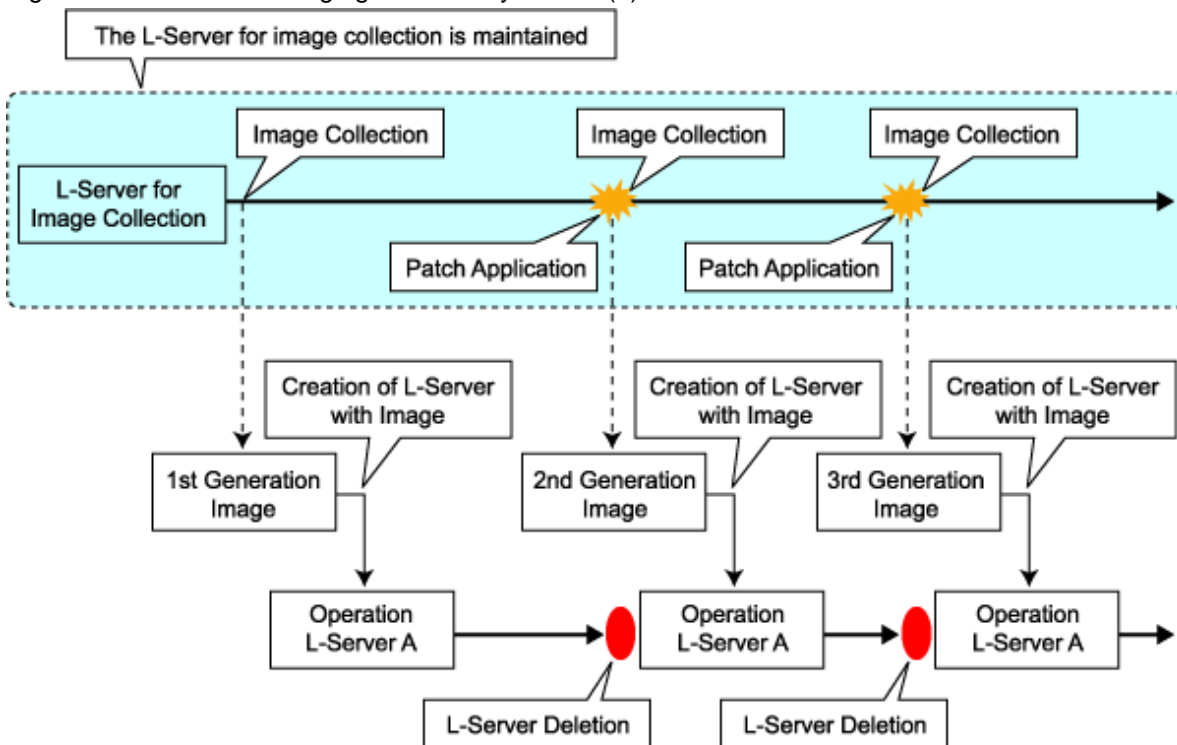
Cloning images cannot be collected four times or more from L-Servers to which cloning images have been deployed.

Collect cloning images by creating a dedicated L-Server for cloning image collection.

Operation Methods for Cloning Image Collection

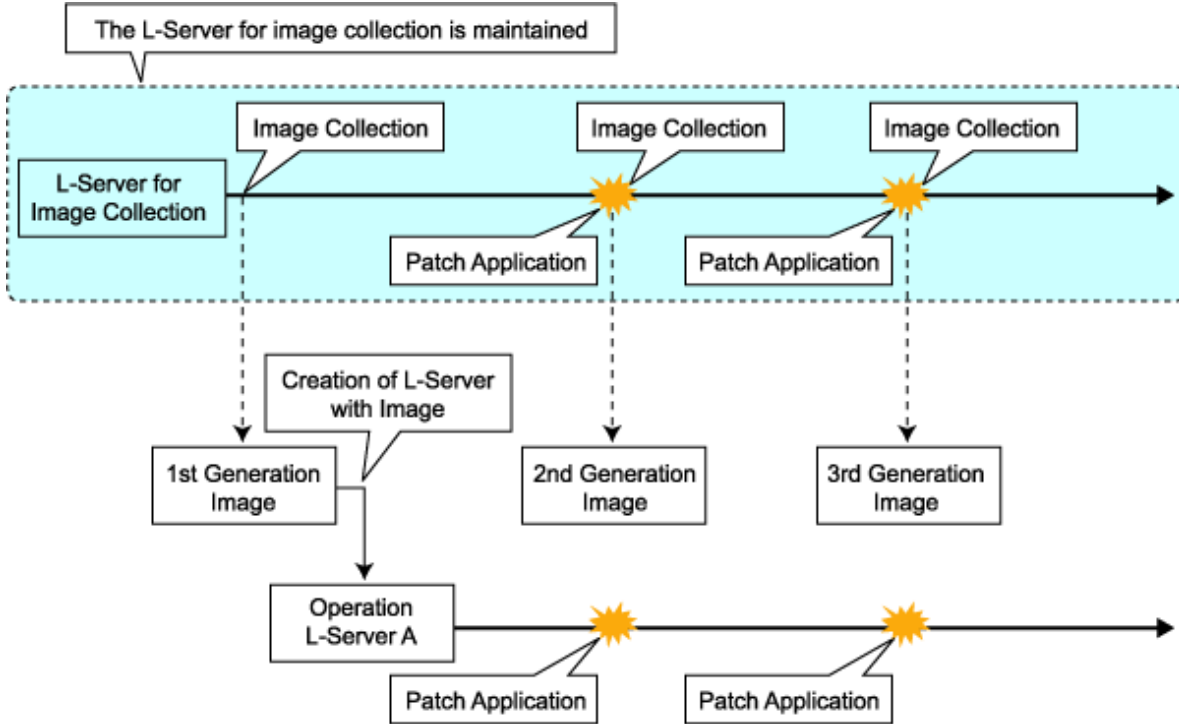
Use the following methods to collect cloning images.

Figure 8.3 When not Changing the Primary Server (1)



*As there cannot be multiple L-Servers with the same name, the old L-Server must be deleted.

Figure 8.4 When not Changing the Primary Server (2)



[VMware]

Note the following points when collecting cloning images from an L-Server that was created using a cloning image.

- As L-Servers which have not been used even once after creation do not have server specific information set, creation of L-Servers using cloning images collected from an L-Server may fail. When collecting cloning images, set the server specific information on L-Server, after starting the target L-Server.

8.6.3 When Registering a Cloning Image Created from a Physical Server in Advance to the Image Pool

Refer to "7.7.2 Physical Image Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

8.6.4 When Registering an Image (Template) Created with VM Management Software in Advance to the Image Pool

Refer to "7.7.1 Virtual Image Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Note

In the following cases, Sysprep is executed and included in the count:

- Customizing a guest OS using a template in VMware
- Template creation in SCVMM

For details on operation, refer to "Note Operation Methods for Cloning Image Collection" in "8.6.2 When Collecting Cloning Images from Virtual L-Servers".

8.7 Creating L-Platform Templates

This section explains how to create an L-Platform template.

An L-Platform template defines systems of various levels and the logical OS structure in advance.

An L-Platform template can be specified to easily create L-Platforms.

Create L-Platform templates in the [Template] tab of the ROR console.

For details on the [Template] tab, refer to "Chapter 5 Template" in the "User's Guide for Infrastructure Administrators CE".

8.8 Saving Environment Settings

This section explains how to save environment settings.

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

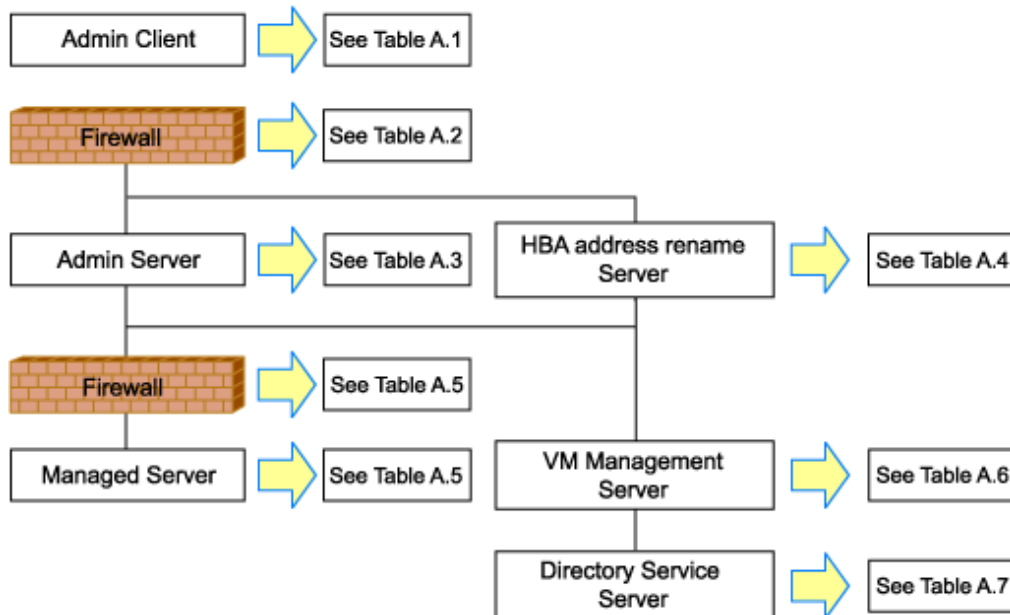
- For details the admin server backup command, refer to "Chapter 8 Backup and Restoration of Admin Servers" in the "Operation Guide CE".
- For details on the collection of troubleshooting data, refer to "4.1 Collection of Troubleshooting Data" in the "Reference Guide (Resource Management) CE".
- For details on these commands, refer to "5.1 rcxadm agtctl" and "5.7 rcxadm mgrctl" in the "Command Reference".

Appendix A Port List

This appendix explains the ports used by Resource Orchestrator.

The following figure shows the connection configuration of Resource Orchestrator components.

Figure A.1 Connection Configuration



Resource Orchestrator ports should be set up during the system configuration of each related server.

For details on how to configure the ports, refer to "3.1.2 Changing Port Numbers" or "3.2.6 Changing Port Numbers" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

If any of those ports is already used by another service, allocate a different port number.

The following tables show the port numbers used by Resource Orchestrator. Communications should be allowed for each of these ports for Resource Orchestrator to operate properly.

Table A.1 Admin Client

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
ServerView Operations Manager (*1)	Admin client	-	Variable value	Not possible	Admin server	http	3169	Not possible	tcp
						https	3170		
Interstage Business Process Manager Analytics operation management console	Admin client	-	Variable value	Not possible	Admin server	http	80	Not possible	tcp
ROR console - L-Platform - Template - Tenant Management	Admin client	-	Variable value	Not possible	Admin server	rcxctext	3500	Possible	tcp
						rcxctext2	3501	Possible	tcp

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
- Request - Usage Condition - Dashboard									
Systemwalker Runbook Automation Web console	Admin client	-	Variable value	Not possible	Admin server	http	80	Possible	tcp

*1: Required for PRIMERGY servers.

Table A.2 Firewall

Function Overview	Direction	Source		Destination		Protocol
		Server	Port	Server	Port	
ROR console	One-way	Admin client	Variable value	Admin server	23461	tcp
ServerView Operations Manager (*1)					3169	
					3170	
Interstage Business Process Manager Analytics operation management console	One-way	Admin client	Variable value	Admin server	80	tcp
ROR console - L-Platform - Template - Request - Tenant Management - Usage Condition - Dashboard	One-way	Admin client	Variable value	Admin server	3500 3501	tcp
Systemwalker Runbook Automation Web console	One-way	Admin client	Variable value	Admin server	80	tcp
ROR CE e-mail delivery (*2)	One-way	Admin server	Variable value	Mail server	25	smtp
Systemwalker Runbook Automation e-mail delivery	One-way	Admin server	Variable value	Mail server	25	smtp

Function Overview	Direction	Source		Destination		Protocol
		Server	Port	Server	Port	
(*2)						
ROR CE API	One-way	Admin client	Variable value	Admin server	8014	tcp

*1: Required for PRIMERGY servers.

*2: When a mail server is not in an admin LAN

Table A.3 Admin Server

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
ROR console	Admin client	-	Variable value	Not possible	Admin server	rcxweb	23461	Possible	tcp
ServerView Operations Manager (*1)						http	3169	Not possible	
						https	3170		
Internal control	Admin server	-	Variable value	-	Admin server (*2)	- (*3)	3172	Not possible	tcp
						nfdomain	[Windows] 23457 [Linux] 23455	Possible	tcp
						rcxmgr	23460	Possible	tcp
						rcxtask	23462	Possible	tcp
						rcxmongrel1	23463	Possible	tcp
						rcxmongrel2	23464	Possible	tcp
						rcxdb	23465	Possible	tcp
						rcxmongrel3 (*4)	23466	Possible	tcp
						rcxmongrel4 (*4)	23467	Possible	tcp
						rcxmongrel5 (*4)	23468	Possible	tcp
Monitoring and controlling resources	Admin server	-	Variable value	-	Managed server (Physical OS)	nfagent	23458	Possible	tcp

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
		-	Variable value	-	Server management unit (management blade)	snmp	161	Not possible	udp
		-	Variable value	-		snmptrap	162	Not possible	udp
		-	Variable value	-	Server management unit (Remote Management Controller)	ipmi	623	Not possible	udp
		-	Variable value	-		snmptrap	162	Not possible	udp
		-	Variable value	-		telnet	23	Not possible	tcp
ServerView Agents (*1)	Admin server	-	Variable value	-	Managed server	snmp	161	Not possible	tcp udp
	Managed server	-	Variable value	-	Admin server	snmptrap	162	Not possible	udp
Backup, restore, Cloning	Admin server	-	4972	Not possible	Managed server	-	4973	Not possible	udp
	Managed server	-	4973	Not possible	Admin server	-	4972	Not possible	udp
		bootpc	68	Not possible		bootps	67	Not possible	udp
		-	Variable value	-		pxe	4011	Not possible	udp
		-	Variable value	-		tftp	69	Not possible	udp
	Admin server	-	Variable value	-	Admin server	-	4971	Not possible	tcp
Backup, cloning (collection)	Managed server	-	14974 - 14989 (*4) 4974 - 4989 (*5)	-	Admin server	-	14974 - 14989 (*5) 4974 - 4989 (*6)	-	udp

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
Restore, cloning (deployment)	Managed server	-	Variable value	-	Admin server	-	14974 - 14989 (*5) 4974 - 4989 (*6)	-	tcp udp
Monitoring server power status	Admin server	-	-	-	Managed server	-	-	-	ICMP (*7)
VMware ESX/ESXi, vCenter Server (*8)	Admin server	-	Variable value	-	Managed server, vCenter Server	-	443	Not possible	tcp
System Center Virtual Machine Manager	Admin server	-	Variable value	-	System Center Virtual Machine Manager	-	80	Not possible	tcp
						WinRM	443 5985		
OpenDS	Admin server	-	Variable value	-	OpenDS	ldaps	1474	Possible	tcp
			Variable value	-		ldap	1473	Not possible	tcp
Active Directory	Admin server	-	Variable value	-	Active Directory	ldaps	636	Possible	tcp
Discover LAN switches	Admin server	-	-	-	LAN switch	-	-	-	ICMP
Collection of performance information	Admin server	-	-	-	Managed server (VMware ESX/ESXi)	https	443	Not possible	tcp
Collection of performance information	Managed server (Hyper-V/physical OS)	-	-	-	Admin server	-	2344	Not possible	tcp
Collection of performance information	Admin server	-	-	-	Managed server (Xen)	ssh	22	Possible	tcp
Acquisition of performance information from PDB	Admin server	-	-	-	Admin server	-	2345	Not possible	tcp

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
CMDB	Admin server	-	13300 13301 - 13322 13323 - 13325 13326 - - - - -	Not possible	Admin server	-	13300 13301 13321 - - 13324 - - 13327 13328 13331 13332 13333	Not possible	tcp
Interstage Business Process Manager Analytics rule engine	Admin server	-	-	-	Admin server	-	40320	Not possible	tcp
ROR console - L-Platform - Template - Tenant Management - Request	Admin client	-	Variable value	Not possible	Admin server	rxctext	3500	Not possible (*9)	tcp
						rxctext2	3501	Possible (*9)	tcp
Systemwalker Runbook Automation Web console	Admin client	-	Variable value	Not possible	Admin server	http	80	Possible	tcp
ROR CE management function	Admin server	-	Variable value	Not possible	Admin server	rxcfvsys	8013	Possible (*9)	tcp
ROR CE API	Admin client	-	Variable value	Not possible	Admin server	rxcfapi	8014	Possible (*9)	tcp
ROR CE for internal control	Admin server	-	Variable value	-	Admin server	rxctrestchg	3550	Not possible	tcp
	Admin server	-	Variable value	-	Admin server	rxctint	3551	Not possible	tcp
	Admin server	-	Variable value	-	Admin server	rxctdbchg	5441	Possible (*9)	tcp
	Admin server	-	Variable value	-	Admin server	rxctdbdsb	5442	Not possible	tcp

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
	Admin server	-	Variable value	-	Admin server	CORBA	8002	Possible (*9)	tcp
	Admin server	-	Variable value	-	Admin server	Servlet	Six empty port numbers are used from 9000/tcp.	Not possible	tcp
ROR CE e-mail delivery	Admin server	-	Variable value	-	Mail server	smtp	25	Possible	tcp
Systemwalker Runbook Automation e-mail delivery	Admin server	-	Variable value	-	Mail server	smtp	25	Possible	tcp
Interstage management console	Admin client	-	Variable value	-	Admin server	http	12000	Possible	tcp
Systemwalker Runbook Automation file transfer platform	Admin client	-	Variable value	-	Admin server	-	9664	Possible	tcp
Systemwalker Runbook Automation (snmp)	Admin client	-	Variable value	-	Admin server	snmp	161	Not possible	udp
Systemwalker Runbook Automation (CMDB)	Admin client	-	Variable value	-	Admin server	-	18443	Not possible	tcp
						-	18444	Not possible	tcp
Systemwalker Runbook Automation for internal control	Admin server	-	Variable value	-	Admin server	CORBA	8002	Possible (*9)	tcp
	Admin server	-	Variable value	-	Admin server	-	9657	Possible (*10)	tcp

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
	Admin server	-	Variable value	-	Admin server	-	12200	Not possible	tcp
	Admin server	-	Variable value	-	Admin server	-	12210	Not possible	tcp
	Admin server	-	Variable value	-	Admin server	-	18005	Not possible	tcp
	Admin server	-	Variable value	-	Admin server	-	18009	Not possible	tcp

*1: Required for PRIMERGY servers.

*2: For the port used by the ESC manager when coordinating with ETERNUS SF Storage Cruiser, refer to the ESC User's Guide.

For details on ports used when coordinating with the ETERNUS SF AdvancedCopy Manager Copy Control Module, refer to the "ETERNUS SF AdvancedCopy Manager Operator's Guide for Copy Control Module".

*3: ServerView Remote Connector Service. This is necessary when using VIOM coordination or when running VMware ESXi on managed servers.

*4: In Basic mode, these services are not supported.

*5: Required when the OS of the admin server is Windows.

*6: Required when the OS of the admin server is Linux.

*7: ICMP ECHO_REQUEST datagram.

*8: Required when running VMware ESX/ESXi on managed servers.

*9: Can be changed, only when installing a server.

*10: Can be changed, only when setting up a server.

Table A.4 HBA address rename Server

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
HBA address rename setup service	HBA address rename server	-	Variable value	Not possible	Admin server	rcxweb	23461	Possible	tcp
		bootps	67	Not possible	Managed server	bootpc	68	Not possible	udp
		pxe	4011	Not possible					
		tftp	69	Not possible					

Table A.5 Managed Server or Firewall

Functional Overview	Source				Destination				Protocol	
	Server	Service	Port	Modification	Server	Service	Port	Modification		
Monitoring and controlling resources	Admin server	-	Variable value	-	Managed server (Physical OS)	nfagent rcvat (*1)	23458	Possible	tcp	
					Managed server (VMware)	https	443	Not possible	tcp	
					Managed server (Xen, KVM, Solaris container)	ssh	22	Not possible	tcp	
					Managed server (Hyper-V)	RPC	135	Not possible	tcp	
						NETBIOS Name Service	137	Not possible	tcp udp	
						NETBIOS Datagram Service	138	Not possible	udp	
	System Center Virtual Machine Manager	-	Variable value	-	Managed server (Hyper-V)	RPC	135	Unused port greater than 1024	Not possible	tcp
						SMB	445	Not possible	tcp udp	
ServerView Agents (*2)	Admin server	-	Variable value	-	Managed server	snmp	161	Not possible	tcp udp	
	Managed server	-	Variable value	-	Admin server	snmptrap	162	Not possible	udp	
Backup, restore, Cloning	Admin server	-	4972	Not possible	Managed server	-	4973	Not possible	udp	
	Managed server	-	4973	Not possible	Admin server	-	4972	Not possible	udp	
		-	Variable value	-		tftp	69	Not possible	udp	

Functional Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
HBA address rename setup service	Managed server	bootpc	68	Not possible	HBA address rename server	bootps	67	Not possible	udp
						pxe	4011	Not possible	udp
		-	Variable value	-		tftp	69	Not possible	udp
VMware ESX/ESXi (*3)	Admin server	-	Variable value	-	Managed server	-	443	Not possible	tcp
Collection of performance information	Managed Server (Hyper-V/physical OS)	-	-	-	Admin server	-	2344	Not possible	tcp
Collection of performance information	Admin server	-	-	-	Managed server (Xen)	ssh	22	Not possible	tcp
Collection of performance information	Admin server	-	-	-	Managed server (VMware ESX/ESXi)	https	443	Not possible	tcp

*1: Required for SPARC Enterprise servers.

*2: Required for PRIMERGY servers.

*3: Required when running VMware ESX/ESXi on managed servers.

Table A.6 VM Management Server

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
vCenter Server	Admin server	-	Variable value	-	vCenter Server	-	443	Not possible	tcp
System Center Virtual Machine Manager	Admin server	-	Variable value	-	System Center Virtual Machine Manager	-	80	Not possible	tcp
					WinRM	443	5985		

Table A.7 Directory Service Server

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
OpenDS	Admin server	-	Variable value	-	OpenDS	ldaps	1474	Possible	tcp

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
Active Directory	Admin server	-	Variable value	-	Active Directory	ldaps	636	Possible	tcp

Table A.8 NetApp Storage

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
NetApp Storage	Admin server	-	Variable value	-	Data ONTAP	-	443	Not possible	tcp

Table A.9 EMC CLARiiON Storage

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
EMC CLARiiON Storage	Navisphere CLI	-	Variable value	-	EMC Navisphere Manager	-	443 or 2163	Not possible	tcp

Table A.10 EMC Symmetrix DMX Storage or EMC Symmetrix VMAX Storage

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
EMC Symmetrix DMX Storage or EMC Symmetrix VMAX Storage	SYMCLI	-	Variable value	-	SYMAPI Server	-	2707	Possible	tcp

Table A.11 [Hyper-V] L-Server Console

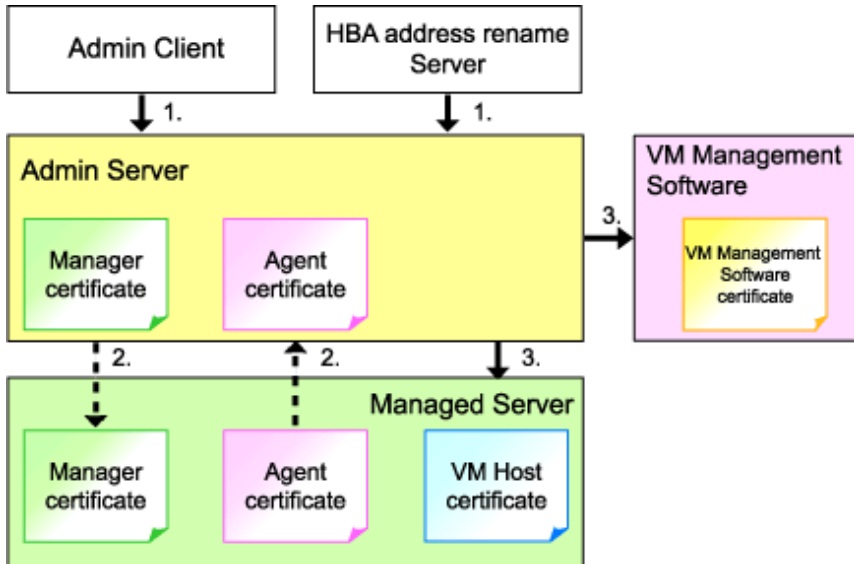
Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
Hyper-V	Admin server	-	Variable value	-	Managed server	-	2179	Possible	tcp

Appendix B HTTPS Communications

This appendix explains the HTTPS communication protocol used by Resource Orchestrator and its security features.

Resource Orchestrator uses HTTPS communication for the three cases shown in the figure below. Certificates are used for mutual authentication and for encrypting communication data.

Figure B.1 HTTPS Communication



1. Between the Admin Client and the Admin Server, or Between the HBA address rename Server and the Admin Server

The admin client and HBA address rename server automatically obtain a certificate from the admin server at each connection. This certificate is used to encrypt the communicated data.

2. Between the Admin Server and Managed Servers (Communication with Agents)

Certificates are created on both the admin server and managed servers when Resource Orchestrator (manager or agent) is first installed. Certificates of other communication targets are stored at different timings, as described below (refer to "Certificate Creation Timing"). Those certificates are used for HTTPS communication based on mutual authentication.

When re-installing the manager, its agent certificates (stored on the admin server) are renewed. Because the renewed certificates differ from those stored on the agent side (on managed servers), agents are not able to communicate with the admin server. To avoid such communication issues, it is recommended to backup agent certificates (on the admin server) before uninstalling the manager, and restore them after re-installation. When reinstalling, refer to "3.1 Manager Uninstallation" and "2.1 Manager Installation" of the "Installation Guide CE".

3. Between the Admin server and Managed servers (Communication with VM Hosts), or Between the Admin Server and VM Management Software [VMware]

The admin server obtains and stores certificates for each connection with a managed server (VM host) or VM management software. Those certificates are used to encrypt communications.

Certificate Creation Timing

Between the Admin Client and the Admin Server, or Between the HBA address rename Server and the Admin Server

Certificates are automatically obtained each time HTTPS connections are established. They are not stored on the admin server.

Between the Admin Server and Managed Servers (Communication with Agents)

The certificates used for HTTPS communication are automatically exchanged and stored on the manager and agents on the following occasions:

- When registering a managed server

- Right after re-installing and starting an agent

Between the Admin server and Managed servers (Communication with VM Hosts), or Between the Admin Server and VM Management Software [VMware]

Certificates are automatically obtained each time HTTPS connections are established. They are not stored on the admin server.

Types of Certificates

Resource Orchestrator uses the following certificates.

Between the Admin Client and the Admin Server, or Between the HBA address rename Server and the Admin Server

The public keys included in the certificates are created using X.509-based RSA encryption. These keys are 1024 bits long.

Between the Admin Server and Managed Servers (Communication with Agents)

The public keys included in the certificates are created using X.509-based RSA encryption. These keys are 2048 bits long.

Between the Admin server and Managed servers (Communication with VM Hosts), or Between the Admin Server and VM Management Software [VMware]

The public keys included in the certificates are created using X.509-based RSA encryption. These keys are 1024 bits long.

Adding the Admin Server's Certificate to Client Browsers

Resource Orchestrator automatically generates a unique, self-signed certificate for each admin server during manager installation. This certificate is used for HTTPS communication with admin clients.

Use of self-signed certificates is generally safe within an internal network protected by firewalls, where there is no risk of spoofing attacks and communication partners can be trusted. However, Web browsers, which are designed for less-secure networks (internet), will see self-signed certificates as a security threat, and will display the following warnings.

- Warning dialog when establishing a connection

When opening a browser and connecting to the admin server for the first time, a warning dialog regarding the security certificate received from the admin server is displayed.

- Address bar and Phishing Filter warning in Internet Explorer 8 or 9

The background color of the address bar will become red and the words "Certificate Error" will be displayed on its right side of the address bar of the login screen, the ROR console, and BladeViewer.

Furthermore, the Phishing Filter may show a warning on the status bar.

When using Internet Explorer 8 or 9, the above warnings can be disabled by creating a certificate for the admin server's IP address or host name (FQDN) that is specified in the address bar's URL, and installing it to the browser.

On the admin server, a certificate for "localhost" is automatically created during installation of the manager.

When using other servers as admin clients, use the following procedure to install the admin server's certificate on each client.

Therefore, the certificate creation step in the following procedure can be skipped when using the admin server as an admin client. In that case, use "localhost" in the URL and proceed to step 2.

1. Create a certificate
 - a. Open the command prompt on the admin server.
 - b. Execute the following command to move to the installation folder.

[Windows]

```
>cd "Installation_folder\Manager\sys\apache\conf" <RETURN>
```

[Linux]

```
# cd /etc/opt/FJSVrcvmr/sys/apache/conf <RETURN>
```

- c. After backing up the current certificate, execute the certificate creation command bundled with Resource Orchestrator (openssl.exe).

When using the -days option, choose a value (number of days) large enough to include the entire period for which you plan to use Resource Orchestrator. However, the certificate's expiration date (defined by adding the specified number of days to the current date) should not go further than the 2038/1/19 date.

Example

When the Manager is installed in the "C:\Fujitsu\ROR" folder, and generating a certificate valid for 15 years (or 5479 days, using the -days 5479 option)

[Windows]

```
>cd "C:\Fujitsu\ROR\Manager\sys\apache\conf" <RETURN>
>..\..\bin\rcxmgrctl stop <RETURN>
>copy ssl.crt\server.crt ssl.crt\server.crt.org <RETURN>
>copy ssl.key\server.key ssl.key\server.key.org <RETURN>
>..\bin\openssl.exe req -new -x509 -nodes -out ssl.crt\server.crt -keyout ssl.key\server.key -days 5479 -
config openssl.cnf <RETURN>
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'ssl.key\server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []: <RETURN>
State or Province Name (full name) []: <RETURN>
Locality Name (eg, city) [Kawasaki]: <RETURN>
Organization Name (eg, company) []: <RETURN>
Organizational Unit Name (eg, section) []: <RETURN>
Common Name (eg, YOUR name) [localhost]: IP_address or hostname (*1) <RETURN>
Email Address []: <RETURN>
>..\..\bin\rcxmgrctl start <RETURN>
```

[Linux]

```
# cd /etc/opt/FJSVrcvmr/sys/apache/conf <RETURN>
# /opt/FJSVrcvmr/bin/rcxmgrctl stop <RETURN>
# cp ssl.crt/server.crt ssl.crt/server.crt.org <RETURN>
# cp ssl.key/server.key ssl.key/server.key.org <RETURN>
# /opt/FJSVrcvmr/sys/apache/bin/openssl req -new -x509 -nodes -out ssl.crt/server.crt -keyout ssl.key/
server.key -days 5479 -config /opt/FJSVrcvmr/sys/apache/ssl/openssl.cnf <RETURN>
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'ssl.key/server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
```

```

There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []: <RETURN>
State or Province Name (full name) []: <RETURN>
Locality Name (eg, city) [Kawasaki]: <RETURN>
Organization Name (eg, company) []: <RETURN>
Organizational Unit Name (eg, section) []: <RETURN>
Common Name (eg, YOUR name) [localhost]: IP_address_or_hostname (*1) <RETURN>
Email Address []: <RETURN>

# /opt/FJSVrcvvr/bin/rcxmgrctl start <RETURN>

```

*1: Enter the IP address to be entered in the Web browser or the host name (FQDN).



Example

```

IP address: 192.168.1.1
Host name: myhost.company.com

```

2. Add the certificate to the Web browser

Open the Resource Orchestrator login screen, referring to "[7.1 Login](#)".

When opening the ROR console, enter the same IP address or host name (FQDN) as that used to generate the certificate in the previous step. Once the login screen is displayed, perform the following operations.

- a. Open the [Certificate] dialog.

For Internet Explorer 8 and 9, open the "Certificate is invalid dialog" by clicking the "Certificate Error" displayed in the address bar. This will open an "Untrusted Certificate" or "Certificate Expired" message.
Click the "View certificates" link displayed at the bottom of this dialog.
- b. Confirm that the "Issued to" and "Issued by" displayed in the [Certificate] dialog are both set to the IP address or host name (FQDN) used to generate the certificate.
- c. In the [Certificate] dialog, click <Install Certificate>.

The [Certificate Import Wizard] dialog is displayed.
- d. Click <Next>>.
- e. Select "Place all certificates in the following store".
- f. Click <Browse>.

The [Select Certificate Store] dialog is displayed.
- g. Select "Trusted Root Certification Authorities".
- h. Click <OK>.
- i. Click <Next>>.
- j. Check that "Trusted Root Certification Authorities" is selected.
- k. Click <Finish>.
- l. Restart the Web browser.

If multiple admin clients are used, perform this operation on each admin client.

Note

Enter the IP address or host name (FQDN) used to generate the certificate in the Web browser's URL bar. If the entered URL differs from that of the certificate, a certificate warning is displayed.

Example

A certificate warning is displayed when the following conditions are met.

- The entered URL uses an IP address while the certificate was created using a host name (FQDN)
- The admin server is set with multiple IP addresses, and the entered URL uses an IP address different from that used to generate the certificate

In environments where the admin server is Windows, and multiple IP addresses are used, when a login window with a different URL from the address bar's URL in which the IP address or host name (FQDN) is specified, the warning may not disappear. As a corrective action, set a higher priority for binding of the network adapter used on the admin LAN than for other network adapters.

Example

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

1. Click <Start>, and then click [Control Panel].
2. When [Network and Internet] is displayed, click this item.
When [Network and Internet] is not displayed, proceed to the next step without clicking.
3. Click [Network and Sharing Center], and click [Change adapter settings] in the left side of the window.
4. Click [Advanced Settings] in the [Advanced] menu.
When [Advance settings] is not displayed, push the Alt key.
5. From the list of [Connections] in the [Adapters and Bindings] tab, click the target network adapter, and the "Up" or "Down" buttons to change the order of priority of connections.
6. Click <OK>.

Appendix C Hardware Configuration

This appendix explains how to configure hardware.

C.1 Connections between Server Network Interfaces and LAN Switch Ports

Configuring VLAN settings on internal LAN switch ports requires an understanding of the network connections between LAN switches and physical servers (between LAN switch ports and the network interfaces mounted in each server).

This appendix shows which network interfaces (on PRIMERGY BX600 server blades) are connected to which LAN switch blade ports. For servers other than PRIMERGY BX servers, refer to the server manual for details on the connections between server blades and LAN switch blades.

The connections between server blades and LAN switch blades are shown in the following table.

Table C.1 Connections between Server Blades and LAN Switch Blades (PG-SW107)

NIC index	NIC placement (on a server blade)	Connected port number (on a LAN switch blade)
Index 1	Onboard LAN1	NET1 port "3N-2"
Index 2	Onboard LAN2	NET2 port "3N-2"
Index 3	Onboard LAN3	NET1 port "3N-1"
Index 4	Onboard LAN4	NET2 port "3N-1"
Index 5	Onboard LAN5	NET1 port "3N"
Index 6	Onboard LAN6	NET2 port "3N"
Index 7	LAN expansion card LAN1	NET3 port "N"
Index 8	LAN expansion card LAN2	NET4 port "N"

N: Slot number of the connected server blade

PG-SW104/105/106 is mounted in NET3 and NET4.

For details, refer to the chassis hardware manual.

Table C.2 Connections between Server Blades and LAN Switch Blades (PG-SW104/105/106)

NIC index	NIC placement (on a server blade)	Connected port number (on a LAN switch blade)
Index 1	Onboard LAN1	NET1 port "N"
Index 2	Onboard LAN2	NET2 port "N"
Index 3	LAN expansion card LAN1	NET3 port "N"
Index 4	LAN expansion card LAN2	NET4 port "N"
Index 5	-	-
Index 6	-	-
Index 7	-	-
Index 8	-	-

-: None

N: Slot number of the connected server blade



VLAN settings cannot be configured on the following devices.

- PRIMERGY BX600 Ethernet Blade Panel 1Gb 10/6 (IBP 10/6) and 30/12 (IBP 30/12)
- A LAN switch directly connected to a PRIMERGY BX 600 LAN pass-thru blade
- A LAN switch directly connected to servers other than PRIMERGY BX servers

LAN switch blade product names may differ between countries.

This appendix refers to the product names used in Japan.

The following table shows product references often used in other countries.

Reference	Product Name
PG-SW104	PRIMERGY BX600 Switch Blade (1Gbps) PRIMERGY BX600 Ethernet Switch 1GB 10/6(SB9)
PG-SW105	PRIMERGY BX600 Switch Blade (10Gbps) PRIMERGY BX600 Ethernet Switch 1GB 10/6+2(SB9)
PG-SW106	Cisco Catalyst Blade Switch 3040 PRIMERGY BX600 Ethernet Switch 1GB 10/6(Cisco CBS 3040)
PG-SW107	PRIMERGY BX600 Switch Blade (1Gbps) PRIMERGY BX600 Ethernet Switch 1GB 30/12(SB9F)

C.2 WWN Allocation Order during HBA address rename Configuration

This section explains the order in which WWNs are allocated during configuration of HBA address rename.

With HBA address rename, as WWNs are allocated to the I/O addresses of HBAs in descending order, the order may not match the port order listed in the HBA.

When specifying the locations for WWN allocation, check the I/O addresses of HBAs.

The I/O addresses of HBAs can be confirmed using tools provided by HBA vendors or FC-HBA BIOS.

- For blade servers



For a blade server with an HBA with 2 ports, allocation is performed as follows:

```

WWN value provided by "I/O Virtualization Option": 20:00:00:17:42:51:00:00
WWNN value for ports 1 and 2 of the HBA           : 20:00:00:17:42:51:00:00
WWPN value for HBA port 1                         : 9:00:00 PM:17:42:51:00:00
WWPN value for HBA port 2                         : 10:00:00 PM:17:42:51:00:00

```

- For rack mount or tower servers

For the PCI slots of rack mount or tower servers, WWNs are allocated in the following order:

```

PRIMERGY RX200 S4   slot2 -> slot1 -> slot3
PRIMERGY RX200 S5   slot1 -> slot2 -> slot3
PRIMERGY RX300 S4   slot5 -> slot6 -> slot1 -> slot7 -> slot4 -> slot2 -> slot3
PRIMERGY RX300 S5   slot2 -> slot3 -> slot4 -> slot5 -> slot6 -> slot7 -> slot1
PRIMERGY RX600 S4   slot6 -> slot3 -> slot4 -> slot1 -> slot2 -> slot7 -> slot5
PRIMERGY TX300 S4   slot5 -> slot6 -> slot1 -> slot7 -> slot4 -> slot2 -> slot3

```

In a single PCI slot, allocate WWNs in the following order:

port 2 -> port 1

Example

When one port HBAs are mounted in slot 2 and slot 3 of an RX600 S4, WWNs are allocated in the following order:

slot 3 -> slot 2

```
WWN value provided by "I/O Virtualization Option": 20:00:00:17:42:51:00:00
WWNN value for slots 2 and 3 of the HBA           : 20:00:00:17:42:51:00:00
WWPN value for HBA slot 2                         : 22:00:00:17:42:51:00:00
WWPN value for HBA slot 3                         : 21:00:00:17:42:51:00:00
```

When two port HBAs are mounted in slot 2 of an RX600 S4, WWNs are allocated in the following order:

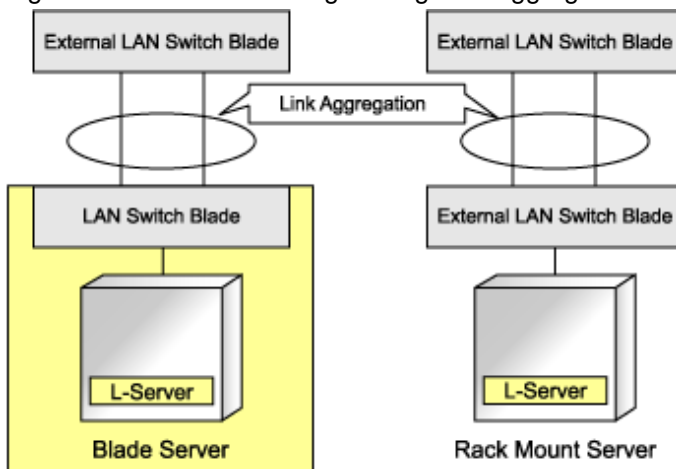
slot 2 (port 2) -> slot 2 (port 1)

```
WWN value provided by "I/O Virtualization Option": 20:00:00:17:42:51:00:00
WWNN value for ports 1 and 2 of the HBA           : 20:00:00:17:42:51:00:00
WWPN value for HBA port 1                         : 10:00:00 PM:17:42:51:00:00
WWPN value for HBA port 2                         : 9:00:00 PM:17:42:51:00:00
```

C.3 Using Link Aggregation

This appendix explains the procedure to use Resource Orchestrator and link aggregation at the same time. By using link aggregation between switches, it is possible to increase the bandwidth and reliability of the network used by L-Servers.

Figure C.1 Connection Image Using Link Aggregation



C.3.1 Configuration of Link Aggregation and a Server

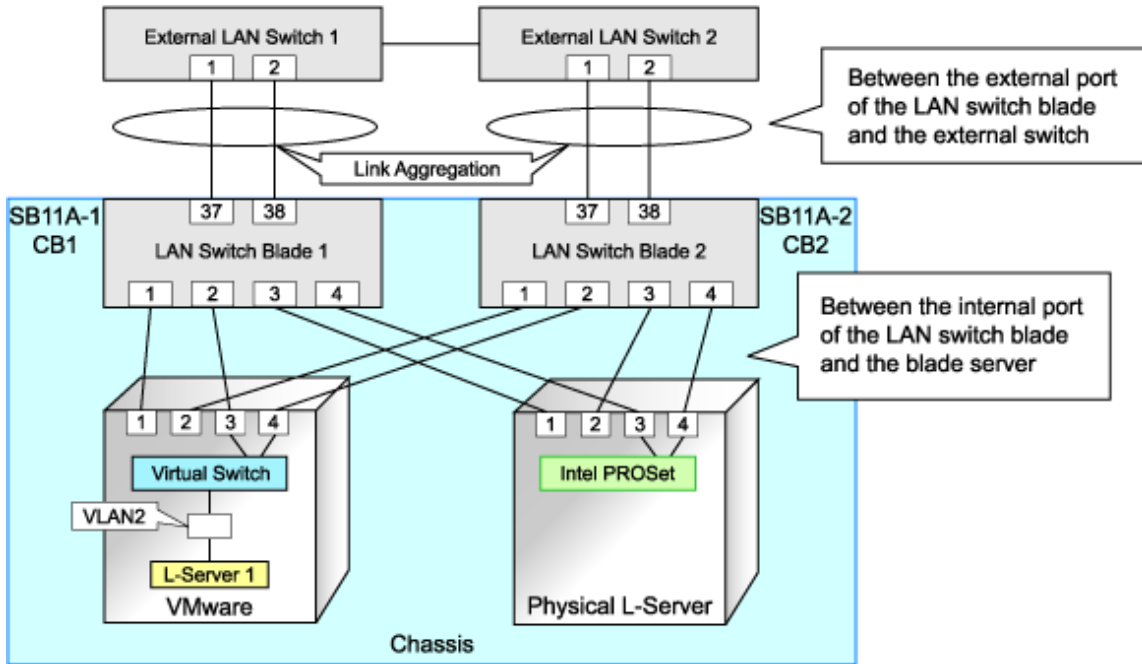
This section explains about link aggregation configuration.

Configuration for Blade Servers

Connect an external port of a LAN switch blade and an external port using link aggregation. Usually, link aggregation is not used for connecting an internal port of a LAN switch blade and a blade server. Configure the NIC on the server in active/standby and connect.

In "Figure C.2 Configuration Example for Blade Servers", Intel PROSet is used for configuring the NIC on a physical L-Server in active/standby. In VMware, the NICs in a VM host are configured in active/standby using VM host functions.

Figure C.2 Configuration Example for Blade Servers



Configuration for Rack Mount Servers

Usually, link aggregation is not used between rack mount servers and switches that are directly connected to rack mount servers. Link aggregation can be used between switches.

C.3.2 Preparations

Preparations should be performed by infrastructure administrators.

Defining VLAN IDs for Network Resources

Define a VLAN ID for use on Resource Orchestrator. For "Figure C.2 Configuration Example for Blade Servers" in "C.3.1 Configuration of Link Aggregation and a Server", define VLAN IDs for ports 37 and 38.

Link Aggregation Configuration for LAN Switch Blades

This section explains how to configure link aggregation for LAN switch blades.

When Using LAN Switch Blade PY CB Eth Switch/IBP 10Gb 18/8

The following settings are possible for PY CB Eth Switch/IBP 10Gb 18/8 LAN switch blades.

- VLAN settings to the link aggregation configuration port
- Setting link aggregation groups in the external ports of network resources, and VLAN auto-configuration

The following shows the procedure for setting link aggregation in PY CB Eth Switch/IBP 10Gb 18/8 LAN switch blades.

1. Set link aggregation for the external port of the LAN switch blade.

From the admin console of the LAN switch blade, configure link aggregation for the LAN switch blade and enable LLDP.

Do not set VLAN if VLAN auto-configuration is to be used.

Refer to the manual for the LAN switch blade for information on how to configure it.

2. Configure link aggregation and a VLAN on the adjacent network devices.

Refer to the manual for the network device for information on how to configure it.

3. Reflect the configuration information for the link aggregation of the LAN switch blade on this product.

Right-click the target LAN switch blade from the ROR console server resource tree.

In the displayed menu, click <Update> and reflect the configuration information for the link aggregation of the LAN switch blade on this product.

4. Confirm that the configuration information for the link aggregation of the LAN switch blade has been reflected on this product.

Select the target LAN switch blade from the server resource tree on the ROR console, and display the [Resource Details] tab.

Check if the link aggregation configuration information configured in 1. is displayed in "Link Aggregation Group" on the [Resource Details] tab.

When the link aggregation configuration information configured in 1. is not displayed, check the settings are configured in 1. and 2., and then perform 3. again.

5. Create a network resource.

Refer to "[Create Network Resources](#)" in "[C.3.3 Operating Resource Orchestrator](#)" for information on creating network resources.

When Using a LAN Switch Blade Other Than PY CB Eth Switch/IBP 10Gb 18/8

The following shows the procedure for setting link aggregation in LAN switch blades other than PY CB Eth Switch/IBP 10Gb 18/8.

1. Set link aggregation for the external port of the LAN switch blade.
Refer to the manual for the network device for information on how to configure it.
2. Create a network resource.
Refer to "[Create Network Resources](#)" in "[C.3.3 Operating Resource Orchestrator](#)" for information on creating network resources.

Example settings for link aggregation settings to the LAN switch blade (for PY CB Eth Switch/IBP 1Gb 36/8+2 LAN switch blades)

The following shows the procedure for setting link aggregation in a PY CB Eth Switch/IBP 1Gb 36/8+2 LAN switch blade.

1. Create a link aggregation (port channel) group.
2. Set the port channel group's mode to LACP.
3. Include the uplink port of the LAN switch blade used in link aggregation in the port channel.
4. Create a VLAN in the switch.
5. Include the port channel into the created VLAN.

Log in to the two LAN switch blades and execute the command to configure them.

The following is an example of how to set the link aggregation for 1 LAN switch blade. For details, refer to the manual of the LAN switch blade.

- Create a port channel and configure external ports.

```
#port-channel pc-1 <RETURN>          Create port channel
Interface BX900-CB1/1/1 created for port-channel pc-1
#interface BX900-CB1/1/1 <RETURN>    Configure a port channel
#no staticcapability <RETURN>      Configure static link aggregation
(for LACP)

#exit <RETURN>
#interface range 0/37 - 0/38 <RETURN>  Configure an uplink port
#channel-group BX900-CB1/1/1 <RETURN>

#exit <RETURN>
#exit <RETURN>
#show port-channel all <RETURN>      Check the configuration
Port- Link
Log. Channel Adm. Trap STP Mbr Port Port
```

Intf	Name	Link	Mode	Mode	Mode	Type	Lb	Ports
Speed	Active							
-----	----	-----	----	-----	-----	-----	-----	-----
BX900-CB1/1/1	pc-1	Down	En.	En.	En.	St.	SDM	BX900-CB1/0/37 Auto
False								
								BX900-CB1/0/38 Auto
False								

Confirm that the port channel has been created and the specified port is configured properly.

- Create a VLAN

```
#configure <RETURN>
#vlan database <RETURN>
#vlan 2 <RETURN>          Create VLAN ID2
#exit <RETURN>
#exit <RETURN>
#show vlan <RETURN>
VLAN ID  VLAN Name  VLAN Type  Interface(s)
-----  -
2         VLAN0002  Static
```

Confirm that VLAN ID2 has been created.

- Configure a port channel on the VLAN

```
#configure <RETURN>
#interface BX900-CB1/1/1 <RETURN>
#switchport allowed vlan add 2 tagging <RETURN>
#exit <RETURN>
#exit <RETURN>
#show vlan id 2 <RETURN>

VLAN ID: 2
VLAN Name: VLAN0002
VLAN Type: Static
Interface      Current  Configured  Tagging
-----
BX900-CB1/1/1  Include  Autodetect  Tagged
```

Confirm that the port channel is configured properly on the VLAN.

Example settings for link aggregation settings to the LAN switch blade (for PY CB Eth Switch/IBP 10Gb 18/8 LAN switch blades)

The following shows the procedure for setting link aggregation in PY CB Eth Switch/IBP 10Gb 18/8 LAN switch blades.

1. Set the external ports (uplink ports) of all of the LAN switch blades included in the link aggregation so that they use all the same VLAN.
2. Set link aggregation groups for all of the external ports included in the link aggregation.
3. Enable the LLDP of all of the external ports included in the link aggregation.
When setting LLDP, make the setting for "VLAN name information" invalid. Make the other settings valid.

Log in to the two LAN switch blades and execute the command to configure them.

The following is an example of how to set the link aggregation for 1 LAN switch blade. For details, refer to the manual of the LAN switch blade.

- Link aggregation of two external ports (0/19 and 0/20)

```
# configure <RETURN>
(config)# interface range 0/19-0/20 <RETURN>
(config-if)# vlan untag 10 <RETURN>
(config-if)# vlan tag 20 <RETURN>
(config-if)# type linkaggregation 1 <RETURN>
```

- Enable the LLDP of the external port

```
(config-if)# lldp mode enable <RETURN>
(config-if)# lldp info vlan-name disable <RETURN>
(config-if)# exit <RETURN>
(config)# save <RETURN>
```

Note

- For a PY CB Eth Switch/IBP 10Gb 18/8 LAN switch blade, if the member ports of the link aggregation meet any of the following conditions, this product will be unable to recognize the information for the member ports of the link aggregation.
 - When the LLDP of link aggregation member port is disable or receive
 - When the VLAN of the member ports of the link aggregation are different to other member ports
 - When the "VLAN Name" of the LLDP of the member ports of the link aggregation is enabled

Example of LAN switch blade settings when the LLDP is disable

```
(config)# interface range 0/19-0/20 <RETURN>
(config-if)# vlan untag 10 <RETURN>
(config-if)# vlan tag 20 <RETURN>
(config-if)# type linkaggregation 1 <RETURN>
(config-if)# lldp mode disable <RETURN>
(config-if)# exit <RETURN>
(config)# save <RETURN>
```

Link aggregation information recognized by this product

Link aggregation group name: linkaggregation1

Member port :-

C.3.3 Operating Resource Orchestrator

Create Network Resources

Network resources should be created by infrastructure administrators.

For details on parameters to configure, refer to "7.3 Network Resources" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Create an L-Server

L-Servers should be created by infrastructure administrators.

Specify the created network resources and create an L-Server.

Communication Checks between L-Servers and External Devices

Communication between L-Server and devices outside the chassis should be checked by tenant administrators. Enable the TCP/IP protocol. Link aggregation configuration can be used to check whether L-Servers can operate.

Appendix D Design and Configuration when Creating a Physical L-Server

This appendix explains how to perform configuration when creating a physical L-Server.

D.1 System Configuration

This section explains system configuration when creating a physical L-Server.

Prerequisites

To create a physical L-Server, Virtual I/O using VIOM or HBA address rename is required.

For details on VIOM, refer to the ServerView Virtual-IO Manager manual.

For details about the HBA address rename, refer to "[8.2 HBA address rename Settings](#)".

Usage methods of VIOM and HBA address rename differ depending on the hardware of managed servers used to configure a physical L-Server.

- Blade Servers
Use VIOM.
- Rack Mount Servers
Use HBA address rename.



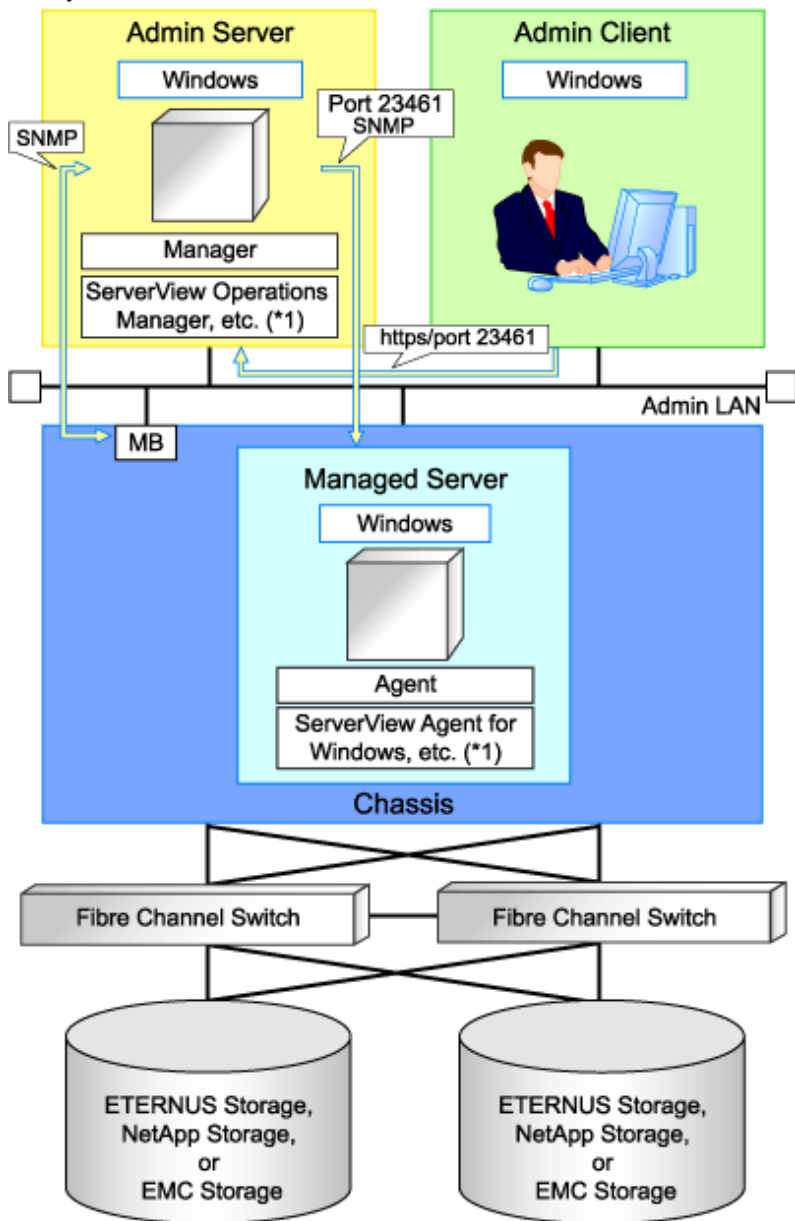
When using iSCSI boot, VIOM is required in the server environment.

Example of System Configuration using VIOM's Virtual I/O

An example system configuration for L-Server creation using Virtual I/O by VIOM is given below.

Install ServerView Virtual-IO Manager on the admin server.

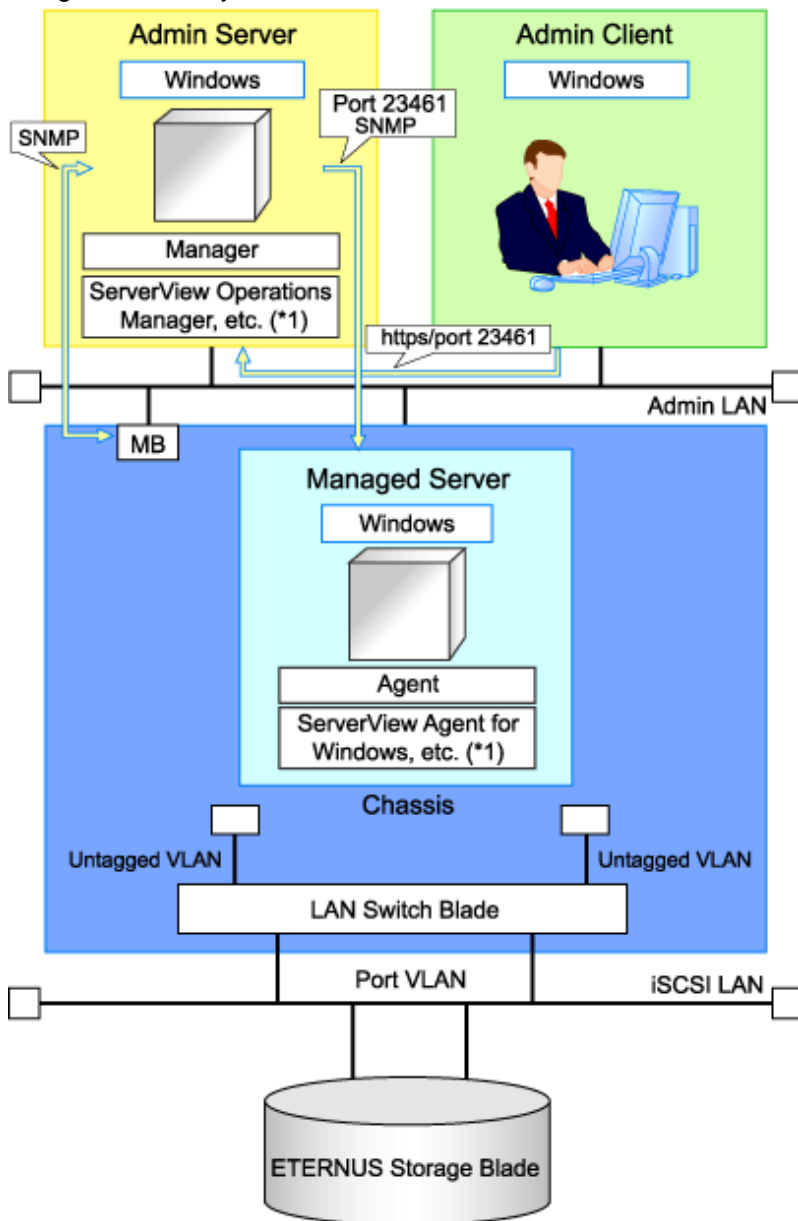
Figure D.1 Example of System Configuration for L-Server Creation in a SAN Storage Environment using Virtual I/O by VIOM



MB: Management Blade

*1: For details on required software, refer to "[1.4.2.2 Required Software](#)".

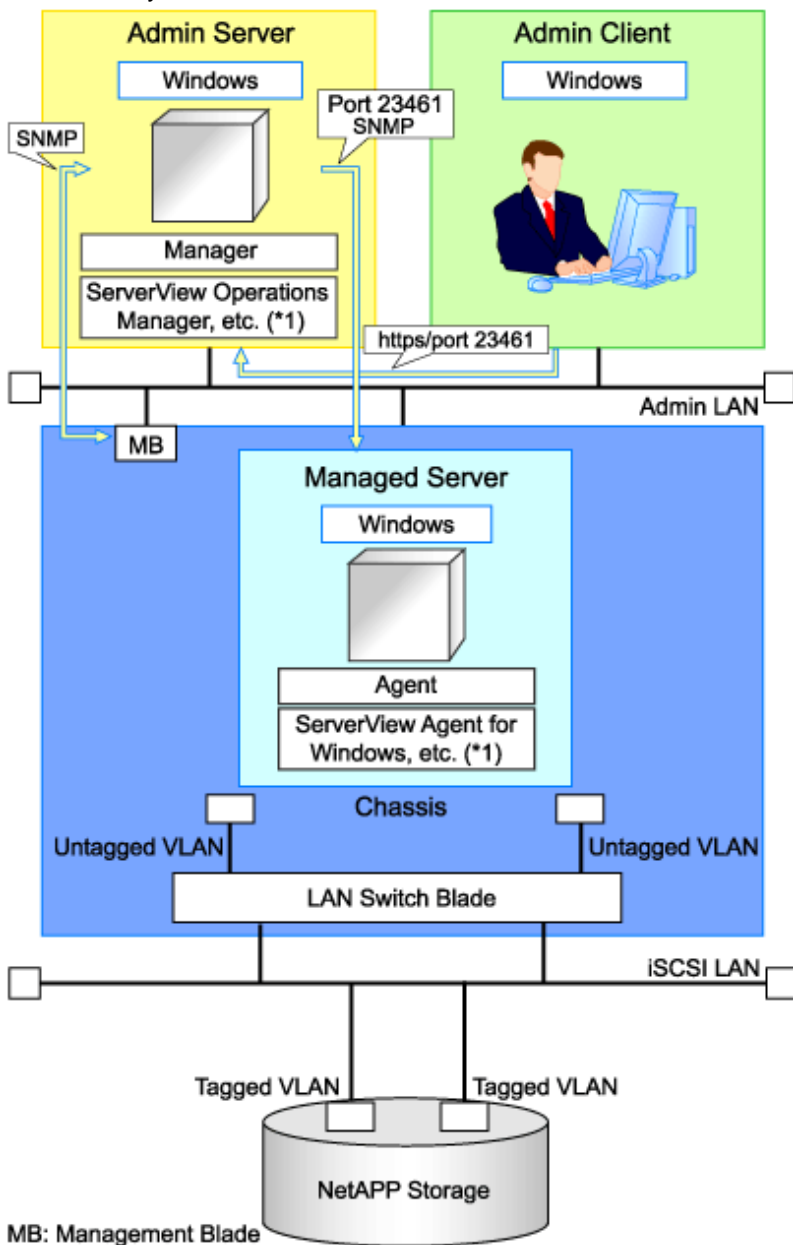
Figure D.2 Example of System Configuration for L-Server Creation in an ETERNUS-iSCSI Storage Environment using Virtual I/O by VIOM



MB: Management Blade

*1: For details on required software, refer to "[1.4.2.2 Required Software](#)".

Figure D.3 Example of System Configuration for L-Server Creation in a NetApp-iSCSI Storage Environment using Virtual I/O by VIOM



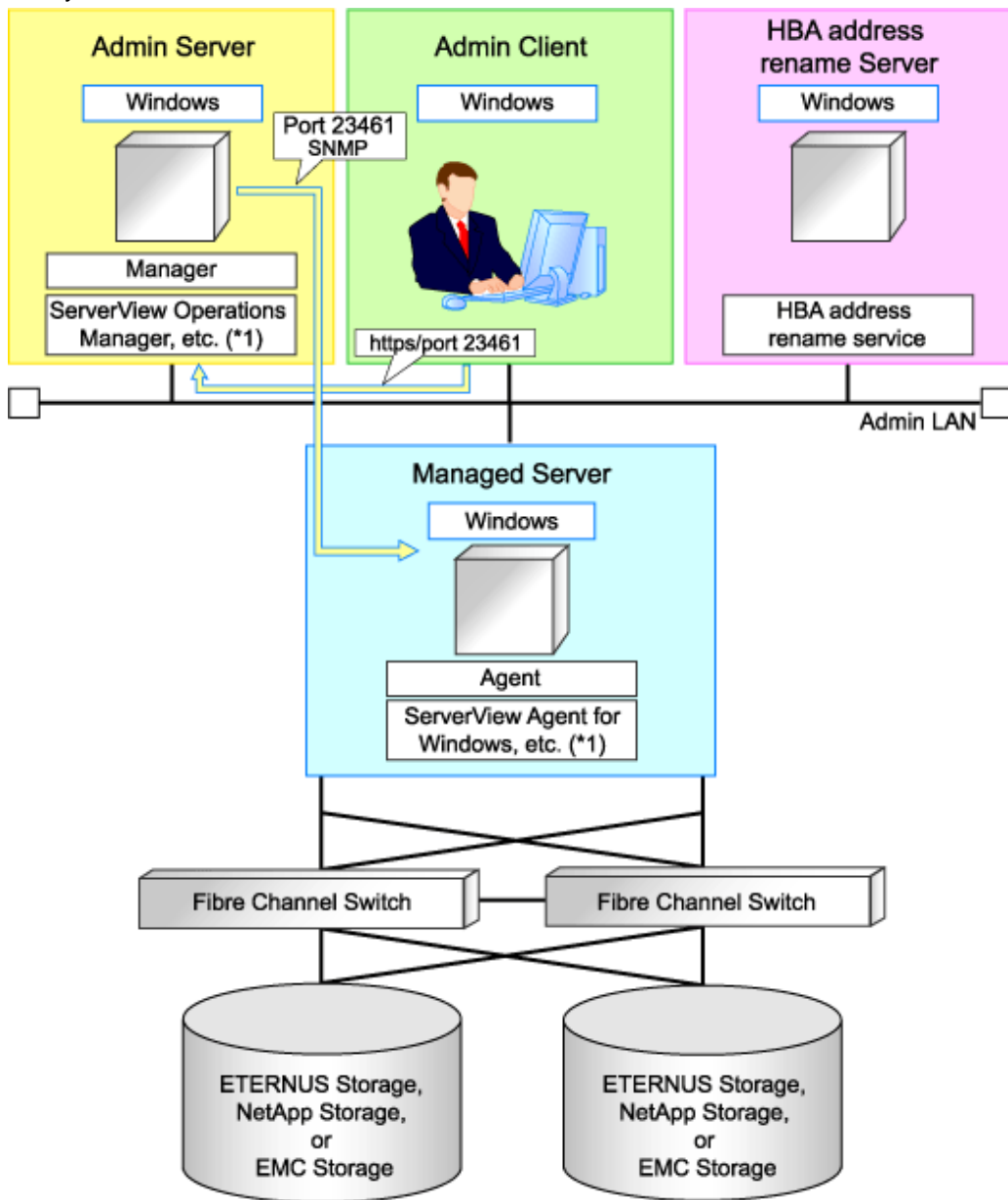
*1: For details on required software, refer to "1.4.2.2 Required Software".

Example of System Configuration Using Virtual I/O by HBA address rename

An example of system configuration for L-Server creation using Virtual I/O by HBA address rename is given below.

Prepare a server to configure the HBA address rename setup service.

Figure D.4 Example of System Configuration for L-Server Creation in a SAN Storage Environment Using Virtual I/O by HBA address rename

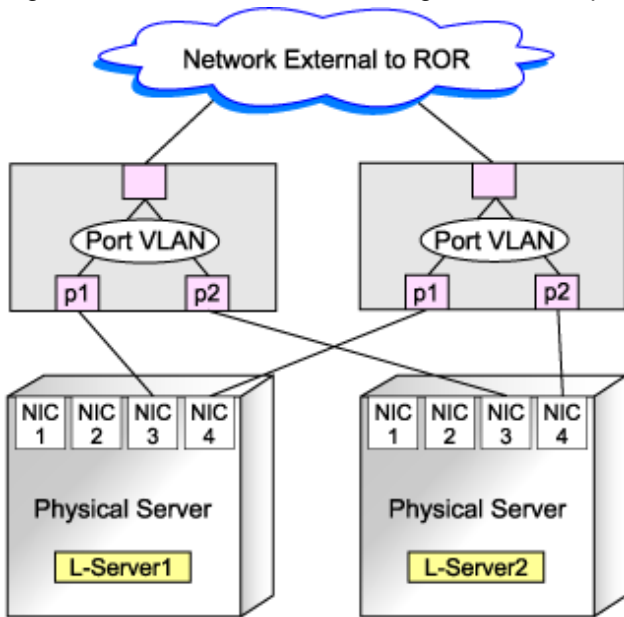


*1: For details on required software, refer to "1.4.2.2 Required Software".

Network Configuration Example

An example of network configuration when a physical server is used as an L-Server is given below:

Figure D.5 LAN Switch Blade Configuration Example Using Network Resources



D.2 Pre-setup Preparations (Servers)

This section explains preparations for server setup when creating a physical L-Server.

When creating a physical L-Server, it is necessary to configure the following VIOM settings as well as performing the server environment definition and configuration given in "[4.1.1.1 Preparations for Server Environments](#)".

When using Virtual I/O by VIOM

- Install VIOM

For details on how to install VIOM, refer to the ServerView Virtual-IO Manager manual.

Note

When installing VIOM, do not configure virtual MAC addresses or Range for WWNs.

- Settings for ServerView Operations Manager

Add blade servers for use as managed servers to the ServerView server list.

For details, refer to the ServerView Operations Manager manual.

Note

Configure a valid FC-HBA BIOS in the system BIOS.

Configure FC-HBA BIOS, referring to "[4.1.2 Configuring the Server Environment](#)".

- When using HBA address rename for SAN boot

When using Virtual I/O by HBA address rename

- BIOS Settings of Managed Servers

Refer to "[4.1.2 Configuring the Server Environment](#)".

- When using HBA address rename for SAN boot

Configuration Using PXE Boot

When using PXE boot, the server for boot must be located and configured.



Note

PXE boot is unavailable on networks that use tagged VLAN settings.

Do not configure tagged VLANs for PXE boot servers.

D.3 Pre-setup Preparations (Storage)

This section explains how to prepare storage when configuring a physical server for use as an L-Server.

This section explains details on the configuration necessary when using storage units from a physical L-Server.

Prerequisites When Creating L-Servers Using Physical Servers

For details, refer to "[1.2.8 Simplifying Storage](#)".

Regarding Storage Configuration

For details, refer to "[1.2.8 Simplifying Storage](#)".

Preparations for Storage Environments

The settings necessary when using storage environments are performed using the following flow.

1. Storage Unit Configuration

- When using ETERNUS storage

Refer to "[ETERNUS Storage Configuration](#)" of "[D.3.1 When Using ETERNUS Storage](#)".

- When Using NetApp FAS Series/V Series

Refer to "[NetApp FAS Storage Configuration](#)" of "[D.3.2 When Using NetApp FAS Storage](#)".

- When using EMC CLARiiON storage

Refer to "[EMC CLARiiON Storage Configuration](#)" of "[D.3.3 When Using EMC CLARiiON Storage](#)".

- When Using EMC Symmetrix DMX Storage or EMC Symmetrix VMAX Storage

Refer to "[Configuration of EMC Symmetrix DMX Storage or EMC Symmetrix VMAX Storage](#)" of "[D.3.4 When Using EMC Symmetrix DMX Storage or EMC Symmetrix VMAX Storage](#)".

2. Fibre Channel Switch Configuration

- When Connecting ETERNUS Storage to Fibre Channel Switches

Refer to "[When Connecting ETERNUS Storage to Fibre Channel Switches](#)" of "[D.3.1 When Using ETERNUS Storage](#)".

- When Connecting NetApp Storage to Fibre Channel Switches

Refer to "[When Connecting NetApp Storage to Fibre Channel Switches](#)" of "[D.3.2 When Using NetApp FAS Storage](#)".

- When Connecting EMC CLARiiON Storage to Fibre Channel Switches

Refer to "[When Connecting EMC CLARiiON Storage to Fibre Channel Switches](#)" of "[D.3.3 When Using EMC CLARiiON Storage](#)".

- When Using EMC Symmetrix DMX Storage or EMC Symmetrix VMAX Storage with Fibre Channel Switches

Refer to "When Connecting EMC Symmetrix DMX Storage or EMC Symmetrix VMAX Storage to Fibre Channel Switches" of "D.3.4 When Using EMC Symmetrix DMX Storage or EMC Symmetrix VMAX Storage".

D.3.1 When Using ETERNUS Storage

This section explains how to configure ETERNUS storage.

ETERNUS Storage Configuration

Resource Orchestrator manages only ETERNUS registered on ESC. Register the target ETERNUS on ESC.

For details on how to register to ESC, refer to the "ETERNUS SF Storage Cruiser User's Guide" of version 14.2 or later.

URL: http://software.fujitsu.com/jp/manual/manualindex/P10000250e.html (As of February 2012)
--



- Definition of ETERNUS hot spares, RAID groups, and TPP is not possible in Resource Orchestrator. Predefine hot spares, RAID groups, and TPP using ETERNUSmgr or other software.
- Resource Orchestrator supports access path settings on the FC-CA ports of ETERNUS connected using Fabric connections. It is necessary to select "Fabric connection" in the settings of the connection method of ETERNUS FC-CA ports.
- Resource Orchestrator uses ETERNUS host affinity to enable recognition of LUNs by servers. Therefore, for affinity mode settings of ETERNUS FC-CA ports, "ON" must be selected.

When Connecting ETERNUS Storage to Fibre Channel Switches

When creating a disk from an ETERNUS RAID group, configure one-to-one WWPN zoning for the Fibre Channel switch registered on ESC. Therefore, it is necessary to register the Fibre Channel switch connected to ETERNUS and all Fibre Channel switches connected to it using a cascade connection on ESC.

For details on how to register to ESC, refer to the "ETERNUS SF Storage Cruiser User's Guide" of version 14.2 or later.

Zoning settings may not have been configured for Fibre Channel switches. When zoning is not configured, ensure that temporary zoning is configured, since there is a chance that one-to-one WWPN zoning settings cannot be configured. For details on how to perform configuration, refer to the ESC manual.

When Using iSCSI Boot

Define the following using ESC or ETERNUSmgr. Regarding the defined information, register a disk on a resource, using the operation command (rcxadm iscsictl) for iSCSI boot.

- LUN used for iSCSI boot and LUN mapping



If iSCSI boot information already registered is specified, the registered information continues to exist.

If the registered information is changed, delete the iSCSI boot information using the unregister subcommand, and then register the iSCSI boot information by using the register subcommand again.

The definition information registered using the operation command (rcxadm iscsictl) for iSCSI boot is as follows:

For details, refer to "2.4.2 iSCSI Boot Information" of the "Reference Guide (Resource Management) CE".

- Storage Information
 - IP address of the storage port used for iSCSI
 - Storage port IQN name used for iSCSI
- Server Information
 - IP address of the server used for iSCSI
 - Server IQN name used for iSCSI
- Disk Information
 - LUN disk size used for iSCSI boot
- Authentication Information for iSCSI

When using dynamic LUN mirroring

When using dynamic LUN mirroring, copying chassis is possible by coordinating with CCM.

When using this function, make settings so that copying between ETERNUS storage chassis is possible.

For details on the configuration method, refer to the "ETERNUS SF AdvancedCopy Manager Operator's Guide for Copy Control Module".

D.3.2 When Using NetApp FAS Storage

This section explains how to configure NetApp storage.

NetApp FAS Storage Configuration

- For Fibre Channel Connections

Use the following procedure to configure NetApp FAS series/V series settings:

1. Initial Configuration

Set the password of the Data ONTAP root account (using more than one character) and the admin IP address of Data ONTAP, referring to the "Data ONTAP Software Setup Guide" manual.

Note

- Resource Orchestrator uses the NetApp FAS series/V series which is not registered on storage management software such as DataFabric Manager.
- Only one admin IP address can be registered for the NetApp FAS series/ V series on Resource Orchestrator.

2. Configuration of SSL

Configure SSL, referring to the "Data ONTAP System Administration Guide" manual.

For Data ONTAP7.3, execute the following command on the Data ONTAP that is to be managed:

```
>secureadmin setup ssl <RETURN>
>options tls.enable on <RETURN>
>secureadmin enable ssl <RETURN>
```

3. Creation of Aggregates

Create more than one aggregate, referring to the "Data ONTAP Storage Management Guide" manual.

Set any desired number when subdividing the management, such as when managing by users.

Aggregates can be added later.

4. Fibre Channel Connection Environment Settings

Configure the following settings, referring to the "Data ONTAP Block Access Management Guide for iSCSI and FC" manual.

- Configure the license settings of the Fibre Channel service.
- Confirm the port settings, and configure the FC port for connection with the managed server as the target port.

5. Creation of portset

Refer to the "Data ONTAP Block Access Management Guide for iSCSI and FC" manual, and create one or more portsets that combine FC ports used for access to the L-Server disk.

Up to two port numbers can be set up per portset.

When using NetApp storage with multiple controllers, create it combining the FC ports of the different controllers.

Use the following name for the portset name:

rcx-portset*NN*(*1)

*1: For *NN*, specify a number from 00 - 99

Note

- For the FC port to register in a portset, specify an FC port that is not registered in another portset.
- Specify the FC port the Fibre Channel cable was connected to.
- No portset other than the rcx-portset*NN* is used.

- For iSCSI Connections

Perform the following operations referring to the "Data ONTAP Block Access Management Guide for iSCSI and FC":

- Creation of LUNs to connect to L-Servers
- Confirmation of storage information to register using the operation command for iSCSI boot (rcxadm iscsiicl)

The main definition information is as follows:

For details, refer to "2.4.2 iSCSI Boot Information" of the "Reference Guide (Resource Management) CE".

- Storage Information
 - IP address of the storage port used for iSCSI
 - Storage port IQN name used for iSCSI
- Server Information
 - IP address of the server used for iSCSI
 - Server IQN name used for iSCSI
- Disk Information
 - LUN disk size used for iSCSI boot
- Authentication Information for iSCSI

Note

- Disks with iSCSI boot information registered may be detected as resources of registered storage management software.
Do not use the disks for iSCSI boot as the LUNs created in advance.

- If iSCSI boot information already registered is specified, the registered information continues to exist.

If the registered information is changed, delete the iSCSI boot information using the unregister subcommand, and then register the iSCSI boot information by using the register subcommand again.

When Connecting NetApp Storage to Fibre Channel Switches

In Resource Orchestrator, when creating disks from NetApp aggregates, configuration of Fibre Channel switches connected to NetApp is not performed.

It is necessary to configure one-to-one WWPN zoning for Fibre Channel switches in advance.

It is necessary to define zoning combining the fibre channel switch combining the HBA Port WWPN value based on the WWN provided by the I/O Virtualization Option and the FC port WWPN value defined in the NetApp portset used in Resource Orchestrator. For details on the configuration method, refer to the manual of the fibre channel switch.

Fibre Channel Switch Zoning Settings

Set zoning combining the WWPN value of HBA Port1 and the WWPN value of defined FC port first in portset, and combining the WWPN value of HBA Port2 and the WWPN value of defined FC port second in portset.

In the following conditions, an example command for an ETERNUS SN200 is as follows:

Conditions

- WWN value provided by the I/O Virtualization Option: "20:00:00:17:42:51:00:0x"
- WWPN value of HBA Port1: "21:00:00:17:42:51:00:0x"
- WWPN value of HBA Port2: "22:00:00:17:42:51:00:0x"
- Definition of the NetApp storage portset (rcx-portset01): "0a,0b"
- WWPN value of FC port(0a) for NetApp storage: "50:0a:09:81:88:bc:43:dc"
- WWPN value of FC port(0b) for NetApp storage: "50:0a:09:82:88:bc:43:dc"

Example Command

```
zoneCreate "f2020_a_0","50:0a:09:81:88:bc:43:dc;21:00:00:17:42:51:00:00"
zoneCreate "f2020_b_0","50:0a:09:82:88:bc:43:dc;22:00:00:17:42:51:00:00"
...
zoneCreate "f2020_a_f","50:0a:09:81:88:bc:43:dc;21:01:00:17:43:50:00:0f"
zoneCreate "f2020_b_f","50:0a:09:82:88:bc:43:dc;22:01:00:17:43:50:00:0f"
cfgCreate "ror_cfg","f2020_a_0;f2020_b_0; ... ;f2020_a_f;f2020_b_f"
cfgEnable "ror_cfg"
cfgSave
```

D.3.3 When Using EMC CLARiiON Storage

This section explains how to configure EMC CLARiiON storage.

EMC CLARiiON Storage Configuration

Resource Orchestrator controls EMC CLARiiON storage through EMC Navisphere Manager.

A user ID and a password are required to use EMC Navisphere Manager.

For details on how to add a user ID, refer to the EMC Navisphere Manager manual.

In order to enhance communication security between Resource Orchestrator and EMC Navisphere Manager, security files are used for issuing Navisphere CLIs.

Create security files in the following directories of the server on which Resource Orchestrator is installed, using the command to create security files.

[Windows]

Installation_folder\Manager\etc\storage\emc\xxx.xxx.xxx.xxx (*1)

[Linux]

/etc/opt/FJSVrcvmr/storage/emc/xxx.xxx.xxx.xxx (*1)

*1: IP address of SP for EMC CLARiiON storage.

When there are multiple EMC CLARiiONs, create multiple directories.

For the user ID to execute commands to create security files, set SYSTEM for Windows, or root for Linux.

Use the following procedure to execute the command for SYSTEM users on Windows.

- For Windows Server 2003

1. Confirm the current time of servers.
2. Set the schedule for creating the security files using the navisecli command, after the time set by the AT command in 1.
3. Check if the security files have been created after the time scheduled in 2., by registering storage management software.



Example

```
>C:\Program Files\Resource Orchestrator\Manager\bin>time <RETURN>
The current time is: 16:32:14.39
Enter the new time:

>C:\Program Files\Resource Orchestrator\Manager\bin>at 16:36 navisecli -AddUserSecurity -password password -
scope 0 -user administrator -secfilepath " C:\Program Files\Resource Orchestrator\Manager\etc\storage\emc
\192.168.99.101" <RETURN>
Added a new job with job ID = 1

>C:\Program Files\Resource Orchestrator\Manager\bin>time <RETURN>
The current time is: 4:36:00 PM.79
Enter the new time:

>C:\Program Files\Resource Orchestrator\Manager\bin>rcxadm storagemgr register -name A -ip 192.168.99.101 -
soft_name emcns -soft_url http://192.168.99.101/start.html <RETURN>
```

- For Windows Server 2008

1. Create a task for creating the security files using the navisecli command executed using the SHTASKS command.
2. Execute the task created in 1. using the SHTASKS command.
3. Delete the task created in 1. using the SHTASKS command.



Example

```
C:\Program Files (x86)\EMC\Navisphere CLI>SHTASKS /Create /TN doc /TR "\"C:\Program Files (x86)\EMC\Navisphere
CLI\NaviSECCli.exe" -h 172.17.75.204 -AddUserSecurity -user admin -password admin -scope 0 -secfilepath \"c:\tmp
\SYSTEM\" /SC ONSTART /RU SYSTEM
SUCCESS: The scheduled task "doc" has successfully been created.

C:\Program Files (x86)\EMC\Navisphere CLI>SHTASKS /Run /I /TN doc
INFO: scheduled task "doc" is currently running.
SUCCESS: Attempted to run the scheduled task "doc".

C:\Program Files (x86)\EMC\Navisphere CLI>SHTASKS /delete /tn doc
```



```
WARNING: Are you sure you want to remove the task "doc" (Y/N)? y
SUCCESS: The scheduled task "doc" was successfully deleted.

C:\Program Files (x86)\EMC\Navisphere CLI>
```

Information

For details on how to create security files, refer to the explanation in "-AddUserSecurity" switches of Navisphere CLI.

Note

- The following settings are not configured in Resource Orchestrator. Therefore, configure these settings beforehand.
 - Define hot spares
 - Define RAID Groups
 - Create Traditional LUNs
- For details on how to create RAID Groups and Traditional LUNs, refer to the manual of EMC CLARiiON storage.
- Existing RAID Groups are also recognized as virtual storage, but RAID Groups are not recognized when they are used as hot spares.
- It is not necessary to create a Storage Group which defines LUN masking (LUN mapping), as one is automatically created when creating an L-Server.
- Pool and Thin LUN are not recognized.
- When installing an OS and a multipath driver, it is necessary to make only one access path from the server to the storage.
- It is necessary to install Resource Orchestrator and Navisphere CLI on the same server.
- Only Fibre channel connections using FC ports (target mode) are supported.
- The connection form to FC ports only supports fabric connections.
- For EMC CLARiiON storage, after installing Resource Orchestrator it is necessary to create definition files combining ports for SAN storage.

When Connecting EMC CLARiiON Storage to Fibre Channel Switches

In Resource Orchestrator, when connecting EMC CLARiiON storage, Fibre Channel switches are not configured.

It is necessary to configure one-to-one WWPN zoning for Fibre Channel switches in advance.

It is necessary to define zoning combining the fibre channel switch combining the HBA Port WWPN value based on the WWN provided by the I/O Virtualization Option and the SP port WWPN value in the EMC CLARiiON storage used in Resource Orchestrator. For details on the configuration method, refer to the manual of the fibre channel switch.

Fibre Channel Switch Zoning Settings

Set zoning combining the WWPN value of HBA Port1 and the WWPN value of the first SP port defined in the storage_portset.rcxprop definition file, and combining the WWPN value of HBA Port2 and the WWPN value of the second SP port defined in portset.

Examples of command execution for an ETERNUS SN200 are as follows:

Example

Conditions

- WWN value provided by the I/O Virtualization Option
"20:00:00:17:42:51:00:0x"
- WWPN value of HBA Port1
"9:00:00 PM:17:42:51:00:0x"
- WWPN value of HBA Port2
"10:00:00 PM:17:42:51:00:0x"
- WWPN value of SP port defined for the first portset
"50:0a:09:81:88:bc:43:dc"
- WWPN value of SP port defined for the first portset
"50:0a:09:82:88:bc:43:dc"

```
zoneCreate "emc_a_0","50:0a:09:81:88:bc:43:dc;21:00:00:17:42:51:00:00" <RETURN>
zoneCreate "emc_b_0","50:0a:09:82:88:bc:43:dc;22:00:00:17:42:51:00:00" <RETURN>
...
zoneCreate "emc_a_f","50:0a:09:81:88:bc:43:dc;21:01:00:17:42:50:00:0f" <RETURN>
zoneCreate "emc_b_f","50:0a:09:82:88:bc:43:dc;22:01:00:17:42:50:00:0f" <RETURN>
cfgCreate "ror_cfg","emc_a_0;emc_b_0; ... ;emc_a_f;emc_b_f" <RETURN>
cfgEnable "ror_cfg" <RETURN>
cfgSave <RETURN>
```

D.3.4 When Using EMC Symmetrix DMX Storage or EMC Symmetrix VMAX Storage

This section explains how to configure EMC Symmetrix DMX storage and EMC Symmetrix VMAX storage.

Configuration of EMC Symmetrix DMX Storage or EMC Symmetrix VMAX Storage

Resource Orchestrator manages only EMC Symmetrix DMX registered on Solutions Enabler. Register the target EMC Symmetrix DMX on Solutions Enabler.

For details on how to register Solutions Enabler, refer to the Solutions Enabler manual.

There are the following advisory notes:

- For Resource Orchestrator, host spare definitions, DISK group definitions (corresponding to RAID groups), and devices (corresponding to LUNs) are not created. Create hot spare definitions, DISK group definitions, or devices in advance.
- Map devices and director ports in advance.
- It is not necessary to create devices, LUN mapping and LUN masking, as these are automatically created when creating an L-Server.
- For details on defining hot spares and DISK groups, creating devices, and mapping devices and director ports, refer to the manual of EMC Symmetrix DMX storage or EMC Symmetrix VMAX storage.
- When installing an OS and a multipath driver, it is necessary to make only one access path from the server to the storage.
- It is necessary to install Resource Orchestrator and SYMCLI in the same server.
SYMAPI Server can also be installed on a different server.
- The server to install SYMAPI Server on must be able to access EMC Symmetrix DMX storage or EMC Symmetrix VMAX storage from FC-HBA.

When Connecting EMC Symmetrix DMX Storage or EMC Symmetrix VMAX Storage to Fibre Channel Switches

In Resource Orchestrator, when connecting EMC Symmetrix DMX storage or EMC Symmetrix VMAX storage, Fibre Channel switches are not configured.

It is necessary to configure one-to-one WWPN zoning for Fibre Channel switches in advance.

It is necessary to define zoning combining the fibre channel switch combining the HBA Port WWPN value based on the WWN provided by the I/O Virtualization Option and the DIRECTOR port WWPN value in the EMC Symmetrix DMX storage or EMC Symmetrix VMAX storage used in Resource Orchestrator. For details on the configuration method, refer to the manual of the fibre channel switch.

Fibre Channel Switch Zoning Settings

Set zoning combining the WWPN value of HBA Port1 and the WWPN value of the first Director port defined in the storage_portset.rcxprop definition file, and combining the WWPN value of HBA Port2 and the WWPN value of the second Director port defined in portset.

Examples of command execution for an ETERNUS SN200 are as follows:



Example

Conditions

- WWN value provided by the I/O Virtualization Option
"20:00:00:17:42:51:00:0x"
- WWPN value of HBA Port1
"9:00:00 PM:17:42:51:00:0x"
- WWPN value of HBA Port2
"10:00:00 PM:17:42:51:00:0x"
- WWPN value of the DIRECTOR portset defined first
"50:0a:09:81:88:bc:43:dc"
- WWPN value of the DIRECTOR portset defined first
"50:0a:09:82:88:bc:43:dc"

```
zoneCreate "emc_a_0","50:0a:09:81:88:bc:43:dc;21:00:00:17:42:51:00:00" <RETURN>
zoneCreate "emc_b_0","50:0a:09:82:88:bc:43:dc;22:00:00:17:42:51:00:00" <RETURN>
...
zoneCreate "emc_a_f","50:0a:09:81:88:bc:43:dc;21:01:00:17:42:50:00:0f" <RETURN>
zoneCreate "emc_b_f","50:0a:09:82:88:bc:43:dc;22:01:00:17:42:50:00:0f" <RETURN>
cfgCreate "ror_cfg","emc_a_0;emc_b_0; ... ;emc_a_f;emc_b_f" <RETURN>
cfgEnable "ror_cfg" <RETURN>
cfgSave <RETURN>
```

D.4 Pre-setup Preparations (Network)

This section explains the preparations for setting up a network.

The network environment and physical server required to run Resource Orchestrator must satisfy the following prerequisites:

- The configuration for the admin and public LANs has been designed
- The network environment for the admin LAN is configured

For details on the network environment for the admin LAN, refer to "[4.2.1.1 Admin LAN Network Design](#)".

Perform the following procedures if necessary.

- The configuration for the iSCSI LAN has been designed

For details on how to design and configure a network environment for iSCSI, refer to "4.2.1.3 Physical Network Design for the Public LAN and iSCSI LAN" in the "ServerView Resource Orchestrator Setup Guide".

Note

When using a physical L-Server, the default physical network adapter numbers available for the admin LAN are as given below.

- When not performing redundancy, "1" is available
- When performing redundancy, "1" and "2" are available

When using a NIC other than the default one, the configuration at the time of physical server registration and at L-Server creation must be the same. Thus when designing systems it is recommended that physical servers registered in the same server pool use the same NIC index.

Information

The first NIC that is available for the admin LAN can be changed.

For details, refer to "2.4.2 Registering Blade Servers" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

When Using IBP

When using IBP, it is necessary to create IBP uplink set for the public LAN and the admin LAN in advance.

When using physical L-Servers, it is necessary to create an IBP uplink set for the public LAN and the admin LAN in advance, using VIOM.

- Public LAN

Create a network resource with the same name as the created uplink set.

- Admin LAN

Describe the name of the admin LAN uplink set in the uplink set definition file for the admin LAN.

When the definition file does not exist, define it as follows.

Storage Location of the Uplink Set Definition File for the Admin LAN

[Windows]

Installation_folder\Manager\etc\customize_data\vnetwork_ibp.rcxprop

Format of the Uplink Set Definition File for the Admin LAN

Describe the definition file in individual lines as below:

<i>Key = Value</i>

Table D.1 List of Items Specified in the Definition File

Item	Key	Value	Remarks
Presence or absence of IBP environment	support_ibp_mode	<ul style="list-style-type: none"> - true - false 	Specify one of the following: <ul style="list-style-type: none"> - If LAN switch blades are being operated using IBP firmware Specify "true". - If other than the above Specify "false".

Item	Key	Value	Remarks
			If left blank, "false" is set.
Admin LAN settings	external_admin_net_name	The name of the admin LAN uplink set	Enabled when ibp_mode is set to "true"

When using iSCSI

When using iSCSI, create an iSCSI network definition file.

Network Definition File for iSCSI

Create the following file in advance to define the network information used for iSCSI boot.

The network information is linked with the iSCSI boot information that is registered using the iSCSI boot operation command (rcxadm iscsictl).

Refer to "2.4.2 iSCSI Boot Information" in the "Reference Guide (Resource Management) CE" beforehand.

Storage Location of the Definition File

[Windows]

Installation_folder\Manager\etc\customize_data

[Linux]

/etc/opt/FJSVrcvmr/customize_data

Definition File Name

- User Groups

iscsi_user_group_name.rcxprop

- Common on System

iscsi.rcxprop

Definition File Format

In the definition file, an item to define is entered on each line. Enter the items in the following format.

<i>Variable</i> = <i>Value</i>

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

Definition File Items

Table D.2 Network Definition File Items for iSCSI Boot

Variable	Meaning	Value
server_model.model_name.boot_nic	Specify the server model name and NIC to be booted using iSCSI. Multiple NICs can be specified. - BX620 - BX920 - BX922 - BX924 - BX960 When setting the default, specify an asterisk ("*").	Specify the items in the following format. NIC[<i>index</i>] <i>index</i> is an integer starting from "1".



Example

```
#Server Section
server_model.BX922.boot_nic = NIC1
server_model.BX924.boot_nic = NIC1,NIC2
server_model.*.boot_nic = NIC1,NIC2
server_model.RX300. boot_nic = NIC1,NIC2
```

D.5 Configuration after Installation

This section explains configurations after the installation.

Configure the definition file after installing the manager.

D.5.1 Definition Files

This section explains the definition file.

When using a physical L-Server, the configuration of the definition file may be necessary.

- When using SAN storage
Refer to "[6.1.1 Creating Definition Files Combining Ports of SAN Storage](#)".
- When using ETERNUS storage
Refer to "[Format Selection for the Names of Virtual Storage Resources and Disk Resources Managed by ESC](#)".
- When configuring Thin Provisioning attributes on a storage pool
Refer to "Configuring Thin Provisioning Attributes for Storage Pools" in "12.2 Resource Pool Operations" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".
- When using configuration of priority for resource selection on Thin Provisioning and Automatic Storage Layering
Refer to "[Configuration of Priority for Resource Selection on Thin Provisioning on Thin Provisioning and Automatic Storage Layering](#)".
- When using dynamic LUN mirroring
Refer to "[Creating Mirroring Definition Files for Dynamic LUN Mirroring](#)".
- When using EMC storage
For details, refer to "[Definition File for EMC Storage](#)".
- When creating a physical L-Server without specifying a model name in the L-Server template
Refer to "[Configuration when Creating a Physical L-Server without Specifying a Model Name in the L-Server Template](#)".
- When the number of FCs fitted and their position are different depending on the physical server
Refer to "[Setting the Number of FCs Fitted and their Position for Each Physical Server](#)".
- When using alive monitoring
Refer to "[Definition File for Alive Monitoring](#)".

Format Selection for the Names of Virtual Storage Resources and Disk Resources Managed by ESC

The format of the names of virtual storage resources and disk resources managed by ESC can be selected. When the definition file has been edited, restart the manager.

Location of the Definition File

[Windows]

Installation_folder\Manager\etc\customize_data

[Linux]

/etc/opt/FJSVrcvmt/customize_data

Definition File Name

storage.rcxprop

Definition File Format

In the definition file, the items to set are entered on individual lines. Each line is entered in the following format.

<i>Item_specified = Value_specified</i>

Definition File Items

ETERNUS_VOLUME_NAME_TO_DISK_NAME

Select the format of the name of disk resources managed by ESC.

- If "true" is specified

The disk resource name is used as the alias name for ESC. If the format of the alias name is unavailable for the format of the disk resource name, Resource Orchestrator automatically sets a disk resource name that conforms to the alias name. Even if "true" has been specified, when ESC does not support the alias name, the combination of the IP address of ETERNUS, the RAID group number, and the volume number will be used as the disk resource name.

- If "false" is specified

The combination of the IP address of ETERNUS, the RAID group number, and the volume number will be used as the disk resource name.

- If nothing is specified

"false" is set.



Note

If the disk has been separated from the virtual storage and saved, then the ETERNUS LUN alias name is not reflected on the disk resource name even if the value is "true".

ETERNUS_RAIDGROUP_NAME_TO_VSTORAGE_NAME

Select the format of the name of virtual storage resources managed by ESC.

- If "true" is specified

The RAID group name of ESC is used as the disk resource name. If the format of the RAID group name is unavailable for the format of the virtual storage resource name, Resource Orchestrator automatically set a virtual storage resource name that conforms to the RAID group name. Even if "true" has been specified, when ESC does not support the RAID group name, the combination of the IP address of ESC and the RAID group number will be used as the virtual storage resource name.

- If "false" is specified

The combination of the IP address of ESC and the RAID group number will be used as the virtual storage resource name.

- If nothing is specified

"false" is set.



Example

An example definition file is indicated below.

ETERNUS_VOLUME_NAME_TO_DISK_NAME = true ETERNUS_RAIDGROUP_NAME_TO_VSTORAGE_NAME = true

Configuration of Priority for Resource Selection on Thin Provisioning on Thin Provisioning and Automatic Storage Layering

The following resources can be registered in a storage pool with thin provisioning attributes set:

- FTRP and FTV for Automatic Storage Layering
- TPP and TPV for Thin Provisioning

When setting to automatic selection for resource selection while creating L-Server or attaching a disk under the condition that both storage pools with and without the configuration of thin provisioning attributes remain the same priority, either of their resources can be given higher priority.

When the definition file has been edited, restart the manager.

Location of the Definition File

[Windows]

Installation_folder\Manager\etc\customize_data

[Linux]

/etc/opt/FJSVrcvnr/customize_data

Definition File Name

storage.rcxprop

Definition File Format

In the definition file, the items to set are entered on individual lines. Each line is entered in the following format.

<i>Specified item = Specified value</i>

Definition File Items

SELECT_THIN_PROVISIONING_POOL_FIRST

When both storage pools with and without the configuration of thin provisioning attributes remain the same priority, either of their resources can be given higher priority for automatic selection of storage resource.

- If "true" is specified
A storage pool with thin provisioning attributes will be given priority.
- If "false" is specified
A storage pool without thin provisioning attributes will be given priority.
- If nothing is specified
"false" is set.



Example

An example definition file is indicated below.

SELECT_THIN_PROVISIONING_POOL_FIRST = true
--

Creating Mirroring Definition Files for Dynamic LUN Mirroring

When using dynamic LUN mirroring, create a mirroring definition file and configure the ETERNUS storage to create a copied volume.

Location of the Definition File

[Windows]

Installation_folder\Manager\etc\customize_data

[Linux]

/etc/opt/FJSVrcvmt/customize_data

Definition File Name

storage_mirroring.rcxprop

Definition File Format

Describe the virtual storage information. Each virtual storage information must be described using a single line, and be in the following format starting from the start of the line. Use of line breaks is not allowed.

<i>local_storage_ipaddr,virtual_storage_type,local_storage_number,remote_storage_boxid,remote_storage_number,copy_group</i>

Definition File Items

local_storage_ipaddr

Enter the IP address of the local site ETERNUS storage device that will automatically create the disk resource.

virtual_storage_type

Specify the virtual server type.

Specify "RAID" for RAID group.

Specify "TPP" for TPP.

local_storage_number

Specify the RAID group or TPP number from which the disk resource will be extracted in the ETERNUS storage on the local site. Specify 4-digit hexadecimal numbers starting with 0x.

remote_storage_boxid

Specify the BOX-ID of ETERNUS storage in the remote side to create the copied volume.

Check the BOX-ID in "Advanced Copy Path Status" which is the Web GUI for ETERNUS.

remote_storage_number

Specify the RAID group or TPP number that will be used to create the copied volume in the ETERNUS storage on the remote site. Specify 4-digit hexadecimal numbers starting with 0x.

copy_group

Specify the name for the copy group created when setting inter-chassis copying.



Example

.....
An example definition file is indicated below.

192.168.1.24,RAID,0x0011,00ETERNUSDXLS2ET092DD#####LN4521132A09##,0x0022,group1 192.168.1.24,TPP,0x0033,00ETERNUSDXLS2ET092DD#####LN4521132A09##,0x0044,group2

.....

Definition File for EMC Storage

When registering EMC Navisphere Manager or EMC Solutions Enabler as storage management software, it is necessary to specify the installation folder of Navisphere CLI or SYMCLI in the definition file for EMC storage.

Storage Location of the Definition File for EMC Storage

[Windows]

Installation_folder\Manager\sys\usm\etc

[Linux]

/opt/FJSVrcvmr/sys/usm/etc

Definition File Name for EMC Storage

emcpath.conf

Definition File Format for EMC Storage

The format of the definition file for EMC storage is as follows:

When registering EMC Navisphere Manager as storage management software, modify the line beginning with "naviseccli".

```
naviseccli=Navisphere CLI_installation_folder
```

When registering EMC Solutions Enabler for storage management software, modify the line beginning with "symcli".

```
symcli=SYMCLI_installation_folder
```

[Windows]

Use "\\" for the file separator. Do not modify the line beginning with "secfilepath".



Example

[Windows]

```
naviseccli=C:\Program Files\EMC\Navisphere CLI
secfilepath=..\..\etc\storage\emc
symcli=C:\Program Files\EMC\SYMCLI\bin
```

[Linux]

```
naviseccli=/opt/Navisphere/bin
secfilepath=/etc/opt/FJSVrcvmr/storage/emc
symcli=/opt/symcli/bin
```

Configuration when Creating a Physical L-Server without Specifying a Model Name in the L-Server Template

To create a physical L-Server without specifying a model name in the L-Server template, create the definition file, define the configuration information (CPU core count, CPU clock speed, memory capacity, etc.), and then register the server as a managed server.

In the following cases, create the definition file first, and then register the hardware information with Resource Orchestrator again.

- If the target server was registered with Resource Orchestrator before creation of the definition file
- When modifying the configuration information (CPU core count, CPU clock speed, memory capacity, etc.) in the definition file of a server that has been registered with Resource Orchestrator

For details, refer to "Chapter 7 Hardware Maintenance" in the "Operation Guide CE".



Note

If the value entered in the definition file differs from the actual configuration information of the server, creation or starting of physical L-Servers may fail, or physical servers may be deployed with incorrect information about CPU and memory.

Be sure to confirm that the values entered in the definition file and the actual configuration information of the server are the same.

Storage Location of the Definition File

[Windows]
Installation_folder\Manager\etc\customize_data

[Linux]
/etc/opt/FJSVrcvmt/customize_data

Definition File Name

server_spec.rcxprop

Character Code

[Windows/Linux]
UTF-8

Line Break Code

[Windows]
CR/LF

[Linux]
LF

Definition File Format

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

```
ServerSpec,V1.0
```

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

When defining two or more servers, use line breaks.
Each line is entered in the following format.

```
physical_server, cpu_core_count, cpu_clock, memory_size[, cpu_type]
```

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

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

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

Definition File Items

physical_server

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

cpu_core_count

Enter the total number of physical CPU cores.
Enter an integer between 0 and 999.
When entering "0", hyphens ("-") are displayed in the basic information on the resource details screen, and physical L-Servers cannot be created.

cpu_clock

Enter the CPU clock speed.
Enter an integer between 0 and 999,999.
Use megahertz for the unit. Enter 1,000 MHz for 1 GHz, for example.

When entering "0", hyphens ("-") are displayed in the basic information on the resource details screen, and physical L-Servers cannot be created.

memory_size

Enter the total memory size.

Enter an integer between 0 and 999,999,999.

Use megabytes for the unit. Enter 1,024 MB for 1 GB, for example.

When entering "0", hyphens ("-") are displayed in the basic information on the resource details screen, and physical L-Servers cannot be created.

cpu_type

Enter the CPU type.

The string must be composed of alphanumeric characters and symbols (ASCII characters 0x20 to 0x7e), except for commas (","), and can be up to 64 characters long.

When omitted, a hyphen ("-") is displayed.



Example

An example definition file is indicated below.

```
ServerSpec,V1.0

#####
# server_spec.rcxprop
#
#All Rights Reserved, Copyright(C) FUJITSU LIMITED 2011
#####
#
# physical_server, cpu_core_count, cpu_clock, memory_size, cpu_type
#

server001, 8, 3160, 4096, Intel(R) Xeon(R)
server002, 8, 2660, 12288, Intel(R) Xeon(R)
server003, 2, 2000, 65536
server004, 4, 4000, 4096, Intel(R) Xeon(R) Processor E5501
```

Setting the Number of FCs Fitted and their Position for Each Physical Server

If the number of FCs fitted or their location differs from physical server to physical server, prepare an FC connection pattern and define the number of FCs and their location for each physical server.

This setting can be made when the storage units are the following:

- EMC CLARiiON Storage
- EMC Symmetrix DMX Storage
- EMC Symmetrix VMAX Storage

Location of the Definition File

[Windows]

Installation_folder\Manager\etc\customize_data\fc_connection_pattern

[Linux]

/etc/opt/FJSVrcvnr/customize_data/fc_connection_pattern

Definition File Name

Make the file extension .rcxprop and then allocate a file with an arbitrary file name. Specify the file name using the following string:

The file name must start with an alphanumeric character, and can contain up to 64 alphanumeric characters, underscores ("_"), and hyphens ("-").

Definition File Format

Create a different FC pattern file for each system that has a different pattern.

```
NUM_OF_FC=Number_of_FCs_used
BOOT_FC_PORT =["HBA_number", "HBA_number"]
STORAGE_X="Storage_chassis_identifier", "HBA_number", "target_port_number"
```

Definition File Items

NUM_OF_FC (mandatory)

Specify the number of FCs to be used. 1, 2, and 4 can be specified for the number.

BOOT_FC_PORT

Specify the number of HBAs that are actually mounted on the server.

Allocate a sequential number to all of the ports, sorted in the expansion slot order.

By specifying the HBA number, up to two FC ports can be set as Boot paths.

The priority of HBA numbers is set based on the order in which they are listed.

Only numbers under the value specified in NUM_OF_FC can be specified.

NUM_OF_FC value	Valid Range of HBA Numbers
4	0 - 3
2	0 - 1
1	0

STORAGE_X (mandatory)

Specify as many as there are connected storage chassis. However, the number in X must be a decimal between 0 and 99, starting from 0 and counting up.

"Storage chassis identification number"

Specify the storage chassis identification number.

"HBA number"

Define the FCPort pairing on the server to be used, separating with a colon (:).

"target port number"

Define the FCPort pairing on the storage side, separating with a colon (:).

By specifying separate HBA numbers for each STORAGE_X, logical paths to two storage chassis can be set from each single physical server.

However, if the same storage chassis identification number is defined multiple times, the one defined first will be valid.



- The file names of FC connection patterns cannot be changed after performing the following operations:
 - Import of the L-Server template specifying an FC connection pattern
 - Turning on of the physical L-Server with a definition specifying an FC connection pattern
 - Creation of a physical L-Server specifying an FC connection pattern

- The details of FC connection pattern files can only be changed in the following cases:

When a physical L-Server with an FC connection pattern specified is in the defined state

Example

An example definition file is indicated below.

- If 2 paths (1 boot path)

```
NUM_OF_FC = "2"
BOOT_FC_PORT=["1"]
STORAGE_1="000192601264","0:1","07GPort1:08GPort1"
```

- If 2 paths (2 boot path)

```
NUM_OF_FC = "2"
BOOT_FC_PORT=["0", "1"]
STORAGE_1="000192601264","0:1","07GPort1:08GPort1"
```

- If 4 paths (1 chassis)

```
NUM_OF_FC = "4"
BOOT_FC_PORT=["1", "2"]
STORAGE_1="000192601264","0:1:2:3","07GPort1:08GPort1:09GPort1:10GPort1"
```

- If 4 paths (2 chassis)

```
NUM_OF_FC = "4"
BOOT_FC_PORT=["1", "2"]
STORAGE_1="000192601264","0:1","07GPort1:08GPort1"
STORAGE_2="000192601265","2:3","09GPort1:10GPort1"
```

Definition File for Alive Monitoring

When using alive monitoring, create the definition file and specify the parameters for alive monitoring. The configuration of this parameter must be unique in the system.

When using alive monitoring on a physical L-Server, monitor hang-up of the operating system corresponding to a physical L-Server using the OS Ping response.

For details on Ping monitoring, refer to "8.4 Configuring Monitoring Information" in the "Setup Guide VE".

Storage Location of the Definition File

The file in which the default values are described is located during installation.

[Windows]

Installation_folder\Manager\etc\customize_data\alive_monitoring

[Linux]

/etc/opt/FJSVrcvmr/customize_data/alive_monitoring

Definition File Name

Physical.rcxprop

The file name is not case sensitive.

Definition File Format

In the definition file, the items to set are entered on individual lines. Each line is entered in the following format.

Item_specified= Value_specified

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

Definition File Items

timeout

Specify the the number of seconds of time-out for ping monitoring.

Enter an integer between 5 and 3,600. The unit is seconds.

"600" is specified as the default.

recovery

Specify recovery operations for when an error is detected.

Specify one of the following:

- reboot (reboot)
- force_reboot (forced reboot)
- switchover (server switchover)
- reboot_and_switchover (reboot and switchover)
- force_reboot_and_switchover (forced reboot and switchover)

"reboot_and_switchover" is specified as the default.

When specifying "switchover" or "force_reboot_and_switchover" for recovery method, server redundancy need to be configured at Physical L-Server creation.

reboot

Specify the number of reboots for recovery operations.

Enter an integer between 1 and 3. The unit is seconds.

"1" is specified as the default.



Example

An example definition file is indicated below.

```
timeout = "600"  
recovery = "reboot_and_switchover"  
reboot = "1"
```



Note

When applying the modified details to an already created L-Server, execute the rcxadm lserver modify command after changing the definition files.

D.6 Setup

The setup procedure for using a physical server as an L-Server is as follows:

1. Register Resources
 - a. Register VIOM coordination (for blade servers)

Refer to "2.1 Registering VIOM Coordination" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".



Note

It is not necessary to register a VIOM server profile.

When creating a physical L-Server, VIOM server profiles are automatically created.

b. Register storage management software

When storage management software is registered, RAID groups or aggregates that were created during pre-setup preparations are automatically registered in Resource Orchestrator as virtual storage resources.

Execute the `rcxadm storagemgr register` command to register storage management software with Resource Orchestrator. For details on the `rcxadm storagemgr register` command, refer to "1.7.1 `rcxadm storagemgr`" in the "Reference Guide (Resource Management) CE".

c. Register managed servers

1. Register Chassis (for Blade Servers)

Refer to "2.4.1 Registering Chassis" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

2. Register Managed Servers

Refer to "2.4.2 Registering Blade Servers" or "2.5.1 Registering Rack Mount or Tower Servers" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

When performing admin LAN NIC redundancy and registering a physical server, check the "Use Admin LAN redundancy" checkbox in the "Register Server" dialog when registering the server.

When directly specifying an IP address during physical L-Server creation, do not configure the same IP address on a managed server.

An error will occur during the following operations, if there are managed servers configured with the same IP addresses as those allocated to physical L-Servers, in other than physical servers.

- Create physical L-Servers
- Start a physical L-Server for which only the configuration definition has been created



Note

When not using the default NIC, specify the NIC for admin LAN during the physical server registration.

For details, refer to "'Apply Admin LAN NIC settings' checkbox" in "2.4.2 Registering Blade Servers" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

3. Register LAN Switches

Refer to "2.4.3 Registering LAN Switch Blades" and "2.5.2 Registering LAN Switches" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

2. Register Resources in Resource Pools

a. Register physical server resources

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

The [Register Resources] dialog is displayed.

2. Select the VM host to register.
3. Click <OK>.

b. Register storage resources

1. In the ROR console orchestration tree, right-click the target storage pool, and select [Register Resources] from the popup menu.

The [Register Resources] dialog is displayed.

2. Select the storage resource or disk resource to register.
3. Click <OK>.



Note

Register a resource for iSCSI boot, using the operation command (rcxadm iscsictl) for iSCSI boot.

c. Register network resources

If network resources are connected when creating an L-Server, LAN switch blades will be registered automatically as the physical server that the L-Server will operate on. If an image is specified, the IP address is configured.

For details, refer to "[D.6.1 Automatic Network Configuration](#)".

1. In the ROR console orchestration tree, right-click the target network pool, and select [Create Resource] from the popup menu.

The [Create a network resource] dialog is displayed.

2. Enter the items necessary for network resources.
For details, refer to "7.3 Network Resources" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".



Note

When the destination of a physical L-Server is a PRIMERGY BX920 series or BX922 series server and LAN switch blades (PG-SW109 or PG-SW201) are mounted in CB1 and CB2, only NIC1 and NIC2 can be used.

d. Register address set resources

Creates and registers an address set resource in the address pool.

For details, refer to "7.6 Address Set Resources" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

3. Create an L-Server Template

- a. Export an L-Server template

Refer to "8.2.1 Exporting a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- b. Edit an L-Server template

Refer to "8.2.2 Editing a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- c. Import an L-Server template

Refer to "8.2.3 Importing a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

D.6.1 Automatic Network Configuration

If network resources are connected when creating an L-Server, LAN switch blades will be registered automatically as the blade server that the L-Server will operate on.

If an image is specified, the IP address is configured.

Specify an IP address in a different subnet from the admin LAN.

For rack mount and tower servers, only connect network resources.

When creating a physical L-Server, the IP address cannot be automatically configured if specifying a Red Hat Enterprise Linux image. Manually configure the IP address after the image has been deployed to the L-Server.

Physical Server (Blade Server) Configuration to Support Automation of Network Configuration in Resource Orchestrator

The physical server (blade server) configuration to support automation of network configuration (server blades, specification of uplink port for network resources, correspondence relations of numbers of LAN switch blades and physical network adapters, etc.) in Resource Orchestrator are shown in the following list. In this list, show the specifiable scope of physical network adapter numbers according to the server blade models, uplink port specifications and combination of LAN switch blades to use.

Table D.3 Physical Server (Blade Servers) Configuration (for PRIMERGY BX900 S1 Chassis)

Server Blade	Specification of Uplink Port (Location of LAN Switch Blade)	LAN Switch Blade to Use	Physical Network Adapter Number
BX920 S1 BX920 S2 BX922 S2	CB1 and CB2, or no specification for uplink port	PG-SW111 PG-SW112	1 - 4
		PG-SW109 (*1) PG-SW201	1, 2
	CB3 and CB4	PG-SW111 PG-SW112	5 - 8
		PG-SW109 PG-SW201	5, 6
BX924 S2	CB1 and CB2, or no specification for uplink port	PG-SW111 PG-SW112 PG-SW109 PG-SW201	1, 2
		PG-SW111 PG-SW112	3 - 6
	CB3 and CB4	PG-SW109 PG-SW201	3, 4
BX960 S1	CB1 and CB2, or no specification for uplink port	PG-SW111 PG-SW112 PG-SW109 PG-SW201	1, 2, 11, 12
		PG-SW111 PG-SW112	3 - 6
	CB3 and CB4 (*2)	PG-SW109 PG-SW201	3, 4

*1: When installing a PG-SW109 on CB1 or CB2, set the transmission speed at the down link port of PG-SW109 to 1 Gbps. For details on how to configure the settings, refer to the corresponding hardware manual.

*2: Only configurations where LAN expansion cards are mounted in expansion slot 1 are supported.

Table D.4 Physical Server (Blade Servers) Configuration (for PRIMERGY BX400 S1 Chassis)

Server Blade	Specification of Uplink Port (Location of LAN Switch Blade)	LAN Switch Blade to Use	Physical Network Adapter Number
BX920 S2 BX922 S2	CB1 and CB2 (*1), or no specification for uplink port	PG-SW111 PG-SW112	1 - 8
		PG-SW109 (*2) PG-SW201	1, 2, 5, 6

Server Blade	Specification of Uplink Port (Location of LAN Switch Blade)	LAN Switch Blade to Use	Physical Network Adapter Number
BX924 S2	CB1 and CB2 (*1), or no specification for uplink port	PG-SW111 PG-SW112	1 - 6
		PG-SW109 PG-SW201	1 - 4

*1: The same LAN switch blade model should be mounted in CB1 and CB2.

*2: When installing a PG-SW109 on CB1 or CB2, set the transmission speed at the down link port of PG-SW109 to 1 Gbps. For details on how to configure the settings, refer to the corresponding hardware manual.

Table D.5 Physical Server (Blade Servers) Configuration (for PRIMERGY BX600 S3 Chassis)

Server Blade	Specification of Uplink Port (Location of LAN Switch Blade)	LAN Switch Blade to Use	Physical Network Adapter Number
BX600 series servers	NET1 and NET2, or no specification for uplink port	PG-SW107	1 - 6
	NET3 and NET4	PG-SW104	7, 8

The NIC number of the L-Server the network resource above is allocated to is the number of the physical network adapter of the physical server.

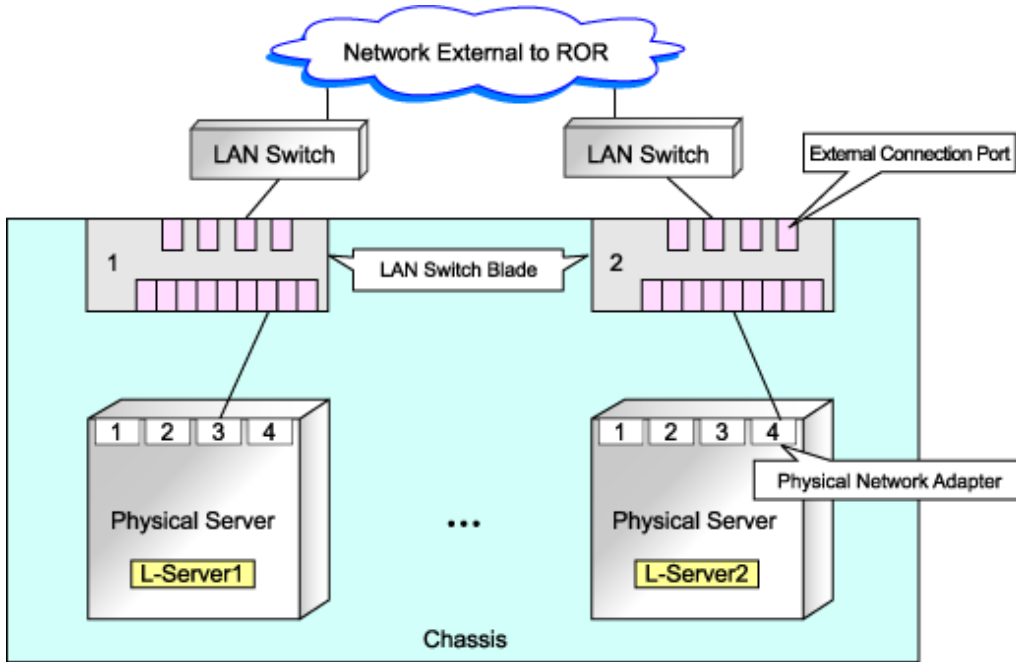
When the LAN switch blade is in IBP mode, specify the NIC of the L-Server that network resources are allocated to as in the case when uplink ports have not been specified (internal network).

The physical server (blade server) configuration as described in the following configuration example when using a PRIMERGY BX900 S1 chassis is as shown below.

Table D.6 Configuration Example

Server blades	BX920 S2
Specification of uplink port	CB1 and CB2
LAN switch blade to use	PG-SW112

Figure D.6 Physical Server (Blade Servers) Configuration (for PRIMERGY BX900 S1 Chassis)



D.6.2 Manual Network Configuration

When using a physical network adapter number that is different from the one used in the physical server configuration patterns, create network resources using the following procedure.

- From the GUI:

1. In the ROR console orchestration tree, right-click the target network pool, and select [Create Resource] from the popup menu.

The [Create a network resource] dialog is displayed.

2. Enter the items necessary for network resources.

For details, refer to "7.3 Network Resources" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Create a network resource by checking the "Use configured virtual switches." checkbox.

- From the Command-line:

1. Create the XML file that defines network resources.

In this case, specify auto="false" in the Network tag.

For details on the Network element and creation of XML files that define network resources, refer to "2.5 Network Resources" of the "Reference Guide (Resource Management) CE".

2. Execute the rcxadm network create command specifying the XML file created in 1.



See

- For details on the Network element and creation of XML files that define network resources, refer to "2.5 Network Resources" of the "Reference Guide (Resource Management) CE".

- For details on the rcxadm network command, refer to "1.3.5 rcxadm network" of the "Reference Guide (Resource Management) CE".

D.7 Creating an L-Server

Use the following procedure to create L-Servers:

Creating an L-Server Using an L-Server Template

- When there are no cloning images, or when not using already registered cloning images

1. Creating an L-Server Using an L-Server Template

Create an L-Server, referring to "10.1 Creation Using an L-Server Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

In this case, perform the following configuration:

- Select "None" for images.
- Check if the "Single path mode" checkbox for FC path is checked.
- When specifying "None" for images, the "Single path mode" checkbox for FC path is automatically checked.

2. Manually Install an OS

For manual OS installation, installation by remote console is recommended after starting the MB (Management Blade) or iRMC (Remote Management Controller) screen.

3. Multipath Driver Installation (When Using Multipaths for SAN Paths)

When using multipaths between L-Server and SAN, install the multipath driver for the L-Server.

For details on how to install the multipath driver, refer to the multipath driver manual.

4. Stop the L-Server

For details on stopping L-Servers, refer to "11.1.2 Stopping an L-Server" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

5. Change the SAN Path Status of the L-Server

Follow the procedure below to change the SAN path status of the L-Server.

- a. Right-click the target L-Server in the orchestration tree, and select [Change Settings]-[Modify Specification] from the popup menu.

The [Modify an L-Server] dialog is displayed.

- b. Uncheck the "Single path mode" checkbox for FC path.
- c. Click <OK>.

6. Start the L-Server

For details on starting L-Servers, refer to "11.1.1 Starting an L-Server" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

7. Install the Agent

It is necessary to install an agent after installing the OS, and then register it.

For details on installing agents, refer to "2.2 Agent Installation" in the "Installation Guide CE".

8. Register the Agent

Use the following procedure to register an agent on the server used as an L-Server.

- a. Right-click the target L-Server in the orchestration tree, and select [Register]-[Agent] from the popup menu.
- b. Click <OK>.

The [Register Agent] dialog is displayed.

- c. Click <OK>.

9. Collect Cloning Images

When collecting cloning images after creating an L-Server, the cloning images are stored in the image pool. Collect cloning images, referring to "Collect Cloning Images" of "D.7.2 Cloning Images".

- When using an existing cloning image

Create an L-Server, referring to "10.1 Creation Using an L-Server Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE". In this case, specify the cloning image that you want to use as an image.

Creating an L-Server Specifying Individual Specifications

- When there are no cloning images, or when not using already registered cloning images

Refer to "10.2 Creation of Physical L-Servers Using Parameters" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

In this case, perform the following configuration:

- Select "None" for images.
- Check if the "Single path mode" checkbox for FC path is checked.

When specifying "None" for images, the "Single path mode" checkbox for FC path is automatically checked.

Perform steps 2 to 10 in "[Creating an L-Server Using an L-Server Template](#)".

- When using an existing cloning image

Refer to "10.2 Creation of Physical L-Servers Using Parameters" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

In this case, perform the following configuration:

- Specify a cloning image to deploy.
- Check if the "Single path mode" checkbox for FC path is unchecked.

When specifying an image, the "Single path mode" checkbox for FC path is automatically unchecked.

For details on how to configure the [OS] tab, refer to "10.2.5 [OS] Tab" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Installation of an Operating System Using PXE Boot

For details on how to install an operating system using PXE boot, refer to "[D.7.1 Installation of an Operating System Using PXE Boot](#)".

L-Server Network Redundancy, Tagged VLAN Settings, and Untagged VLAN Settings

For details on L-Server network redundancy, tagged VLAN settings and untagged VLAN settings, refer to "[D.7.4 Network Redundancy and VLAN Settings of L-Servers](#)".

D.7.1 Installation of an Operating System Using PXE Boot

This section explains how to install an operating system using PXE boot.

Installation of an Operating System Using PXE Boot

To manually install an operating system using PXE boot, use the following procedure.



Note

When using PXE boot, VIOM is required.

1. Create a physical L-Server, selecting "NIC for PXE boot" and "Network for PXE boot" of "Boot device priority" on the [Server] tab.

For details on how to configure the [Server] tab, refer to "10.2 Creation of Physical L-Servers Using Parameters" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

In this case, perform the following configuration:

- Specify the network boot (PXE) for the boot mode.
 - Select the network resource for PXE boot.
 - Select "None" for images.
 - Check if the "Single path mode" checkbox for FC path is checked.
 - When specifying "None" for images, the "Single path mode" checkbox for FC path is automatically checked.
2. Using the DHCP service settings of the PXE boot server, set the relevant physical L-Server to perform PXE boot.
 3. Using PXE boot, install an OS on the physical L-Server.
 4. Stop the physical L-Server after installing the OS.
 5. In the [Modify an L-Server] dialog, change "Network for PXE boot" to "Default" under "Boot mode".
 6. Using the DHCP service settings of the PXE boot server, set the relevant physical L-Server so as not to perform PXE boot.
 7. Start the L-Server.

For details on starting L-Servers, refer to "11.1.1 Starting an L-Server" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

8. Install a multipath driver.

When using multipaths between L-Server and SAN, install the multipath driver for the L-Server.

Refer to the manual of the multipath driver for details on installing multipath drivers.

9. Stop the L-Server.

For details on stopping L-Servers, refer to "11.1.2 Stopping an L-Server" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

10. Change the status of SAN paths for the L-Server.

Follow the procedure below to change the SAN path status of the L-Server.

- a. Right-click the target L-Server in the orchestration tree, and select [Change Settings]-[Modify Specification] from the popup menu.

The [Modify an L-Server] dialog is displayed.

- b. Uncheck the "Single path mode" checkbox for FC path, and click <OK>.

11. Start the L-Server.

For details on starting L-Servers, refer to "11.1.1 Starting an L-Server" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

12. Install the agent.

It is necessary to install an agent after installing the OS, and then register it.

For details on installing agents, refer to "2.2 Agent Installation" of the "Installation Guide CE".

13. Register the agent.

Use the following procedure to register an agent on the server used as an L-Server.

- a. Right-click the target L-Server in the orchestration tree, select [Register]-[Agent] from the popup menu, and click <OK>.

The [Register Agent] dialog is displayed.

- b. Click <OK>.

D.7.2 Cloning Images

Use the following procedure to collect cloning images:

Register the Agent

It is also necessary to install an agent after installing an OS, and then register the server used by an L-Server for an agent.

Use the following procedure to register agents.

1. Right-click the target L-Server in the orchestration tree, and select [Register]-[Agent] from the popup menu.
The [Register Agent] dialog is displayed.
2. Click <OK>.

Collect Cloning Images

For details on how to collect cloning images, refer to "Collect Cloning Images from L-Servers with an OS Installed" in "11.5.1 Collecting and Registering Cloning Images" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

The network parameter auto-configuration function defined in a cloning image cannot be used for Resource Orchestrator.

When the target server of cloning image collection has a redundant NIC configured, release redundancy and then perform collection of cloning images.

Collect cloning images in the state where a multi driver is installed.

D.7.3 [OS] Tab Configuration

Enter the parameters to set for the OS when creating the L-Server. This setting is valid only if an image is specified in the [General] tab. The setting process is performed the first time the L-Server is started.

If an image name is not specified, entry is not necessary.

Table D.7 List of Settings

Item	Description
Host name/Computer name	Enter the host name or computer name. [Windows] Specify up to 63 characters, including alphanumeric characters, underscores ("_"), and hyphens ("-"). The string cannot be composed solely of numbers. [Linux] Specify up to 64 characters, including alphanumeric characters, hyphens ("-"), periods ("."), and underscores ("_"). Underscores ("_") in the L-Server name will be converted to hyphens ("-"). If the basic information is not specified, the L-Server name is converted and set as indicated above.

D.7.4 Network Redundancy and VLAN Settings of L-Servers

In Resource Orchestrator, when images of Red Hat Enterprise Linux are specified, IP address settings of public LANs are not configured. Server NIC redundancy and the OS settings of tagged VLANs are also not configured.

When starting an OS after L-Server creation, set the image to be configured automatically after creating an L-Server. For this setting, use the image collected in the state where the scripts to configure the network settings have been prepared beforehand.

In this case, prepare a script like the following, and perform collection of a cloning image with the script executed once on starting of the OS.

According to the description in the network information file, perform the following settings for using NIC redundancy software (such as Windows Intel PROSet/Linux bonding).

- NIC redundancy
- Tagged VLAN configuration
- IP address configuration

For details on the specifications of the network information file, refer to "[Network Information File](#)".

Network Information File

The settings for NIC redundancy and tagged VLANs for a physical L-Server are described in the file. It is automatically transferred to a physical L-Server during creation. When the `rcxadm lserver` command is executed after creation of the physical L-Server, the network information file will be transferred to the L-Server.

Network Information File Storage Destination

```
[Windows]
Installation_folder\Resource Orchestrator\Agent\etc\net

[Linux]
/etc/opt/FJSVrcxat/net/
```

File Name of the Network Information File

net_info.conf

Character Code

UTF-8

Line Break Code

```
[Windows]
CR/LF
```

```
[Linux]
LF
```

Format for the Network Information File

The formats are shown below.

Table D.8 List of Items Specified in the Network Information File

Variable	Meaning	Value
NIC[index]_MacAddress	NIC MAC address	MAC addresses, noted in hexadecimal form, separated by colons (":")
Groups	List of groups of redundant NICs	Group numbers, separated by spaces
Group[index]_NetworkLinks	NetworkLink list allocated to groups	NetworkLinkIndex separated by spaces
Group[index]_[NetworkLinkIndex]_Nics	List of NICs comprising groups	NIC numbers separated by spaces
Group[index]_[NetworkLinkIndex]_IpAddress	Group IP address	IPv4 addresses separated by periods (".")
Group [index]_[NetworkLinkIndex]_Netmask	Net masks of groups	
Group [index]_[NetworkLinkIndex]_DNSServer	DNS addresses of groups [Windows]	
Group [index]_[NetworkLinkIndex]_DefaultGateway	Default gateway	

Variable	Meaning	Value
Group [index]_[NetworkLinkIndex]_Vlanid	VLANID of NetLink allocated to the group	2-4094
Group [index]_[NetworkLinkIndex]_VlanMode	Specification of tagged VLANs or untagged VLANs	tagged or untagged
Group[index]_[NetworkLinkIndex]_ExtParams_[ParamName]	Additional group parameters For [ParamName], the parameter name specified during L-Server creation is used.	Parameter value specified by the user
SingleNics	List of non-redundant NICs in single configurations	NIC numbers separated by spaces
NIC [index]_NetworkLinks	NetworkLink list allocated to groups	NetworkLinkIndex separated by spaces
NIC [index]_[NetworkLinkIndex]_IpAddress	NIC IP addresses	IPv4 addresses separated by periods (".")
NIC [index]_[NetworkLinkIndex]_Netmask	NIC Net masks	
NIC [index]_[NetworkLinkIndex]_DNSServer	NIC DNS addresses [Windows]	
NIC [index]_[NetworkLinkIndex]_DefaultGateway	Default gateway	
NIC [index]_[NetworkLinkIndex]_Vlanid	VLANID of NetLink allocated to NICs	2-4094
NIC [index]_[NetworkLinkIndex]_VlanMode	Specification of tagged VLANs or untagged VLANs	tagged or untagged
NIC [index]_[NetworkLinkIndex]_ExtParams_[ParamName]	Additional NIC parameters For [ParamName], the parameter name specified during L-Server creation is used.	Parameter value specified by the user
DNSServer	DNS Server [Linux]	-
Route [index]	Static routing configuration Type, destination address for packet, net mask and gateway address are specified, separated by commas	- type: type of destination address - net: net address - host: host address - destination address: destination address for packet - mask: net mask - gateway address: gateway address

Information

When using a driver specific parameter such as GLS or Bonding for the script configuring the network, describe the information in the following files:

- Network unit parameter (describes IP addresses of monitoring targets for GLS or Bonding)

`/etc/opt/FJSVrcvmr/customize_data/net/net_info.network_resource_name.conf`

- L-Server unit parameter (configures QoS or others to set for NICs)

`/etc/opt/FJSVrcvmr/customize_data/l_server/net/net_info.l_server_name.conf`

When deploying L-Servers, send a network information file with content matching the L-Server name or the name of a network resource connected to the L-Server, to the destination server.

Example

```
#MAC information list of NIC equipped on Physical Server
NIC1_MacAddress="XX:XX:XX:XX:XX:X1"
NIC2_MacAddress="YY:YY:YY:YY:YY:Y2"
NIC3_MacAddress="XX:XX:XX:XX:XX:X3"
NIC4_MacAddress="YY:YY:YY:YY:YY:Y4"
NIC5_MacAddress="XX:XX:XX:XX:XX:X5"
NIC6_MacAddress="YY:YY:YY:YY:YY:Y6"
#####
#NIC redundancy information
#####
Groups="0 1"#Redundant group list(#0,#1 Group exist in this example)
Group0_NetworkLinks="0" #One NetworkLink exists in group 0 (index 0 only)
Group1_NetworkLinks="0 1" #Multiple NetworkLinks exist in group 1 (index 0 to 1)

#Group is written in Group_[NICGroupIndex]_[NetworkLinkIndex]
Group0_0_Nics="1 2" #Bonding NIC 1 and 2
Group0_0_IpAddress="192.168.0.1"
Group0_0_Netmask="255.255.255.0"
Group0_0_DefaultGateway="192.168.0.253"
Group0_0_Vlanid=2
Group0_0_VlanMode="tagged"
Group0_0_DNSServer="ipaddress"

Group1_0_Nics="3 4" #Bonding NIC 3 and 4
Group1_0_IpAddress="192.168.1.1"
Group1_0_Netmask="255.255.255.0"
Group1_0_Vlanid=3
Group1_0_VlanMode="tagged"

Group1_1_Nics="3 4" #Bonding NIC 3 and 4
Group1_1_IpAddress="192.168.2.1"
Group1_1_Netmask="255.255.255.0"
Group1_1_VlanMode="untagged"#Example that VLANID is not specified, since this group is
untagged VLAN
Group1_1_DNSServer="ipaddress"
#####
#Non redundant NIC information
#####
SingleNics="5 6"#List of non-redundant NIC
NIC5_NetworkLinks ="0" #One NetworkLink exists in NIC5(index 0 only)
NIC6_NetworkLinks ="0 1" #Multiple NetworkLinks exist in NIC6(index 0 to 1)

NIC5_0_IpAddress="192.168.20.1"
NIC5_0_Netmask="255.255.255.0"
```

```

NIC5_0_VlanMode="untagged"#Example where VLANID is not specified, since this group is
untagged VLAN
NIC5_0_DNSServer="ipaddress"

NIC6_0_IpAddress="192.168.30.1"
NIC6_0_Netmask="255.255.255.0"
NIC6_0_VlanMode="untagged"#Example where VLANID is not specified, since this group is
untagged VLAN

NIC6_1_IpAddress="192.168.40.1"
NIC6_1_Netmask="255.255.255.0"
NIC6_1_Vlanid=40
NIC6_1_VlanMode="tagged"#Tagged VLAN
NIC6_1_DNSServer="ipaddress"
Route0=net,192.168.200.0,255.255.255.0,192.168.1.254

```

D.8 Selection of Physical Servers for Physical L-Servers

When performing the following operations, choose a physical server that satisfies the conditions:

- Create Physical L-Servers
- Start a physical L-Server
- Switch over spare servers of physical L-Servers

Explains the prerequisites when using physical servers, and method for selecting a physical server while searching physical servers that satisfy the conditions.

Prerequisites when Using Physical Servers

The physical server that satisfies the following conditions will be the target of selection.

- When "status" of physical server is "normal", "warning", or "stop"
- Server switchover is not configured in the server resource tree
- The information of the admin LAN specified in the physical L-Server and the information of the admin LAN for a physical server are the same
- The server types (blade server or rack mount server) of the physical L-Server and the physical server are the same
- The physical server is not used for another physical L-Server
- All information for a physical server such as "CPU core count", "CPU clock speed", and "memory capacity" can be collected

Selection Method for Physical Servers

Select a physical server from a group of physical servers satisfying prerequisites using the following order of priority:

Describe the items in order of their priority.

- Create Physical L-Servers
 - Priority of resource pools (*1)
 - The server with the least difference between the physical server configuration check and the L-Server definition (*2)
 - There are no physical L-Servers that are [preserved]
 - A physical server that is in the same chassis as the server started at the last startup (when using a blade server)
 - A physical server which was started at the last startup

- Start a physical L-Server
 - Priority of resource pools (*1)
 - The server with the least difference between the physical server configuration check and the L-Server definition (*2)
 - There are no physical L-Servers that are [preserved]
 - A physical server that is in the same chassis as the server started at the last startup (when using a blade server)
 - A physical server which was started at the last startup
- Switch over spare servers of physical L-Servers
 - Priority of resource pools (*1)
 - The server with the least difference between the physical server configuration check and the L-Server definition (*2)
 - There are no physical L-Servers that are [preserved]
 - A physical server that is in the same chassis as the server started at the last startup (when using a blade server)

*1: When "Resource type" and "Spare server pool" are "Automatic", priority is given to a resource pool. If the priority of resource pools is the same, the resource pool is selected randomly.

*2: Compare the physical L-Server definition and the physical server using the following conditions. A physical server with the same conditions or meeting all conditions is selected.

- If model names are specified when specifying a physical L-Server
 - The "model names" are the same, or compatible
 - Number of NICs
- If CPUs and memories are specified when specifying a physical L-Server
 - CPU core count
 - CPU clock speed
 - Memory capacity
 - Number of NICs

When the "Use a low spec server" checkbox for "Spare server specs" is unchecked, the servers will be selected as follows:

- If model names are specified when specifying a physical L-Server
 - A physical server with the same server model as that in the L-Server definition is selected.
- If CPUs and memories are specified when specifying a physical L-Server
 - Configurations are not checked.

When there are multiple physical servers meeting the same conditions, the server is selected randomly.

D.9 Advisory Notes for Creation of Physical L-Servers

This section explains advisory notes regarding creation of physical L-Servers.

Prerequisites

To create a physical L-Server, Virtual I/O using VIOM or HBA address rename is required.

Usage methods of VIOM and HBA address rename differ depending on the hardware of managed servers used to configure a physical L-Server.

- Blade Servers
 - Use VIOM.

- Rack Mount Servers

Use HBA address rename.

It is also necessary to enter configuration information (CPU core count, CPU clock speed, memory capacity, etc.) of the physical servers in the definition file.

For details, refer to "[6.1 Creating Definition Files](#)".

Deleting an L-Server

When deleting an L-Server, log out from the ETERNUSmgr of ETERNUS storage registered on ESC.

When operating NetApp storage in cluster environments and operating a partial system due to system trouble, perform the operation after recovering the NetApp storage and returning the system to cluster operation.

When the disk resource is a LUN created in advance or a LUN for iSCSI boot, it is recommended to delete the data on the disk, as the data is not deleted when deleting an L-Server to which the disk resource is allocated.

For details on how to delete data on disks, refer to "7.5 Storage Resources" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

L-Server Snapshots

Snapshots of L-Servers cannot be used.

Moving an L-Server between Servers (Migration)

Moving between servers (migration) cannot be used.

Network Settings for L-Servers OS's

In Resource Orchestrator, settings for an operating system, such as NIC redundancy on servers or tagged VLANs, are not performed.

When specifying an image of Red Hat Enterprise Linux, the IP address cannot be automatically configured.

When starting an OS after L-Server creation, set the image to be configured automatically after creating an L-Server. For this setting, use the image collected in the state where the scripts to configure the network settings have been prepared beforehand.

For details, refer to "[D.7.4 Network Redundancy and VLAN Settings of L-Servers](#)".

Appendix E Design and Configuration for Creating Virtual L-Servers

This section explains how to perform design and configuration when creating a virtual L-Server.

E.1 Common Functions of Server Virtualization Software

This section explains functions available for all supported server virtualization software.

E.1.1 Definition Files

This section explains the definition files used when creating a virtual L-Server.

When using an L-Server, configuration of a definition file may be necessary.

- When using overcommit
Refer to "[Overcommit Definition Files](#)".
- When defining VM specific information
Refer to "[VM Specific Information Definition File](#)".
- When using thin provisioning
Refer to "[Configuration of Priority for Resource Selection on Thin Provisioning](#)".
- When creating a virtual L-Server using a server which cannot use ServerView Agents
Refer to "[Configuration when Creating a Virtual L-Server Using a Server which cannot Use ServerView Agents](#)".
- Configuration when Creating a Virtual L-Server Using VMware ESXi on Other Vendor's Servers
Refer to "[Configuration when Creating a Virtual L-Server Using VMware ESXi on Other Vendor's Servers](#)".
- When using alive monitoring
Refer to "[Definition File for Alive Monitoring](#)".

Overcommit Definition Files

This section explains overcommit definition files.

Storage Location of the Definition File

[Windows]
Installation_folder\Manager\etc\customize_data

[Linux]
/etc/opt/FJSVrcvmr/customize_data



In the storage location above, the sample definition file (pool.sample.rcxprop) is stored. When using the sample as the definition file, place the file after deleting the ".sample" included in the file name.

Name of the Overcommit Configuration File

pool.rcxprop

Format of the Overcommit Configuration File

```
over_commit=pool1,pool2,...
over_commit_calculate_by_reserve_value=true|false
```

over_commit

Multiple VM pool names can be specified. When specifying multiple resource pools, separate them using commas (",").
If the VM pool is arranged in a hierarchy, specify the name using an absolute path.
For a VM pool directly under the orchestration tree, specify only its name.

 **Example**

```
over_commit=VMPool,/folder1/VMPool
```

 **Point**

When creating L-Servers that use overcommit and L-Servers that do not, both a VM pool that uses overcommit and a VM pool that does not must be created.

over_commit_calculate_by_reserve_value

Specify the calculation method for available space for a VM pool used for overcommit.
One of the following values can be specified.

- When using a reservation value
Specify "true".
- When using a maximum value
Specify "false".

"false" is specified in the following cases:

- When specification of "over_commit_calculate_by_reserve_value" is omitted
- When an invalid value is specified

 **Example**

```
over_commit_calculate_by_reserve_value=true
```

VM Specific Information Definition File

This file contains the information to be specified for a virtual machine when creating an L-Server or when modifying a configured (defined) L-Server.

VM specific information definition files can be created for each user group.

Use the UTF-8 character code.

The order of the priority of the parameters is as follows:

L-Server XML file > L-Server template > Definition file (User group) > Definition file (Shared on the system)

Storage Location of the Definition File

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

[Linux]
/etc/opt/FJSVrcvnr/customize_data/vm_prop

Point

In the storage location above, the sample definition file (vm_VMTYPE.rcxprop.sample) is stored. When using the sample as the definition file, place the file after changing "VMTYPE" to the VM type and deleting ".sample".

Definition File Name

Definition files can be divided into definitions that are available for each user group and definitions that are common on the system.

If the same key is configured in the definition file common on the system and the definition file for a specific user group, priority is given to the values indicated in the definition file for the user group.

- User Groups

`vm_user_group_name_VM_type.rcxprop`

- Common on System

`vm_VM_type.rcxprop`

Note

- For *VM_type*, enter the VM type to be specified when creating an L-Server, such as VMware, Hyper-V, Oracle VM, or RHEL-KVM. This value is not case-sensitive.
- When there are multiple files with the same *VM_type* specified in the filename, the *VM_type* of the filenames are sorted in ascending order of character code, and the one listed first will be selected.

Example

```
usergroup1_VMware
usergroup1_VMWARE -> This file will be selected.
usergroup1_vmware
```

- Remove any blank spaces in the *VM_type*.

Example

```
Oracle VM -> OracleVM
```

Definition File Format

In the definition file, an item to define is entered on each line. Each line is entered in the following format.

```
Key = Value
```

Definition File Items

Specify the following items.

Table E.1 The List of Parameters

Key	Description
processor_reserve_spec	Specify the minimum amount of CPU resources to be allocated. Enter a value in the range from 0 to the limit of CPU performance, using a number with up to one decimal place, in units of gigahertz. In the XML files for L-Servers and L-Server templates, set the value for "CPUReserve".

Key	Description
processor_share	<p>Specify the relative proportion of CPU resources for allocation.</p> <p>Enter an integer equal to or greater than 1.</p> <p>In the XML files for L-Servers and L-Server templates, set the value for "CPUShare".</p> <p>Enabled when the VM type is set to "VMware".</p>
memory_reserve_size	<p>Specify the minimum amount of memory resources to be allocated.</p> <p>Enter a value in the range from 0 to the limit of memory size, using a number with up to one decimal place, in units of gigabytes.</p> <p>In the XML files for L-Servers and L-Server templates, set the value for "MemoryReserve".</p> <p>Enabled when the VM type is set to "VMware".</p>
memory_share	<p>Specify the relative proportion of memory resources for allocation.</p> <p>Enter an integer equal to or greater than 0.</p> <p>In the XML files for L-Servers and L-Server templates, set the value for "MemoryShare".</p> <p>Enabled when the VM type is set to "VMware".</p>
processor_weight	<p>Specify the priority for CPU allocation.</p> <p>Enter an integer between 1 and 10,000.</p> <p>In the XML files for L-Servers and L-Server templates, set the value for "CPUWeight".</p> <p>Enabled when the VM type is set to "Hyper-V".</p>
dynamic_memory	<p>Specify the dynamic memory settings.</p> <ul style="list-style-type: none"> - When dynamic memory is enabled Specify "true". - When dynamic memory is disabled Specify "false". <p>When omitted, the value varies depending on the initial memory size and memory buffer specified when creating an L-Server.</p> <ul style="list-style-type: none"> - When the initial memory size or memory buffer is configured Dynamic memory is enabled - When neither initial memory size nor memory buffer is configured Dynamic memory is disabled <p>When dynamic memory is disabled, the values specified for memory_startup_size and memory_buffer_rate will be ignored.</p> <p>Enabled when the VM type is set to "Hyper-V".</p>
memory_startup_size	<p>Specify the initial amount of memory to be allocated at startup.</p> <p>Enter a value between 0.1 and the limit of memory size.</p> <p>In the XML files for L-Servers and L-Server templates, set the value for "StartupRAM".</p> <p>When setting this value for a virtual machine, enable dynamic memory in the XML file to be specified when creating an L-Server template or L-Server, or do not specify dynamic memory.</p> <p>When no L-Server template is used and dynamic memory settings are not specified in the XML file specified when creating an L-Server, dynamic memory is enabled or disabled based on the existence of this setting and the setting for memory_buffer_rate.</p> <ul style="list-style-type: none"> - When this setting or memory_buffer_rate are set Dynamic memory is enabled - When this setting and memory_buffer_rate are not set Dynamic memory is disabled

Key	Description
	<p>When dynamic memory is disabled, this setting is ignored. Enabled when the VM type is set to "Hyper-V".</p>
memory_buffer_rate	<p>Specify the percentage of memory to be reserved as a buffer.</p> <p>Enter an integer between 5 and 2000 in units of percent.</p> <p>In the XML files for L-Servers and L-Server templates, set this value for "MemoryBuffer". When setting this value for a virtual machine, either enable dynamic memory in the XML file to be specified when creating an L-Server template or L-Server, or do not specify dynamic memory.</p> <p>When no L-Server template is used and dynamic memory is not specified in the XML file specified during L-Server creation, dynamic memory setting is enabled or disabled based on whether this setting and the setting for memory_startup_size exist.</p> <ul style="list-style-type: none"> - When this setting or memory_startup_size exists Dynamic memory is enabled - When this setting and memory_startup_size are not set Dynamic memory is disabled <p>When dynamic memory is disabled, this setting is ignored. Enabled when the VM type is set to "Hyper-V".</p>
memory_weight	<p>Specify the priority for allocation of memory.</p> <p>Enter an integer between 0 and 10,000.</p> <p>In the XML files for L-Servers and L-Server templates, set this value for "MemoryWeight". Enabled when the VM type is set to "Hyper-V".</p>
max_definable_memory_size	<p>Specify the maximum amount of memory that can be configured for the VM guest on KVM.</p> <p>Enter a value in the range from the limit of memory size to the memory size of a physical server, using a number with up to one decimal place, in units of gigabytes.</p> <p>The memory amount for the VM guest can be changed up to this value setting as the upper limit.</p> <p>When omitted, this memory size is the same as the amount of physical memory for the VM host.</p> <p>When the amounts of memory mounted on the VM hosts registered in a VM pool are not the same, specify the memory capacity less than the value of VM host with the minimum memory capacity, when specifying this item.</p> <p>When specifying the values exceeding the physical memory capacity, starting of an L-Server fails.</p>

 See

When not describing a parameter in the VM specific information definition file, refer to each element name in "2.3.2 Definition Information for Virtual L-Servers (XML)" in the "Reference Guide (Resource Management) CE".

 Note

When modifying specifications of an L-Server to which resources have been allocated, the settings in this definition file are not reflected because priority is given to the values already configured for the L-Server. In this case, enter new values in the XML file and then execute the appropriate commands to reflect the changes.

When individual parameters are specified when creating an L-Server template or L-Server, priority is given to those settings over those in this definition file.

Configuration of Priority for Resource Selection on Thin Provisioning

When setting to automatic selection for resource selection while creating L-Server or attaching a disk under the condition that both storage pools with and without the configuration of thin provisioning attributes remain the same priority, either of their resources can be given higher priority.

When the definition file has been edited, restart the manager.

Location of the Definition File

[Windows]

Installation_folder\Manager\etc\customize_data

[Linux]

/etc/opt/FJSVrcvnr/customize_data

Definition File Name

storage.rcxprop

Definition File Format

In the definition file, the items to set are entered on individual lines. Each line is entered in the following format.

<i>Item_specified</i> = <i>Value_specified</i>

Definition File Items

- SELECT_THIN_PROVISIONING_POOL_FIRST

When both storage pools with and without the configuration of thin provisioning attributes remain the same priority, either of their resources can be given higher priority for automatic selection of storage resource.

- If "true" is specified

A storage pool with thin provisioning attributes will be given priority.

- If "false" is specified

A storage pool without thin provisioning attributes will be given priority.

- If nothing is specified

"false" is set.



Example

.....
An example definition file is indicated below.

SELECT_THIN_PROVISIONING_POOL_FIRST = true
--

.....

Configuration when Creating a Virtual L-Server Using a Server which cannot Use ServerView Agents

As ServerView Agents cannot be used for the following servers, the hardware configuration information (CPU core count, CPU clock speed, memory capacity, etc.) cannot be acquired.

- PRIMERGY CX1000 series servers
- Other vendor's servers

When creating a virtual L-Server after installing VM management software on the servers above, it is necessary to register a managed server, after creating a definition file first, and defining the configuration information.

In the following cases, create the definition file first, and then register the hardware information with Resource Orchestrator again.

- If the target server was registered with Resource Orchestrator before creation of the definition file
- When modifying the configuration information (CPU core count, CPU clock speed, memory capacity, etc.) in the definition file of a server that has been registered with Resource Orchestrator

For details, refer to "Chapter 7 Hardware Maintenance" in the "Operation Guide CE".

Note

When there are differences between the values in the definition file and the actual configuration information of the server, creation or starting of the virtual L-Server may fail, or the virtual machine may be deployed using incorrect CPU and memory information.

Be sure to confirm that the values entered in the definition file and the actual configuration information of the server are the same.

Storage Location of the Definition File

[Windows]

Installation_folder\Manager\etc\customize_data

[Linux]

/etc/opt/FJSVrcvmr/customize_data

Definition File Name

server_spec.rcxprop

Character Code

[Windows/Linux]

UTF-8

Line Break Code

[Windows]

CR/LF

[Linux]

LF

Definition File Format

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

```
ServerSpec,V1.0
```

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

When defining two or more servers, use line breaks.

Each line is entered in the following format.

```
physical_server, cpu_core_count, cpu_clock, memory_size[, cpu_type]
```

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

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

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

Definition File Items

physical_server

Enter the same physical server name as the one entered when registering a managed server.

cpu_core_count

Enter the total number of physical CPU cores.

Enter an integer between 0 and 999.

If "0" is entered, a hyphen ("-") will be displayed in the General information of the Resource Details window, indicating that no virtual L-Server will be created.

cpu_clock

Enter the CPU clock speed.

Enter an integer between 0 and 999,999.

Use megahertz for the unit. Enter 1,000 MHz for 1 GHz, for example.

If "0" is entered, a hyphen ("-") will be displayed in the General information of the Resource Details window, indicating that no virtual L-Server will be created.

memory_size

Enter the total memory size.

Enter an integer between 0 and 999,999,999.

Use megabytes for the unit. Enter 1,024 MB for 1 GB, for example.

If "0" is entered, a hyphen ("-") will be displayed in the General information of the Resource Details window, indicating that no virtual L-Server will be created.

cpu_type

Enter the CPU type.

The string must be composed of alphanumeric characters and symbols (ASCII characters 0x20 to 0x7e), except for commas (","), and can be up to 64 characters long.

When omitted, a hyphen ("-") is displayed.



Example

An example definition file is indicated below.

```
ServerSpec,V1.0

#####
# server_spec.rcxprop
#
#All Rights Reserved, Copyright(C) FUJITSU LIMITED 2011
#####
#
# physical_server, cpu_core_count, cpu_clock, memory_size, cpu_type
#

server001, 8, 3160, 4096, Intel(R) Xeon(R)
server002, 8, 2660, 12288, Intel(R) Xeon(R)
server003, 2, 2000, 65536
server004, 4, 4000, 4096, Intel(R) Xeon(R) Processor E5501
```

Configuration when Creating a Virtual L-Server Using VMware ESXi on Other Vendor's Servers

It is necessary to define that the server can be used as a VM software agent without using an agent for Resource Orchestrator, by creating the definition files before registering a server. When registering the server, select the "Register agent" checkbox, and register the server as VM host. In VM hosts registered using these definitions, obtain the server status or hardware configuration information (CPU core count, CPU clock speed, memory capacity, etc.) from VM software.

When the definition file is changed after registration, the modification is not valid.

Note

- The server cannot be used for anything other than a VM host (spare server or Windows/Linux server).
- Even the following settings are configured, priority is given to the information obtained from VM software.
 - Configuration when Creating a Virtual L-Server Using a Server which cannot Use ServerView Agents
 - Configurations to specify "Enable" for server management software (ServerView) when creating a server
- On VM hosts registered using this definition, the following functions cannot be used.
 - Server switchover
- In the configuration definition file for pre-configuration, do not describe the values in the following section header parameter for section name [Server]: If the values are described, registration fails.
 - snmp_community_name

Storage Location of the Definition File

[Windows]
Installation_folder\Manager\etc\customize_data

[Linux]
/etc/opt/FJSVrcvmr/customize_data

Point

In the storage location above, the sample definition file (server_control.sample.rcxprop) is stored. When using the sample as the definition file, place the file after deleting the ".sample" included in the file name.

Definition File Name

server_control.rcxprop

Character Code

[Windows/Linux]
UTF-8

Line Break Code

[Windows]
CR/LF

[Linux]
LF

Definition File Format

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

```
ServerControl,V1.0
```

- In the definition file, the name of each server is described on an individual line.

When defining two or more servers, use line breaks.
Each line is entered in the following format.

```
physical_server
```

Even if there are multiple same physical server names in the individual lines, no errors occur.

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

Definition File Items

physical_server

Enter the same physical server name as the one entered when registering a managed server.

Enter a character string beginning with an alphabetical character and containing up to 15 alphanumeric characters and hyphens ("-"). The following physical server names are ignored.

- Blade Servers
- PRIMEQUEST Servers
- SPARC Enterprise Servers
- Unregistered Servers



Information

When there are no definition files when registering a server, or when the physical server name to register is not described, the server is regarded as being a Fujitsu server.



Example

An example definition file is indicated below.

```
ServerControl,V1.0

#####
# server_control.rcxprop
#
#All Rights Reserved, Copyright(C) FUJITSU LIMITED 2012
#####
#
# physical_server
#

server1
server2
```

Definition File for Alive Monitoring

When using alive monitoring, create the definition file and specify the parameters for alive monitoring. The configuration of this parameter must be unique in the system.

The alive monitoring of virtual L-Server monitors the heartbeat of VM guests corresponding to the virtual L-Server by using the heartbeat monitoring functions of server virtualization software.

For details on heartbeat monitoring functions, refer to the server virtualization software manual.

[VMware]

For Resource Orchestrator alive monitoring functions, configure the heartbeat monitoring settings in "VMMonitoring" for VMware HA on each VM guest.

[Hyper-V]

For Resource Orchestrator alive monitoring functions, configure the heartbeat monitoring settings in "Heartbeat setting" for MSFC on each VM guest.



Note

When changing configuration of alive monitoring on server virtualization software, the modification is not reflected on Resource Orchestrator.

Therefore, do not change alive monitoring configurations on server virtualization software.

Storage Location of the Definition File

The file in which the default values are described is located during installation.

[Windows]

Installation_folder\Manager\etc\customize_data\alive_monitoring

[Linux]

/etc/opt/FJSVrcvmr/customize_data/alive_monitoring

Definition File Name

- vm_VMware.rcxprop
- vm_Hyper-V.rcxprop

The file name is not case sensitive.

Definition File Format

In the definition file, the items to set are entered on individual lines. Each line is entered in the following format.

<i>Item_specified= Value_specified</i>
--

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

Specified Items for vm_VMware.rcxprop

min_uptime

Specify "Minimum uptime" in the heartbeat monitoring settings for VMware.

Enter an integer between 0 and 100000. The unit is seconds.

"120" is specified as the default.

failure_interval

Specify "Failure interval" in the heartbeat monitoring settings for VMware.

Enter an integer between 1 and 100000. The unit is seconds.

"30" is specified as the default.

max_failures

Specify "Maximum per-VM resets" in the heartbeat monitoring settings for VMware.

Enter an integer between 1 and 1000.

"3" is specified as the default.

max_failure_window

Specify "Maximum resets time window" in the heartbeat monitoring settings for VMware.

Enter -1, and an integer between 1 and 1000. The unit is hours.

When -1 is specified, "None" is configured.

"1" is specified as the default.

off_override_cluster

When configuring to disable alive monitoring in Resource Orchestrator, overwrite the heartbeat monitoring settings for VMware clusters, and specify if disabling the heartbeat monitoring settings of VM guests.

To disable heartbeat monitoring configuration of VM guests, specify "true".

To configure the same settings of VM guest heartbeat monitoring as the settings of VMware cluster, specify "false".

"false" is specified as the default.

Note

When applying the modified details to an already created L-Server, execute the `rcxadm lserver modify` command after changing the definition files.

For details on the following parameters, refer to the VMware manual.

- Minimum uptime
- Failure interval
- Maximum per-VM resets
- Maximum resets time window

Specified items for `vm_Hyper-V.rcxprop`

`restart_period`

Specify "Period for restarts [mm:ss]" in the heartbeat monitoring settings for MSFC.

Enter an integer between 0 and 3599. The unit is seconds.

Specify a smaller value of time than that specified in "retry_period_on_failure".

"900" is specified as the default.

`restart_threshold`

Specify "Maximum restarts in the specified period" in the heartbeat monitoring settings for MSFC.

Enter an integer between 0 and 4294967295.

"1" is specified as the default.

`failover`

Specify "If restart is unsuccessful, fail over all resources in this service or application" in the heartbeat monitoring settings for MSFC.

When performing failover, specify "true".

When not performing failover, specify "false".

"true" is specified as the default.

`retry_period_on_failure`

Specify "If all the restart attempts fail, begin restarting again after the specified period [hh:mm]" in the heartbeat monitoring settings for MSFC.

Enter -1, and an integer between 0 and 1439. The unit is minutes.

When -1 is specified, it is disabled.

When specifying 0 to 1,439, specify a larger value of time than that specified in "restart_period".

"60" is specified as the default.

Note

When applying the modified details to an already created L-Server, execute the `rcxadm lserver modify` command after changing the definition files.

Refer to the MSFC manual for details on each parameter.

E.2 VMware

This section explains how to use VMware as server virtualization software.

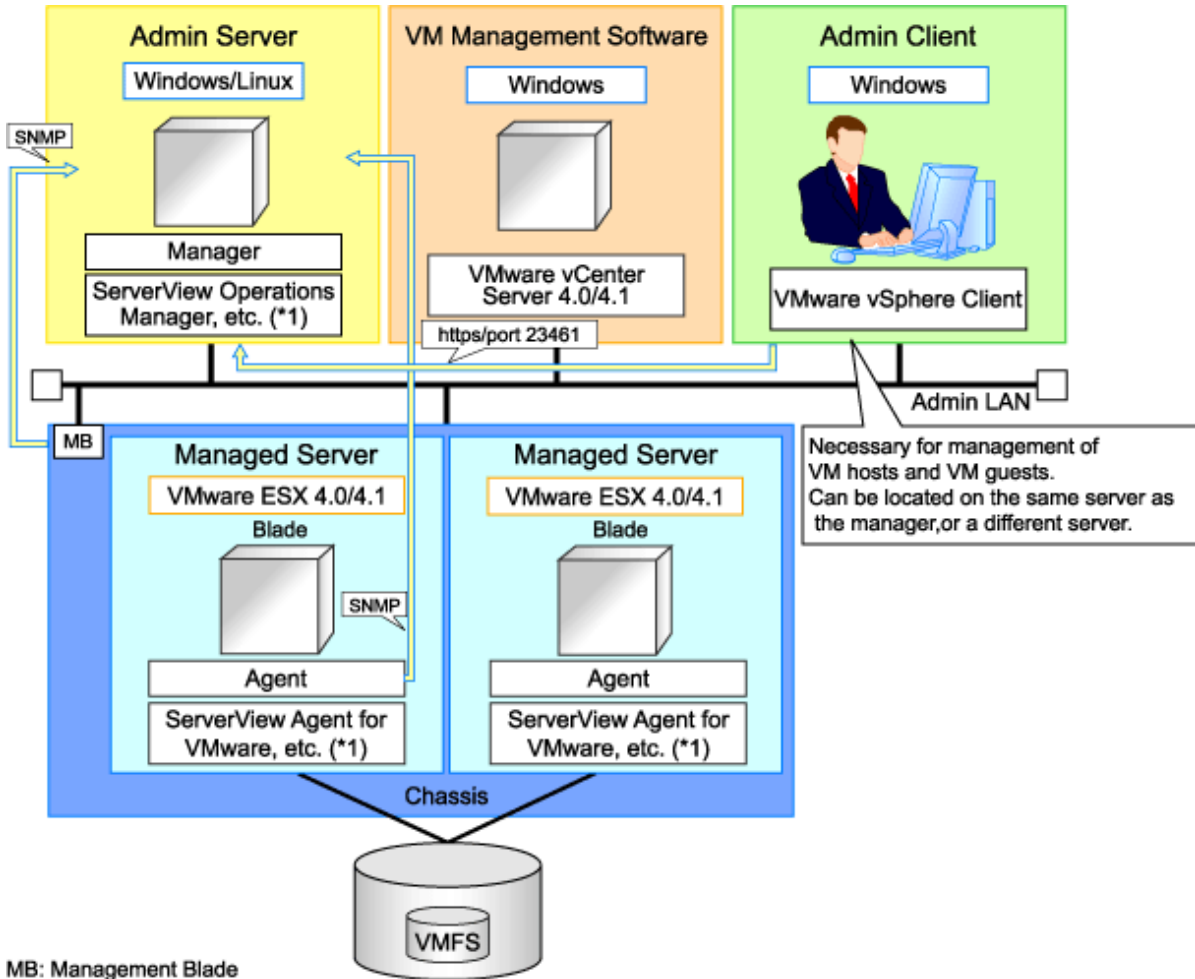
E.2.1 System Configuration

This explains how to configure VMware for use as server virtualization software.

Example of System Configuration

An example system configuration using VMware ESX is given below.

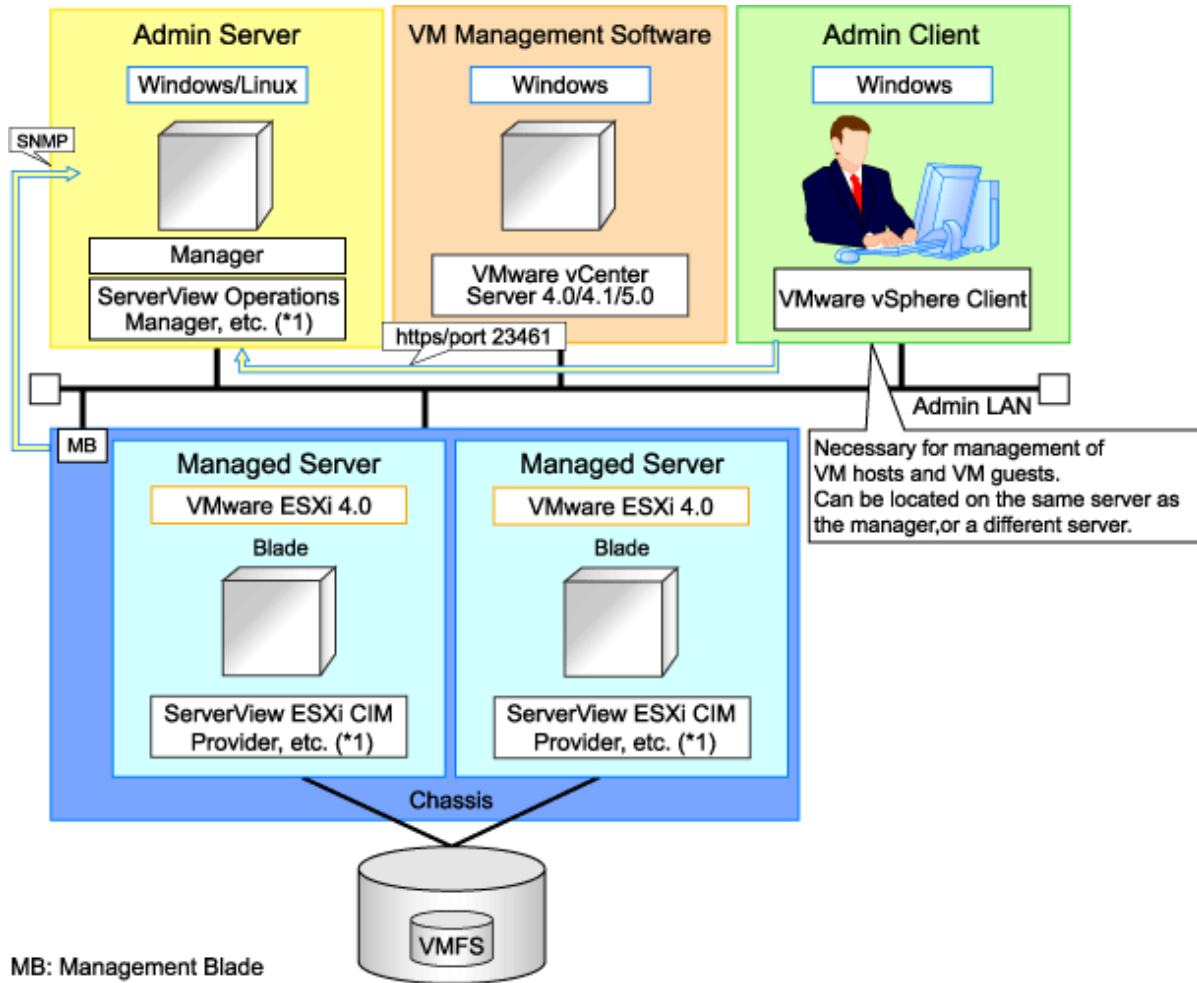
Figure E.1 System Configuration Example Using VMware ESX



*1: For details on required software, refer to "1.4.2.2 Required Software".

An example system configuration using VMware ESXi is given below.

Figure E.2 System Configuration Example Using VMware ESXi

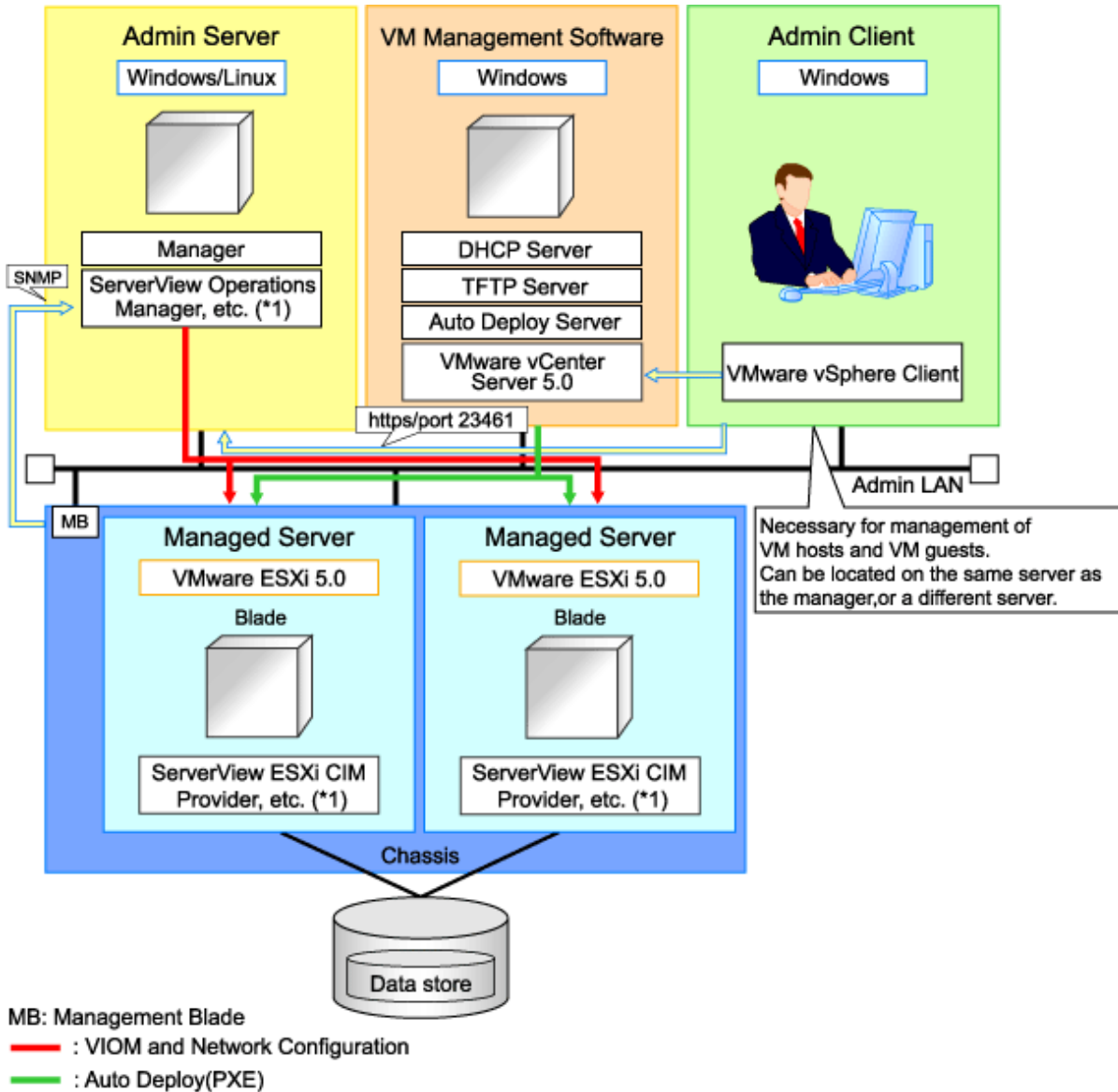


MB: Management Blade

*1: For details on required software, refer to "[1.4.2.2 Required Software](#)".

An example system configuration for deploying VMware ESXi using Auto Deploy is given below.

Figure E.3 Example of System Configuration for Installing VMware ESXi Using Auto Deploy



*1: For details on required software, refer to "1.4.2.2 Required Software".

Note

For a configuration example for rack mount servers, delete the chassis and management blades from the diagram above.

Simplifying Network Settings

Network settings can be easily configured by Resource Orchestrator when creating L-Servers.

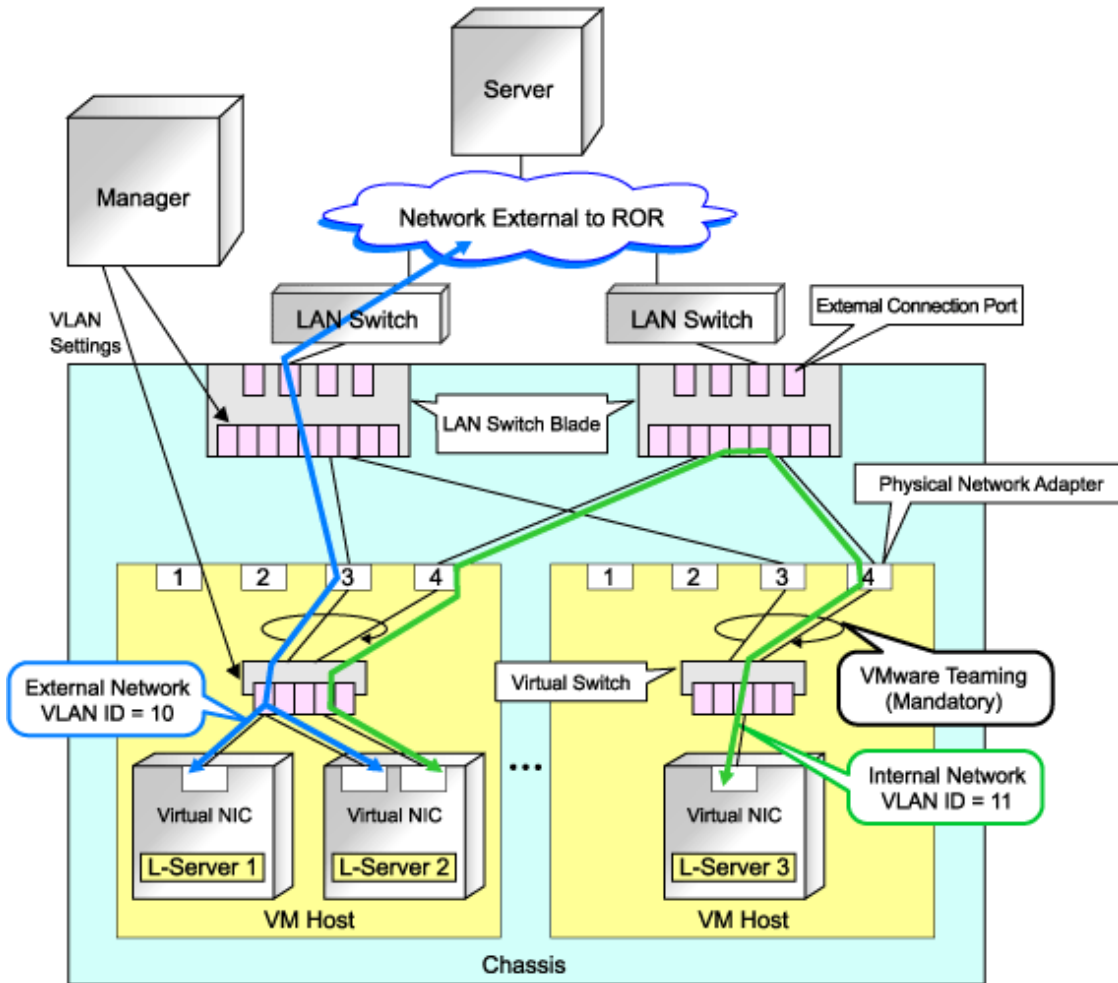
Depending on the conditions, such as hardware (blade servers or rack mount servers) and the presence or absence of network redundancy for L-Servers, the setting ranges of networks differ.

For details, refer to "1.2.7 Simplifying Networks" and "4.2.4 Preparations for Resource Orchestrator Network Environments".

Network Configuration Example

An example network configuration using VMware is given below:

Figure E.4 LAN Switch Blade and Virtual Switch Configuration Using Network Resources [VMware]



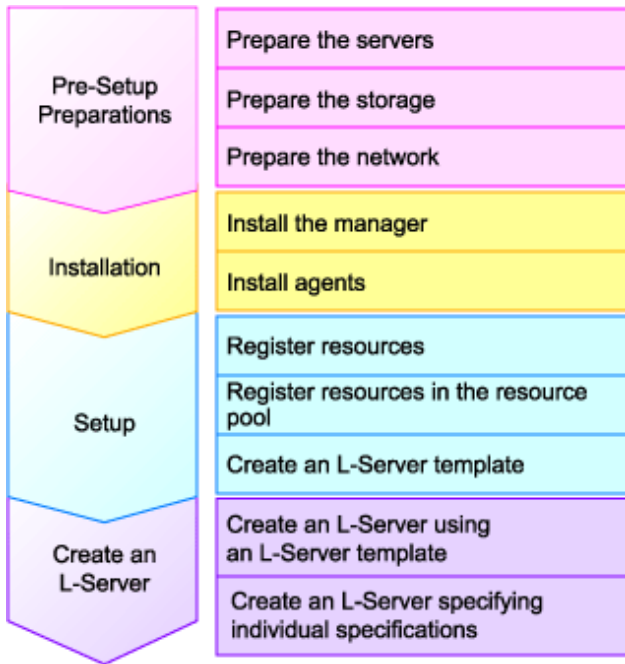
Note

- When network settings have been performed automatically for an L-Server in a VMware environment, redundancy of virtual switches and physical network adapters will be performed using VMware Teaming.
- For Resource Orchestrator, configure the LAN switch blades when using switch mode or end-host mode.
- Configure the admin and public LANs as physically separate. For details, refer to "4.2 Defining and Configuring the Network Environment".

L-Server Creation Procedure

Use the following procedure to create L-Servers:

Figure E.5 Resource Orchestrator Setup Procedure



For details on pre-setup preparations, refer to "[E.2.2 Preparations](#)".

For details on how to install Resource Orchestrator, refer to "[E.2.3 Installation](#)".

For details on how to set up Resource Orchestrator, refer to "[E.2.5 Setup](#)".

For details on how to create an L-Server, refer to "[L-Server Creation](#)" of "[E.2.5 Setup](#)".



Point

- When using VMware ESX
Install Resource Orchestrator agents and ServerView for VMware agents.
- When using VMware ESXi
Install ServerView ESXi CIM Provider agents.

E.2.2 Preparations

Pre-setup preparations are required to create and manage VMware virtual machines as L-Servers of Resource Orchestrator.

For details on pre-setup preparations for VMware environments, refer to the VMware manual.

Preparations for Servers

In addition to the operations in "[4.1.1.1 Preparations for Server Environments](#)", the following operations are necessary.

- Configure VIOM
When using I/O virtualization, configuration of VIOM is necessary.
- Install and configure VMware ESX
When installing an OS on a physical server, refer to the server virtualization software manual.
When installing a VM host in an L-Server, refer to "[Appendix F Installation of VM Hosts on Physical L-Servers](#)".
- Install and configure VMware vCenter Server
Necessary for management of VM hosts and L-Servers.

It is necessary to install the Microsoft Sysprep tools for VMware vCenter Server to enable collection of L-Server cloning images. For details on how to install the Microsoft Sysprep tools, refer to the installation section of "vSphere Basic System Administration" of VMware.

Refer to the relevant version of document, referring to the following URL:

vSphere Basic System Administration

URL: http://www.vmware.com/support/pubs/vs_pubs.html (As of February 2012)

- Configure VMware clusters

When performing movement between servers (migration), register the source and destination VM hosts for migration in the same cluster.

When not performing redundancy of L-Servers, it is not necessary to enable VMware HA or VMware DRS.

- Design and configure VMware HA

When performing redundancy of L-Servers, VMware HA configuration must be done in advance.

- Design and configure VMware DPM, VMware DRS, VMware FT, and VMware Storage VMotion

When using VMware DPM, VMware DRS, VMware FT, or VMware Storage VMotion, configure them in advance using VMware vCenter Server.

When setting configuration of VMware DRS or VMware DPM to "Manual", startup of L-Servers and VM guests may fail. For details, refer to "When using VMware DRS or VMware DPM".

- When using VMware DRS or VMware DPM

It is necessary to configure the following settings beforehand, when moving L-Servers between VM hosts on VMware DRS or when turning on a VM host during an L-Server startup.

1. Configure VMware DRS and VMware DPM

Refer to VMware manuals and configure VMware DRS as "partly automatic" or "full automatic", or configure VMware DPM as "off" or "automatic".

When setting configuration of VMware DRS or VMware DPM to "Manual" and enabling the power control configuration of VMware DRS or DPM, startup of the L-Server may fail. In this case, start the L-Server from VM management software.

2. Configure power control for VMware DRS and DPM

When configuring power control for VMware DRS or DPM, specify "true", referring to "[Server Virtualization Software Definition File](#)" of "[E.2.4 Configuration after Installation](#)".

For details, refer to the VMware manual.

 **Information**

When performing inter-cluster movement (migration), for VMware this means inter-resource pool movement (migration). Moving an L-Server (migration) is only possible in the same cluster (the same resource pool) because resource pools of VMware are not managed in Resource Orchestrator. For details on resource pools of VMware, refer to the "vSphere Resource Management Guide" of VMware.

Refer to the relevant version of the document, referring to the following web site:

URL: http://www.vmware.com/support/pubs/vs_pubs.html (As of February 2012)

When Deploying VM Hosts Using Auto Deploy

1. Setup the Auto Deploy Server

Setup the Auto Deploy server.

For details, refer to the manual of server virtualization software.

2. Configure the DHCP Server

Prepare a server other than admin server, and configure the DHCP server to be used by the Auto Deploy function.

Perform configuration so the DHCP server assigns IP addresses only to VM hosts that have been configured using network boot services that use DHCP protocols such as Auto Deploy.

For details, refer to the manual of the server used as the DHCP server.

3. Configure the TFTP Server

Prepare a server other than admin server, and configure the TFTP server to be used by the Auto Deploy function.

For details, refer to the manual of the server used as the TFTP server.

4. Setup a VM Host

Setup a VM host for a physical L-Server.

Refer to "[Appendix F Installation of VM Hosts on Physical L-Servers](#)" and set up VM hosts.

Point

- When creating an L-Server, prepare a disk for the dump area.

At least one disk should be prepared specifying a disk that is not shared with other L-Servers.

On that disk, create a dump area for VMware ESXi.

- For the first L-Server that uses Auto Deploy, prepare the necessary number of disks with the disk capacity necessary for storing VM guests to share with other L-Servers.

When there are two or more L-Servers, prepare the disk for storing VM guests connected to the first L-Server.

On that disk, create an area for VMFS to use as a datastore.

- When configuring a VM host using Auto Deploy, use VIOM for I/O virtualization.

Note

As HBA address rename requires PXE boot, use in combination with Auto Deploy using the same PXE boot is not possible.

Storage Preparations

Check the following:

- Volumes to allocate to VMware ESX have been already created
- Zoning and affinity have been set
- VMware ESX has been configured to recognize a VMFS datastore

Network Preparations

Check the following:

- The configuration for the admin and public LANs has been designed
- The network environment for the admin LAN is configured
- The virtual switch to connect to the admin LAN has been designed and configured

When Using IBP

When using virtual L-Servers, connect the IBP uplink sets used for the public LAN and admin LAN to the VM host regardless of VIOM, after creating each IBP uplink set.

It is not necessary to use the same name for the uplink set and the name of the network resource.

Point

- For VMware virtual switches, configuration is not necessary as they are automatically configured by Resource Orchestrator.
- When performing movement between servers (migration), configure the VMkernel port group for VMotion on each VM host.
- For details on how to configure the VMkernel port group, refer to the information in "vSphere Basic System Administration" of VMware.

Refer to the relevant version of the document, referring to the following web site:

vSphere Basic System Administration

URL: http://www.vmware.com/support/pubs/vs_pubs.html (As of February 2012)

When Using Distributed Virtual Switch (VMware vDS)

In Resource Orchestrator, the NICs of VM guests and port groups can be connected to the port groups of a distributed virtual switch (VMware vDS). The port groups of the distributed virtual switch should be configured beforehand manually.

When using VMware vDS, the following preparation is necessary:

1. Create Port Groups of the Distributed Virtual Switch

Refer to the VMware manual, and create them manually.

2. Define the Correspondence of the Port Groups of the Distributed Virtual Switch and VLAN IDs

Create the distributed virtual network definition file shown below, and associate the port groups and the VLAN IDs:

Storage Location of Distributed Virtual Network Definition Files

[Windows]

Installation_folder\Manager\etc\customize_data

[Linux]

/etc/opt/FJSVrcvmr/customize_data

Distributed virtual network definition file name

vnetwork_vmware.rcxprop

File format for distributed virtual network definitions

Describe the distributed virtual network definition file in individual lines in the following format:

```
"Port_group_name_of_Distributed_Virtual_Switch"=VLAN ID[, VLAN ID...]
```

For the *VLAN ID*, an integer between 1 and 4094 can be specified. When specifying a sequence of numbers, use a hyphen ("-") such as in "1-4094".

Example

```
"Network A"=10  
"Network B"=21,22,23  
"Network C"=100-200,300-400,500
```

- Blank spaces before and after equal signs ("=") and commas (",") are ignored.
 - Describe the port group name of the distributed virtual switch correctly, as entry is case-sensitive.
 - Use the UTF-8 character code.
 - When there are multiple lines with the same distributed virtual switch port group name, all specified lines are valid.
 - When the same VLAN ID is used in lines where the port group names of different distributed virtual switches are described, the VLAN ID in the first line is valid.
3. Place the Distributed Virtual Switch Usage Configuration File

Place the distributed virtual switch use configuration file. Create the following folder and place an empty file in it.

Storage Location of Distributed Virtual Switch Usage Configuration Files

[Windows]
Installation_folder\Manager\etc\vm

[Linux]
 /etc/opt/FJSVrcvnr/vm

Distributed Virtual Switch Usage Configuration Name

vds_vc

When Using the Definition for Port Groups Excluded from the Selections for Automatic Network Configuration

If the names of the port groups to be excluded from automatic network configuration have been specified in the VMware excluded port group definition file, creation of L-Servers is possible, even if the VLAN set for the service console or VMkernel network and the one set for the port group on the virtual switch is the same.

When using a VMware excluded port group definition, the following preparation is necessary:

1. On the managed server, create a port group of the service console (or VMkernel) and the virtual switch that use the same VLAN ID.

Refer to the VMware manual, and create them manually.

2. Create a VMware excluded port group definition file, and define the name of the service console created at 1. as the port group name to be excluded.

Storage location of the VMware excluded port group definition file

[Windows]
Installation_folder\Manager\etc\customize_data

[Linux]
 /etc/opt/FJSVrcvnr/customize_data

File name of the VMware excluded port group definition file

vnetwork_excluded_vmware.rcxprop

File format for the VMware excluded port group definition file

Describe the VMware excluded port group definition file in individual lines in the following format:

<i>Port_group_name_to_be_excluded</i>



Service Console VMkernel Service Console2

- Lines starting with "#" are regarded as comments, and ignored.
- Blank lines are ignored.
- Describe *Port_group_name_to_be_excluded* correctly, as the entry is case-sensitive.
- Use the UTF-8 character code.
- For the *Port_group_name_to_be_excluded*, from the front of the line to the line break code in each line is regarded as a single name.
- When there are multiple lines with the same *Port_group_name_to_be_excluded*, all specified lines are valid.

Note

When using the definition of the port groups excluded from the selections for automatic network configuration, take note of the following points:

- The VLAN of the service console and VMkernel network is the admin LAN. As this configuration allows a public LAN using the same VLAN, security risks increase.

For these reasons, that this configuration is for users using the same VLAN in the system configuration. The infrastructure administrator should determine if these directions can be used or not, taking possible security risks into account.

When Performing Alive Monitoring (Heartbeat Monitoring) for L-Server

For Resource Orchestrator alive monitoring functions, "VM Monitoring" functions for VMware HA are used. Therefore, configure the following settings:

1. Configure VMware clusters
Configure VMware clusters in a VM host operating an L-Server.
2. Configure VMware HA
Enable VMware HA in VMware clusters configured in 1.

When using Console Connections from Public LAN

Use the following procedure when using console connections from the public LAN. For details on the configuration method, refer to the VM management software manual.

1. Create a virtual switch to connect with the public LAN on VM management software.
2. Create a Service Console or port group for VMKernel on the created virtual switch on VM management software.
 - When using VMware ESX
Create a port group for Service Console.
 - When using VMware ESXi
Create a port group for VMKernel.

When creating port groups for Service Console or VMkernel, configure IP addresses and VLAN IDs for the VM host to match to the settings of the public LAN which is the destination for connection. When using multiple network resources as public LANs, create port groups for Service Console or VMKernel corresponding to each resource, and configure the IP addresses and VLAN IDs appropriately.

3. Configure port groups excluded from the selection for automatic network configuration in Resource Orchestrator.

The VLAN ID for network resources corresponding to the public LAN and the VLAN ID for Service Console or VMKernel may be the same. Therefore, define the port group for the Service Console or VMKernel created in 2. for the port group to be excluded from selection for automatic network configuration.

For details, refer to ["When Using the Definition for Port Groups Excluded from the Selections for Automatic Network Configuration"](#).

4. Configure the IP addresses to exclude from allocation in Resource Orchestrator.

Set the IP address of the VM host configured for public LANs in 2., in the network corresponding to the public LAN, to be excluded from allocation.

For details, refer to the following:

- "3.6 Modifying Network Resource Specifications" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".
- "7.3.1 Creating New Network Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

E.2.3 Installation

This section explains installation methods.

Installing the Manager

Install the Resource Orchestrator manager. For details on how to install a manager, refer to "2.1 Manager Installation" of the "Installation Guide CE".

Installing the Agent

Install Resource Orchestrator agents on managed servers. For details on how to install agents, refer to "2.2.3 Installation [Linux/VMware/Xen/KVM/Oracle VM]" of the "Installation Guide CE".

When using VMware ESXi, install ServerView ESXi CIM Provider agents.

E.2.4 Configuration after Installation

This section explains configurations after the installation.

Server Virtualization Software Definition File

Operations related to server virtualization software can be changed by configuring values in the following definition files beforehand.

Use the UTF-8 character code for definition files.

Location of the Definition File

[Windows]

Installation_folder\Manager\etc\customize_data

[Linux]

/etc/opt/FJSVrcvmr/customize_data

Definition File Name

vm.rcxprop

Definition File Format

Describe each line of the definition file in the following format:

<i>Key = Value</i>

Definition File Items

Table E.2 List of Items

Item	Key	Value	Remarks
Configuration of power control for VMware DRS and DPM	drs_power_on_vm	true false	<p>When server virtualization software is VMware, the values are valid.</p> <ul style="list-style-type: none"> - When starting an L-Server (VM guest), if moving an L-Server (VM guest) between VM hosts using VMware DRS, or turning on a VM host using VMware DPM Specify "true". - If other than the above Specify "false". <p>If left blank, "false" is set. Restarting of the server is not required after changing this configuration.</p> <p>When specifying "true", set VMware DRS and VMware DPM as follows:</p> <ul style="list-style-type: none"> - VMware DRS "partly automatic" or "full automatic" - VMware DPM "off" or "automatic" <p>When specifying "Manual", startup of L-Servers and VM guests may fail.</p> <p>For detail on VMware DRS/DPM, refer to "When using VMware DRS or VMware DPM" in "E.2.2 Preparations"</p>

Definition Files to Configure using Console Connections from Public LAN

When using console connections from the public LAN, configure the connection destination for the VM host in the following definition files:

Location of the Definition File

[Windows]
Installation_folder\Manager\etc\customize_data

[Linux]
 /etc/opt/FJSVrcvmr/customize_data

Definition File Name

vm_console.rcxprop

Definition File Format

Specify a folder or tenant name, the physical server name of the VM host, and the corresponding connection destination in one line, separated by commas (",").

<i>folder_or_tenant_name, physical_server_name, destination_to_connect</i>
--

Definition File Items

Table E.3 List of Items

Item	Description
Folder or tenant name	Specify the folder name or tenant name using a full path (the first letter must be "/").

Item	Description
Physical server name	Specify the physical server name of the VM host.
Connection destination	Specify the IP address for a VM host that can be connected to through the admin client, or the host name for which name resolution is available in the admin client environment.

Example Definition File

```

/, bx900-1, 192.168.10.100 (*1)
/folderA, bx900-1, host1 (*2)
/folderA/tenantB, bx900-1, 192.168.30.100 (*3)
/folderA/tenantB, bx900-2, 192.168.30.200 (*3)

```

- *1: Definition for root folder (/). The default settings in all tenants.
- *2: Definition for folder (/folderA). Specify the destination to connect to using using host name.
- *3: Definition of tenants (/folderA/tenantB). Specify multiple hosts.

Note

- When describing more than three commas (",") in one line, any descriptions after the third comma are ignored.
- When the descriptions start with a "#", the string is regarded as a comment line.
- If reading of the definition file fails, set the IP address of the admin LAN for the VM host registered in Resource Orchestrator as the connection destination.
- When the folder or tenant name, and the physical server name do not match the definition file specifications, perform console connections using the IP address of the admin LAN for the VM host.
- When there are multiple VM hosts used in a folder or a tenant, settings using the same folder or tenant must be described separately, in multiple lines.
- When specifying a folder, apply the relevant settings to the sub folders and tenants under that folder.
- When settings targeting the sub folders or tenants under the specified folder are configured, and definitions with the same physical server name also exist, the priority is given to the definitions.

Example

When there are the following definitions of (1) and (2), the folder or tenant name is "/folderA/tenantB" and the physical server name is virtual L-Server of "bx900-1", console connections are performed by using the IP address (2).

```

(1)/folderA,bx900-1,192.168.10.100
(2)/folderA/tenantB,bx900-1,192.168.20.100

```

- When describing the same physical server configurations in the same folder or tenant using multiple lines, the configurations in the latter descriptions are valid.

Example

When there are the following definitions of (1) and (2), the definition (2) is valid.

```

(1)/folderA,bx900-1,192.168.10.100
(2)/folderA,bx900-1,192.168.20.100

```

E.2.5 Setup

The setup procedure when using VMware as server virtualization software is as follows:

1. Register Resources

a. Register VM Management Software

When registering VM management software, datastores that are created in advance during pre-setup preparations, are automatically registered in Resource Orchestrator as virtual storage resources.

For details on how to register VM management software, refer to "2.2 Registering VM Management Software" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

b. Register managed servers

1. Register Chassis

Refer to "2.4.1 Registering Chassis" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

2. Register Managed Servers (within Chassis)

Refer to "2.4.2 Registering Blade Servers" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

3. Register LAN Switch Blades

Refer to "2.4.3 Registering LAN Switch Blades" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

c. Network resources

To register a network resource, specify a network pool when creating the network resource.

By creating network resources in advance, if the NIC and network resources are connected when an L-Server is created, the following settings matching the network resource definition will be registered automatically.

A redundant NIC configuration will be configured. When configuring a non-redundant NIC, refer to "[Manual Network Configuration](#)".



Information

For details on automatic configuration of network resources, refer to "[Automatic Network Configuration](#)".

- When using VMware vDS

Refer to "[When Using Distributed Virtual Switch \(VMware vDS\)](#)" in "[E.2.2 Preparations](#)".

- When Using the Definition for Port Groups Excluded from the Selections for Automatic Network Configuration

Refer to "[When Using the Definition for Port Groups Excluded from the Selections for Automatic Network Configuration](#)" in "[E.2.2 Preparations](#)".

2. Register Resources in Resource Pools

a. Register VM host resources

1. In the ROR console orchestration tree, right-click the target VM pool, and select [Register Resources] from the popup menu.

The [Register Resources] dialog is displayed.

2. Select the VM host to register.
3. Click <OK>.

b. Register virtual storage resources

1. In the ROR console orchestration tree, right-click the target storage pool, and select [Register Resources] from the popup menu.

The [Register Resources] dialog is displayed.

2. Select the virtual storage resource to register.
3. Click <OK>.

c. Register network resources

If the NIC and network resources are connected when an L-Server is created, the settings matching the network resource definition will be registered automatically for the VM host that the L-Server will operate on.

For details, refer to "[Automatic Network Configuration](#)".

1. In the ROR console orchestration tree, right-click the target network pool, and select [Create Resource] from the popup menu.

The [Create a network resource] dialog is displayed.

2. Enter the items necessary for network resources.



When using VMware vDS, in port group creation for distributed virtual switches, set the same VLAN ID used for the port group to the network resource.

For details on how to create a network resource, refer to "7.3 Network Resources" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

3. Create an L-Server Template

a. Export an L-Server template

Refer to "8.2.1 Exporting a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

b. Edit an L-Server template

Refer to "8.2.2 Editing a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

c. Import an L-Server template

Refer to "8.2.3 Importing a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Automatic Network Configuration

If the NIC and network resources are connected when an L-Server is created, the following settings matching the network resource definition will be registered automatically for the VM host that the L-Server will operate on.

- LAN Switch Blade (When Using Blade Servers)

When using a LAN switch blade in switch mode or end-host mode, a VLAN is configured on the internal connection port.

When creating a network resource, a tagged VLAN is automatically configured on the port of the LAN switch blade specified in the uplink port, using the following procedure.

- From the GUI:

In the [Create a network resource] dialog, check the "Automatically configure VLANs for the uplink ports." checkbox.

- From the Command-line:

In the XML definition for the network resource, specify "true" for vlnautosetting (Automatic VLAN configuration for uplink ports).

- Virtual Switches, Port Groups

If the required network resources do not exist, they are automatically created. A redundant NIC configuration will be configured.

If it already exists, the virtual switch and port group are used.

When the user configures the network automatically using an arbitrary physical NIC, define the physical NIC to be used in the server NIC definition file, and then specify the physical LAN segment in the server NIC definition from the network resource. To reflect the physical NIC configuration specified in the server NIC definition file on Resource Orchestrator, use the `rcxadm nicdefctl commit` command.

This enables automatic network configuration even in configurations using an arbitrary physical NIC. However, when using server NIC definitions, the operation must be performed from the command-line.

In addition, when using rack mount and tower servers, automatic network configuration including the configuration using an arbitrary physical NIC is possible by defining the physical NIC to be used in the server NIC definition file and then specifying the physical LAN segment defined in the server NIC definition from the network resource.

- VM Guests

VM guests are connected to port groups. If an image is specified, the IP address is automatically configured.

In environments using the clustering function of VM management software, in order to enable the migration of VM guests and operation using the HA function, settings for LAN switch blades, virtual switches, and port groups are performed automatically for all VM hosts comprising the cluster.

When not configuring the tagged VLAN automatically for the uplink port of network resources, use the ROR console to configure the VLAN settings of uplink ports. Right-click the LAN switch in the server resource tree, and select [Modify]-[Network Settings] from the popup menu.

For details, refer to "2.4.4 Configuring VLANs on LAN Switch Blades" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".



See

- For details on the server NIC definitions, refer to "2.11 Server NIC Definition" of the "Reference Guide (Resource Management) CE".
- For details on the `rcxadm nicdefctl` command, refer to "1.7.16 rcxadm nicdefctl" of the "Reference Guide (Resource Management) CE".
- For details on how to configure VLAN settings of LAN switch blade uplink ports, refer to "2.4.4 Configuring VLANs on LAN Switch Blades" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".



Note

- After creating an L-Server, if VM hosts are added to the cluster afterwards, Resource Orchestrator network settings are not performed automatically.
Perform the same settings as the existing VM hosts in the cluster configuration for the LAN switch blades and virtual switches of the additional VM hosts.
- For the gateway address, set the IP address of the existing node.

Default Blade Server Configuration to Support Automation of Network Configuration in Resource Orchestrator

Show the default blade server configuration to support automation of network configuration in Resource Orchestrator (server blade, specification of uplink port for network resource, correspondence relation of numbers of LAN switch blade and physical network adapter, etc.) in the following list. When there are no server NIC definitions, for network auto-configuration, the physical network adapter within the server blade is selected according to this list.

Table E.4 Default Blade Server Configuration for Network Auto-Configuration (for PRIMERGY BX900 S1 Chassis)

Server Blade	Specification of Uplink Port (Location of LAN Switch Blade)	LAN Switch Blade to Use	Physical Network Adapter Number (*4)
BX920 S1 BX920 S2 BX922 S2	CB1 and CB2, or no specification for uplink port	PG-SW111 PG-SW112	3, 4
		PG-SW109 (*1) PG-SW201	1, 2
	CB3 and CB4	PG-SW111 PG-SW112 PG-SW109 PG-SW201	5, 6
	CB5 and CB6	PG-SW109	9, 10
	CB7 and CB8	PG-SW111 PG-SW112	11, 12
PG-SW201		9, 10	
BX924 S2	CB1 and CB2, or no specification for uplink port	PG-SW111 PG-SW112 PG-SW109 PG-SW201	1, 2
		PG-SW111 PG-SW112 PG-SW109 PG-SW201	3, 4
	CB5 and CB6	PG-SW109	7, 8
	CB7 and CB8	PG-SW111 PG-SW112	9, 10
		PG-SW201	7, 8
BX960 S1	CB1 and CB2, or no specification for uplink port	PG-SW111 PG-SW112 PG-SW109 PG-SW201	11, 12
		PG-SW111 PG-SW112 PG-SW109 PG-SW201	3, 4
	CB5 and CB6 (*3)	PG-SW109	7, 8
	CB7 and CB8 (*3)	PG-SW111 PG-SW112	9, 10
	CB7 and CB8 (*3)	PG-SW201	7, 8

*1: When installing a PG-SW109 on CB1 or CB2, set the transmission speed at the down link port of PG-SW109 to 1 Gbps. For details on how to configure the settings, refer to the corresponding hardware manual.

*2: A LAN expansion card is mounted in expansion slot 1.

*3: A LAN expansion card is mounted in expansion slot 2.

*4: Use each physical network adapter, by performing redundancy using teaming.

Table E.5 Default Blade Server Configuration for Network Auto-Configuration (for PRIMERGY BX400 S1 Chassis)

Server Blade	Specification of Uplink Port (Location of LAN Switch Blade)	LAN Switch Blade to Use	Physical Network Adapter Number (*3)
BX920 S2 BX922 S2	CB1 and CB2 (*1), or no specification for uplink port	PG-SW111 PG-SW112	3, 7
		PG-SW109 (*2) PG-SW201	2, 6
	CB3 and CB4	PG-SW111 PG-SW112 PG-SW109 PG-SW201	9, 10
BX924 S2	CB1 and CB2 (*1), or no specification for uplink port	PG-SW111 PG-SW112 PG-SW109 PG-SW201	2, 4
	CB3 and CB4	PG-SW111 PG-SW112 PG-SW109 PG-SW201	7, 8

*1: The same LAN switch blade model should be mounted in CB1 and CB2.

*2: When installing a PG-SW109 on CB1 or CB2, set the transmission speed at the down link port of PG-SW109 to 1 Gbps. For details on how to configure the settings, refer to the corresponding hardware manual.

*3: Use each physical network adapter, by performing redundancy using teaming.

Table E.6 Default Blade Server Configuration for Network Auto-Configuration (for PRIMERGY BX600 S3 Chassis)

Server Blade	Specification of Uplink Port (Location of LAN Switch Blade)	LAN Switch Blade to Use	Physical Network Adapter Number (*1)
BX600 series servers	NET1 and NET2, or no specification for uplink port	PG-SW107	3, 4
	NET3 and NET4	PG-SW104	7, 8

*1: Use each physical network adapter, by performing redundancy using teaming.

The numbers of physical network adapters given above can be checked in "Network Properties" on the [Resource Details] tab.

When the LAN switch blade is in IBP mode, the same physical network adapter as in the case of "no specification for uplink port" in the list above is selected.

When the user configures the network automatically using an arbitrary physical NIC, define the physical NIC to be used in the server NIC definition file, and specify the physical LAN segment in the server NIC definition from the network resource.

To reflect the physical NIC configuration specified in the server NIC definition file on Resource Orchestrator, use the `rcxadm nicdefctl commit` command. This enables automatic network configuration even in configurations using an arbitrary physical NIC.

However, when using server NIC definitions, the operation must be performed from the command-line.

In addition, when using rack mount and tower servers, automatic network configuration including the configuration using an arbitrary physical NIC is possible by defining the physical NIC to be used in the server NIC definition file and then specifying the physical LAN segment defined in the server NIC definition from the network resource.



See

- For details on the server NIC definitions, refer to "2.11 Server NIC Definition" of the "Reference Guide (Resource Management) CE".

- For details on the `rcxadm nicdefctl` command, refer to "1.7.16 `rcxadm nicdefctl`" of the "Reference Guide (Resource Management) CE".

In the diagram, the default blade server configurations as described in the following configuration example when using a PRIMERGY BX900 S1 chassis are shown.

Table E.7 Configuration Example 1

Server blades	BX920 S2
Specification of uplink port	CB1 and CB2
LAN switch blade to use	PG-SW112

Table E.8 Configuration Example 2

Server blades	BX920 S2
Specification of uplink port	Both "no specification for uplink port" and "CB3 and CB4" are specified
LAN switch blade to use	PG-SW109

Figure E.6 Blade Server Diagram of Configuration Example 1

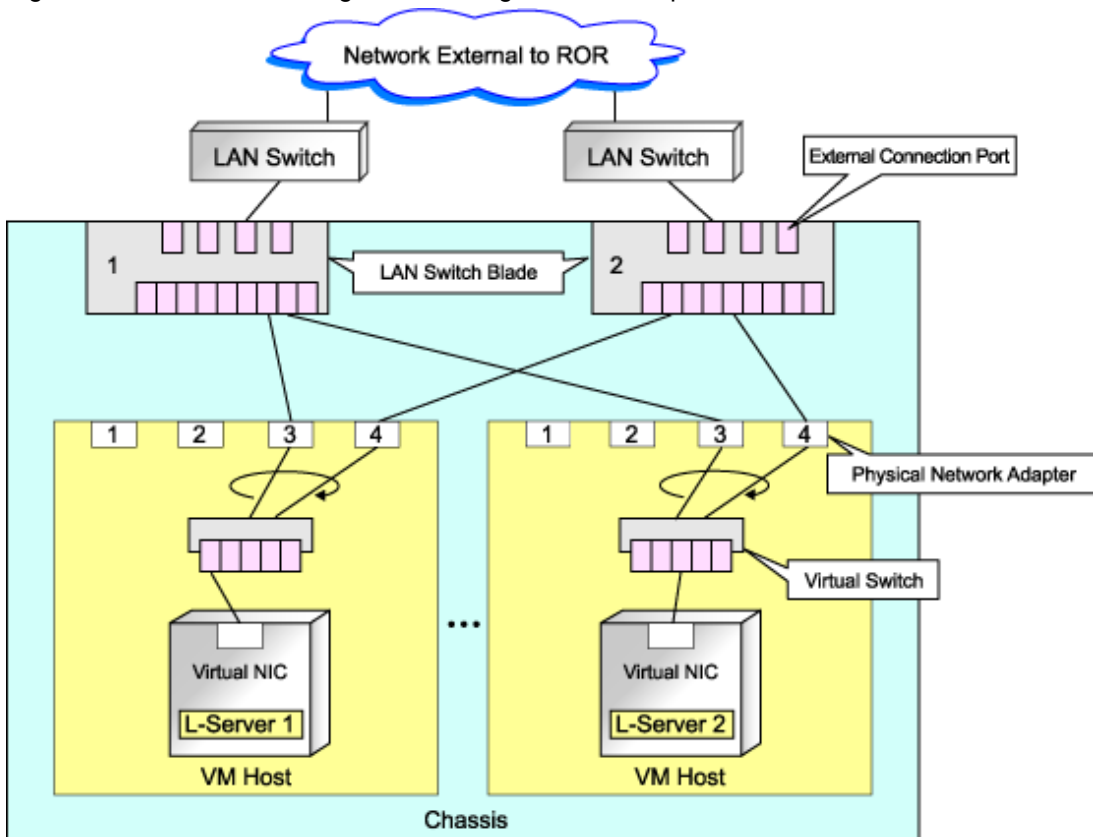
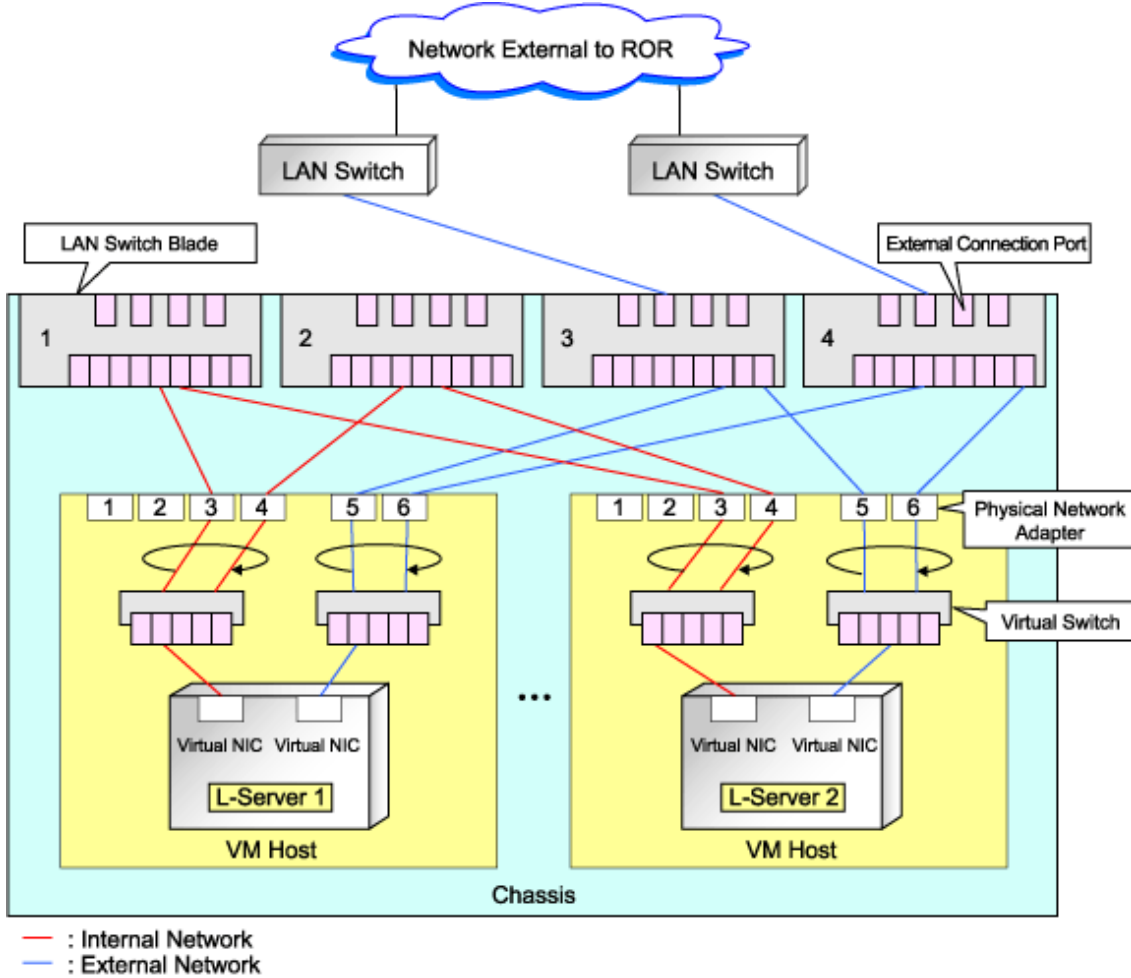


Figure E.7 Blade Server Diagram of Configuration Example 2



Manual Network Configuration

When using a configuration which is not supported for the network auto-configuration (such as triplicity or quadruplicity of NICs), configure the network using the following procedure:

1. Manually create a virtual switch connected to a physical NIC.
For details on how to create virtual switches, refer to the VMware manual.
2. On the virtual switch created in 1., manually create a port group for which a VLAN ID has been set.
For details on how to create port groups, refer to the VMware manual.

When manually configuring a port group, for the name of port groups using the same VLAN ID, it is necessary to use a common name on all VM hosts. When using server virtualization software other than VMware with the same manager, set a different port group name from the one used for the virtual switch, virtual network, and virtual bridge on the other server virtualization software.

3. For the LAN switch blade connected to the physical NICs, configure a VLAN that includes a downlink port.
 - a. Right-click the target LAN switch in the server resource tree on the ROR console, and select [Modify]-[Network Settings] from the popup menu.
The [VLAN Settings] dialog is displayed.
 - b. Configure a VLAN.

4. Create a network resource.

- From the GUI:

- a. In the [Create a network resource] dialog containing the VLAN ID that was specified in 2. and 3., check the "Use configured virtual switches." checkbox and create a network resource.

- From the Command-line:

- a. Create the XML file that defines network resources.

Define the VLAN ID specified at 2. and 3. in the XML file.

In this case, specify auto="false" in the Network tag.

- b. To create the network resource, execute the `rcxadm network create` command specifying the XML file created in a.

The network resources are created.

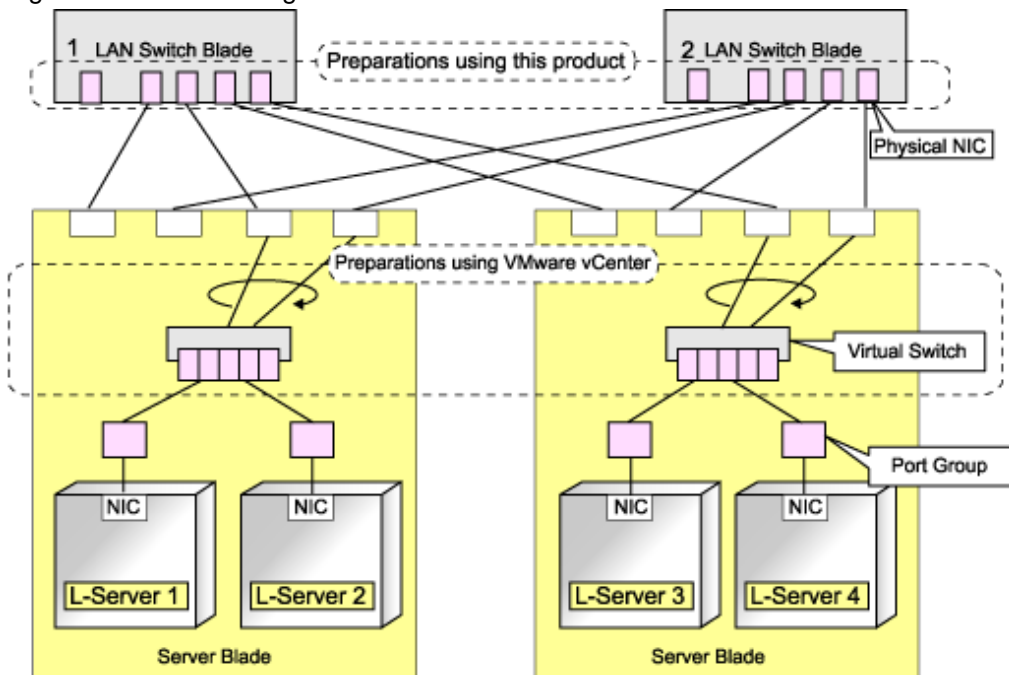
For details on the `rcxadm network` command, refer to "1.3.5 `rcxadm network`" of the "Reference Guide (Resource Management) CE".



See

- For details on the Network element and creation of XML files that define network resources, refer to "2.5 Network Resources" of the "Reference Guide (Resource Management) CE".
- For details on how to configure VLAN settings of LAN switch blade uplink ports, refer to "2.4.4 Configuring VLANs on LAN Switch Blades" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".
- For details on the `rcxadm network` command, refer to "1.3.5 `rcxadm network`" of the "Reference Guide (Resource Management) CE".

Figure E.8 Network Diagram



L-Server Creation

Use the following procedure to create L-Servers:

1. Create an L-Server Using an L-Server Template

a. When there are no cloning images, or when not using already registered cloning images

1. Create an L-Server, referring to "10.1 Creation Using an L-Server Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE". When creating the L-Server, select "None" for images.
2. Install an OS, referring to "[Manual OS Installation](#)".
3. When collecting cloning images after creating an L-Server, the cloning images are stored in the image pool. When collecting cloning images, refer to "[Collecting a Cloning Image](#)".

b. When using an existing cloning image

Create an L-Server, referring to "10.1 Creation Using an L-Server Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE". In this case, specify the cloning image that you want to use as an image.

2. Create an L-Server Specifying Individual Specifications

Refer to "10.3 Creation of Virtual L-Servers Using Parameters" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

For details on how to configure the [OS] tab, refer to "10.3.5 [OS] Tab" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Manual OS Installation

To manually install an operating system, use the following procedure.

1. Stop the L-Server.

If an L-Server is operating, stop it.

For details on how to stop an L-Server, refer to "11.1.2 Stopping an L-Server" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

2. Connect a console to the L-Server.

Connect a console to the L-Server.

For details on how to connect the console, refer to "Console" in "11.3 Using the L-Server Console" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

3. Connect DVD drives.

Perform connection of DVD drives from the console window.

4. Install an OS manually on the L-Server.

Start an L-Server, and manually install an OS on the L-Server.

When installing an OS manually, refer to the Guest Operating System Installation Guide.

Refer to the relevant version of the document, referring to the following web site:

Guest Operating System Installation Guide

URL: http://www.vmware.com/support/pubs/vs_pubs.html (As of February 2012)
--

Configuration after OS Installation

Install VMware Tools after installing an OS.

Use the following procedure to install VMware Tools.

1. Right-click the target L-Server in the orchestration tree, and select [Install VM Tool] from the popup menu.

The confirmation dialog is displayed.

2. Click <OK>.

The ISO images are connected to the L-Server for VM guest.

For details on VMware Tools, refer to the information on VMware Tools in "vSphere Basic System Administration" of VMware.

Refer to the relevant version of the document, referring to the following web site:

vSphere Basic System Administration

URL: http://www.vmware.com/support/pubs/vs_pubs.html (As of February 2012)

Note

When a connection with the ISO image of VMware Tools has already been established, subsequent operations for the connection will be completed normally. In some cases, a task error may be output on VMware vCenter Server. This error is output by ignoring the message already received from VMware vCenter Server that informs the user that connection has already been established, and does not affect the system operations.

Collecting a Cloning Image

This section explains how to collect cloning images.

Use the following procedure to collect cloning images:

After installing an OS, stop the target L-Server.

1. Right-click the target L-Server in the orchestration tree, and select [Cloning]-[Collect] from the popup menu.
2. Click <OK>.

A cloning image is collected.

A given cloning image (identified by its name attribute) can be managed by image version.

If a cloning image is created using VM management software, it can be used as is.

Point

When "Select Automatically" is specified in the [Collect a Cloning Image] dialog, it is assumed that the virtual storage resource containing the L-Server for collecting cloning images has been specified.

When performing cloning of a Windows OS on an L-Server, the Microsoft Sysprep tool is necessary.

The necessary files vary depending on the CPU architecture (x86, x64) of the target system, and the OS version. When using Windows Server 2008, the modules are already configured in the OS so there is no need to obtain new modules.

For details on obtaining tool and its installation, refer to the information regarding the Microsoft Sysprep tool in the "vSphere Basic System Administration" documentation and the following VMware web site.

Refer to the relevant version of the document, referring to the following web site:

vSphere Basic System Administration

URL: http://www.vmware.com/support/pubs/vs_pubs.html (As of February 2012)

VMware web site

URL:
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1005593 (As of February 2012)

Note

- If an L-Server is created with a specified Windows image, when deploying the image use Sysprep, provided by Microsoft, to re-configure the properties unique to the server. By executing Sysprep, the user information and OS setting information are reset. For details on Sysprep, refer to the information provided by Microsoft.
- If stopping or restarting of the manager is performed during execution of Sysprep, the operation being executed will be performed after the manager is started.
Until the process being executed is completed, do not operate the target resource.
- When using MAK license authentication for activation of Windows Server 2008 image OS, Sysprep can be executed a maximum of three times. Since Sysprep is executed when creating L-Server with images specified or when collecting cloning images, collection of cloning images and creation of L-Servers with images specified cannot be performed more than four times. Therefore, it is recommended not to collect cloning images from L-Servers that have had cloning images deployed, but to collect them from a dedicated master server. The number is also included in the count when Sysprep is performed in the following cases:
 - When customizing a guest OS using template functions in VMware
 - When creating templates in SCVMM
- If an L-Server is created with a Windows image specified, use Sysprep to set the server specific information again, when starting for the first time after creating the L-Server. After startup and resetting of the server specific information, when the L-Server console is opened from the server virtualization software management window, you will be logged on with Administrator status. Therefore, it is recommended that you log off.
- Note the following points when collecting cloning images from an L-Server that was created using a cloning image.
 - As L-Servers which have not been used even once after creation do not have server specific information set, creation of L-Servers using cloning images collected from an L-Server may fail. When collecting cloning images, set the server specific information on L-Server, after starting the target L-Server.

[OS] Tab Configuration

Enter the parameters to set for the OS when creating the L-Server. This setting is valid only if an image is specified in the [General] tab. The setting process is performed the first time the L-Server is started. If an image name is not specified, it is not necessary to enter all these items.

Table E.9 List of Settings

Item	Windows		Linux		Description
	Necessity of Entry	Values When Omitted	Necessity of Entry	Values When Omitted	
Host name/ Computer name	Possible	<i>L-Server Name</i>	Possible	<i>L-Server Name</i>	Enter the host name or computer name. For Windows, enter a string of between 1 and 15 alphanumeric characters or hyphens ("-"). For Linux, enter between 1 and 63 alphanumeric characters or hyphens ("-"). In either case, the first character must be an alphanumeric character. The string cannot be composed solely of numbers. If underscores ("_") or periods (".") are used in an L-Server name, they will be replaced with hyphens ("-"), because these characters

Item	Windows		Linux		Description
	Necessity of Entry	Values When Omitted	Necessity of Entry	Values When Omitted	
					cannot be used for host names or computer names. If the basic information is not specified, the L-Server name is converted and set as indicated above.
Domain name	Possible	WORKGROUP (*1)	Possible	localdomain (*1)	For Windows, enter the workgroup name. Settings for participation in a domain cannot be made. For Linux, enter the domain name. Enter between 1 and 255 alphanumeric characters, hyphens ("-"), or periods ("."), using an alphabetic character for the first character.
DNS search path	Not Required	-	Essential	-	Enter a list of domain names to use for DNS searching, using between 1 and 32,767 characters. You can specify the same characters as the domain name. To specify multiple domain names, use a blank space as the separator character.
Full name	Possible	WORKNAME (*1)	Not Required	-	Enter the Windows full name using between 1 and 50 characters. By default, the value defined in the OS property definition file is entered.
Organization name	Possible	WORKORGANIZATION (*1)	Not Required	-	Enter the organization name displayed in the Windows system properties using between 1 and 50 characters.
Product key	Possible	If omitted, the following will happen when the OS is operated: (*1) - For Windows Server 2003, the product key entry screen is displayed the first time the server is started. - For Windows Server 2008, the product key is unregistered.	Not Required	-	Enter a product key.

Item	Windows		Linux		Description
	Necessity of Entry	Values When Omitted	Necessity of Entry	Values When Omitted	
License mode	Possible	Server unit (*1)	Not Required	-	Specify "Seat Unit" (number of connected clients) or "Server Unit" (number of servers used at the same time).
Maximum number of connections	Possible	5 (*1)	Not Required	-	Specify this when "Server Unit" is set (number of servers used at the same time: server). Specify a number between 5 and 9,999.
Administrator password	Possible	- (*1)	Not Required	-	Configure the same password as that specified for the local administrator account during L-Server creation. Enter the password using between 1 and 128 alphanumeric characters or symbols. (*2)
Hardware clock configuration	Not Required	-	Possible	Local	Specify one of the following: - UTC - Local (LOCAL)
Time zone	Possible	<i>The same time zone as the OS of the manager</i>	Possible	<i>The same time zone as the OS of the manager</i>	Specify the time zone of the OS.

*1: When the OS property definition file is specified, its values are configured.

*2: When a different password from the password of the local administrator account of the images specified during L-Server creation is specified, enter the values according to VM management software specifications.

For details on administrator password settings, refer to the section of customization for virtual machines of the "vSphere Basic System Administration".

vSphere Basic System Administration

URL: http://www.vmware.com/support/pubs/vs_pubs.html (As of February 2012)



Information

OS Property Definition File

By setting the default values in an OS property definition file in advance, the default values of the information on the [OS] tab, etc. are generated when creating an L-Server. Use the UTF-8 character code for OS property definition files.

Location of the Definition File

[Windows]

Installation_folder\Manager\etc\customize_data

[Linux]

/etc/opt/FJSVrcvnr/customize_data

Definition File Name

The definition file name can be used by dividing into definitions that are available for each user group and definitions that are common to the system. If the key of the definition file common to the system is the same as a definition file for a user group, priority is given to the values indicated in the definition file for the user group.

- For User Groups

os_setting_user_group_name.rcxprop

- Common on System

os_setting.rcxprop

Definition File Format

In the definition file, an item to define is entered on each line. Each line is entered in the following format.

<i>Key = Value</i>

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

Definition File Items

Specify the following items in a definition file.

Table E.10 List of Items

Item	Key	Value	Remarks
Domain name	workgroup_name	(*1)	For Windows
	domain_name	(*1)	For Linux
DNS search path	dns_search_path	(*1)	-
Full name	full_name	(*1)	-
Organization name	org_name	(*1)	-
Product key	product_key	(*1)	-
License mode	license_mode	Specify "seat" (number of connected clients) or "server" (per server: number of servers used at the same time).	-
Maximum number of connections	license_users	(*1)	-
Administrator password	admin_password	(*1)	-
Hardware clock configuration	hwclock	Specify either "UTC" or "LOCAL".	-
DNS server (When configuring for each NIC on Windows) (*2)	nic N _dns_address X	Specify the IP address using numeric values (between 0 and 255) and periods. (*2) When not configuring a DNS server, specify a hyphen ("-").	For N , specify the NIC number. For X , specify primary ("1") or secondary ("2").
DNS server (When configuring all NICs using the same settings on Windows)	dns_address X	Specify the IP address using numeric values (between 0 and 255) and periods.	For X , specify primary ("1") or secondary ("2"). Priority is given to nic N _dns_address X specifications.
DNS server (for Linux)	dns_address X	Specify the IP address using numeric values (between 0 and 255) and periods.	For X , specify primary ("1"), secondary ("2"), or tertiary ("3").

*1: For more information on this value, refer to "[Table E.9 List of Settings](#)".

*2: When omitting keys or values, use the value "dns_address X " to configure the same values for the NIC definitions of all NICs on Windows.

Example

An example definition file is indicated below.

```
# Windows
workgroup_name = WORKGROUP
full_name = WORKNAME
org_name = WORKORGANIZATION
product_key = AAAA-BBBB-CCCC-DDDD
license_mode = server
license_users = 5
admin_password = xxxxxxxx
nic1_dns_address1 = 192.168.0.60
nic1_dns_address2 = 192.168.0.61
nic2_dns_address1 =
nic2_dns_address2 =

# Linux
domain_name = localdomain
dns_search_path = test.domain.com
hwclock = LOCAL
dns_address1 = 192.168.0.60
dns_address2 = 192.168.0.61
dns_address3 =
```

E.2.6 Advisory Notes for VMware Usage

This section explains advisory notes for VMware.

Values for CPU Share and Memory Share

If CPU share and memory share for a virtual L-Server have been set to a value of 1,000,000 or greater using the ROR console, when the VM guest is edited from vSphereClient, these values may be forcibly replaced with 1,000,000.

When setting a value greater than 1,000,000, modify the configuration from the ROR console again.

Operating Systems for which Parameters can be Set and the Prerequisites for Performing the Settings

Depending on the server virtualization software used, some restrictions may apply to the operating systems that parameters can be set for and the prerequisites for performing the settings.

For details, refer to the manual of server virtualization software.

Information

Snapshot

The snapshot function provided by server virtualization software records the disk from the last update. Consequently, when a disk failure occurs, the snapshot function becomes unavailable at the same time.

Snapshot can be used as a corrective measure for problems such as the following:

Example

- For recovery when a problems occurs with the applied patch

- For recovery when a problem occurs when changing operating system parameters

VMware Storage VMotion

The following are advisory notes for when using VMware Storage VMotion.

- When disk resources are moved to a newly created datastore which has not yet been detected by Resource Orchestrator, the information of moved disk resources is reflected as follows:
 1. The newly created datastore is detected as a virtual storage resource during regular update.
 2. After being detected as virtual storage resources, the information of moved disk resources is reflected on Resource Orchestrator.
- When using VMware vSphere Client, after completing moving of disk resources, the newest datastore status may not be reflected. When performing update of the datastore, the newest status is displayed.

VMware FT

When an L-Server is linked with a virtual machine on which VMware FT has been configured, the secondary VM host information can be checked using the following method:

1. Select the target L-Server on the orchestration tree.

In the "Server recovery" on the [Resource Details] tab, VMware FT (*Secondary_VM_host_name*) is displayed.



Example

VMware FT(host2)

When migration to the secondary VM host occurs, the secondary VM host information will be updated by periodic update.

VMware DPM, VMware DRS

When starting an L-Server using VMware DPM or VMware DRS, if moving an L-Server (VM guest) between VM hosts by VMware DRS, or turning on a VM host using VMware DPM, refer to "When using VMware DRS or VMware DPM" in "E.2.2 Preparations".

E.2.7 Overcommit

This section explains the VMware overcommit function for L-Servers.

Overcommit

The VMware overcommit function for the CPU and memory is available on Resource Orchestrator.

The VMware overcommit function for the CPU and memory virtually allows a guest OS to use more resources than that of the actual CPU and memory of a server.

Resource Orchestrator provides the following functions to utilize the VMware overcommit function for the CPU and memory when creating L-Servers.

- Creating an L-Server with the overcommit function for the CPU and memory
 - CPU Performance
The maximum number of CPU resources to be allocated to a virtual machine (Limitation)
 - CPU Reservation Performance
The minimum number of CPU resources to be reserved for a virtual machine (Reservation)

- CPU Shares
The relative proportion for allocation of CPU resources when there are competing virtual machines (Share)
- Memory Size
 - Memory Reserved
The maximum amount of memory resources to be allocated to a virtual machine (Limitation)
 - Memory Size
The maximum amount of memory resources to be allocated to a virtual machine by the VM host (Memory Size)

For the virtual L-Server created using Resource Orchestrator, the same value is set for both Memory Reserved and Memory Size.
- Memory Reservation Capacity
The minimum amount of memory resources to be reserved for a virtual machine (Reservation)
- Memory Shares
The relative proportion for allocation of memory resources when there are competing virtual machines (Share)
- Setting an overcommit attribute for a resource pool
Overcommit attributes can be set for resource pools. An L-Server with overcommit attributes can be created using overcommit attributes settings or a resource pool.
- Calculation of available space on VM pools, which uses values set for CPU reservation performance and memory reservation capacity
- Conversion of the free CPU capacity and free memory capacity of VM pools with overcommit attributes
For a VM pool with overcommit attributes, the conversion of free CPU capacity and free memory capacity can be displayed based on the CPU reservation values and memory allocation capacity of an L-Server created beforehand.
- Display of the number of L-Servers that can be created for a VM pool with overcommit attributes
For a VM pool with overcommit attributes, the number of L-Servers that can be created based on the CPU reservation values and memory reservation capacity specified in the L-Server template can be displayed.

For details on an L-Server, refer to "[1.2.3 L-Servers](#)" and "[L-Server Creation](#)" of "[E.2.5 Setup](#)" or "Chapter 10 Creating L-Servers" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

For details on resource pools, refer to "[1.2.2 Resource Pool](#)" or "Chapter 12 Resource Pool Operations" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

For details on the available capacity view or the L-Server conversion view, refer to "12.4 Viewing a Resource Pool" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Prerequisites

Admin Server

When using the function for coordination with Resource Orchestrator, VMware, or the overcommit function for the CPU and memory, the only supported admin server OS is Windows.

Installation Procedure

Use the following procedure to install overcommit.

1. Create a VM Pool for Overcommit

For details on how to create a VM pool, refer to "12.2 Resource Pool Operations" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".



For the VM pool for overcommit, register only VM hosts that support overcommit (VMware, Hyper-V, or RHEL-KVM). If VM hosts other than VMware, Hyper-V, or RHEL-KVM have been registered, move those VM hosts to another VM pool.

The following operations cannot be performed on the VM hosts other than VMware, Hyper-V, or RHEL-KVM registered in the VM pool for overcommit.

- Create an L-Server
- Linking L-Servers with configured virtual machines

2. Create an Overcommit Configuration File for a VM Pool

For the VM pool created in 1., specify a reservation value or a maximum value after calculating the available space for the VM pool used for overcommit settings or performing overcommit.

Create an overcommit configuration file for a VM pool.

For details on definition files, refer to "[E.1.1 Definition Files](#)".

 **Point**

When creating L-Servers that use overcommit and L-Servers that do not, both a VM pool that uses overcommit and a VM pool that does not must be created.

3. Create a VM Specific Information Definition File

Create a VM specific information definition file. Create a VM specific information definition file when configuring different settings for individual user groups without configuring overcommit settings on the L-Server template.

For details on creating VM specific information definition files, refer to "[E.1.1 Definition Files](#)".

4. Export an L-Server Template

For details on how to export L-Server templates, refer to "8.2.1 Exporting a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

5. Edit an L-Server Template

Configure the overcommit settings for an L-Server template.

For details on the XML definition of L-Server templates, refer to "2.2.2 Virtual L-Server Templates" in the "Reference Guide (Resource Management) CE".

When configuring overcommit settings using the VM specific information definition file, do not configure the following parameters except "Enabling/disabling overcommit". When overcommit settings are configured in the L-Server template, priority is given to those settings.

- CPU Reservation Performance
- CPU Shares
- Memory Reservation Capacity
- Memory Shares

 **Information**

If a template is imported without editing the L-Server template name, the content of the existing L-Server template is overwritten. If an L-Server template is imported after the name is edited from when it was exported, the L-Server template is added.

6. Import an L-Server Template

For details on how to import L-Server templates, refer to "8.2.3 Importing a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

7. Create an L-Server

Create an L-Server using the L-Server template created in 5.

For details, refer to "10.1 Creation Using an L-Server Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

When not using an L-Server template, create an L-Server using a command. Edit the L-Server XML referring to "Chapter 10 Creating L-Servers" of the "User's Guide for Infrastructure Administrators (Resource Management) CE", and then execute the `rcxadm lserver create` command.

For details on the `rcxadm lserver` command, refer to "1.3.1 `rcxadm lserver`" of the "Reference Guide (Resource Management) CE".

8. Confirm the Overcommit Function Settings for an L-Server

To confirm overcommit settings configured for an L-Server, execute the `rcxadm lserver show` command.

Confirm that the command output result includes the line starting with "OverCommit: true".

For details on the `rcxadm lserver` command, refer to "1.3.1 `rcxadm lserver`" of the "Reference Guide (Resource Management) CE".

Note

When starting of an L-Server fails, the retrieval method varies depending on the L-Server settings.

Perform the following:

- When "Boot Location" of the L-Server is set to "Relocate at startup"

Start the L-Server again. When there is a VM host with an available resource, the L-Server will start on that VM host after several attempts at startup.

- When "Boot Location" of the L-Server is set to "Fixed"

As no VM host is automatically selected, start the L-Server after changing its boot location, or moving or stopping other L-Servers on the same VM host.

For details on how to change the boot location, refer to "10.3 Creation of Virtual L-Servers Using Parameters" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

For details on how to move the boot location, refer to "11.7 Moving an L-Server between Servers (Migration)" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Changing L-Server Specifications

This section explains how to modify L-Server specifications.

To change L-Server specifications, execute the `rcxadm lserver modify` command.

For details on the `rcxadm lserver` command, refer to "1.3.1 `rcxadm lserver`" of the "Reference Guide (Resource Management) CE".

Note

Changing of L-Server specifications will fail if the resources (the number of CPUs, CPU frequency, and memory capacity) of a physical server where a VM host operates are less than the CPU reservation performance and memory reservation capacity.

When CPU performance and memory capacity are smaller than the CPU reservation performance and memory reservation capacity, modification of L-Server specifications fails.

When modifying specifications of an L-Server to which resources have been allocated, the information in the VM specific information definition file is not reflected because priority is given to the values already configured to the L-Server. In that case, enter the new values in the XML file and then use the appropriate commands to reflect the changes.

E.3 Hyper-V

This section explains how to configure Hyper-V as server virtualization software.

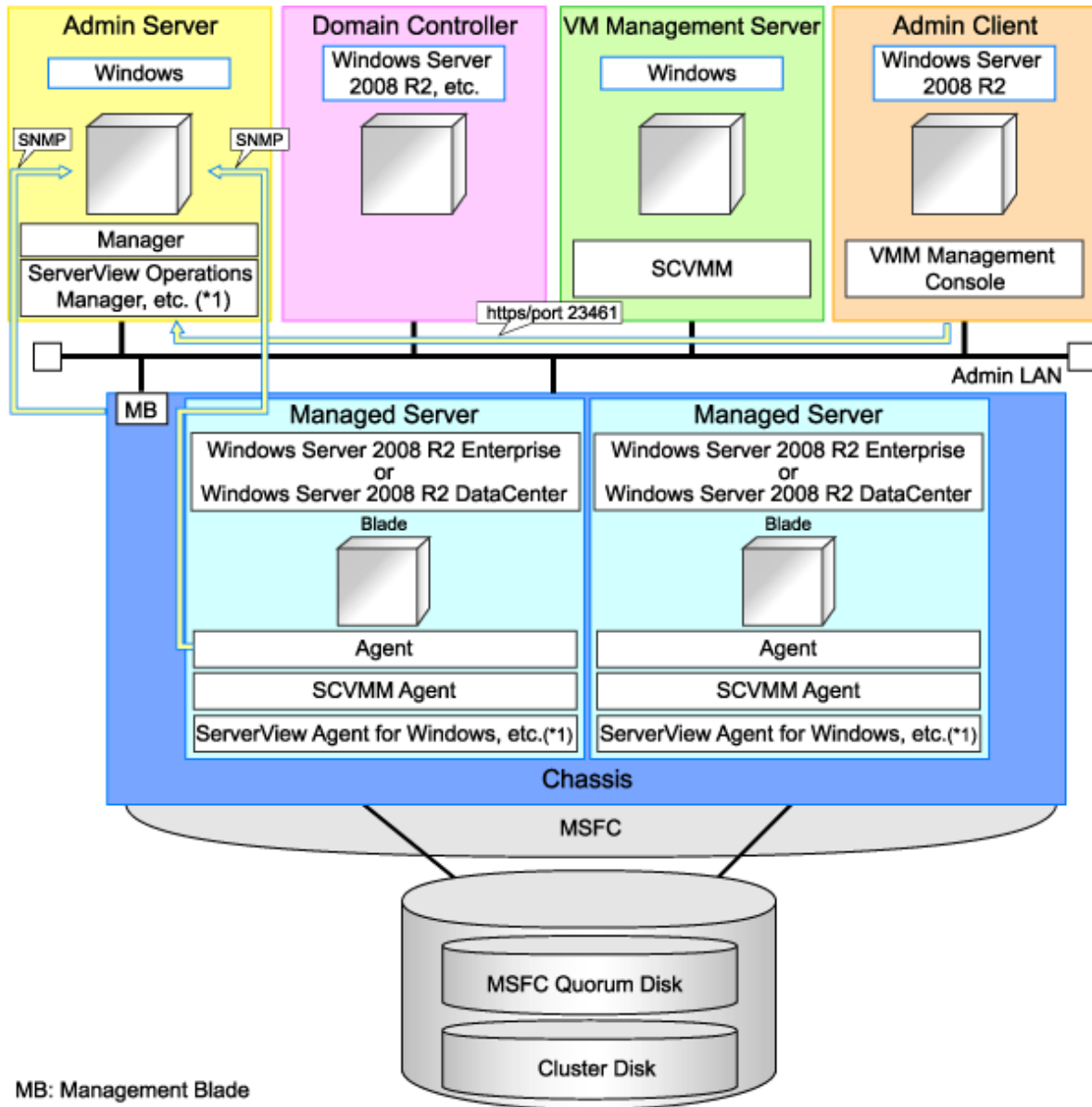
E.3.1 System Configuration

This section explains the system configuration when using Hyper-V as server virtualization software.

Example of System Configuration

This section explains how to configure Hyper-V as a managed server.

Figure E.9 Example of System Configuration



MB: Management Blade

*1: For details on required software, refer to "[1.4.2.2 Required Software](#)".

Note

- For a configuration example for rack mount servers, delete the chassis and management blades from the diagram above.
- For the manager, agents, SCVMM, SCVMM agents, and Windows guest OS's, apply the latest updated program using Microsoft Update. Necessary for installing the latest integrated services provided by each OS on VM guests.

SCVMM

Necessary for management of VM hosts and VM guests.

Can be placed on the same admin server as the manager or on another server.

Can be placed on the same server as the domain controller or on another server.
SCVMM must be in the domain of the domain controller in this configuration.

Domain Controller

Can be placed on the same admin server as the manager or on another server.
Can be placed on the same server as SCVMM or on another server.

Managed Server

Create a cluster using MSFC.
Managed servers must be in the domain of the domain controller in this configuration.

Admin Client

Must be in the same domain as SCVMM and the VM host. The SCVMM administrator console must be installed.

Advisory Notes for System Configuration

- SCVMM and the VM host must be in the same domain.
- The VM host must be connected to the Resource Orchestrator admin LAN.
- For the Resource Orchestrator manager, it is recommended that the configuration enables access to SCVMM through the Resource Orchestrator admin LAN.
- When opening the SCVMM management window from an ROR console executed on a Resource Orchestrator admin client, the admin client must be in the same domain as SCVMM, and logged in to the domain account.
- When connecting with the L-Server console from the ROR console executed on the admin client of Resource Orchestrator, the admin client must be in the same domain as SCVMM.

Simplifying Network Settings

Network settings can be easily configured by Resource Orchestrator when creating L-Servers.
Depending on the conditions, such as hardware (such as blade servers or rack mount servers) used and whether or not network redundancy is performed for L-Servers, the setting ranges of networks differ.
For details, refer to "[1.2.7 Simplifying Networks](#)" and "[4.2.4 Preparations for Resource Orchestrator Network Environments](#)".

Network Configuration Example

An example network configuration using Hyper-V is given below:

Figure E.10 Configuration when Performing Network Redundancy for L-Servers on Blade Servers (Using Intel PROSet or PRIMECLUSTER GLS)

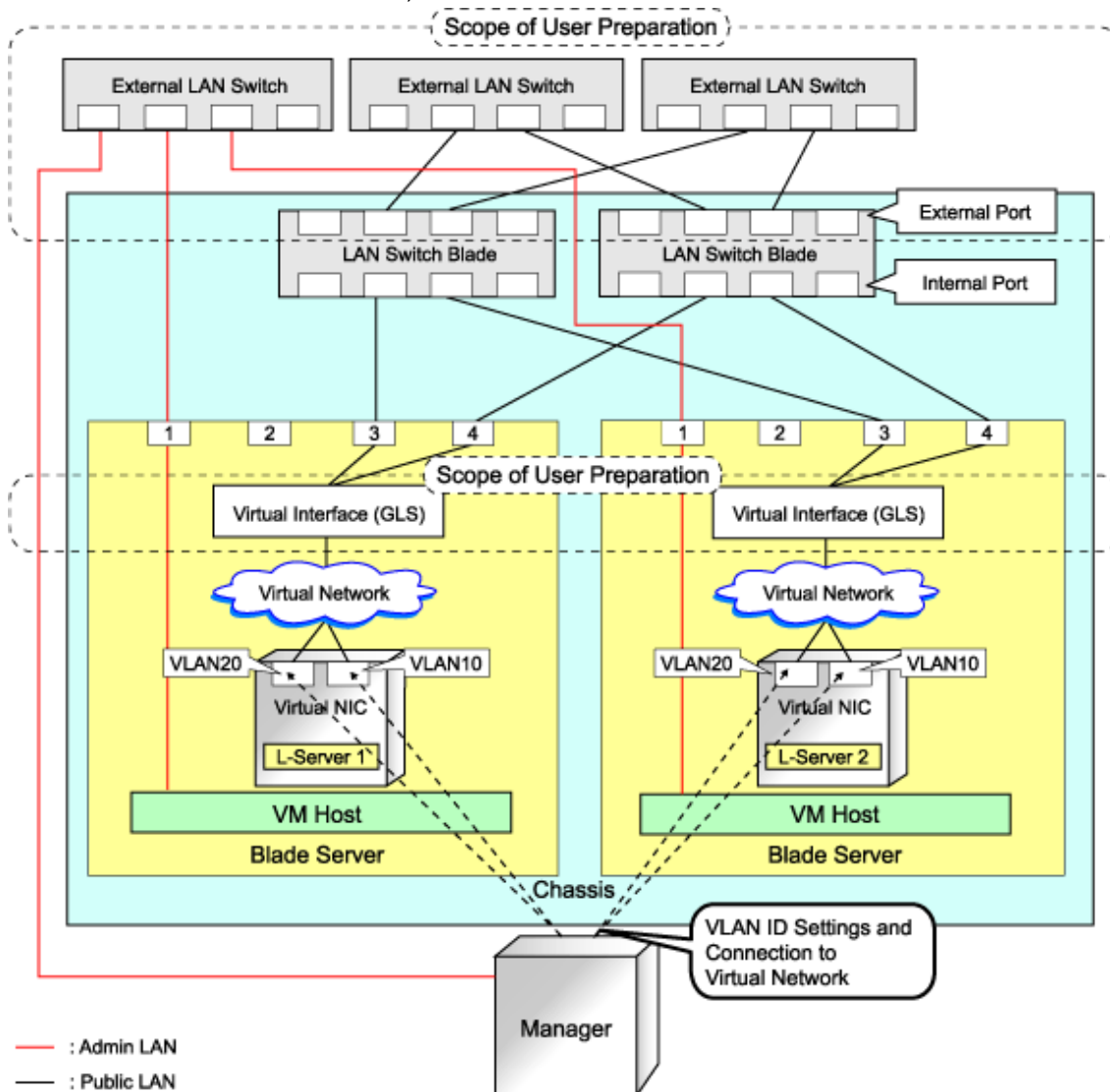
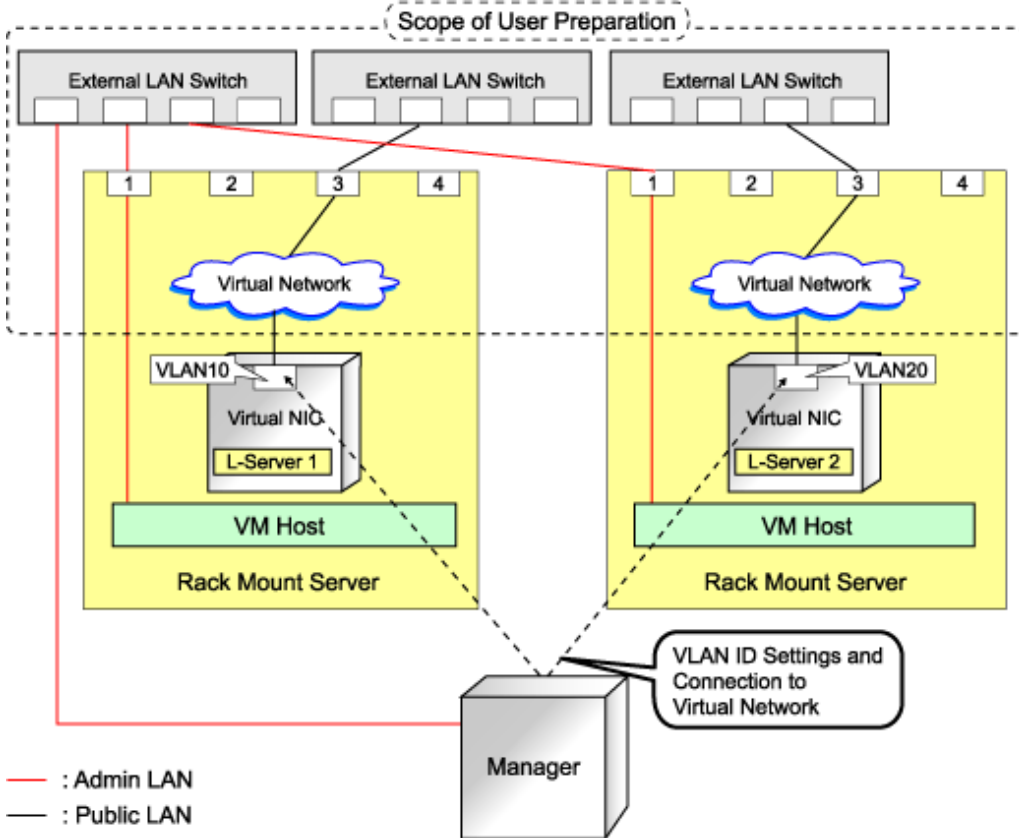


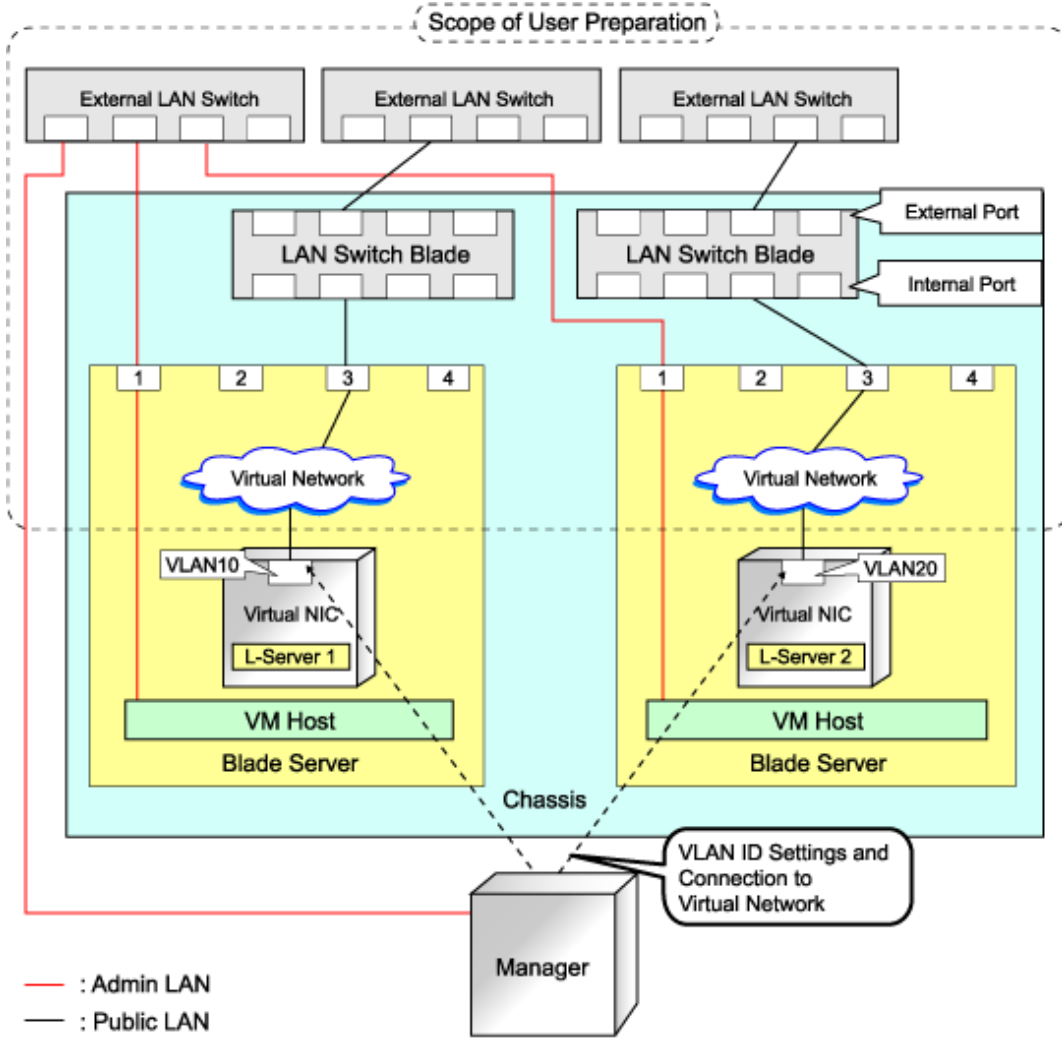
Figure E.11 Network Configurations of L-Servers for Rack Mount Servers



Note

- For environments using servers other than blade servers or environments where network redundancy is not performed for L-Servers, it is necessary to configure the external connections of the network manually.
For details, refer to "Manual Network Configuration" in "E.3.4 Setup".
- For Resource Orchestrator, configure the LAN switch blades when using switch mode or end-host mode.

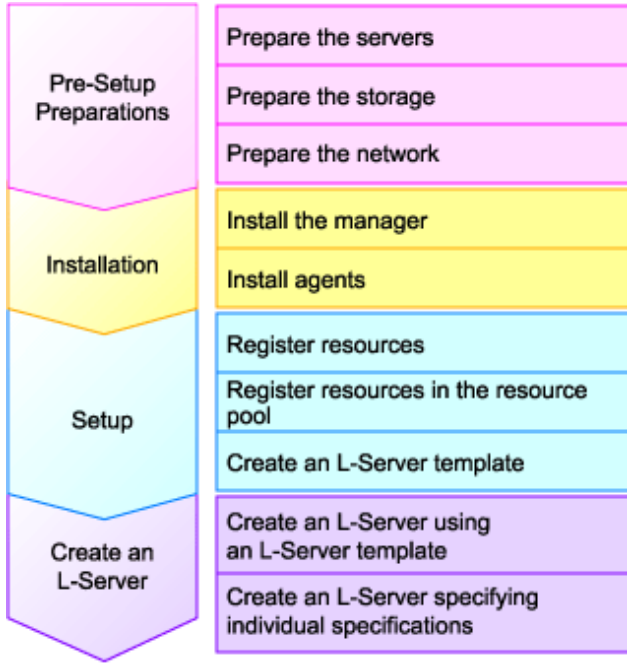
Figure E.12 Configuration When not Performing Network Redundancy for L-Servers with Blade Servers



L-Server Creation Procedure

The procedure for creating L-Servers is shown below.

Figure E.13 Resource Orchestrator Setup Procedure



For details on pre-setup preparations, refer to "[E.3.2 Preparations](#)".

For details on how to install Resource Orchestrator, refer to "[E.3.3 Installation](#)".

For details on how to set up Resource Orchestrator, refer to "[E.3.4 Setup](#)".

For details on how to create an L-Server, refer to "[L-Server Creation](#)" of "[E.3.4 Setup](#)".

E.3.2 Preparations

Pre-setup preparations are necessary when using a Hyper-V environment to create and manage an L-Server of Resource Orchestrator.

For details on pre-setup preparations for Hyper-V environment, refer to the Hyper-V manual.

Preparations for Servers

In addition to the operations in "[4.2.4 Preparations for Resource Orchestrator Network Environments](#)", confirm the following:

- When using I/O virtualization, that VIOM has been configured
- MSFC has been added to VM hosts
- A cluster disk has been configured as a shared cluster volume

All created L-Servers are located on a cluster as high availability VMs.

Storage Preparations

Check the following:

- A SAN volume has been configured as a cluster disk
- Zoning and affinity have been set
- The configuration enables use of SAN environments on VM hosts

Network Preparations

In addition to the operations in "[4.2 Defining and Configuring the Network Environment](#)", confirm the following:

- The configuration for the admin and public LANs has been designed
- The network environment for the admin LAN is configured
- The virtual switch to connect to the admin LAN has been designed and configured
- When performing network redundancy for L-Servers, using Intel PROSet or PRIMECLUSTER GLS with blade servers
 - The external LAN switch to connect to the LAN switch blade has been designed and configured
 - The LAN switch blade has been designed
- When not performing network redundancy for L-Servers with blade servers
 - The external LAN switch to connect to the LAN switch blade has been designed and configured
 - The LAN switch blade has been designed and configured
- When using servers other than blade servers
 - The external LAN switch to connect to servers other than blade servers has been designed and configured



See

-
- For details on the server NIC definitions, refer to "2.11 Server NIC Definition" of the "Reference Guide (Resource Management) CE".
 - For details on the rcxadm nicdefctl command, refer to "1.7.16 rcxadm nicdefctl" of the "Reference Guide (Resource Management) CE".
-

When Using IBP

When using virtual L-Servers, connect the IBP uplink sets used for the public LAN and admin LAN to the VM host regardless of VIOM, after creating each IBP uplink set.

It is not necessary to use the same name for the uplink set and the name of the network resource.

Pre-setup Preparations in Hyper-V Environments

Use the following procedure for pre-setup preparations for Hyper-V environments.

For details, refer to the MSFC help.

1. Installation of an Operating System and Configuration of a Domain Controller on the Domain Controller Server
2. Storage Environment Preparation
 - Creation of the volume (LUN) for allocation to the MSFC of the managed server (quorum disk and cluster disk)
3. Configuration of Managed Servers
 - a. BIOS configuration (hardware virtualization and Data Execution Prevention (DEP))
 - b. Install an OS
 - When installing an OS on a physical server, refer to the server virtualization software manual.
 - When installing a VM host in an L-Server, refer to "[Appendix F Installation of VM Hosts on Physical L-Servers](#)".
 - c. Join a domain
 - d. Add SNMP services
 - e. Configure SNMP services and SNMP traps
 - f. Add Hyper-V roles
 - g. Add a failover cluster function

4. Cluster Configuration of Managed Servers (MSFC)

- a. Create an access point for cluster management on the admin LAN side.
- b. In a quorum configuration, select one of the following:
 - When the number of nodes is even
Select "Node and Disk Majority", and specify a quorum disk.
 - When the number of nodes is uneven
Select "Node Majority".
- c. Enable the shared volume of the cluster.
- d. Add a cluster disk to a shared cluster volume.

5. Configuration After Creation of Clusters for Managed Servers

- a. Enable remote WMI settings.
 1. In each VM host, access the Control Panel and open the [Administrative Tools]-[Computer Management].
The [Computer Management] window is displayed.
 2. Open [Services and Applications], right-click on [WMI Control] and select [Properties].
The [WMI Control Properties] dialog is displayed.
 3. Open the [Security] tab, select [Root]-[virtualization] and click <Security>.
The [Security for ROOT\virtualization] window is displayed.
 4. Select the login user for the VM host, and check "Allow" from "Remote Enable".
 5. Open the [Security] tab, select [Root]-[MSCluster] and click <Security>.
The [Security for ROOT\MSCluster] window is displayed.
 6. Check if all checkboxes are selected, excluding "Special Permissions" for the local Administrators group for the VM host. When these checkboxes are not selected, check the checkboxes.
In the default settings, these checkboxes, other than, "Special Permissions" are all selected.
 7. Click <OK>.

The remote WMI settings are enabled.

b. Configure the Windows firewall to enable remote WMI management.

1. On each VM host, run the "Gpedit.msc" command.
The [Local Group Policy Editor] dialog is displayed.
2. Select the following folder:
[Computer Configuration]-[Administrative Templates]-[Network]-[Network Connections]-[Windows Firewall]
3. If the VM host is a member of a domain, double-click [Domain Profile]; otherwise double-click [Standard Profile].
Either one of the [Domain Profile] or [Standard Profile] screen is displayed.
4. Right-click [Windows Firewall: Allow remote administration exception properties], and select [Properties].
The [Windows Firewall: Allow remote administration exception properties] window is displayed.
5. Select "Enabled".
6. Click <OK>.

c. Configure DCOM.

1. On each VM host, run the "Dcomcnfg.exe" command.
The [Component Services] window is displayed.

2. Right-click [Component Services]-[Computers]-[My Computer], and select [Properties].
The [My Computer Properties] window is displayed.
3. Select the [COM Security] tab.
4. Click <Edit Limits> from "Launch and Activation Permissions".
The [Launch and Activation Permission] window is displayed.
5. Select the VM host's user name under "Groups or user names:", and select the "Allow" checkbox for "Remote Launch" and "Remote Activation".
6. Click <OK>.
7. Click <Edit Limits> under "Access Permissions".
The [Access Permission] window is displayed.
8. Select "ANONYMOUS LOGON" under "Group or user names", and check the "Allow" checkbox for "Remote Access".
9. Click <OK>.

6. Configuration and Installation of SCVMM

Use the following procedure to install and configure SCVMM:

- a. Install an OS
- b. Join a domain
- c. Register a VM Host
Register by the cluster. An SCVMM agent is automatically installed on newly registered VM hosts.
- d. Configure Windows remote management environment
Configure remote administration on VM management software registered with Resource Orchestrator.
 1. Log in to the server on which VM management software operates, using administrative privileges.
 2. Execute the following command from the command prompt.

```
>winrm quickconfig <RETURN>
```

3. Enter "y", when requested.

- e. SCVMM Server MaxShellPerUser Settings

7. Configure the Resource Orchestrator Admin Server

Configure remote management authentication settings on the machine the Resource Orchestrator admin server will be set up.

- a. Log on to the admin server as the administrator.
- b. Execute the following command from the command prompt to record the configuration details for TrustedHosts.

```
>winrm get winrm/config/client <RETURN>
```

Record the displayed details in TrustedHosts.

Example

When multiple SCVMMs are registered

```
*** ***, ***, ***, ***
```

When a single asterisk ("*") is displayed, the following procedure is unnecessary as all hosts will be trusted in the configuration.

- c. Execute the following command.

Enter the result obtained from b. for *Recorded_content_in_b.*

```
>winrm set winrm/config/client @{TrustedHosts="Recorded_content_in_b.", "Additionally_
registered_SCVMM_address"} <RETURN>
```

Example

The command specification when multiple SCVMMs are registered

```
>winrm set winrm/config/client @{TrustedHosts="***.***.***.***, ***.***.***.***, Additionally_
registered_SCVMM_address"} <RETURN>
```

- d. Execute the following command to check the details for TrustedHosts.

```
>winrm get winrm/config/client <RETURN>
```

If the address of the SCVMM additionally registered has been added to the details recorded in b., there are no problems.

Note

When registering multiple SCVMMs in Resource Orchestrator as VM management software, specify the IP addresses for multiple VM management softwares separated by commas (",") using the command registered in TrustedHosts.

8. Apply the Latest Update Program

For the server on which the manager will be installed, managed VM hosts, SCVMM, and SCVMM agents, apply the latest updates using Microsoft Update, etc.

SCVMM Server MaxShellPerUser Settings

Resource Orchestrator controls SCVMM using PowerShell Web Services for Management (hereinafter WS-Management).

With standard Windows settings, the maximum number of processes that can start shell operations per user (MaxShellsPerUser) is set to "5". For Resource Orchestrator, change settings to enable a maximum of 31 sessions.

Since WS-Management is used for Windows administrator tools and Resource Orchestrator, set a value 31 or larger for MaxShellsPerUser.

Change the MaxShellsPerUser settings using the following procedure:

1. Execute Windows PowerShell as an administrator.
2. Change the current directory using the Set-Location commandlet.

```
PS> Set-Location -Path WSMAN:\localhost\Shell <RETURN>
```

3. Check the current MaxShellsPerUser configuration information using the Get-ChildItem commandlet.

The content displayed in MaxShellsPerUser is the current setting.

```
PS WSMAN:\localhost\Shell> Get-ChildItem <RETURN>
```

Example

```
PS WSMAN:\localhost\Shell> Get-ChildItem
WSManConfig: Microsoft.WSMan.Management\WSMan::localhost\Shell

Name                               Value                               Type
```

-----	-----	----
AllowRemoteShellAccess	true	System.String
IdleTimeout	180000	System.String
MaxConcurrentUsers	5	System.String
MaxShellRunTime	2147483647	System.String
MaxProcessesPerShell	15	System.String
MaxMemoryPerShellMB	150	System.String
MaxShellsPerUser	5	System.String

4. Configure MaxShellsPerUser using the Set-Item commandlet.

Example

When setting MaxShellsPerUser "36"

```
PS WSMAN:\localhost\Shell> Set-Item .\MaxShellsPerUser 36 <RETURN>
```

E.3.3 Installation

This section explains installation methods.

Installing the Manager

Install the Resource Orchestrator manager. For details on how to install a manager, refer to "2.1.2 Installation [Windows]" of the "Installation Guide CE".

When using Hyper-V on managed servers, the only supported OS of the admin server is Windows.

When Windows PowerShell 2.0 or later has not been installed on the admin server, install it.

Installing the Agent

Install Resource Orchestrator agents on managed servers. For details on how to install agents, refer to "2.2.2 Installation [Windows/Hyper-V]" of the "Installation Guide CE".

E.3.4 Setup

The setup procedure when using Hyper-V as server virtualization software is as follows:

1. Register Resources

- a. Register VM Management Software

When registering VM management software, CSV files that are created in advance during pre-setup preparations, are automatically registered in Resource Orchestrator as virtual storage resources.

When configuring L-Server alive monitoring, domain users which belong to the Administrators group for all VM hosts must be specified for the login account for VM management software registered in Resource Orchestrator.

For details on how to register VM management software, refer to "2.2 Registering VM Management Software" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

b. Register managed servers

1. Register Chassis

Refer to "2.4.1 Registering Chassis" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

2. Register Managed Servers (within Chassis)

Refer to "2.4.2 Registering Blade Servers" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

3. Register LAN Switch Blades

Refer to "2.4.3 Registering LAN Switch Blades" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

c. Preparations for networks (for manual network configuration)

Preparation is necessary in the following cases.

For details, refer to "Preparations" of "[Connections with Virtual Networks Created in Advance](#)".

- When not performing network redundancy for L-Servers with blade servers
- When using servers other than blade servers

d. Network resources

To register a network resource, specify a network pool when creating the network resource.

By creating network resources in advance, if the NIC and network resources are connected when an L-Server is created, the following settings matching the network resource definition will be registered automatically.

For details on automatic configuration of network resources, refer to "[Automatic Network Configuration](#)".

2. Register Resources in Resource Pools

a. Register VM host resources

1. In the ROR console orchestration tree, right-click the target VM pool, and select [Register Resources] from the popup menu.

The [Register Resources] dialog is displayed.

2. Select the VM host to register.
3. Click <OK>.

b. Register virtual storage resources

1. In the ROR console orchestration tree, right-click the target storage pool, and select [Register Resources] from the popup menu.

The [Register Resources] dialog is displayed.

2. Select the virtual storage resource to register.
3. Click <OK>.

c. Register network resources

If the NIC and network resources are connected when an L-Server is created, a VLAN ID is automatically configured for the NIC of the VM guest, and connected to the virtual network.

For details, refer to "[Automatic Network Configuration](#)".

1. In the ROR console orchestration tree, right-click the target network pool, and select [Create Resource] from the popup menu.

The [Create a network resource] dialog is displayed.

2. Enter the items necessary for network resources.

For details, refer to "7.3 Network Resources" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

3. Create an L-Server Template

a. Export an L-Server template

Refer to "8.2.1 Exporting a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

b. Edit an L-Server template

Refer to "8.2.2 Editing a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

c. Import an L-Server template

Refer to "8.2.3 Importing a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Automatic Network Configuration

Network settings on Hyper-V differ depending on hardware (such as blade servers and rack mount servers), and whether network redundancy will be performed for L-Servers.

- Automatic network configuration for blade servers

Refer to "[Automatic Network Configuration for Blade Servers](#)".

- When not performing network redundancy for L-Servers with blade servers

Refer to "[Manual Network Configuration](#)".

Automatic network configuration using an arbitrary physical NIC is also possible by defining the physical NIC to be used in the server NIC definition file and then specifying the physical LAN segment defined in the server NIC definition from the network resource. To reflect the physical NIC configuration specified in the server NIC definition file on Resource Orchestrator, use the `rcxadm nicdefctl` commit command.

This enables automatic network configuration even in configurations using an arbitrary physical NIC. However, when using server NIC definitions, the operation must be performed from the command-line.



See

- For details on the server NIC definitions, refer to "2.11 Server NIC Definition" of the "Reference Guide (Resource Management) CE".
- For details on the `rcxadm nicdefctl` command, refer to "1.7.16 `rcxadm nicdefctl`" of the "Reference Guide (Resource Management) CE".

- Network configuration for servers other than blade servers

Refer to "[Manual Network Configuration](#)".

Automatic Network Configuration for Blade Servers

If the NIC and network resources are connected when an L-Server is created, the following settings will be registered automatically for the VM host that the L-Server will operate on.

- LAN Switch Blades

When using a LAN switch blade in switch mode or end-host mode, a VLAN is configured on the internal connection port.

When creating a network resource, a VLAN can be configured on the port of LAN switch blade specified as the uplink port, by using the following procedure.

- From the GUI:

In the [Create a network resource] dialog, check the "Automatically configure VLANs for the uplink ports." checkbox.

- From the Command-line:

In the XML definition for the network resource, specify "true" for vlnautosetting (Automatic VLAN configuration for uplink ports).

- Virtual Network

When there is no virtual network on the public LAN, it will be created automatically using the virtual interface (IntelPROSet or PRIMECLUSTER GLS)) manually created in advance.

When a network already exists, the virtual network can be used.

- VM Guests

Configure a VLAN on the virtual NIC of the VM guest, and connect with the virtual network.

If an image is specified, the IP address is automatically configured. For details on how to configure IP addresses automatically, refer to "Network (NIC)" of "10.3.1 [General] Tab" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

In environments using the clustering function of VM management software, in order to enable the migration of VM guests and operation using the HA function, settings for LAN switch blades and virtual switches are performed automatically for all VM hosts comprising the cluster.

When not configuring the tagged VLAN automatically for the uplink port of network resources, use the ROR console to configure the VLAN settings of uplink ports. Right-click the LAN switch in the server resource tree, and select [Modify]-[Network Settings] from the popup menu.

For details, refer to "2.4.4 Configuring VLANs on LAN Switch Blades" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".



After creating an L-Server, if VM hosts are added to the cluster afterwards, Resource Orchestrator network settings are not performed automatically.

Perform the same settings as the existing VM hosts in the cluster configuration for the LAN switch blades and virtual networks of the additional VM hosts.

Virtual network definition files for blade servers

- When configuring the network for blade servers automatically

It is not necessary to create a virtual network definition file.

- When a virtual network definition file exists and no virtual network with a VLAN ID is defined

The virtual network is automatically configured.

- When a virtual network with a VLAN ID is defined, using a virtual network definition file

It is necessary that a virtual network with the VLAN ID be manually configured beforehand.

For details, refer to "[Manual Network Configuration](#)".

Default Blade Server Configuration to Support Automation of Network Configuration in Resource Orchestrator

The default blade server configuration to support automation of network configuration in Resource Orchestrator (server blades, specification of uplink ports for network resource, correspondence relation of numbers of LAN switch blades and physical network adapters, etc.) is shown in the following list. When there are no server NIC definitions, for network auto-configuration, a virtual network is created using the physical network adapter selected according to this list.

Table E.11 Default Blade Server Configuration for Network Auto-Configuration (for PRIMERGY BX900 S1 Chassis)

Server Blade	Specification of Uplink Port (Location of LAN Switch Blade)	LAN Switch Blade to Use	Physical Network Adapter Number (*4)
BX920 S1 BX920 S2 BX922 S2	CB1 and CB2, or no specification for uplink port	PG-SW111 PG-SW112	3, 4
		PG-SW109 (*1) PG-SW201	1, 2
	CB3 and CB4	PG-SW111 PG-SW112 PG-SW109 PG-SW201	5, 6
	CB5 and CB6	PG-SW109	9, 10
	CB7 and CB8	PG-SW111 PG-SW112	11, 12
PG-SW201		9, 10	
BX924 S2	CB1 and CB2, or no specification for uplink port	PG-SW111 PG-SW112 PG-SW109 PG-SW201	1, 2
		PG-SW111 PG-SW112 PG-SW109 PG-SW201	3, 4
	CB5 and CB6	PG-SW109	7, 8
	CB7 and CB8	PG-SW111 PG-SW112	9, 10
		PG-SW201	7, 8
BX960 S1	CB1 and CB2, or no specification for uplink port	PG-SW111 PG-SW112 PG-SW109 PG-SW201	11, 12
		PG-SW111 PG-SW112 PG-SW109 PG-SW201	3, 4
	CB5 and CB6 (*3)	PG-SW109	7, 8
	CB7 and CB8 (*3)	PG-SW111 PG-SW112	9, 10
		PG-SW201	7, 8

*1: When installing a PG-SW109 on CB1 or CB2, set the transmission speed at the down link port of PG-SW109 to 1 Gbps. For details on how to configure the settings, refer to the corresponding hardware manual.

*2: A LAN expansion card is mounted in expansion slot 1.

*3: A LAN expansion card is mounted in expansion slot 2.

*4: Configure a virtual network automatically on a virtual interface configured beforehand in a redundant configuration using individual physical network adapters. Configure the virtual interface on the managed server using one of following products beforehand.

- Intel PROSet
- PRIMECLUSTER GLS for Windows

Table E.12 Default Blade Server Configuration for Network Auto-Configuration (for PRIMERGY BX400 S1 Chassis)

Server Blade	Specification of Uplink Port (Location of LAN Switch Blade)	LAN Switch Blade to Use	Physical Network Adapter Number (*3)
BX920 S2 BX922 S2	CB1 and CB2 (*1), or no specification for uplink port	PG-SW111 PG-SW112	3, 7
		PG-SW109 (*2) PG-SW201	2, 6
	CB3 and CB4	PG-SW111 PG-SW112 PG-SW109 PG-SW201	9, 10
BX924 S2	CB1 and CB2 (*1), or no specification for uplink port	PG-SW111 PG-SW112 PG-SW109 PG-SW201	2, 4
	CB3 and CB4	PG-SW111 PG-SW112 PG-SW109 PG-SW201	7, 8

*1: The same LAN switch blade model should be mounted in CB1 and CB2.

*2: When installing a PG-SW109 on CB1 or CB2, set the transmission speed at the down link port of PG-SW109 to 1 Gbps. For details on how to configure the settings, refer to the corresponding hardware manual.

*3: Configure a virtual network automatically on a virtual interface configured beforehand in a redundant configuration using individual physical network adapters. Configure the virtual interface on the managed server using one of following products beforehand.

- Intel PROSet
- PRIMECLUSTER GLS for Windows

Table E.13 Default Blade Server Configuration for Network Auto-Configuration (for PRIMERGY BX600 S3 Chassis)

Server Blade	Specification of Uplink Port (Location of LAN Switch Blade)	LAN Switch Blade to Use	Physical Network Adapter Number (*1)
BX600 series servers	NET1 and NET2, or no specification for uplink port	PG-SW107	3, 4
	NET3 and NET4	PG-SW104	7, 8

*1: Configure a virtual network automatically on a virtual interface configured beforehand in a redundant configuration using individual physical network adapters. Configure the virtual interface on the managed server using one of following products beforehand.

- Intel PROSet
- PRIMECLUSTER GLS for Windows

The numbers of physical network adapters given above can be checked on the details window of the LAN switch blade.

The MAC address (IP address) information of managed servers can be confirmed in "Hardware Maintenance" on the [Resource Details] tab.

Configure the Intel PROSet or PRIMECLUSTER GLS settings on the managed server in advance, using this MAC address information.

When the LAN switch blade is in IBP mode, create a virtual network on the virtual interface configured beforehand in the redundant configuration using the same physical network adapter as in the case of "no specification for uplink port" in the list above.

Performing the following procedure enables automatic network configuration using an arbitrary physical NIC.

1. Create a server NIC definition and reflect it on Resource Orchestrator.
 - a. Create a Server NIC Definition

Edit the template file and create a server NIC definition.
 - b. Reflect the Server NIC Definition

Execute the `rcxadm nicdefctl commit` command to reflect the physical NIC configuration specified in the server NIC definition file on Resource Orchestrator.
 - c. Confirm the Reflected Server NIC Definition

Execute the `rcxadm nicdefctl show` command and confirm the server NIC definition has been reflected on Resource Orchestrator.
2. Create the XML file that defines network resources, and then create the network resources.
 - a. Create the XML File that Defines Network Resources

Specify the physical LAN segment name that was specified for "PhysicalLANSegment name" in the server NIC definition file for "PhysicalLANSegment" in the XML file that defines network resources.

In this case, specify `auto="true"` in the Network element.
 - b. Create Network Resources

Execute the `rcxadm network create` command specifying the XML file created in a.



See

- For details on the server NIC definitions, refer to "2.11 Server NIC Definition" of the "Reference Guide (Resource Management) CE".
- For details on the `rcxadm nicdefctl` command, refer to "1.7.16 rcxadm nicdefctl" of the "Reference Guide (Resource Management) CE".
- For details on how to define network resources, refer to "2.5 Network Resources" in the "Reference Guide (Resource Management) CE".
- For details on the `rcxadm network` command, refer to "1.3.5 rcxadm network" of the "Reference Guide (Resource Management) CE".



Note

- If there are VM hosts that meet the following conditions, automation of network configuration is not supported in the chassis.
 - Network resources with uplink ports specified are used
 - There is a virtual network that uses a NIC in a VM host configuration pattern that differs from the ones supporting automation of network configuration
- If there are VM hosts that meet the following conditions, automation of network configuration is not supported.
 - Network resources with no uplink port specified are used
 - There is a virtual network that uses a NIC in a VM host configuration pattern that differs from the ones supporting automation of network configuration

In the diagram, the default blade server configurations as described in the following configuration example when using a PRIMERGY BX900 S1 chassis are shown.

Table E.14 Configuration Example 1

Server blades	BX920 S2
Specification of uplink port	CB1 and CB2
LAN switch blade to use	PG-SW112

Virtual interface	PRIMECLUSTER GLS
-------------------	------------------

Table E.15 Configuration Example 2

Server blades	BX920 S2
Specification of uplink port	Both "no specification for uplink port" and "CB3 and CB4" are specified
LAN switch blade to use	PG-SW109
Virtual interface	PRIMECLUSTER GLS

Figure E.14 Blade Server Diagram of Configuration Example 1

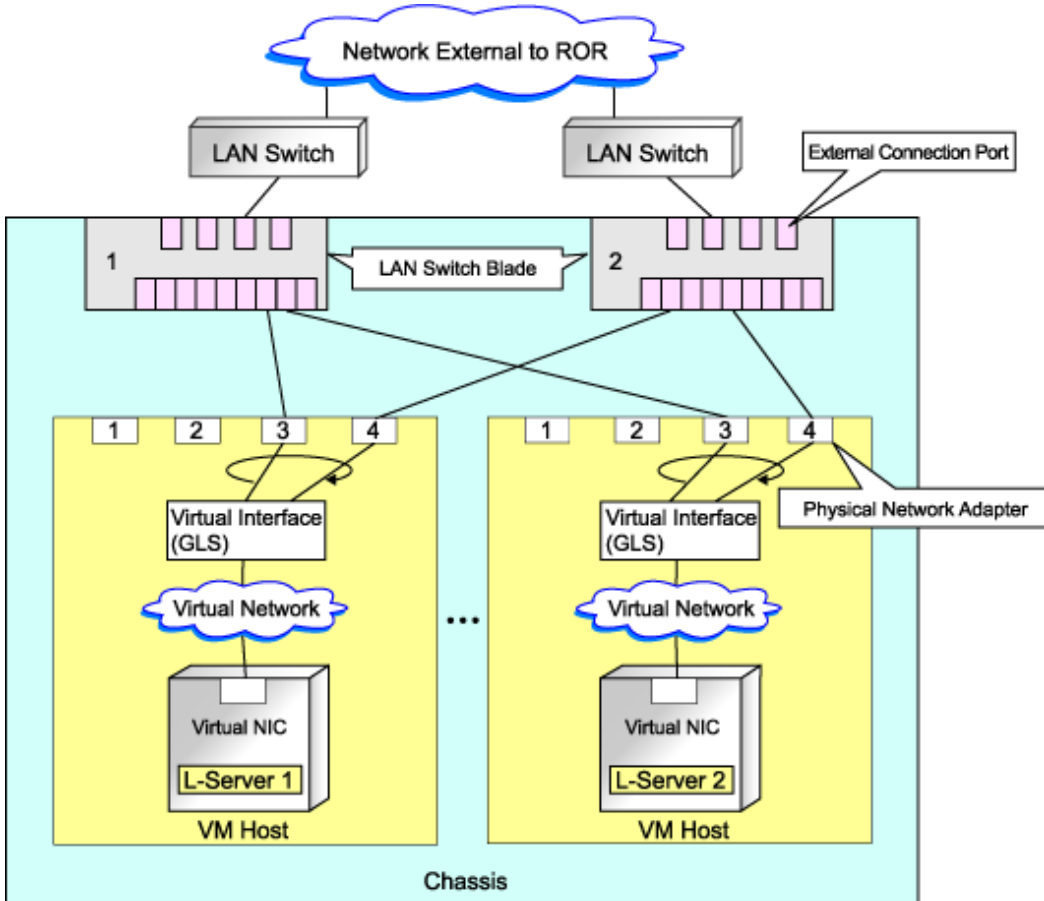
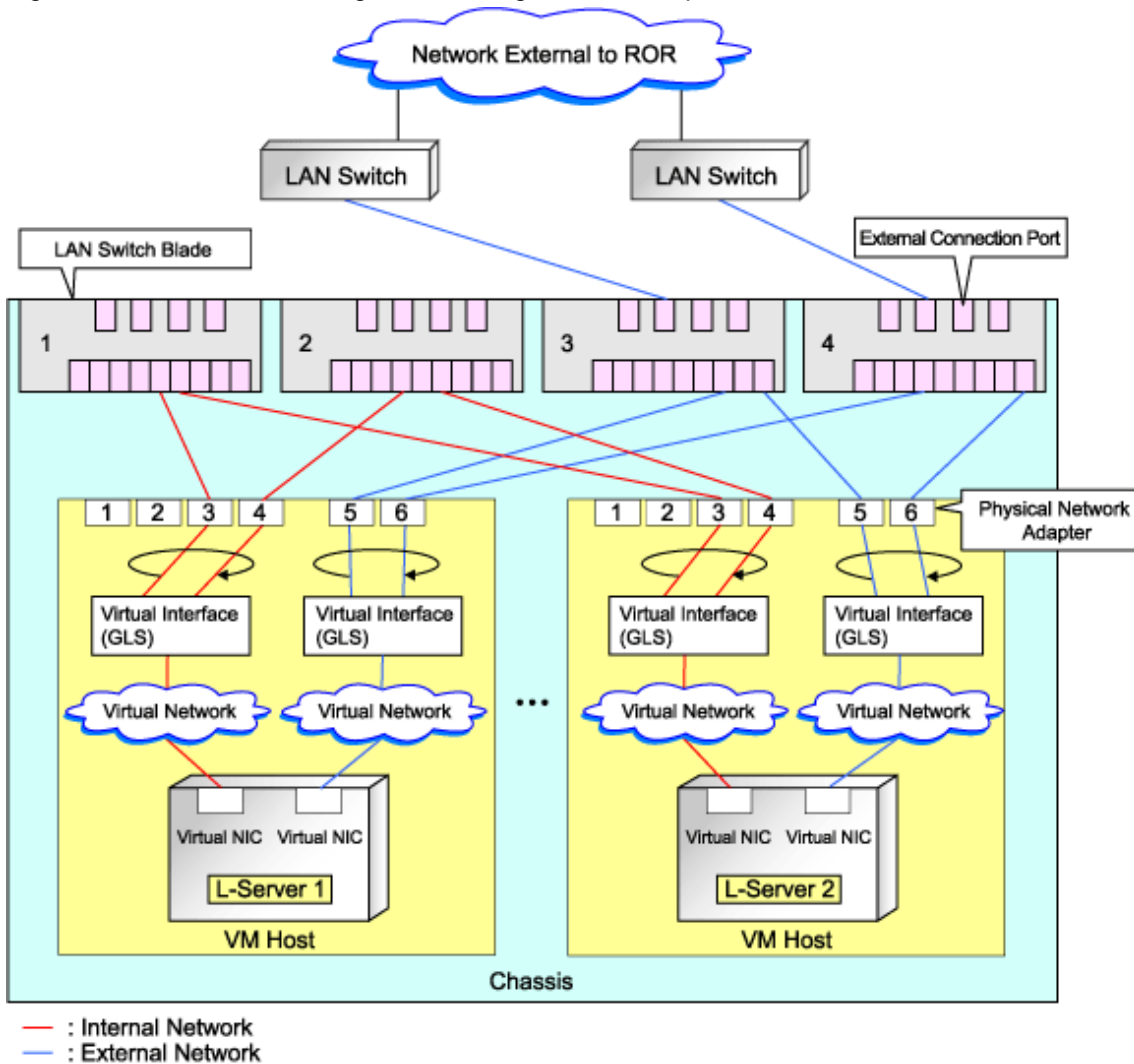


Figure E.15 Blade Server Diagram of Configuration Example 2



Manual Network Configuration

In the following cases, configure the network manually.

- When using a physical network adapter number that differs from configuration patterns of VM hosts which support automation of network configuration

Refer to ["Configuring Network Resources when Using a Physical Network Adapter Number that Differs from Configuration Patterns of VM Hosts which Support Automation of Network Configuration"](#) in "G.1.4 Setup".

- When not performing network redundancy for L-Servers with blade servers

Refer to ["Connections with Virtual Networks Created in Advance"](#).

- For environments using servers other than blade servers

Refer to ["Connections with Virtual Networks Created in Advance"](#).

When a virtual network has already been manually configured and server virtualization software other than Hyper-V is being used with the same manager, set a different name from the one used by the virtual switch, virtual network, and virtual bridge on the other virtualization software.

Configuring Network Resources when Using a Physical Network Adapter Number that Differs from Configuration Patterns of VM Hosts which Support Automation of Network Configuration

When using a physical network adapter number that is different from the one used in the configuration patterns mentioned above, create networks using the following procedure.

1. Create a virtual network with the same name (including upper and lower case characters) for all VM hosts comprising the cluster.

This enables migration of VM guests between VM hosts. When using System Center 2012 Virtual Machine Manager as VM management software, only "External" can be used for the type of virtual network which is the connection destination for the VM guest.

For details on how to create networks, refer to the SCVMM help.

2. Configure LAN switches to enable communication using the tagged VLAN between virtual networks using the same name.

Right-click the target LAN switch in the server resource tree on the ROR console, and select [Modify]-[Network Settings] from the popup menu.

The [VLAN Settings] dialog is displayed.

3. Configure a VLAN.

4. Define supported virtual networks and VLAN IDs in the following definition file:

Installation_folder\Manager\etc\customize_data\vnetwork_hyperv.rcxprop

For details on definition file format, refer to "[File Format for Virtual Network Definitions](#)".

5. Create Network Resources

- From the GUI:

- a. In the [Create a network resource] dialog containing the VLAN ID that was specified in 2. and 4., uncheck the "Use configured virtual switches." checkbox and create a network resource.

- From the Command-line:

- a. Create the XML file that defines network resources.

Define the VLAN ID specified at 2. to 4. in the XML file.

In this case, specify auto="false" in the Network tag.

- b. To create the network resource, execute the rcxadm network create command specifying the XML file created in a.

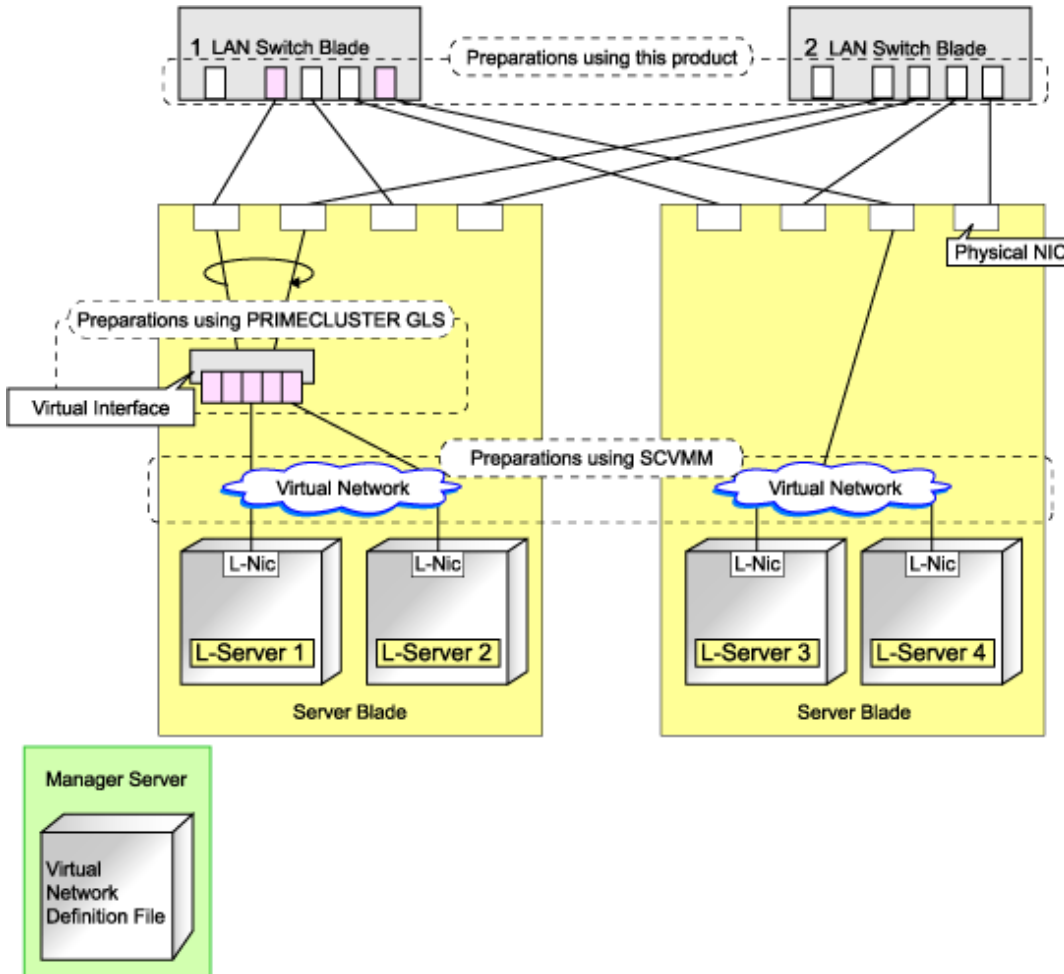
The network resources are created.



See

- For details on how to configure VLAN settings of LAN switch blade uplink ports, refer to "2.4.4 Configuring VLANs on LAN Switch Blades" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".
- For details on the Network element and creation of XML files that define network resources, refer to "2.5 Network Resources" of the "Reference Guide (Resource Management) CE".
- For details on the rcxadm network command, refer to "1.3.5 rcxadm network" of the "Reference Guide (Resource Management) CE".

Figure E.16 Network Diagram



Connections with Virtual Networks Created in Advance

When not performing network redundancy for L-Servers with blade servers, and in environments where blade servers are not used, only the function for configuring IP addresses and VLAN IDs on VM guest NICs and connecting NICs of VM guests is provided for virtual networks created in advance. Manually perform virtual network settings in advance.

Additionally, the following settings must be performed in advance.

Preparations

1. Virtual network creation

Create a virtual network with the same name (including upper and lower case characters) for all VM hosts comprising the cluster. This enables migration of VM guests between VM hosts. When using System Center 2012 Virtual Machine Manager as VM management software, only "External" can be used for the type of virtual network which is the connection destination for the VM guest.

For details on how to create networks, refer to the SCVMM help.

2. Configure the Virtual Network Communication

Configure LAN switches to enable communication using the tagged VLAN between virtual networks using the same name.

- a. Right-click the target LAN switch in the server resource tree on the ROR console, and select [Modify]-[Network Settings] from the popup menu.

The [VLAN Settings] dialog is displayed.

- b. Configure a VLAN.

3. Define the Supported Virtual Network and VLAN ID

Supported virtual networks and VLAN IDs are defined in the following definition file of Resource Orchestrator:

Installation_folder\Manager\etc\customize_data\vnetwork_hyperv.rcxprop

For details on definition file format, refer to "[File Format for Virtual Network Definitions](#)".

4. Create Network Resources

- From the GUI:

In the [Create a network resource] dialog containing the VLAN ID that was specified in 2. and 3., uncheck the "Use configured virtual switches." checkbox and create a network resource.

- From the Command-line:

- a. Create the XML file that defines network resources.

Define the VLAN ID specified at 2. to 3. in the XML file.

In this case, specify auto="false" in the Network tag.

- b. To create the network resource, execute the rcxadm network create command specifying the XML file created in a.

The network resources are created.



See

.....
- For details on how to configure VLAN settings of LAN switch blade uplink ports, refer to "2.4.4 Configuring VLANs on LAN Switch Blades" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- For details on the rcxadm network command, refer to "1.3.5 rcxadm network" of the "Reference Guide (Resource Management) CE".
.....

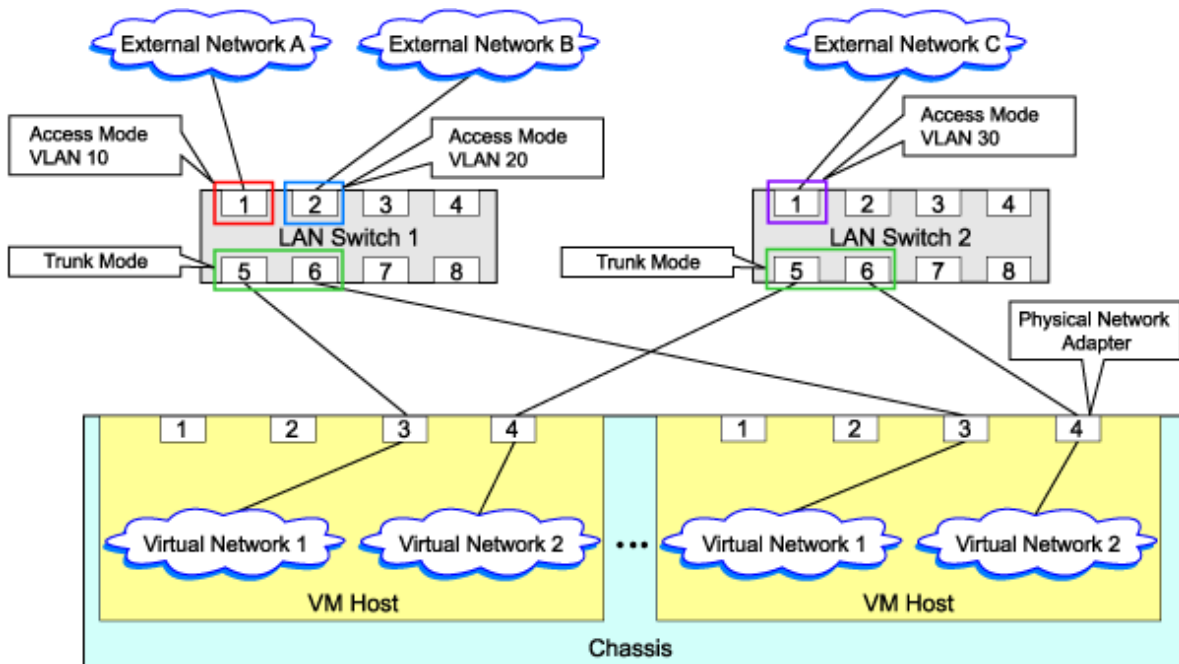
Virtual NIC Automatic Configuration for VM Guests

Configure a VLAN on the virtual NIC of the VM guest, and connect with the virtual network.

If an image is specified, the IP address is automatically configured. For details on how to configure IP addresses automatically, refer to "Network (NIC)" of "10.3.1 [General] Tab" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

For rack mount or tower servers, an example of virtual NIC configuration and connection with virtual networks using network resources is given below:

Figure E.17 Virtual NIC Configuration and Virtual Network Connection Using Network Resources for Rack Mount or Tower Servers



File Format for Virtual Network Definitions

Describe the virtual network definition file in one line as below:

```
"Virtual Network Name"= VLAN ID[, VLAN ID...]
```

For the *VLAN ID*, a value from 1 to 4094 can be specified. When specifying a sequence of numbers, use a hyphen ("-") such as in "1-4094".

Example

```
"Network A"=10
"Network B"=21,22,23
"Network C"=100-200,300-400,500
```

Blank spaces before and after equal signs ("=") and commas (",") are ignored.

Describe the virtual network correctly, as the entry is case-sensitive.

Save files using the UTF-8 character code.

When there are multiple lines with the same virtual network name, all specified lines are valid.

When the same VLAN ID is included in a line with a different virtual network name, the first occurrence in the file is valid and the lines after it are ignored.

Example

```
"Network D"=11
"Network D"=12 (*1)
"Network E"=11,15 (*2)
```

*1: Same as when "Network D"=11,12.

*2: 11 is ignored.

An error occurs during L-Server creation if the definition of the VLAN ID of the network resource connected to the NIC cannot be found.

Configuration for MAC Address Pools

Use MAC address pools for System Center 2012 Virtual Machine Manager, in order to allocate MAC address to the NIC, when creating an L-Server connected with the NIC coordinating with System Center 2012 Virtual Machine Manager.

When not changing the default MAC address pool on System Center 2012 Virtual Machine Manager, or only one MAC address pool exists for a Hyper-V environment, use that MAC address pool.

When there is no MAC address pool for a Hyper-V environment on System Center 2012 Virtual Machine Manager, create a MAC address pool to allocate MAC addresses using System Center 2012 Virtual Machine Manager.

When there are multiple MAC address pools on System Center 2012 Virtual Machine Manager, use the following procedure to define the MAC address pool to use.

1. Settings when using tenants in Resource Orchestrator

When creating multiple host groups on System Center 2012 Virtual Machine Manager, use the following procedure to use the same tenant configurations as that of the host group.

1. Create the same number of tenants as the number of host groups in Resource Orchestrator.
2. Register the VM host located in each host group in the local pool of the corresponding tenant.

2. Definition of a MAC address pool using an L-Server

Define the MAC address pool to use when creating an L-Server in the MAC address pool definition file in Resource Orchestrator.

When dividing MAC address pools for each tenant created in 1., define the MAC address pool used in each tenant in the MAC address definition file.

When creating multiple host groups in System Center 2012 Virtual Machine Manager, create a definition for each tenant, and specify the MAC address pool allocated to the host group.

For details on definition file format for MAC address pool, refer to "Definition File Format for MAC Address Pools".

Definition File Format for MAC Address Pools

Location of the Definition File

[Windows]
Installation_folder\Manager\etc\customize_data

Definition File Name

The definition file name can be used by dividing it into definitions that are available for each tenant and definitions that are common to the system.

If both a definition file for each tenant and a common definition file exist on the system, priority is given to the definitions indicated in the definition file for each tenant.

- By Tenant

scvmm_mac_pool_*tenant_name*.rcxprop

- Common on System

scvmm_mac_pool.rcxprop

Character Code

UTF-8

Line Break Code

CR/LF

Definition Configuration File Format

Key = Value

Table E.16 Definition File Items

Item	Description
Key	<ul style="list-style-type: none"> - When one SCVMM is registered all - When multiple SCVMMs are registered scvmm[SCVMM registered name]
Value	<p>Specify the name of a MAC address pool created in System Center 2012 Virtual Machine Manager.</p> <p>When the MAC address pool name to specify includes blank spaces, enclose the MAC address pool name in double quotes (" ").</p> <p>For details on the character types available for MAC address pools, refer to the SCVMM manual.</p>

 **Example**

- When only one SCVMM is registered, or when multiple SCVMMs are registered and the MAC address pool names used in each SCVMM are the same

```
all = "MAC pool A"
```

- When multiple SCVMMs are registered, and different MAC address pool names are used for each SCVMM

```
scvmm[scvmm1] = "MAC pool A"
scvmm[scvmm2] = "MAC pool B"
```

 **Note**

- When the VM management software to use is System Center Virtual Machine Manager 2008 R2, it is ignored even if the definition files exist.
- If you edit and save a UTF-8 text file using Windows Notepad, the Byte Order Mark (BOM) is stored in the first three bytes of the file, and the information specified on the first line of the file will not be analyzed correctly. When using Notepad, specify the information from the second line.
- More than one blank spaces or tabs at the beginning and end of the line, and before and after equal signs ("=").
- When a line start with "#", that line is regarded as a comment.
- The details of lines that are not based on the format above are ignored.
- Only lower case is valid for "all", "scvmm[registration_name_of_SCVMM]", and "scvmm" used for keys. If upper case characters are included, the string is ignored.
- When the same key exists in the line, the definitions described in the last line are valid.
- When both "all" key and "scvmm[registration_name_of_SCVMM]" key exist together, priority is given to the definitions for "scvmm[registration_name_of_SCVMM]" .
- The definition file configurations are reflected without restarting the manager in Resource Orchestrator.

L-Server Creation

Use the following procedure to create L-Servers:

- Create an L-Server Using an L-Server Template

- When there are no cloning images, or when not using cloning images which have been already registered

1. Create an L-Server, referring to "10.1 Creation Using an L-Server Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE". When creating the L-Server, select "None" for images.

In this case, the created L-Server may not be displayed in the orchestration tree.

For details, refer to "Note- When the created L-Server is not displayed in the orchestration tree".

For details on the created VM guests or cloning images, refer to "Information- Information created during L-Server creation".

2. Install an OS, referring to "[Manual OS Installation](#)".

3. When collecting cloning images after creating an L-Server, the cloning images are stored in the image pool. When collecting cloning images, refer to "[Collecting Cloning Images](#)".

- When using an existing cloning image

Create an L-Server, referring to "10.1 Creation Using an L-Server Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE". In this case, specify the cloning image that you want to use as an image.

- Create an L-Server Specifying Individual Specifications

Refer to "10.3 Creation of Virtual L-Servers Using Parameters" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

For details on the [OS] tab settings, refer to "[\[OS\] Tab Configuration](#)".



Note

When the created L-Server is not displayed in the orchestration tree

When using the following SCVMM functions for the VM of the created L-Server, after this, the L-Server will not be recognized or displayed in the orchestration tree, and operation of the L-Server becomes unavailable.

- Saving in the library, deploying from the library
- New template
- Transfer the template to a cluster node that is not managed by Resource Orchestrator

When "copying" is performed, the copied VM is not recognized as an L-Server.



Information

Information created during L-Server creation

- VM guests created as L-Servers have the following configuration:

Disk and DVD

First disk (system volume)

Connected to the primary channel (0) of IDE device

Second or later disk

Connected to a SCSI adapter as data disk (*1)

DVD drive

Connected to the secondary channel (0) of IDE device

*1: Cannot be used on guest OS's without the integrated service. Only boot disks connected to the IDE adapter can be used.

Virtual network adapter

When a guest OS that Hyper-V supports is specified, a converged network adapter will be used. When a different OS has been selected, an emulated network adapter will be added.

For details on the guest OS's supported by Hyper-V, refer to the following Microsoft web site.

Microsoft download web site

URL: <http://www.microsoft.com/windowsserver2008/en/us/hyperv-supported-guest-os.aspx> (As of February 2012)

CPU type

"1.00GHz Pentium III Xeon" or "3.60 GHz Xeon (2 MB L2 cache)" (the SCVMM default value) is specified. The CPU type is used for internal operations of SCVMM, and it does not indicate the CPU performance.

It is also different from the information displayed for the computer information of the guest OS.

- For cloning images, only system volumes are collected and deployed.

When registering a template created using SCVMM in the image pool of Resource Orchestrator, use a template created from a VM guest that has the system volume (a disk connected to primary channel (0) of the IDE device).

In other configurations, deploying using Resource Orchestrator will create VM guests without system volumes.

Manual OS Installation

Manually install an OS, after configuring the DVD connection settings from the SCVMM management window.

To use a guest OS supported by Microsoft on Hyper-V, it is necessary to install a virtual guest service on the guest OS.

For details on virtual guest service installation, refer to the Help of SCVMM.

Collecting Cloning Images

Use the following procedure to collect cloning images:

After installing an OS, stop the target L-Server.

1. Right-click the target L-Server in the orchestration tree, and select [Cloning]-[Collect] from the popup menu.
2. Click <OK>.

A given cloning image (identified by its name attribute) can be managed by image version.

If a cloning image is created using VM management software, it can be used as is.



Note

- If an L-Server is created with a specified Windows image, when deploying the image use Sysprep, provided by Microsoft, to re-configure the properties unique to the server. By executing Sysprep, the user information and OS setting information are reset. For details on Sysprep, refer to the information provided by Microsoft.
 - If stopping or restarting of the manager is performed during execution of Sysprep, the operation being executed will be performed after the manager is started. Until the process being executed is completed, do not operate the target resource.
 - When using MAK license authentication for activation of Windows Server 2008 image OS, Sysprep can be executed a maximum of three times. Since Sysprep is executed when creating L-Server with images specified or when collecting cloning images, collection of cloning images and creation of L-Servers with images specified cannot be performed more than four times. Therefore, it is recommended not to collect cloning images from L-Servers that have had cloning images deployed, but to collect them from a dedicated master server. The number is also included in the count when Sysprep is performed when a template is created using SCVMM.
 - Creation of L-Servers by specifying cloning images on which Windows 2000 Server and Windows 2000 Advanced Server are installed is not supported.
 - When using System Center 2012 Virtual Machine Manager as VM management software, only cloning images with high-availability attributes can be used in Resource Orchestrator.
-



Images are stored in the SCVMM library.

Specify a library that has sufficient disk space available to store the collected images.

When "Automatic selection" is specified in the [Collect a Cloning Image] dialog, selection is made from libraries registered with SCVMM, but collection of images may fail, as the available disk space of libraries is not managed by SCVMM.

Resource Orchestrator uses SCVMM templates for collection of images.

When collecting images from L-Servers, a template is created using a name with the version number added to the image name. When retrieving the template created by the user as an image, the template is treated as an image.

In order to collect images of L-Servers, a work area equal to the size of the disk (the system volume, all data disks, snapshot, and configuration definition file) of the target of L-Server creation is necessary. This work area is released, when collection of images is complete.

When collecting images, data disks other than the system volume are deleted.

In Resource Orchestrator, the virtual hard disk of the primary channel (0) of the IDE device is managed as the system volume.

DVD drives other than the secondary channel (0) of the IDE device are deleted. A DVD drive is added to the secondary IDE channel (0) even if there is no DVD drive in the image. If DVD drives other than this drive exist, they are deleted.

Collection of images cannot be collected, when there are snapshots. Collect images after deleting snapshots. When creating checkpoints from the SCVMM management console or creating snapshots from Hyper-V manager, collection of images will fail.

When retrieving SCVMM templates created by users using SCVMM, manage them as follows:

- The template name is the image name.
- The virtual hard disk of the primary channel (0) of the IDE device is managed as a system volume.
- When creating an L-Server from an image retrieved from a template with data disks other than the system volume, the data disks other than the system volume are deleted.
- When creating an L-Server from an image with no system volume, an L-Server with no system volume will be created.
- On L-Servers created by retrieving an image from a template where DVD drives are connected to somewhere other than the secondary IDE channel (0), these DVD drives will be deleted.
- When L-Servers are created from an image retrieved from a template not connected to a DVD drive, the DVD drive will be added to the secondary IDE channel (0).

Access Control Configuration File of Image Storage Location

By specifying unavailable library shared path names in the access control configuration file of the image storage destination in advance, cloning image storage destinations can be controlled based on user groups.

Storage Location of the Configuration File

[Windows]

Installation_folder\Manager\etc\customize_data

Configuration File Name

The configuration files can be divided into definitions that are available for each user group and definitions that are common to the system. When there are both types of files, the limitations of both are valid.

- For User Groups
library_share_user group name_deny.conf
- Common on System
library_share_deny.conf

Configuration File Format

In the configuration file, library shared path names are entered on each line.

```
Library_shared_path_name
```



Example

An example configuration file is indicated below:

```
\\rcxvmm1.rcxvmmshv.local\MSSCVMMLibrary  
\\rcxvmm2.rcxvmmshv.local\lib
```

Deleting Cloning Images

Use the following procedure to delete cloning images:

1. Select the target image pool on the orchestration tree.
The [Resource List] tab is displayed.
2. Right-click the cloning image to be deleted, and select [Delete] from the popup menu.
3. Click <OK>.

The cloning image is deleted.

When SCVMM template creation requirements are not met, or configuration changes are performed outside Resource Orchestrator, collection of images may fail.

When deleting cloning images, the corresponding templates in the SCVMM library are deleted.

When deleting these templates, related files (such as .vhd and .vfd) will remain in the SCVMM library as only template definition files are deleted.

When these related files are unnecessary, delete them individually from SCVMM.



Information

By creating the following setting file beforehand, when deleting cloning images, the related files that have no dependencies with other templates can be deleted at the same time.

Storage Location of the Configuration File

```
[Windows]  
Installation_folder\Manager\etc\vm
```

Configuration File Name

```
delete_image_all_files_scvmm
```

Configuration File Format

It is not necessary to describe content in the configuration file.

As in the case of deletion of related files from the SCVMM management console, only the related files are deleted from the SCVMM library. The folder where the related files are stored will remain.

[OS] Tab Configuration

Enter the parameters to set for the OS when creating the L-Server. This setting is valid only if an image is specified in the [General] tab.

The setting process is performed the first time the L-Server is started. If an image name is not specified, it is not necessary to enter all these items.

Table E.17 List of Settings

Item	Windows		Description
	Necessity of Entry	Values When Omitted	
Host name/ Computer name	Possible	<i>L-Server Name</i>	Enter the host name or computer name. Enter a string of between 1 and 15 alphanumeric characters or hyphens ("-"), beginning with an alphanumeric character. The string cannot be composed solely of numbers. If underscores ("_") or periods (".") are used in an L-Server name, they will be replaced with hyphens ("-"), because these characters cannot be used for host names or computer names. If the basic information is not specified, the L-Server name is converted and set as indicated above.
Domain name	Possible	WORKGROUP (*1)	Enter the workgroup name. Settings for participation in a domain cannot be made. Enter between 1 and 255 alphanumeric characters, hyphens ("-"), or periods ("."), using an alphabetic character for the first character.
DNS search path	Not Required	-	Enter a list of domain names to use for DNS searching, using between 1 and 32,767 characters. You can specify the same characters as the domain name. To specify multiple domain names, use a blank space as the separator character.
Full name	Possible	WORKNAME (*1)	Enter the Windows full name using between 1 and 50 characters. By default, the value defined in the OS property definition file is entered. When the OS type is Windows Server 2008, Windows Server 2008 R2, Windows 7, or Windows Vista, a full name cannot be set for guest OS's.
Organization name	Possible	WORKORGANIZATION (*1)	Enter the organization name displayed in the Windows system properties using between 1 and 50 characters. When the OS type is Windows Server 2008, Windows Server 2008 R2, Windows 7, or Windows Vista, an organization name cannot be set for guest OS's.
Product key	Essential	- (*1)	Omission not possible. Ensure that you specify a valid product key.
License mode	Not Required	-	Even if the license mode is specified, it is not configured in the guest OS.
Maximum number of connections	Not Required	-	Even if the maximum number of connections is specified, it is not configured in the guest OS.
Administrator password	Possible	- (*1)	Enter the same password as that specified for the local administrator account during L-Server creation. When specifying a new password, the local administrator account will be overwritten. Enter the password using between 1 and 128 alphanumeric characters or symbols.
Hardware clock configuration	Not Required	-	Specify one of the following: - UTC - Local (LOCAL)

Item	Windows		Description
	Necessity of Entry	Values When Omitted	
Time zone	Possible	<i>The same time zone as the OS of the manager</i>	Specify the time zone of the OS.

*1: When the OS property definition file is specified, its values are configured.

Information

OS Property Definition File

By setting the default values in an OS property definition file in advance, the default values of the information on the [OS] tab, etc. are generated when creating an L-Server. Use the UTF-8 character code for OS property definition files.

Location of the Definition File

[Windows]
Installation_folder\Manager\etc\customize_data

[Linux]
 /etc/opt/FJSVrcvmr/customize_data

Definition File Name

The definition file name can be used by dividing into definitions that are available for each user group and definitions that are common to the system. If the key of the definition file common to the system is the same as a definition file for a user group, priority is given to the values indicated in the definition file for the user group.

- For User Groups

os_setting_user_group_name.rcxprop

- Common on System

os_setting.rcxprop

Definition File Format

In the definition file, an item to define is entered on each line. Each line is entered in the following format.

<i>Key = Value</i>

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

Definition File Items

Specify the following items in a definition file.

Table E.18 List of Items

Item	Key	Value	Remarks
Domain name	workgroup_name	(*1)	For Windows
	domain_name	(*1)	For Linux
DNS search path	dns_search_path	(*1)	-
Full name	full_name	(*1)	-
Organization name	org_name	(*1)	-
Product key	product_key	(*1)	-
License mode	license_mode	Specify one of the following:	-

Item	Key	Value	Remarks
		- "seat"(number of connected clients) - "server"(in the unit of servers: number of servers used at the same time)	
Maximum number of connections	license_users	(*1)	-
Administrator password	admin_password	(*1)	-
Hardware clock configuration	hwclock	Specify one of the following: - UTC - LOCAL	-
DNS server (When configuring for each NIC on Windows) (*2)	nic N _dns_address X	Specify the IP address using numeric values (between 0 and 255) and periods. (*2) When not configuring a DNS server, specify a hyphen ("-").	For N , specify the NIC number. For X , specify primary ("1") or secondary ("2").
DNS server (When configuring all NICs using the same settings on Windows)	dns_address X	Specify the IP address using numeric values (between 0 and 255) and periods.	For X , specify primary ("1") or secondary ("2"). Priority is given to nic N _dns_address X specifications.

*1: For more information on this value, refer to "Table E.17 List of Settings".

*2: When omitting keys or values, use the value "dns_address X " to configure the same values for the NIC definitions of all NICs on Windows.



Example

An example definition file is indicated below.

```
# Windows
workgroup_name = WORKGROUP
full_name = WORKNAME
org_name = WORKORGANIZATION
product_key = AAAA-BBBB-CCCC-DDDD
license_mode = server
license_users = 5
admin_password = xxxxxxxx
nic1_dns_address1 = 192.168.0.60
nic1_dns_address2 = 192.168.0.61
nic2_dns_address1 =
nic2_dns_address2 =

# Linux
domain_name = localdomain
dns_search_path = test.domain.com
hwclock = LOCAL
dns_address1 = 192.168.0.60
```

```
dns_address2 = 192.168.0.61
dns_address3 =
```

Information

VM Guest Administrator Account Settings Necessary When Creating an L-Server with an Image Specified

When creating an L-Server with an image specified, it is necessary to enter the "administrator password" as a parameter.

The entered "administrator password" is the one set for the Administrator of the built-in administrator account, but on some localized editions of Windows the account name may differ. In addition, when the client OS is Windows 7 or Windows Vista, on standard installations the built-in administrator account is disabled, and the user account created during installation becomes the administrator account.

When an L-Server is created with a cloning image that was collected from a localized edition of Windows or a client OS specified, it is necessary to either configure an administrator account for the administrator and set a password, or change the name of the administrator account with the "Administrator password" so that it fits the description given in the definition file below.

Note that when using a definition file, it is not possible to define different administrator ID settings for different versions of images.

Location of the Definition File

[Windows]
Installation_folder\Manager\etc\customize_data

Definition File Name

The definition file name can be used by dividing into definitions that are available for each user group and definitions that are common to the system. Search the definition file of each user group, from the start, for the administrator name corresponding to the image. When there is no corresponding definition, search in the system's common definition file.

Modification of the definition file is soon reflected, and it becomes valid for the creation of L-Servers from that point.

- For User Groups

image_admin_hyperv_user_group_name.rcxprop

- Common on System

image_admin_hyperv.rcxprop

Definition File Format

In the definition file, describe the image name and account name for which the administrator password has been configured on a single line.

```
Image_name = "Administrator_account_name"
```

The *Administrator_account_name* is displayed enclosed in double quotes (").

Blank spaces and tabs other than those in the *Administrator_account_name* are ignored.

It is possible to use an asterisk ("*") as a wildcard in image names. By specifying an asterisk ("*") it is possible to create substitute strings for strings of indefinite length.

When creating an L-Server from an image, the corresponding image name is searched for from the start of the definition file, and the specified "Administrator password" will be set for the specified administrator account name.

It is necessary to create the definition files using the following line break code and character codes:

- Line Break Code

CR+LF(0x0d0a)

- Character Code

Shift-JIS in a Japanese environment, UTF-8 in other environments



Example

An example definition file is indicated below.

- Image names and administrator account names are set in pairs.

```
FR_WIN2003_001 = "Administrator"  
EN_WIN7_001 = "root"  
EN_WIN7_002 = "admin"
```

- For image names that start with "FR_WIN", use "Administrator" as the name of the administrator account.

```
FR_WIN* = "Administrator"
```

- Use "Administrator" as the name of the administrator account for all images. When an image name is specified using only a wildcard, the definition after that line will be ignored.

```
* = "Administrator"
```

E.3.5 Advisory Notes for Hyper-V Usage

This section explains advisory notes for Hyper-V usage.

Operating Systems for which Parameters can be Set and the Prerequisites for Performing the Settings

Depending on the server virtualization software used, some restrictions may apply to the operating systems that parameters can be set for and the prerequisites for performing the settings.

For details, refer to the manual of server virtualization software.

VMware(R) ESX Management

VMware(R) ESX can be managed by SCVMM, but only VM host for Hyper-V can be managed when using SCVMM in Resource Orchestrator.

Management of Citrix(R) XenServer(TM)

Citrix(R) XenServer(TM) can be managed by Microsoft(R) System Center 2012 Virtual Machine Manager, but only VM hosts for Hyper-V can be managed when using SCVMM.

Attaching and Detaching Disks

- Data disks are connected to the L-Server as SCSI disks. They cannot be connected as IDE disks.
- 14 data disks are connected to the first SCSI card, and 15 data disks are connected to each of the second to fourth SCSI cards.
- When changing the configuration, a maximum of up to four disks can be specified at one time. To perform addition of five or more disks, please perform an additional configuration change.
- Adding data disks while the L-Server is operating is possible except when additional SCSI cards become necessary.

Snapshot

The Resource Orchestrator snapshot uses the checkpoint function of SCVMM. To collect snapshots, sufficient free space is necessary to create a difference disk on the storage destination of VM guest.

When connecting the VM management software using the path through disk, snapshot creation will fail.

Operation with snapshots collected is not recommended due to the following reasons:

- When snapshots are collected, operation uses disk difference, and performance may deteriorate.
- If a snapshot is created from a VM guest that has been moved between servers (migration), and the snapshot is restored to a different VM host, the status on SCVMM becomes "Stored" and the VM may not be able to be started. In this situation, it is necessary to return the VM guest to the VM host from which the snapshot was collected and then start it.
- For combining of difference disks, it is necessary to delete not only all snapshots collected using Resource Orchestrator, but also all checkpoints created using VM management software. Combining of the disk is automatically performed by SCVMM, but depending on the status of the VM guest, the operation may take a long time, because it is only performed while the target VM guest is stopped.

Information

The snapshot function provided by server virtualization software records the disk from the last update. Consequently, when a disk failure occurs, the snapshot function becomes unavailable at the same time.

Snapshot can be used as a corrective measure for problems such as the following:

Example

- For recovery when a problems occurs with the applied patch
- For recovery when a problem occurs when changing operating system parameters

L-Server Parameter Details [General] Tab

When a guest OS that Hyper-V supports is specified for the OS type, a converged network adapter will be added to VM.

When another OS has been selected, an emulated network adapter will be added.

When using a converged network adapter, it is necessary to install a virtual guest service on the guest OS.

For details on virtual guest service installation, refer to the Help of SCVMM.

L-Server Parameter Details [Server] Tab

If an unsupported OS type is specified, there is a chance that installation may fail or the OS of the VM guest may not operate correctly. Additionally, if an incorrect OS type is specified, there is a chance that image collection or L-Server creation for a specified image may fail, and a guest OS may start but hang while awaiting entry. This occurs because Microsoft's Sysprep cannot be processed correctly during personalization processing.

The OS types displayed in the list are the guest OS's which can be specified on the SCVMM management console.

Resource Orchestrator displays all guest OS's in the list in order not to limit user selection, however this does not mean that all guest OS's are supported by SCVMM.

Hyper-V does not support some server type settings such as number of CPUs depending on the OS type. When an incorrect OS type and server type are selected, operation is not guaranteed.

Additionally, even when a service pack is not listed in the OS type list, it may be necessary to install the service pack.

When a guest OS that Hyper-V supports is specified for the OS type, a converged network adapter will be added to VM.

When a different OS has been selected, an emulated network adapter will be added.

Creation of L-Servers by specifying cloning images on which Windows 2000 Server and Windows 2000 Advanced Server are installed is not supported.

For details on the guest OS's supported by SCVMM, refer to the Help of SCVMM.

For details on the guest OS's supported by Hyper-V, refer to the following Microsoft web site.

Microsoft download web site

URL: <http://www.microsoft.com/windowsserver2008/en/us/hyperv-supported-guest-os.aspx> (As of February 2012)

L-Server Parameter Details [Disk] Tab

When creating an L-Server or changing the configuration, a maximum of four disks can be specified at one time.

To perform addition of five or more disks, please perform an additional configuration change.

L-Server Parameter Details [Network] Tab

IP addresses can be automatically configured, on the following guest OS's on which the integrated services are installed.

- Microsoft(R) Windows Server(R) 2008 R2
- Microsoft(R) Windows Server(R) 2008
- Microsoft(R) Windows Server(R) 2003 R2
- Microsoft(R) Windows Server(R) 2003
- Microsoft(R) Windows(R) 7
- Microsoft(R) Windows Vista(R)
- Microsoft(R) Windows(R) XP

DVD Disk Operations

DVD disk operations cannot be performed for L-Servers. When using a DVD, use VM management software functions.

Automatic Network Configuration with Intel PROSet for Blade Servers

- The VLAN functions of Intel PROSet are not supported by Resource Orchestrator. Do not use the VLAN functions of Intel PROSet.
- User Accounts used when logging in to the SCVMM server must belong to the Administrator's group of each managed server.
- With SCVMM, NIC information of a managed server recognized once is not updated even if the NIC information is changed.

When changing the Intel PROSet settings of a managed server, use the following procedure to make SCVMM re-realize the NIC information:

1. Disable the virtual NIC of Intel PROSet using the Device Manager of the managed server (Hyper-V).
2. In the SCVMM management console of the admin server (SCVMM), right-click the target host, then select "Refresh".
3. Change the settings of Intel PROSet, and enable the virtual NIC using the Device Manager of the managed server (Hyper-V).
4. In the SCVMM management console of the admin server (SCVMM), right-click the target host, then select "Refresh".

If the information recognized by SCVMM is not reflected even after performing the above operations, follow the steps below to release and reconfigure Intel PROSet.

1. Cancel teaming settings for Intel PROSet on the managed server (Hyper-V).
 2. In the SCVMM management console of the admin server (SCVMM), right-click the target host, then select "Refresh".
 3. Reconfigure teaming settings for Intel PROSet on the managed server (Hyper-V).
 4. In the SCVMM management console of the admin server (SCVMM), right-click the target host, then select "Refresh".
- When setting "ALB" for the teaming mode of Intel PROSet, disable the RLB (Receive Load Balancing) function. This configuration is not supported by Hyper-V.

- Do not disable NIC devices teamed using Intel PROSet.

Note

If this procedure is not performed correctly, automatic network configuration will fail.

E.3.6 Overcommit

This section explains the VMware overcommit function for L-Servers.

Overcommit

Resource Orchestrator supports the Hyper-V overcommit function for the CPU and dynamic memory.

The Hyper-V overcommit function for the CPU allows virtual allocation of more resources than that of the actual CPU installed on a server to a guest OS.

Hyper-V dynamic memory allows virtual allocation of more memory than that of the actual memory installed on a server to a guest OS.

Note

When using dynamic memory and memory weight, Windows Server 2008 R2 Service Pack 1(SP1) or later must be applied to the VM host, and SCVMM must be upgraded to System Center Virtual Machine Manager 2008 R2 Service Pack 1(SP1) or later.

If there is no VM host or SCVMM as above, creation and modification of L-Servers with dynamic memory and memory weight enabled will fail.

The guest OS's able to utilize dynamic memory are limited to particular Windows software versions. Refer to the Microsoft web site below.

URL: [http://technet.microsoft.com/en-us/library/ff817651\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ff817651(WS.10).aspx) (As of February 2012)

Resource Orchestrator provides the following functions to utilize the Hyper-V overcommit function for the CPU and dynamic memory when creating L-Servers.

- Creating an L-Server with CPU overcommit and dynamic memory configured
 - CPU Performance
The maximum number of CPU resources to be allocated to a virtual machine (Limitation)
 - CPU Weight
The priority of CPU allocated to a virtual machine
 - Memory Size
 - Maximum Memory
The maximum amount of memory resources to be allocated to a virtual machine (Limitation)
 - Virtual Machine Memory
The maximum amount of memory resources to be allocated to a virtual machine by the VM host (Memory Size)

For virtual L-Servers created using Resource Orchestrator, set the memory size as follows, depending on the dynamic memory setting:

When Dynamic Memory is Disabled

Set only the virtual machine memory.

When Dynamic Memory is Enabled

Set only the maximum memory.

- Dynamic Memory
 - Initial Memory Size
Initial memory size to be allocated at startup
 - Memory Buffer
Available memory to be reserved for a virtual machine as a buffer
 - Memory Weight
The priority of memory resources to be allocated to a virtual machine
- Setting an overcommit attribute for a resource pool
Overcommit attributes can be set for resource pools. An L-Server with overcommit attributes can be created using overcommit attributes settings or a resource pool.
- Deployment of L-Servers with more resources than those of the server
Creation of an L-Server with more resources than that of the actual CPU or memory installed on a server is possible.
Whether the resulting L-Server can be started depends on the resources available on the VM host.
- Calculation of available space on VM pools, which uses values set for CPU reservation performance
- Conversion of the free CPU capacity and free memory capacity of VM pools with overcommit attributes
For a VM pool with overcommit attributes, the conversion of free CPU capacity and free memory capacity can be displayed based on the CPU reservation values and memory allocation capacity of an L-Server created beforehand.
- L-Server Conversion of a VM Pool with Overcommit Attributes
For the free CPU capacity and free memory capacity of a VM pool with overcommit attributes, L-Server conversion can be displayed based on the CPU reservation values and memory reservation capacity specified in the L-Server template.
For details on L-Servers, refer to "[1.2.3 L-Servers](#)" and "[L-Server Creation](#)" of "[E.3.4 Setup](#)" or "Chapter 10 Creating L-Servers" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".
For details on resource pools, refer to "[1.2.2 Resource Pool](#)" or "Chapter 12 Resource Pool Operations" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".
For details on the available capacity view or the L-Server conversion view, refer to "12.4 Viewing a Resource Pool" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Prerequisites

Admin Server

When using the function for coordination with Resource Orchestrator, Hyper-V, or the overcommit function for the CPU and memory, the only supported admin server OS is Windows.

Installation Procedure

Use the following procedure to install overcommit.

1. Create a VM Pool for Overcommit

For details on how to create a VM pool, refer to "12.2 Resource Pool Operations" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".



Note

For the VM pool for overcommit, register only VM hosts that support overcommit (Hyper-V or VMware). If VM hosts other than VMware and Hyper-V have been registered, move those VM hosts to another VM pool.

The following operations cannot be performed on the VM hosts other than VMware and Hyper-V registered in the VM pool for overcommit:

- Creation of an L-Server
- Linking L-Servers with configured virtual machines

2. Create an Overcommit Configuration File for a VM Pool

For the VM pool created in 1., specify a reservation value or a maximum value after calculating the available space for the VM pool used for overcommit settings or performing overcommit.

Create an overcommit configuration file for a VM pool.

For details on definition files, refer to "[E.1.1 Definition Files](#)".

 **Point**

When creating L-Servers that use overcommit and L-Servers that do not, both a VM pool that uses overcommit and a VM pool that does not must be created.

3. Create the Definition Files

Create a definition file (VM specific information definition file) when configuring different settings for individual user groups without configuring overcommit settings on the L-Server template.

For details on creating VM specific information definition files, refer to "[E.1.1 Definition Files](#)".

4. Export an L-Server Template

For details on how to export L-Server templates, refer to "8.2.1 Exporting a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

5. Edit an L-Server Template

Configure the overcommit settings for an L-Server template.

For details on the XML definition of L-Server templates, refer to "2.2.2 Virtual L-Server Templates" in the "Reference Guide (Resource Management) CE".

- When overcommit settings are configured in both the L-Server template and the VM specific information definition file
Priority is given to the settings in the L-Server template.
- When configuring individual values for overcommit using the VM specific information definition file

Configure only the following element on the L-Server template.

- Enabling/Disabling Overcommit

Do not specify the following elements:

- CPU Reservation Performance
- CPU Weight
- Initial Memory Size
- Memory Buffer
- Memory Weight

 **Information**

If a template is imported without editing the L-Server template name, the content of the existing L-Server template is overwritten. If an L-Server template is imported after the name is edited from when it was exported, the L-Server template is added.

When editing an L-Server template, check the combination of enabling/disabling dynamic memory, initial memory size, and memory buffer.

- When Dynamic Memory is Enabled

Initial memory size and memory buffer will be adopted when creating an L-Server

- When Dynamic Memory is Disabled

Initial memory size and memory buffer will be ignored when creating an L-Server

6. Import an L-Server template

For details on how to import an L-Server template, refer to "8.2.3 Importing a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

7. Create an L-Server

Create an L-Server using the L-Server template created in 5.

For details, refer to "10.1 Creation Using an L-Server Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

When not using an L-Server template, create an L-Server using a command. Edit the L-Server XML referring to "Chapter 10 Creating L-Servers" of the "User's Guide for Infrastructure Administrators (Resource Management) CE", and then execute the `rcxadm lserver create` command.

For details, refer to "1.3.1 rcxadm lserver" and "2.2.2 Virtual L-Server Templates" of the "Reference Guide (Resource Management) CE".

8. Confirm the Overcommit Function Settings for an L-Server

To confirm overcommit settings configured for an L-Server, execute the `rcxadm lserver show` command.

Confirm that the command output result includes the line starting with "OverCommit: true".

Additionally, confirm the combination of the dynamic memory setting, initial memory size, and memory buffer.

For details on the `rcxadm lserver` command, refer to "1.3.1 rcxadm lserver" of the "Reference Guide (Resource Management) CE".

Note

When starting of an L-Server fails, the procedures vary depending on the L-Server settings. Perform the following procedures:

- When "Boot Location" of the L-Server is set to "Relocate at startup"

Start the L-Server again. When there is a VM host with an available resource, the L-Server will start on that VM host after several attempts at startup.

- When "Boot Location" of the L-Server is set to "Fixed"

As no VM host is automatically selected, start the L-Server after changing its boot location, or moving or stopping other L-Servers on the same VM host.

For details on changing the boot location, refer to "10.3 Creation of Virtual L-Servers Using Parameters" of the "User's Guide for Infrastructure Administrators (Resource Management) CE". For details on moving the boot location, refer to "11.7 Migration of VM Hosts between Servers" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Changing L-Server Specifications

This section explains how to modify L-Server specifications.

To change L-Server specifications, execute the `rcxadm lserver modify` command.

For details, refer to "1.3.1 rcxadm lserver" of the "Reference Guide (Resource Management) CE".

Note

Changing of L-Server specifications will fail if the resources (the number of CPUs, CPU frequency, and memory capacity) of a physical server where a VM host operates are less than the CPU reservation performance and memory size.

When CPU performance and memory capacity are smaller than the CPU reservation performance and memory reservation capacity, modification of L-Server specifications fails.

When modifying specifications of an L-Server to which resources have been allocated, the information in the VM specific information definition file is not reflected because priority is given to the values already configured to the L-Server. In that case, enter the new values in the XML file and then execute the appropriate commands to reflect the changes.

E.4 RHEL5-Xen

This section explains how to configure RHEL5-Xen as server virtualization software.

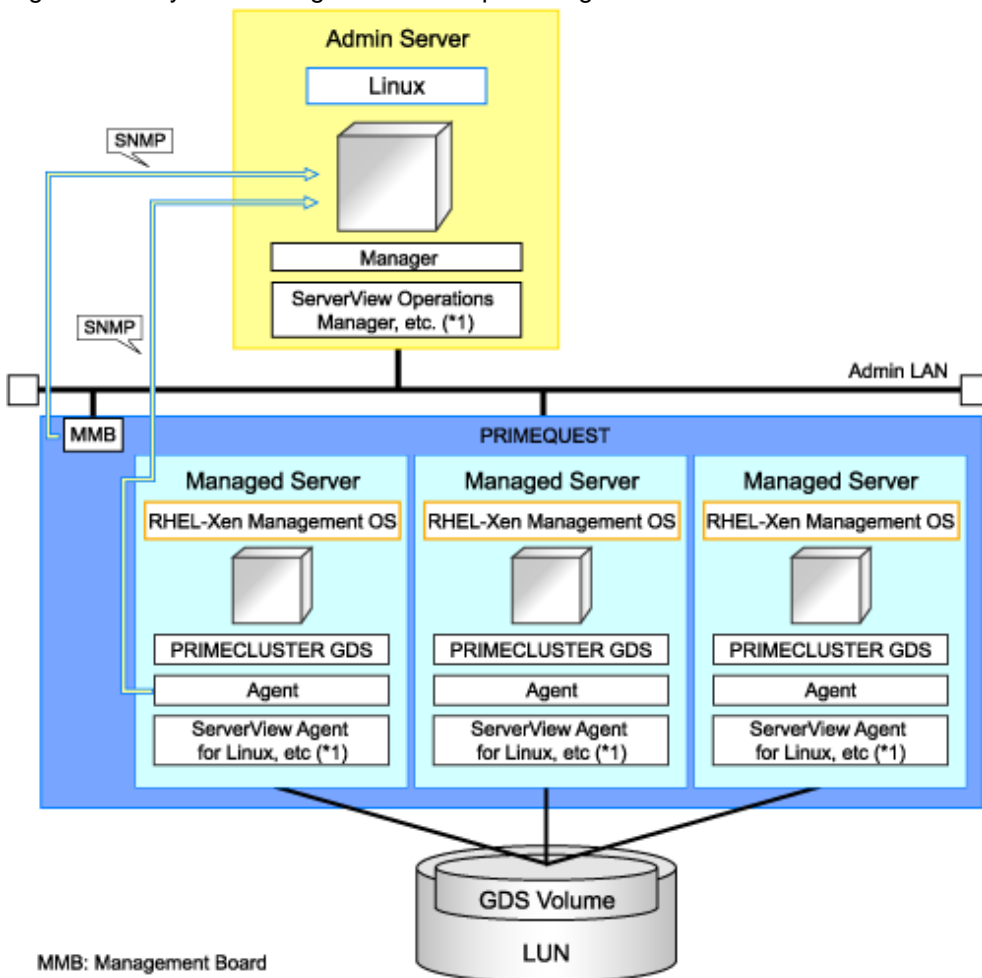
E.4.1 System Configuration

This section explains the system configuration necessary when using RHEL5-Xen as server virtualization software.

Example of System Configuration

An example system configuration using RHEL5-Xen is given below.

Figure E.18 System Configuration Example Using RHEL5-Xen

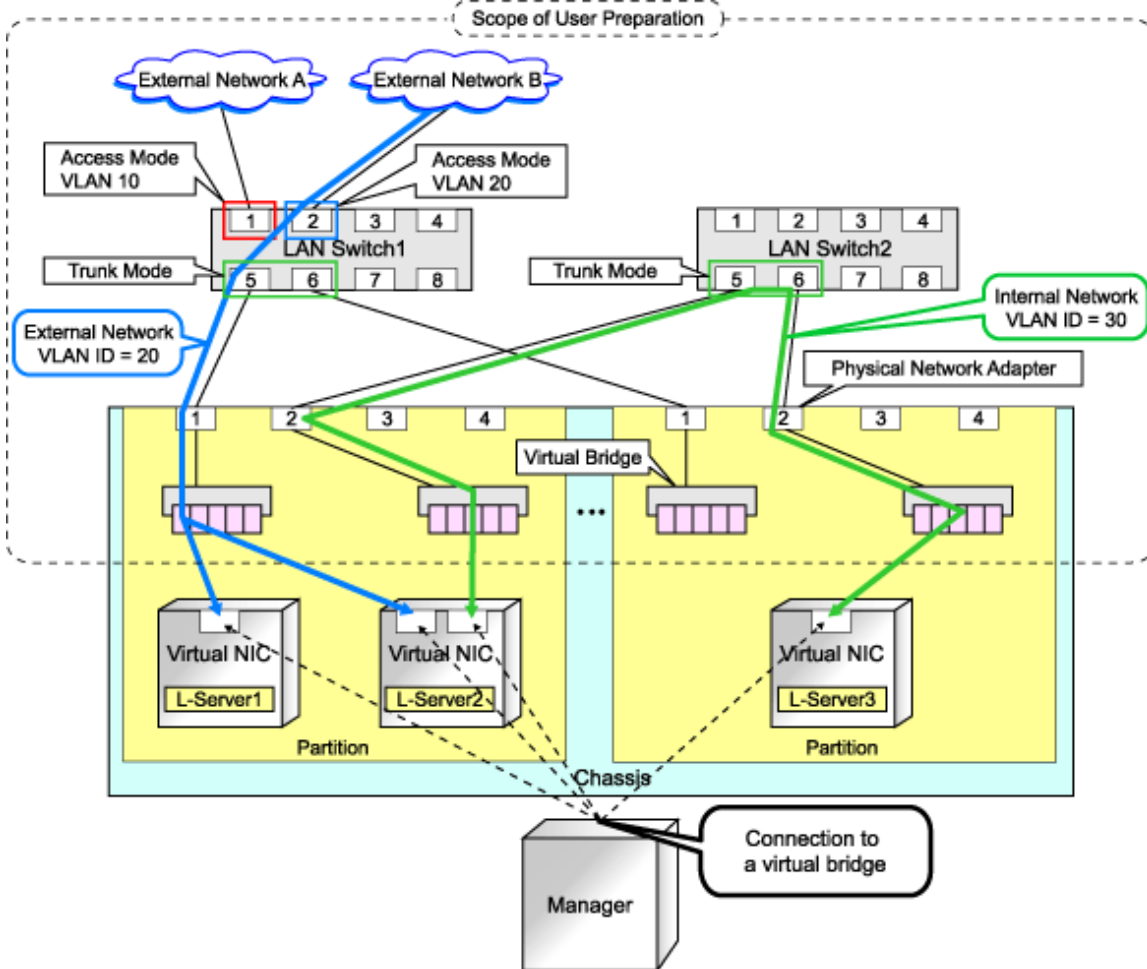


*1: For details on required software, refer to "1.4.2.2 Required Software".

Network Configuration Example

An example network configuration using RHEL5-Xen is given below:

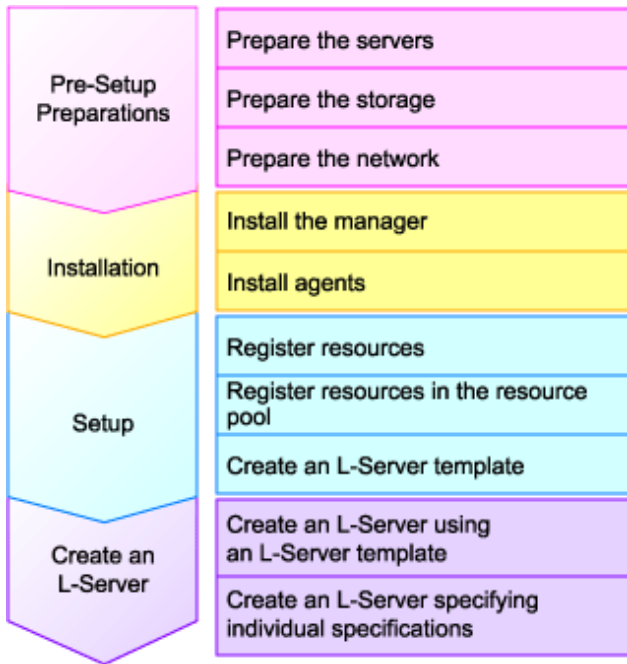
Figure E.19 Virtual Bridge Settings Using Network Resources



L-Server Creation Procedure

Use the following procedure to create L-Servers:

Figure E.20 Resource Orchestrator Setup Procedure



For details on pre-setup preparations, refer to "E.4.2 Preparations".

For details on how to install Resource Orchestrator, refer to "E.4.3 Installation".

For details on how to set up Resource Orchestrator, refer to "E.4.4 Setup".

For details on how to create an L-Server, refer to "L-Server Creation" of "E.4.4 Setup".

E.4.2 Preparations

Pre-setup preparations are required to create and manage RHEL5-Xen virtual machines as L-Servers of Resource Orchestrator.

For details on pre-setup preparations for RHEL5-Xen environment, refer to the RHEL5-Xen manual.

- Red Hat Enterprise Linux 5 Virtualization Guide

URL: http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5/html/Virtualization/index.html (As of February 2012)

Preparations for Servers

In addition to the operations in "4.1.1.1 Preparations for Server Environments", the following operations are necessary.

- Installation and configuration of the admin OS
Install and configure the admin OS of domain 0.
- Installation and configuration of PRIMECLUSTER GDS on the admin OS
For details, refer to the PRIMECLUSTER GDS manual.

Storage Preparations

Check the following:

- Volumes (LUNs) to assign to the admin OS have already been created
The LUN must be larger than the size to allocate to the L-Server.
- Zoning and affinity have been set

- The LUN has already been set as the shared class of PRIMECLUSTER GDS

Start the name of the shared class and single disk with "rcx".

Do not overlap the class name within the VM hosts registered in Resource Orchestrator.

For details, refer to the ETERNUS and PRIMECLUSTER GDS manuals.

Network Preparations

Check the following:

- The configuration for the admin and public LANs has been designed
- The network environment for the admin LAN is configured
- The VLAN ID to allocate to the network resource has been configured
- The virtual bridge has been configured beforehand
- The MAC address range for the virtual network interface (VNIF) has been decided

When Using IBP

When using virtual L-Servers, connect the IBP uplink sets used for the public LAN and admin LAN to the VM host regardless of VIOM, after creating each IBP uplink set.

It is not necessary to use the same name for the uplink set and the name of the network resource.

Creating a Virtual Bridge

The virtual bridge is required on the admin OS, in order to connect the L-Server to the network.

For details on how to configure virtual bridges, refer to the manual for RHEL5-Xen and "[Manual Network Configuration](#)" in "E.4.4 Setup".

E.4.3 Installation

Installing the Manager

Install the Resource Orchestrator manager. For details on how to install a manager, refer to "2.1 Manager Installation" of the "Installation Guide CE".

Installing the Agent

Install agents of Resource Orchestrator on managed servers (admin OS).

For details on how to install agents, refer to "2.2.3 Installation [Linux/VMware/Xen/KVM/Oracle VM]" of the "Installation Guide CE".

E.4.4 Setup

The setup procedure when using Xen as server virtualization software is as follows:

1. Create Storage Connection Definition Files

Give descriptions, separating the admin IP addresses of VM hosts belonging to the scope of PRIMECLUSTER GDS shared classes using commas, and giving the scopes of shared clusters on individual lines.

When changing the shared class configuration, modify the definition files.

Location of the Definition File

```
[Linux]
/etc/opt/FJSVrcvmm/customize_data
```

Definition File Name

storage_vmhost.rcxprop

Definition File Format

`vmhost_ipaddr,vmhost_ipaddr,...`

2. Register Resources

a. Register storage management software

Register PRIMECLUSTER GDS on VM hosts as storage management software.

Register 1 of the VM hosts belonging to the scope of PRIMECLUSTER GDS shared classes. It is not necessary to register all VM hosts which belong to the scope.

When registering PRIMECLUSTER GDS as storage management software, single disks which were created in advance during pre-setup preparations, are automatically registered in Resource Orchestrator as virtual storage resources.

Execute the rcxadm storagemgr command to register storage management software.

For details on the rcxadm storagemgr command, refer to "1.7.1 rcxadm storagemgr" of the "Reference Guide (Resource Management) CE".

b. Register managed servers (domain 0)

1. Register Managed Servers

Refer to "2.5.1 Registering Rack Mount or Tower Servers" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

2. Register LAN Switches

Refer to "2.5.2 Registering LAN Switches" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

3. Register Resources in Resource Pools

a. Register VM host resources (domain 0)

1. In the ROR console orchestration tree, right-click the target VM pool, and select [Register Resources] from the popup menu.

The [Register Resources] dialog is displayed.

2. Select the VM host to register.
3. Click <OK>.

b. Register virtual storage resources

1. In the ROR console orchestration tree, right-click the target storage pool, and select [Register Resources] from the popup menu.

The [Register Resources] dialog is displayed.

2. Select the virtual storage resource to register.
3. Click <OK>.

c. Register network resources

If the NIC and network resources are connected when an L-Server is created, the settings matching the network resource definition will be registered automatically for the VM host that the L-Server will operate on.

For details, refer to "[Manual Network Configuration](#)".

1. In the ROR console orchestration tree, right-click the target network pool, and select [Create Resource] from the popup menu.

The [Create a network resource] dialog is displayed.

2. Enter the items necessary for network resources.

For details, refer to "7.3 Network Resources" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- d. Register address set resources (MAC addresses)

Create and register an address set resource (MAC address) in the address pool.

For details, refer to "7.6 Address Set Resources" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

4. Create an L-Server Template

Create an L-Server using an L-Server template.

The L-Server is the L-Server to collect cloning images from.

- a. Export an L-Server template

Refer to "8.2.1 Exporting a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- b. Edit an L-Server template

For details on the XML definition of L-Server templates, refer to "2.2.2 Virtual L-Server Templates" of the "Reference Guide (Resource Management) CE".

In this case, perform the following configuration:

- Specify RHEL-Xen for the VM type.
- Specify "None" for the redundancy.
- Specify "Fixed" for the positioning.

- c. Import an L-Server template

Refer to "8.2.3 Importing a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Manual Network Configuration

For the virtual bridge created in advance, only provide the function for connection with the virtual bridge. Manually perform virtual bridge settings in advance.

Use a different VLAN ID for each virtual bridge to connect with the virtual bridge.

Additionally, the following settings must be performed in advance.

1. Create a Virtual Bridge

Create a virtual bridge with the same name (including upper and lower case characters) for all VM hosts comprising the cluster. This enables migration of VM guests between VM hosts.

When a virtual bridge has already been manually configured and server virtualization software other than RHEL5-Xen is being used with the same manager, set a different name from the one used by the virtual switch, virtual network, and virtual bridge on the other virtualization software.

2. Configure Virtual Bridge Communication Settings

Right-click the LAN switch in the server resource tree, and select [Modify]-[Network Settings] from the popup menu.

Configure LAN switches to enable communication using the tagged VLAN between virtual bridges using the same name.

The ROR console can be used for VLAN configuration of LAN switch blade external ports.

For details, refer to "2.4.4 Configuring VLANs on LAN Switch Blades" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

3. Define the Supported Virtual Bridge and VLAN ID

Supported virtual bridges and VLAN IDs are defined in the virtual bridge definition file of Resource Orchestrator.

For details on definition file format, refer to "[File Format for Virtual Bridge Definitions](#)".

4. Create Network Resources

- From the GUI:

- a. In the [Create a network resource] dialog containing the VLAN ID that was specified in 2. and 3., check the "Use configured virtual switches." checkbox and create a network resource.

- From the Command-line:

- a. Create the XML file that defines network resources.

Define the VLAN ID specified at 2. and 3. in the XML file.

In this case, specify auto="false" in the Network tag.

- b. To create the network resource, execute the rcxadm network create command specifying the XML file created in a.

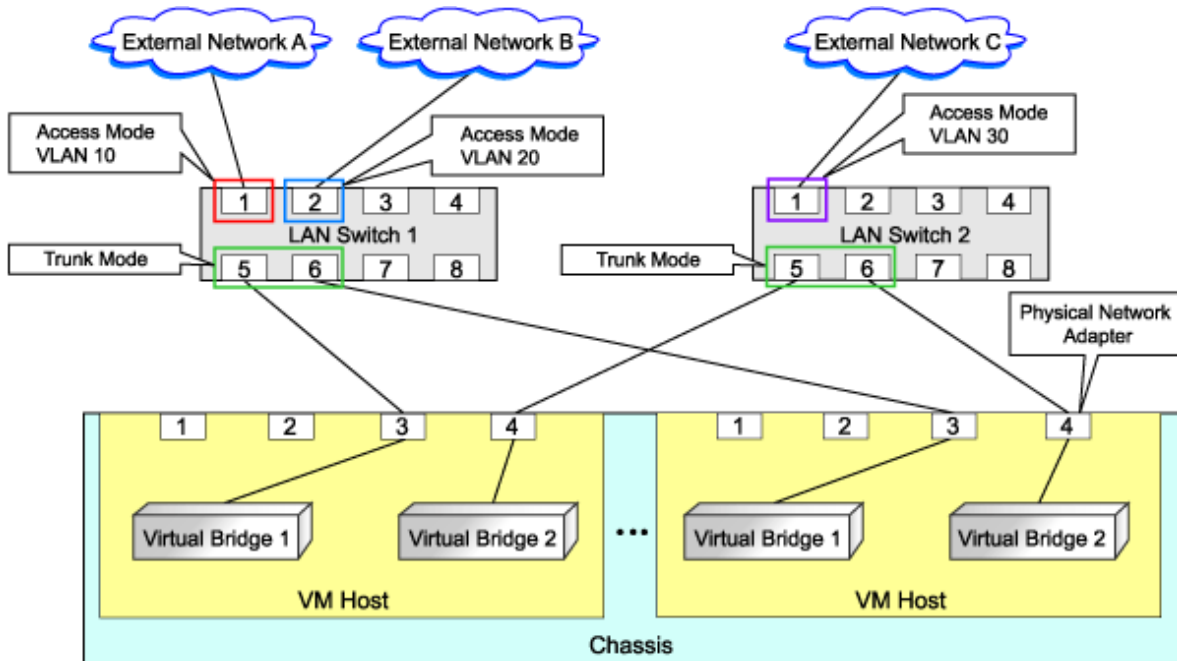
The network resources are created.

For details on the rcxadm network command, refer to "1.3.5 rcxadm network" of the "Reference Guide (Resource Management) CE".

For details on Network elements, refer to "2.5 Network Resources" of the "Reference Guide (Resource Management) CE".

An example of virtual NIC configuration and connection with virtual bridge using network resources is given below:

Figure E.21 Virtual NIC Configuration and Connection with Virtual Networks Using Bridge Resources



File Format for Virtual Bridge Definitions

Location of the Definition File

[Linux]

/etc/opt/FJSVrcvmm/customize_data

Definition File Name

vnetwork_rhelxen.rcxprop

Definition File Format

Describe the virtual bridge definition file in one line as below:

```
"Virtual_bridge_name"=VLAN ID
```

For the *VLAN ID*, a value from 1 to 4094 can be specified.

Example

```
"xenbr0"=10
```

Blank spaces before and after equal signs ("=") are ignored.

Describe the virtual bridge correctly, as the entry is case-sensitive.
Save files using the UTF-8 character code.

When there are multiple lines with the same virtual bridge name, all specified lines are valid.

When the same VLAN ID is included in a line with a different virtual bridge name, the first occurrence in the file is valid and the lines after it are ignored.

An error occurs during L-Server creation if the definition of the VLAN ID of the network resource connected to the NIC cannot be found.

L-Server Creation

Use the following procedure to create L-Servers:

- Create an L-Server using an L-Server template.

1. Create an L-Server using an L-Server Template.

Execute the `rcxadm lserver create` command, and create an L-Server.

For details on the `rcxadm lserver create` command, refer to "1.3.1 `rcxadm lserver`" of the "Reference Guide (Resource Management) CE".

In this case, perform the following configuration:

- For the name of an L-Server template, specify the name of the L-Server template that has been created in advance.
- For VM host, specify the VM host (admin OS) to allocate to the L-Server.

2. Install an OS

For manual OS installation, use the virtual machine manager.

For manual OS installation, refer to the "Red Hat Enterprise Linux 5 Virtualization Guide".

Red Hat Enterprise Linux 5 Virtualization Guide

```
URL: http://docs.redhat.com/docs/en-US/Red\_Hat\_Enterprise\_Linux/5/html/Virtualization/index.html (As of February 2012)
```

3. Collect Cloning Images

Collect cloning images after creating an L-Server. Execute `rcxadm image create` to collect cloning images.

When executing `rcxadm image create`, the cloning images are stored in the storage pool.

For details on the `rcxadm image create` command, refer to "1.4.1 `rcxadm image`" of the "Reference Guide (Resource Management) CE".

Point

When the destination folder for image storage is omitted during the cloning image collection, virtual storage in the same storage pool as the virtual storage used by the L-Server that is the target for collecting cloning images is automatically selected.

- Create an L-Server using Systemwalker Software Configuration Manager.
For details, refer to the "Systemwalker Software Configuration Manager Operation Guide".
In this case, specify the cloning images collected during L-Server creation for images.

Note

When sharing disks among L-Servers, create the Mh L-Server, after completing creation of the Mh-1 L-Server.

When copying the data during the L-Server creation, perform the operation after powering off the L-Server that is the source of the data to be copied. When creating an L-Server while copying data, do not perform power operations on the source of the data to be copied.

L-Server Operations

When using RHEL5-Xen, L-Server operations cannot be performed using the ROR console.

Use the rcxadm lserver command, for L-Server operations.

For details, refer to "1.3.1 rcxadm lserver" of the "Reference Guide (Resource Management) CE".

Changing L-Server Specifications

To change L-Server specifications, execute rcxadm lserver modify.

For details on the specifications that can be changed, refer to "2.3.2 Definition Information for Virtual L-Servers (XML)" in the "Reference Guide (Resource Management) CE".

The value after changing the specifications can be checked in the [Resource List] tab in the orchestration tree.

From the command-line, execute rcxadm lserver list and rcxadm lserver show.

For details, refer to "1.3.1 rcxadm lserver" of the "Reference Guide (Resource Management) CE".

Check the CAP value of a guest domain that is operating, using the virsh schedinfo command.

Check the CAP value of a guest domain that has been stopped, using the domain configuration files.

For details, refer to the "Red Hat Enterprise Linux 5 Virtualization Guide".

Red Hat Enterprise Linux 5 Virtualization Guide

URL: http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5/html/Virtualization/index.html (As of February 2012)

The CAP value is calculated as follows:

$$\text{CAP value} = ((\text{Specified_CPU_clock_speed GHz} * 1000) * \text{CPU_number} * 100) / \text{physical_CPU_clock_speed MHz}$$

E.4.5 Advisory Notes for RHEL5-Xen Usage

This section explains advisory notes for RHEL5-Xen.

Required Software

When using RHEL5-Xen, Systemwalker Software Configuration Manager is required.

Admin Server

When using RHEL5-Xen as managed servers, the only supported OS of the admin server is Linux.

Managed Server

When using RHEL5-Xen as managed servers, the only server type available for use as managed servers is RHEL5-Xen.

L-Server OS

When using RHEL5-Xen as managed servers, the only OS supported for the L-Server is Linux.

Snapshot

When using RHEL5-Xen, snapshots cannot be used.

Collect L-Server snapshots using PRIMECLUSTER GDS.

The part of the virtual storage name before "-" is the PRIMECLUSTER GDS class name, and the part after "-" is the single disk name.

The disk resource name corresponds to the volume name.

For details on snapshots, refer to the PRIMECLUSTER GDS manual.

VM Type View

In the ROR console, the VM type of VM host and VM guest for RHEL5-Xen is displayed as "Xen".

Shared Disk View

On the ROR console, when multiple L-Servers have shared disk resources, only the information of one L-Server to which the resources are allocated is displayed.

Check the disk shared information, using the `rcxadm disk show` command.

Max. Number of Possible L-Servers View

The available space on resources and the space displayed for the number of L-Servers that can be created are calculated as follows:

Available Amount of CPUs and Number of L-Servers that can be Created

$\text{Total resource space} * 80\% - (\text{Total of resources used for L-Server})$
--

Attaching Resources

When attaching VM hosts, virtual storage or networks, perform the same procedure as in ["E.4.4 Setup"](#).

Hardware Maintenance

When server failure is detected on Systemwalker Software Configuration Manager, open the ROR console, and identify the failed server.

For details on server hardware replacement, refer to "Chapter 7 Hardware Maintenance" in the "Operation Guide CE".

E.5 Oracle VM

This section explains how to configure Oracle VM as server virtualization software.

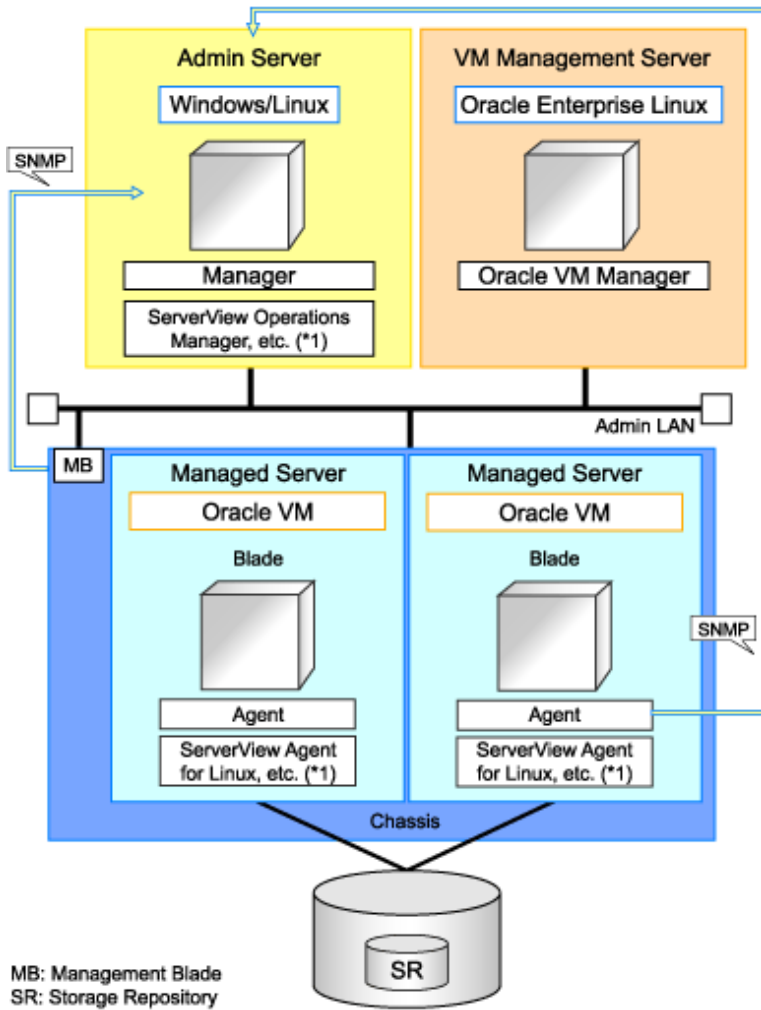
E.5.1 System Configuration

This section explains the system configuration necessary when using Oracle VM as server virtualization software.

Example of System Configuration

An example system configuration using Oracle VM is given below.

Figure E.22 System Configuration Example Using Oracle VM



*1: For details on required software, refer to "[1.4.2.2 Required Software](#)".

Simplifying Network Settings

Network settings can be easily configured by Resource Orchestrator when creating L-Servers.

Depending on the conditions, such as hardware (blade servers or rack mount servers) and the presence or absence of network redundancy for L-Servers, the setting ranges of networks differ.

For details, refer to "[1.2.7 Simplifying Networks](#)".

E.5.2 Preparations

Pre-setup preparations are required to create and manage Oracle VM virtual machines as L-Servers of Resource Orchestrator.

For details on preparations for Oracle VM environments, refer to "Oracle VM Manager User's Guide" and "Oracle VM Server User's Guide".

Refer to the relevant version of the document, referring to the following web site:

URL: <http://www.oracle.com/technetwork/server-storage/vm/documentation/index.html> (As of February 2012)

Preparations for Servers

In addition to the operations in "[4.1.1.1 Preparations for Server Environments](#)", the following operations are necessary.

- Configure VIOM

When using I/O virtualization, configuration of VIOM is necessary.

- Install and configure Oracle VM Server for x86

When installing an OS on a physical server, refer to the server virtualization software manual.

When installing a VM host in an L-Server, refer to "[Appendix F Installation of VM Hosts on Physical L-Servers](#)".

- Install and configure Oracle VM Manager

Necessary for management of VM hosts and L-Servers.

- Configure server pools

Configure the server pool that contains the VM host used as the L-Server location.

For details on the configurations of server pools, refer to the "Oracle VM Server User's Guide".

- Design and configure high availability

When performing redundancy of L-Servers, enable high availability for the server pool.

- Configure SSH connection

Perform configuration to enable SSH connections from the admin server of Resource Orchestrator to the VM host using the admin LAN.

Storage Preparations

Check the following:

- Volumes (LUN) to allocate to domain 0 have been already created

The LUN must be larger than the size to allocate to the L-Server.

- Zoning and affinity have been set

Network Preparations

Check the following:

- The configuration for the admin and public LANs has been designed
- The network environment for the admin LAN is configured
- The VLAN ID to allocate to the network resource has been configured
- The virtual bridge has been configured beforehand

When Using IBP

When using virtual L-Servers, connect the IBP uplink sets used for the public LAN and admin LAN to the VM host regardless of VIOM, after creating each IBP uplink set. It is not necessary to use the same name for the uplink set and the name of the network resource.

Creating a Virtual Bridge

A virtual bridge is required on domain 0, in order to connect the L-Server to the network.

The virtual bridge is configured by default. When changing the settings, refer to the "Oracle VM Server User's Guide" and "[Manual Network Configuration](#)" in "[E.5.4 Setup](#)".

E.5.3 Installation

This section explains installation methods.

Installing the Manager

Install the Resource Orchestrator manager. For details on how to install a manager, refer to "2.1 Manager Installation" of the "Installation Guide CE".

Installing the Agent

Install Resource Orchestrator agents on managed servers (Oracle VM Server).

For details on how to install agents, refer to "2.2.3 Installation [Linux/VMware/Xen/KVM/Oracle VM]" of the "Installation Guide CE".

E.5.4 Setup

The setup procedure when using Oracle VM as server virtualization software is as follows:

1. Register Resources

- a. Register VM management software (Oracle VM Manager)

When registering VM management software, the storage repositories that were created in advance during pre-setup preparations, are automatically registered in Resource Orchestrator as virtual storage resources.

Use the following procedure to register VM management software:

1. In the ROR console, select [Settings]-[Register]-[Management Software (OVM Manager)].

The [Management Software (OVM Manager)] dialog is displayed.

2. Define the following settings:

Management software name

Enter the name of the target VM management software.

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

Location

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

- For Resource Orchestrator admin servers

Select "Admin Server".

- For servers other than Resource Orchestrator admin servers

Select "Other Server".

In the IP address entry field, enter the IP address of the server on which VM management software is operating.

"Admin Server" is selected by default.

IP address

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

Enter the IP address using periods ".".

User ID

Enter the user ID to use to control VM management software.

The string must be composed of alphanumeric characters and symbols (ASCII characters 0x20 to 0x7e), and can be up to 128 characters long.

Specify a user ID with administrative privileges.

Password

Enter the password for VM management software.

The string must be composed of alphanumeric characters and symbols (ASCII characters 0x20 to 0x7e), and can be up to 128 characters long.

3. Click <OK>.

VM management software is registered.

b. Register managed servers (domain 0)

1. Register Chassis (for Blade Servers)

Refer to "2.4.1 Registering Chassis" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

2. Register managed servers

Refer to "2.4.2 Registering Blade Servers" or "2.5.1 Registering Rack Mount or Tower Servers" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

3. Register LAN Switch Blades (for Blade Servers) or LAN Switches (for Rack Mount Servers)

Refer to "2.4.3 Registering LAN Switch Blades" and "2.5.2 Registering LAN Switches" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

c. Network resources

To register a network resource, specify a network pool when creating the network resource.

By creating network resources in advance, if the NIC and network resources are connected when an L-Server is created, the following settings matching the network resource definition will be registered automatically.

For details on automatic configuration of network resources, refer to "[Manual Network Configuration](#)".

2. Register Resources in Resource Pools

a. Register VM host resources (domain 0)

1. In the ROR console orchestration tree, right-click the target VM pool, and select [Register Resources] from the popup menu.

The [Register Resources] dialog is displayed.

2. Select the VM host to register.
3. Click <OK>.

b. Register virtual storage resources

1. In the ROR console orchestration tree, right-click the target storage pool, and select [Register Resources] from the popup menu.

The [Register Resources] dialog is displayed.

2. Select the virtual storage resource to register.
3. Click <OK>.

c. Register network resources

If the NIC and network resources are connected when an L-Server is created, the settings matching the network resource definition will be registered automatically for the VM host that the L-Server will operate on.

For details, refer to "[Manual Network Configuration](#)".

1. In the ROR console orchestration tree, right-click the target network pool, and select [Create Resource] from the popup menu.

The [Create a network resource] dialog is displayed.

2. Enter the items necessary for network resources.

For details, refer to "7.3 Network Resources" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

3. Create an L-Server Template

a. Export an L-Server template

Refer to "8.2.1 Exporting a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

b. Edit an L-Server template

Refer to "8.2.2 Editing a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

c. Import an L-Server template

Refer to "8.2.3 Importing a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Manual Network Configuration

For the virtual bridge created in advance, only provide the function for connection with the virtual bridge. Manually perform virtual bridge settings in advance.

Use a different VLAN ID for each virtual bridge to connect with the virtual bridge.

Additionally, the following settings must be performed in advance.

1. Create a Virtual Bridge

When configuring a cluster, create a virtual bridge with the same name (including upper and lower case characters) for all VM hosts comprising the cluster. This enables migration of VM guests between VM hosts.

When a virtual bridge has already been manually configured and server virtualization software other than Oracle VM is being used with the same manager, set a different name from the one used by the virtual switch, virtual network, and virtual bridge on the other virtualization software.

2. Configure Virtual Bridge Communication Settings

Right-click the LAN switch in the server resource tree, and select [Modify]-[Network Settings] from the popup menu.

Configure LAN switches to enable communication using the tagged VLAN between virtual bridges using the same name.

The ROR console can be used for VLAN configuration of LAN switch blade external ports.

For details, refer to "2.4.4 Configuring VLANs on LAN Switch Blades" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

3. Define the Supported Virtual Bridge and VLAN ID

Supported virtual bridges and VLAN IDs are defined in the virtual bridge definition file of Resource Orchestrator.

For details on definition file format, refer to "[File Format for Virtual Bridge Definitions](#)".

4. Create Network Resources

- From the GUI:

- a. In the [Create a network resource] dialog containing the VLAN ID that was specified in 2. and 3., check the "Use configured virtual switches." checkbox and create a network resource.

- From the Command-line:

- a. Create the XML file that defines network resources.

Define the VLAN ID specified at 2. and 3. in the XML file.

In this case, specify auto="false" in the Network tag.

- b. To create the network resource, execute the rxcadm network create command specifying the XML file created in a.

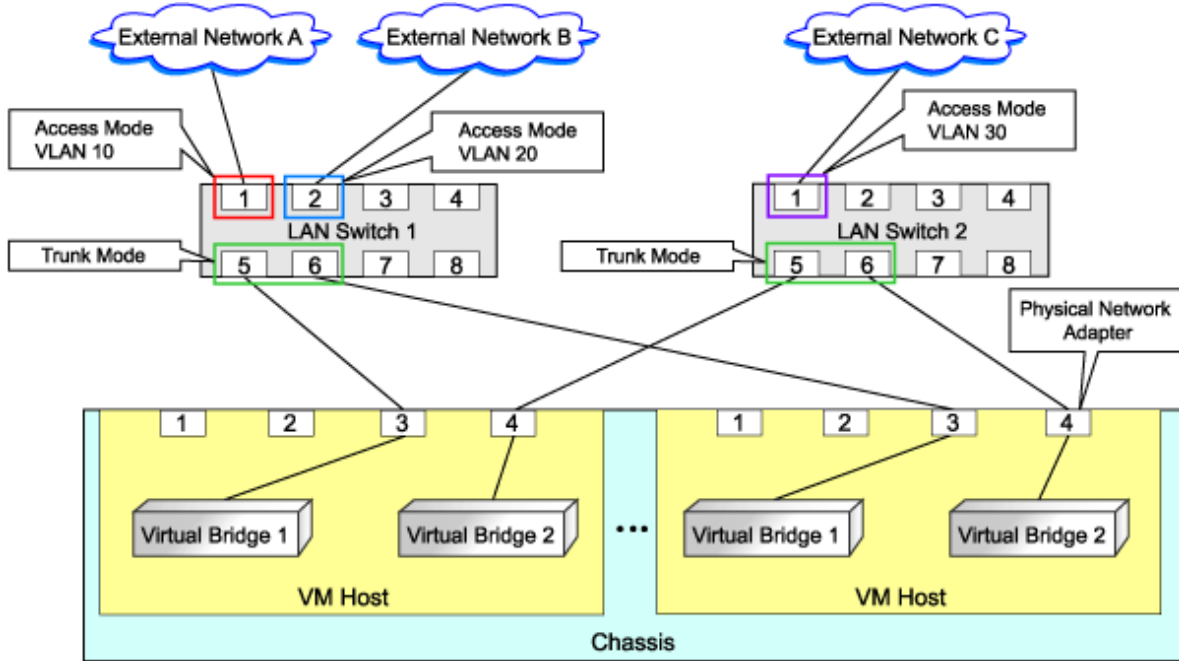
The network resources are created.

For details on the rxcadm network command, refer to "1.3.5 rxcadm network" of the "Reference Guide (Resource Management) CE".

For details on Network elements, refer to "2.5 Network Resources" of the "Reference Guide (Resource Management) CE".

An example of virtual NIC configuration and connection with virtual bridge using network resources is given below:

Figure E.23 Virtual NIC Configuration and Connection with Virtual Networks Using Bridge Resources



File Format for Virtual Bridge Definitions

Location of the Definition File

[Windows]

Installation_folder\Manager\etc\customize_data

[Linux]

/etc/opt/FJSVrcvmr/customize_data

Definition File Name

vnetwork_oraclevm.rcxprop

Definition File Format

Describe the virtual bridge definition file in one line as below:

```
"Virtual_bridge_name"=VLAN ID
```

For the *VLAN ID*, a value from 1 to 4094 can be specified.



Example

```
"xenbr0"=10
```

Blank spaces before and after equal signs ("=") are ignored.

Describe the virtual bridge correctly, as the entry is case-sensitive.

Save files using the UTF-8 character code.

When the same VLAN ID is included in a line with a different virtual bridge name, the first occurrence in the file is valid and the lines after it are ignored.



Example

```
"xenbr4 "=11  
"xenbr5 "=11 (*1)
```

*1: This line is ignored.

An error occurs during L-Server creation if the definition of the VLAN ID of the network resource connected to the NIC cannot be found.

L-Server Creation

Use the following procedure to create L-Servers:

1. Creating an L-Server Using an L-Server Template

Create an L-Server, referring to "10.1 Creation Using an L-Server Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

In this case, specify the cloning image that you want to use as an image.

2. Create an L-Server Specifying Individual Specifications

Refer to "10.3 Creation of Virtual L-Servers Using Parameters" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

For details on how to configure the [OS] tab, refer to "10.3.5 [OS] Tab" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Manual OS Installation

To manually install an operating system, use VM management software.

When installing an OS manually, refer to the virtual machine creation section of the "Oracle VM Server User's Guide".

Refer to the relevant version of the document, referring to the following web site:

URL: http://www.oracle.com/technetwork/indexes/documentation/index.html (As of February 2012)
--

Collect Cloning Images

This section explains how to collect cloning images.

Use the following procedure to collect cloning images:

After installing an OS, stop the target L-Server.

1. On the ROR console, right-click the target L-Server in the orchestration tree, and select [Cloning]-[Collect] from the popup menu.
2. Click <OK>.

A given cloning image (identified by its name attribute) can be managed by image version.

If a cloning image is created using VM management software, it can be used as is.

DVD Drive Configuration

The same DVD drive as the one in the image to be deployed is configured for the L-Server to be created. If there is no DVD drive in the image, no DVD drive will be created on the L-Server.

[OS] Tab Configuration

For Oracle VM, the values specified in the [OS] tab are not set.

Instead, it is necessary to specify a console password in the OS property definition file.

OS Property Definition File

When creating a VM guest using Oracle VM Manager, specify a console password for connection from Oracle VM Manager to VM guest console. The console password should be specified in the OS definition file in advance. Use the UTF-8 character code for OS property definition files.

Location of the Definition File

[Windows]
Installation_folder\Manager\etc\customize_data

[Linux]
/etc/opt/FJSVrcvmr/customize_data

Definition File Name

The definition file name can be used by dividing into definitions that are available for each user group and definitions that are common to the system. If the key of the definition file common to the system is the same as a definition file for a user group, priority is given to the values indicated in the definition file for the user group.

- For User Groups

os_setting_user_group_name.rcxprop

- Common on System

os_setting.rcxprop

Definition File Format

In the definition file, an item to define is entered on each line. Each line is entered in the following format.

<i>Key = Value</i>

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

Definition File Items

Specify the following items in a definition file. Other key specifications will be ignored.

Table E.19 List of Items

Item	Key	Value	Remarks
Console password	console_password	The string must be composed of alphanumeric characters and underscores ("_"), and can be up to 24 characters long.	Specify the password required to open the console.

Example Definition File

An example definition file is indicated below.

group A console_password = xxxxxxxx
--

E.5.5 Advisory Notes for Oracle VM Usage

This section explains advisory notes for when using Oracle VM.

Operating Systems for which Parameters can be Set and the Prerequisites for Performing the Settings

Depending on the server virtualization software used, some restrictions may apply to the operating systems that parameters can be set for and the prerequisites for performing the settings.

For details, refer to the manual of server virtualization software.

VM Host Functions

VM Hosts that have no ability to provide virtual machine and virtual server functions cannot be registered in VM pools.

If those VM Hosts were registered, when a VM host specification used to create L-Servers is omitted, one of the VM host may be selected as the operational VM host.

In this case, even if the VM host is registered in the VM pool, when it is selected to create an L-Server, creation will fail.

Snapshot

When using Oracle VM, snapshots cannot be used.

L-Server Creation

When creating L-Servers, set the destination VM host to the Preferred Server of a created VM guest.

L-Server Disk

Disks cannot be detached while they are powered ON.

L-Server Network (NIC)

One or more networks must be specified.

L-Server CPU Performance

For L-Server CPU performance, do not specify a value of less than 1GHz.

Moving an L-Server between Servers (Migration)

When performing migration with an L-Server powered on, after powering it off, the L-Server may be moved back to the previous server.

In this case, power off the L-Server before migration, and power it on again after moving it.

When the L-Server is an HVM (Hardware Virtualized Machine)

Installation of paravirtual drivers is required to connect data disks as SCSI disks.

If paravirtual drivers are not installed, the OS may fail to recognize the data disks.

SSL Access Method for VM Management Software

When starting VM management software from the management console, SSL-enabled URL or SSL-disabled URL can be specified as the destination. In Oracle VM Manager configurations, if SSL is enabled for access to Oracle VM Manager, the following definition file is required: Use the UTF-8 character code for definition files.

Location of the Definition File

[Windows]
Installation_folder\Manager\etc\customize_data

[Linux]
/etc/opt/FJSVrcvnr/customize_data

Definition File Name

ovmm.rcxprop

Definition File Format

The definition file is entered in the following format.

Key = Value

Definition File Items

Specify the following items in a definition file. Other key specifications will be ignored.

Table E.20 List of Items

Item	Key	Value	Remarks
Enable/Disable SSL	SSL	"vmm_ip[:port][,vmm_ip[:port]...]" vmm_ip: IP address of SSL-enabled VM management software port: Port number of SSL-enabled VM management software	If the port number is omitted, the default port number (4443) is set.

Example Definition File

An example definition file is indicated below.

```
# Oracle VM Manager  
ssl = 192.168.2.2:4443,192.168.2.3:4443
```

Name and Number of Detected Virtual Storage Resources

Even if multiple storage repositories are connected to a VM host, only a single virtual storage resource is detected for each VM host.

The displayed name of virtual storage resources is the string of the VM host root repository, excluding the path name (/var/ovs/mount).



Example

.....
D1567B83A58D41FEB28FB8897801C7ED
.....

Virtual Storage Resource Free Space

When multiple storage repositories have been connected to the VM host, a storage repository that has the largest available space is displayed as the available space of the virtual storage resource.

Therefore, the space may not decrease in proportion to the virtual disk space created during L-Server creation.

Total Virtual Storage Resource Size

Not displayed.

Virtual Storage Resource Used Space

Not displayed.

Cloning Images Collected from L-Servers

Cloning images are stored in Oracle VM Manager, using the following template name:

```
"cloning_image_name[_index]@version_number"
```

However, in the template editor window of Oracle VM Manager, "@" cannot be included in the template name. When using Oracle VM Manager to edit the template information collected using Resource Orchestrator, modify the template name so that it does not contain "@".

VM Host Status

Even when a VM host is running and the xend daemon is not running, "normal" is displayed as the status of the VM host. If L-Server operation fails when the VM host status is "normal", execute the following command from the VM host to check the status of the xend daemon. If the xend daemon is not running, start it.

- Status Check for the xend Daemon

```
>service xend status <RETURN>
```

- Starting the xend Daemon

```
>service xend start <RETURN>
```

When Managing Multiple Server Pools Using Oracle VM Manager

When creating an L-Server or attaching a disk, specify an image, VM host, or virtual storage that satisfies the following conditions:

- Belongs to the same server pool as the image and VM host
- The disk created is a virtual storage recognized by the VM host

Check the server pool to which the image and the VM host belong using Oracle VM Manager

- Image

"Server Pool Name" in the "Virtual Machine Templates" list

- VM Host

"Server Pool Name" in the "Servers" list

The name of a virtual storage recognized by the VM host is the string of the root storage repository, excluding the path name (/var/ovs/mount). To check the root storage repository, log in to the VM host, then execute the following command:

```
# ls -l /OVS <RETURN>
```



Example

```
lrwxrwxrwx 1 root root 47 Apr 11 23:15 /OVS -> /var/ovs/mount/D1567B83A58D41FEB28FB8897801C7ED
```

E.6 KVM

This section explains how to configure RHEL-KVM as server virtualization software.

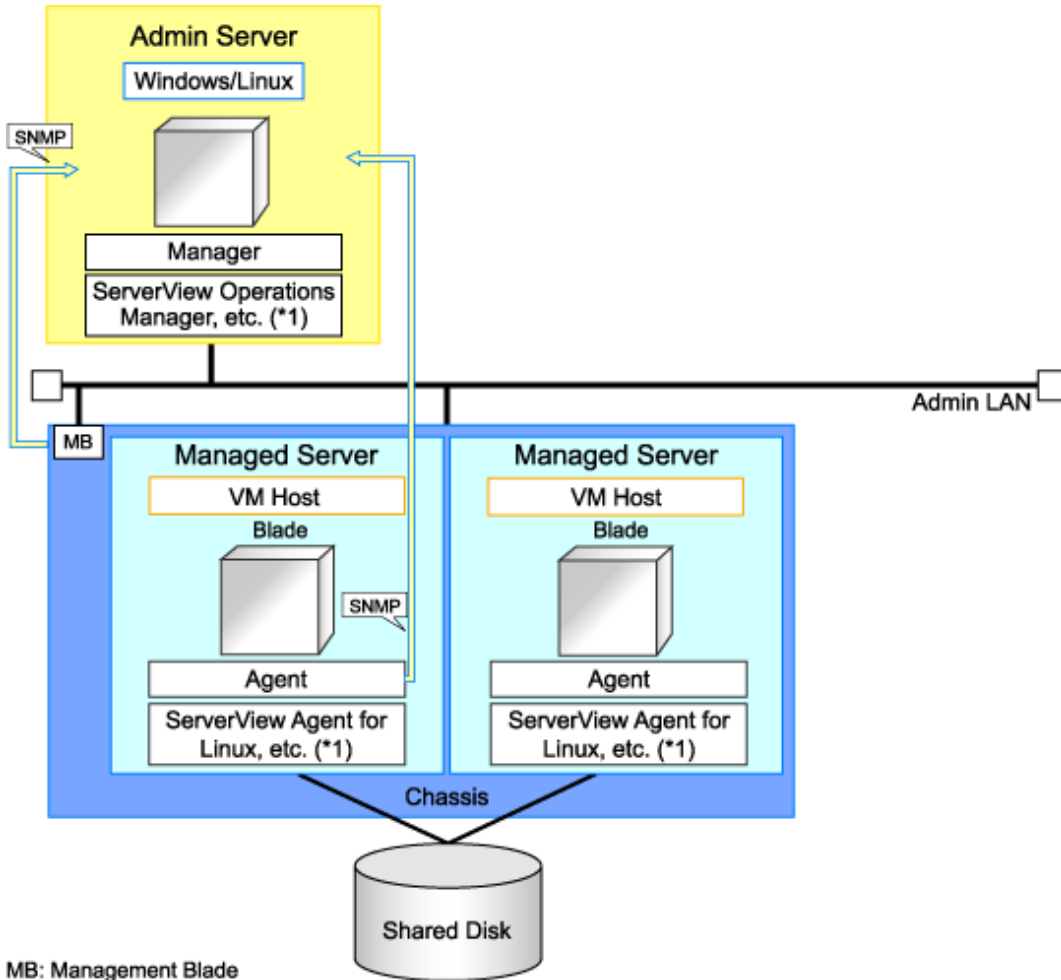
E.6.1 System Configuration

This section explains the system configuration necessary when using RHEL-KVM as server virtualization software.

Example of System Configuration

An example system configuration using RHEL-KVM is given below.

Figure E.24 System Configuration Example Using RHEL-KVM



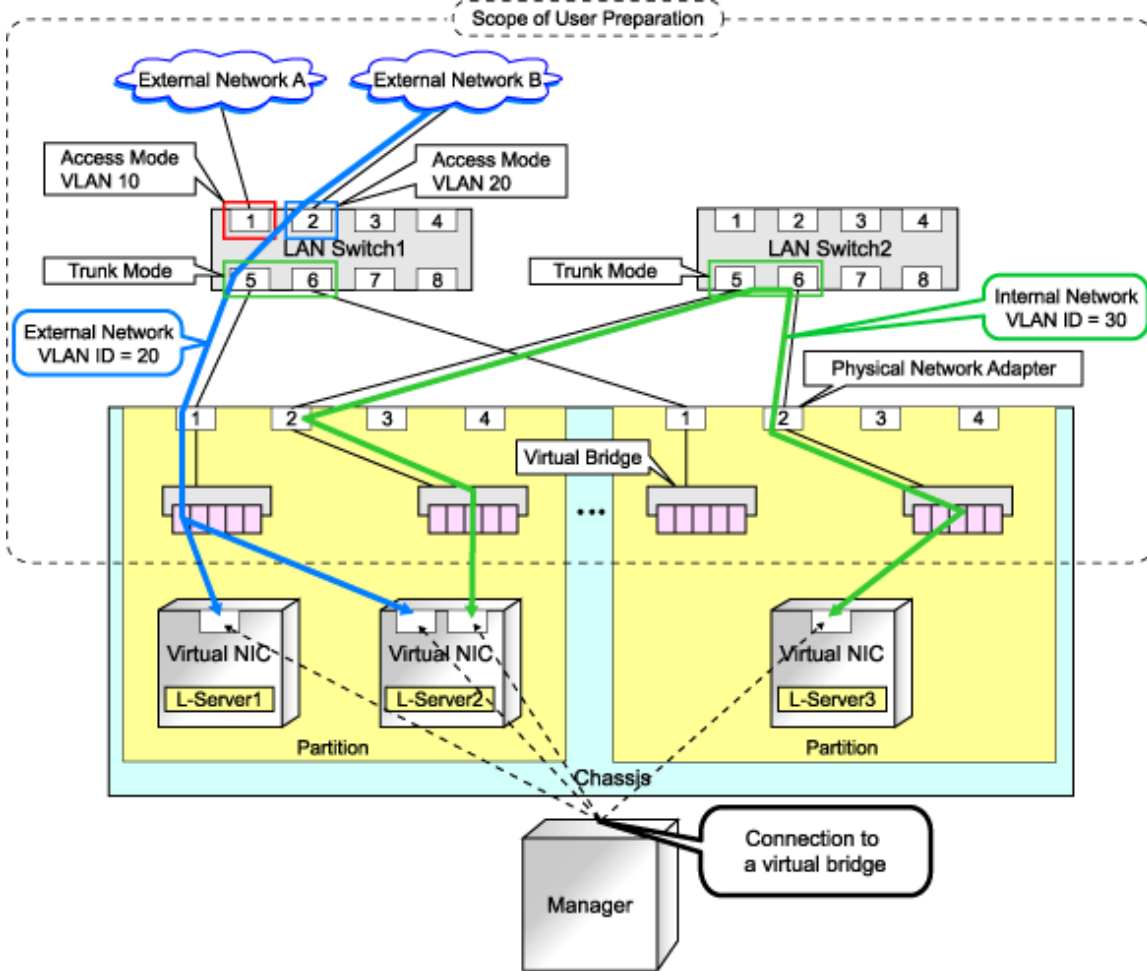
MB: Management Blade

*1: For details on required software, refer to "[1.4.2.2 Required Software](#)".

Network Configuration Example

An example network configuration using RHEL-KVM is given below:

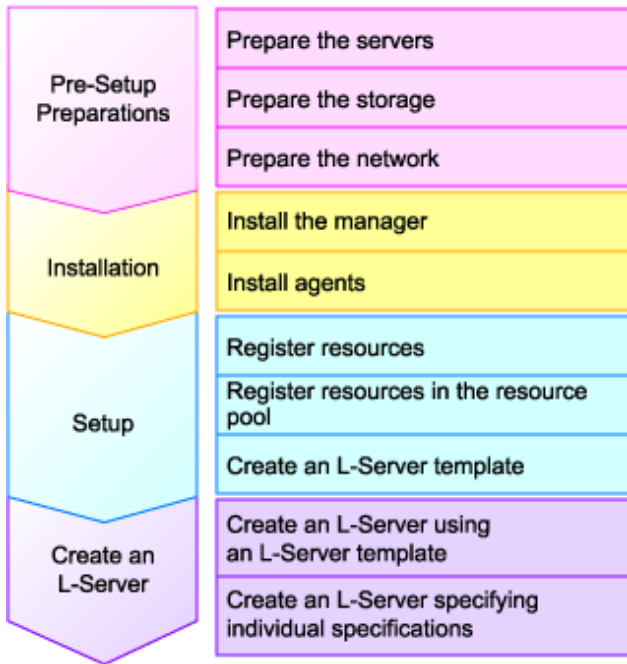
Figure E.25 Virtual Bridge Settings Using Network Resources



L-Server Creation Procedure

The procedure for creating L-Servers is shown below.

Figure E.26 Resource Orchestrator Setup Procedure



For details on pre-setup preparations, refer to "E.6.2 Preparations".

For details on how to install Resource Orchestrator, refer to "E.6.3 Installation".

For details on how to set up Resource Orchestrator, refer to "E.6.4 Setup".

For details on how to create an L-Server, refer to "L-Server Creation" of "E.6.4 Setup".

E.6.2 Preparations

Pre-setup preparations are required to create and manage RHEL-KVM virtual machines as L-Servers of Resource Orchestrator.

For details on pre-setup preparations for RHEL-KVM environment, refer to the RHEL-KVM manual.

- Red Hat Enterprise Linux 6 Virtualization Administration Guide

URL: http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Virtualization_Administration_Guide/index.html
(As of February 2012)

- Red Hat Enterprise Linux 6 Virtualization Getting Started Guide

URL: http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Virtualization_Getting_Started_Guide/index.html (As of February 2012)

- Red Hat Enterprise Linux 6 Virtualization Host Configuration and Guest Installation Guide

URL: http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Virtualization_Host_Configuration_and_Guest_Installation_Guide/index.html (As of February 2012)

Preparations for Servers

In addition to the operations in "4.1.1.1 Preparations for Server Environments", the following operations are necessary.

- Installation and configuration of the host OS

Storage Preparations

Check the following:

- Volumes (LUNs) to assign to the admin OS have already been created

LUNs are used for virtual L-Server disks. Create the same number of LUNs as the number of necessary disks. The size of each LUN must be larger than the size of each disk.

- Volumes (LUN) to allocate to cloning images have been already created

Cloning images are stored on LUNs. Create LUNs based on the number of cloning images to be created. The size of each LUN must be larger than the size of each cloning image.

- Zoning and affinity have been set

When migrating VM guests for Virtual L-Servers, configure zoning and affinity, and set LUNs as shared disks.

Network Preparations

Check the following:

- The configuration for the admin and public LANs has been designed
- The network environment for the admin LAN is configured
- The VLAN ID to allocate to the network resource has been configured
- The virtual bridge has been configured beforehand
- The MAC address range for the virtual network interface (VNIF) has been decided

Perform the following configuration:

- In order to enable the use of virtual bridges, disable the NetworkManager service of the OS.

1. On the managed server, enable the NetworkManager service and then enable the network service.

Execute the following commands:

```
# service NetworkManager stop <RETURN>
# chkconfig NetworkManager off <RETURN>
# service network start <RETURN>
# chkconfig network on <RETURN>
```

2. Edit the `/etc/sysconfig/network-scripts/ifcfg-NIC_name` file to change the value for `NM_CONTROLLED` to "no".

Example

- Before editing

```
DEVICE="eth0"
HWADDR="xx:xx:xx:xx:xx:xx"
NM_CONTROLLED="yes"
ONBOOT="no"
BOOTPROTO=none
```

- After editing

```
DEVICE="eth0"
HWADDR="xx:xx:xx:xx:xx:xx"
NM_CONTROLLED="no"
ONBOOT="no"
BOOTPROTO=none
```

3. Restart the managed server.

Execute the following command:

```
# shutdown -r now <RETURN>
```

- Perform configuration to allow the managed server to use the VLAN.

1. Add "VLAN=yes" in the /etc/sysconfig/network file on the managed server using a text editor.

Example

- Before editing

```
NETWORKING=yes  
HOSTNAME=localhost.localdomain
```

- After editing

```
NETWORKING=yes  
HOSTNAME=localhost.localdomain  
VLAN=yes
```

2. Restart the managed server.

Execute the following command:

```
# shutdown -r now <RETURN>
```

- When using GLS for automatic network configuration, configure GLS.

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

- Creating a virtual bridge

Create a virtual bridge beforehand.

When Using IBP

When using virtual L-Servers, connect the IBP uplink sets used for the public LAN and admin LAN to the VM host regardless of VIOM, after creating each IBP uplink set.

It is not necessary to use the same name for the uplink set and the name of the network resource.

Creating a Virtual Bridge

The virtual bridge is required on the admin OS, in order to connect the L-Server to the network.

For details on how to configure virtual bridges, refer to the manual for RHEL-KVM and "[Manual Network Configuration](#)" in "[E.6.4 Setup](#)".

E.6.3 Installation

Installing the Manager

Install the Resource Orchestrator manager. For details on how to install a manager, refer to "2.1 Manager Installation" of the "Installation Guide CE".

Installing the Agent

Install agents of Resource Orchestrator on managed servers (admin OS).

For details on how to install agents, refer to "2.2.3 Installation [Linux/VMware/Xen/KVM/Oracle VM]" of the "Installation Guide CE".

E.6.4 Setup

The setup procedure when using KVM as server virtualization software is as follows:

1. Register Resources

a. Register managed servers (hosts)

The procedure is different depending on the managed server to be used.

Refer to "2.4 When using Blade Servers" or "2.5 When using Rack Mount and Tower Servers" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

2. Register Resources in Resource Pools

a. Register VM host resources (hosts)

b. Register disk resources (raw devices or partitions)

When migrating VM guests for virtual L-Servers, register the raw devices or the partitions shared between multiple VM hosts as disk resources defined to be shared.

Register the raw devices or the partitions to store cloning images shared between multiple VM hosts as disk resources defined as shared.

For details on how to register disk resources, refer to "1.3.4 rcxadm disk" of the "Reference Guide (Resource Management) CE".

c. Register network resources

If the NIC and network resources are connected when an L-Server is created, the settings matching the network resource definition will be registered automatically for the VM host that the L-Server will operate on.

For details, refer to "[Manual Network Configuration](#)".

- In the ROR console orchestration tree, right-click the target network pool, and select [Create Resource] from the popup menu.

- The [Create a network resource] dialog is displayed.

- Enter the items necessary for network resources. For details, refer to "7.3 Network Resources" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

d. Register address set resources (MAC addresses)

Create and register an address set resource (MAC address) in the address pool.

For details, refer to "7.6 Address Set Resources" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

3. Create an L-Server Template

Create an L-Server to collect cloning images from using an L-Server template.

a. Export an L-Server template

Refer to "8.2.1 Exporting a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

b. Edit an L-Server template

For details on the XML definition of L-Server templates, refer to "2.2 L-Server Template" of the "Reference Guide (Resource Management) CE".

In this case, perform the following configuration:

- Specify "RHEL-KVM" for the VM type.

- Specify "None" for the redundancy.

- Specify "Fixed" for the positioning.
 - c. Import an L-Server template
- Refer to "8.2.3 Importing a Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Manual Network Configuration

For the virtual bridge created in advance, only provide the function for connection with the virtual bridge. Manually perform virtual bridge settings in advance.

Use a different VLAN ID for each virtual bridge to connect with the virtual bridge.

Additionally, the following settings must be performed in advance.

1. Create a Virtual Bridge

Create a virtual bridge with the same name (including upper and lower case characters) for VM hosts managed by Resource Orchestrator.

This enables migration of VM guests between VM hosts.

When configuring a virtual bridge and server virtualization software other than RHEL-KVM is being used with the same manager, set a different name from the one used by the virtual switch, virtual network, and virtual bridge on the other virtualization software.

2. Configure Virtual Bridge Communication Settings

Right-click the LAN switch in the server resource tree, and select [Modify]-[Network Settings] from the popup menu.

Configure LAN switches to enable communication using the tagged VLAN between virtual bridges using the same name.

The ROR console can be used for VLAN configuration of LAN switch blade external ports.

For details, refer to "[4.2.3.6 Pre-configuring LAN Switch Blades on Managed Blade Systems](#)".

3. Define the Supported Virtual Bridge and VLAN ID

Supported virtual bridges and VLAN IDs are defined in the virtual bridge definition file of Resource Orchestrator.

For details on definition file format, refer to "[File Format for Virtual Bridge Definitions](#)".

4. Create Network Resources

- From the GUI:

- a. In the [Create a network resource] dialog containing the VLAN ID that was specified in 2. and 3., check the "Use configured virtual switches." checkbox and create a network resource.

- From the Command-line:

- a. Create the XML file that defines network resources.

Define the VLAN ID specified at 2. and 3. in the XML file.

In this case, specify auto="false" in the Network tag.

- b. To create the network resource, execute the `rcxadm network create` command specifying the XML file created in a.

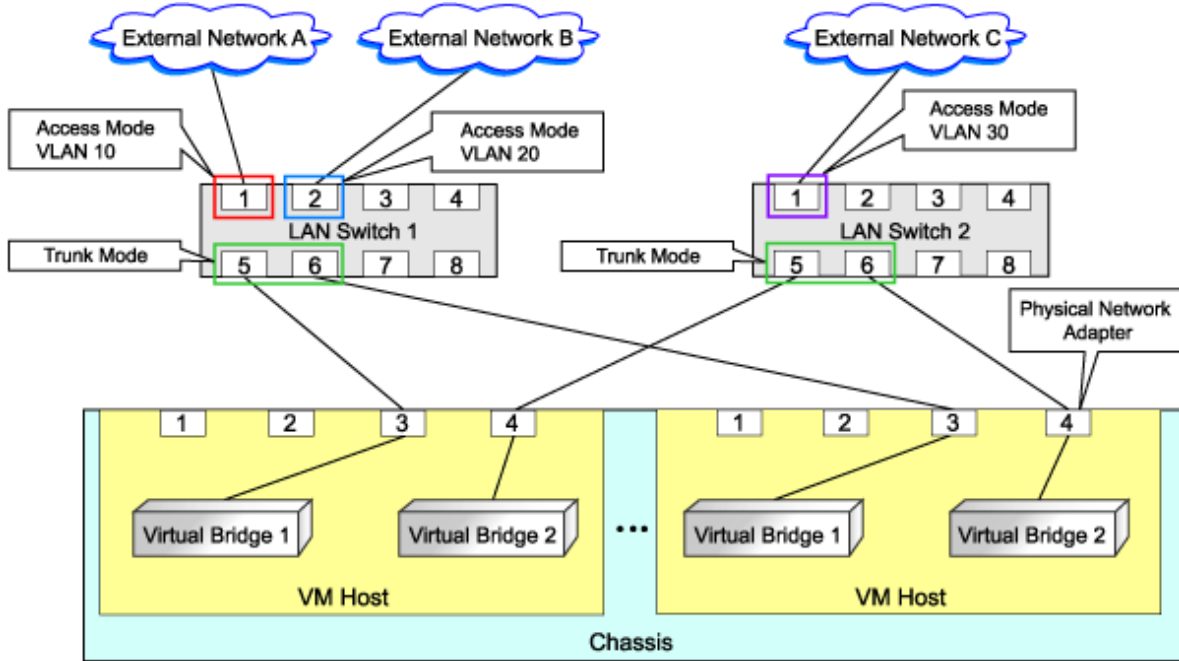
The network resources are created.

For details on the `rcxadm network` command, refer to "1.3.5 `rcxadm network`" of the "Reference Guide (Resource Management) CE".

For details on the Network element, refer to "2.5 Network Resources" in the "Reference Guide (Resource Management) CE".

An example of virtual NIC configuration and connection with virtual bridge using network resources is given below:

Figure E.27 Virtual NIC Configuration and Connection with Virtual Networks Using Bridge Resources



File Format for Virtual Bridge Definitions

Location of the Definition File

[Windows]

Installation_folder\Manager\etc\customize_data

[Linux]

/etc/opt/FJSVrcvmr/customize_data

Definition File Name

vnetwork_rhelkvm.rcxprop

Definition File Format

Describe the virtual bridge definition file in one line as below:

```
"Virtual_bridge_name"=VLAN ID
```

For the *VLAN ID*, a value from 1 to 4094 can be specified.



Example

```
"br0"=10
```

Blank spaces before and after equal signs ("=") are ignored.

Describe the virtual bridge correctly, as the entry is case-sensitive.

Save files using the UTF-8 character code.

When there are multiple lines with the same virtual bridge name, all specified lines are valid.

When the same VLAN ID is included in a line with a different virtual bridge name, the first occurrence in the file is valid and the lines after it are ignored.

An error occurs during L-Server creation if the definition of the VLAN ID of the network resource connected to the NIC cannot be found.

L-Server Creation

Use the following procedure to create L-Servers:

- Create an L-Server Using an L-Server Template
 - When there are no cloning images, or when not using already registered cloning images
 1. Create an L-Server, referring to "10.1 Creation Using an L-Server Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".
When creating the L-Server, select "None" for images.
 2. Install an OS
For manual OS installation, use the virtual machine manager.
For manual OS installation, refer to the "Red Hat Enterprise Linux 6 Virtualization Administration Guide".
Red Hat Enterprise Linux 6 Virtualization Administration Guide

URL: http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Virtualization_Administration_Guide/index.html (As of February 2012)
 3. Collect Cloning Images
When collecting cloning images after creating an L-Server, the cloning images are stored in the image pool.
When collecting cloning images, refer to "[8.6 Collecting and Registering Cloning Images](#)".
 - When using an existing cloning image
Create an L-Server, referring to "10.1 Creation Using an L-Server Template" of the "User's Guide for Infrastructure Administrators (Resource Management) CE". In this case, specify the cloning image that you want to use as an image.
- Create an L-Server Specifying Individual Specifications
Refer to "10.3 Creation of Virtual L-Servers Using Parameters" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".



Note

When a virtual L-Server on which an OS is not installed is powered on, the same amount of memory as the physical memory on the VM host is secured.

Collect Cloning Images

This section explains how to collect cloning images.

Use the following method to collect cloning images:

After installing an OS, stop the target L-Server.

1. Right-click the target L-Server in the orchestration tree, and select [Cloning]-[Collect] from the popup menu.
2. Click <OK>.

A cloning image is collected.

A given cloning image (identified by its name attribute) can be managed by image version.



Point

When the destination folder for image storage is omitted during the collection of cloning images, an accessible disk from a VM host in the same storage pool as the disk used by the L-Server that is the target for collecting cloning images is automatically selected.

Information

The disk resource in which cloning images are stored will be "already allocated" in the "Allocation" in the "Configuration Information" confirmed in "Disk Details", and in the state where there is no information in "L-Server Properties".

When collecting cloning images, enter the disk resource name to use for storing cloning images in Comment. The relationship between the cloning image and the disk resource can be checked in "Comment" for each resource in the "Resource List".

[OS] Tab Configuration

Enter the parameters to set for the OS when creating the L-Server. This setting is valid only if an image is specified in the [General] tab. The setting process is performed the first time the L-Server is started. If an image name is not specified, it is not necessary to enter all these items.

When the OS type on the [Server] tab is "Linux", the items can be entered, but when the OS type is "Windows" or "Linux(SELinux)", the items cannot be entered.

The [OS] tab cannot be configured in the following cases:

- When the SELinux setting for the host OS is "Enable"
- When the SELinux setting for the guest OS is "Enable"
- When the system volume for the guest OS is LVM

Table E.21 List of Settings

Item	Necessity of Entry	Values When Omitted	Description
Host name/Computer name	Possible	<i>L-Server Name</i>	Enter the host name or computer name. Enter a string of between 1 and 63 alphanumeric characters or hyphens ("-"), or periods ("."), beginning with an alphanumeric character.
Domain name	Possible	Values configured in the OS property definition file (*1)	Enter the domain name. Enter between 1 and 255 alphanumeric characters, hyphens ("-"), or periods ("."), beginning with an alphabetical character.
DNS search path	Essential	-	Enter a list of domain names to use for DNS searching, using between 1 and 32,767 characters. You can specify the same characters as the domain name.
Time zone	Possible	<i>The same time zone as the OS of the manager</i>	Specify the time zone of the OS.
Hardware clock configuration	Not Required	Local	Specify one of the following: <ul style="list-style-type: none"> - UTC - Local (LOCAL) Even if the above is specified, it is not reflected on the guest OS.

*1: When the value is not specified in the OS property definition file, nothing is configured.

L-Server Operations

Use the ROR console or the rcxadm lserver command for L-Server operations.

For details on how to operate an L-Server using the ROR console, refer to "Chapter 11 L-Server Operations" of the "User's Guide for

Infrastructure Administrators (Resource Management) CE".

For details on the `rcxadm lserver` command, refer to "1.3.1 `rcxadm lserver`" of the "Reference Guide (Resource Management) CE".

Changing L-Server Specifications

Use the ROR console or the `rcxadm lserver modify` command to change L-Server specifications.

For details on the specifications that can be changed, refer to "Chapter 11 L-Server Operations" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

The value after changing the specifications can be checked in the [Resource List] tab in the orchestration tree.

From the command-line, execute `rcxadm lserver list` and `rcxadm lserver show`.

For details, refer to "1.3.1 `rcxadm lserver`" of the "Reference Guide (Resource Management) CE".

E.6.5 Advisory Notes for RHEL-KVM Usage

This section explains advisory notes for RHEL-KVM.

VM Type View

In the ROR console, the VM type of RHEL-KVM VM hosts and VM guests is displayed as "RHEL-KVM".

Snapshot

When using RHEL-KVM, snapshots cannot be used.

Guest OS Personalization

When using RHEL-KVM, guest OS personalization can only be used only for Linux.

Detaching Disks and Deleting L-Servers

Users are recommended to delete the data on disks, as the data of disk resources for virtual L-Servers is not deleted when detaching disks or deleting L-Servers.

For details on how to delete data on disks, refer to "7.5 Storage Resources" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Configuration of Swap Area for the Host OS

As a guide, set the twice the amount of memory of a VM host for the swap area of a host OS.

When there is insufficient swap area for the host OS, the virtual L-Server may fail to start.

When it is difficult to secure sufficient swap area, it is also possible to configure the kernel parameters (`/proc/sys/vm/overcommit_memory`) to avoid failure of start operations due to a lack of virtual L-Server memory space.

For details, refer to the following section in the "Red Hat Enterprise Linux 6 Virtualization Administration Guide".

- Chapter 6. Overcommitting with KVM

URL: http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Virtualization_Administration_Guide/index.html (As of February 2012)
--

Configuration for L-Server Live Migration

In RHEL-KVM environments, use SSH to perform live migration on virtual L-Servers.

It is necessary to perform the following configuration to enable live migration of an L-Server from the manager.

- Configuration of /etc/hosts
- Configuration when using SSH

Configure the settings, referring to the following section in the "Red Hat Enterprise Linux 6 Virtualization Administration Guide".

- Chapter 4. KVM live migration
- Chapter 5. Remote management of guests

URL: http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Virtualization_Administration_Guide/index.html (As of February 2012)



When performing live migration using the `virsh migrate` command for KVM, specify both the `--undefinesource` and `--persistent` options.

If the command is executed without specifying these two options, the same VM guests may exist on both the destination and source VM hosts. In this state, the VM guests cannot be turned on using Resource Orchestrator. This occurs to prevent double VM guest startup operations in the state that multiple instances of the same VM guest exist on different VM hosts.

When turning on VM guests, the state where there are multiple instances of the same VM guest must be avoided by using the `virsh` command. For details on the `virsh` command, refer to the Command Reference in the following Red Hat manuals:

- 15.1. `virsh` command quick reference

URL: http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Virtualization_Administration_Guide/index.html (As of February 2012)

E.6.6 Overcommit

This section explains the VMware overcommit function for L-Servers.

Overcommit

The RHEL-KVM overcommit function for the CPU and memory is available on Resource Orchestrator.

The RHEL-KVM overcommit function for the CPU and memory virtually allows a guest OS to use more resources than that of the actual CPU and memory of a server.

An L-Server for VM pools with overcommit attributes includes overcommit attributes.

Installation Procedure

1. Create a VM pool for overcommit.

For details on how to create a VM pool, refer to "12.2 Resource Pool Operations" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

2. Create an overcommit configuration file for a VM pool.

Create an overcommit configuration file for the VM pool created in step 1.

For details on definition files, refer to "E.1 Common Functions of Server Virtualization Software".



Due to limitations of the KVM management application, it may take a few minutes until the amount of memory used by VM is reflected on the ROR console.

Appendix F Installation of VM Hosts on Physical L-Servers

This appendix explains how to install a VM host on a physical L-Server.

Installation of VM Hosts on physical L-Servers offers the following benefits:

- Simplified configuration of servers, storage, and networks

When installing a physical L-Server on a VM host, the following configurations can be simplified further than when installing a VM host on a physical server.

- Server configuration such as I/O virtualization
 - Storage configuration such as LUN masking
 - Network configuration such as LAN switch blades
- DR

In order to be able to perform DR of virtual L-Servers, it is necessary to install a VM host on a physical L-Server.



This function cannot be used in RHEL-KVM environments.

F.1 Installation

This section explains how to install a VM host on a physical L-Server.

1. Preparations for Physical L-Server Creation

For physical L-Server creation, configure the necessary settings.

For details, refer to the following:

- "[D.2 Pre-setup Preparations \(Servers\)](#)"
- "[D.3 Pre-setup Preparations \(Storage\)](#)"
- "[D.4 Pre-setup Preparations \(Network\)](#)"
- "[D.6 Setup](#)"

2. Create Resource Folders

Create a resource folder to locate physical L-Servers to install VM hosts on.

For details on how to create a resource folder, refer to "13.2.1 Creating a Resource Folder" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".



To prevent accidental deletion, create a resource folder for the physical L-Server on which the VM host will be installed, and configure it so that tenant administrators cannot access it.

For details, refer to "Appendix B Access Control by Roles" in the "Operation Guide CE".

3. Create Physical L-Servers

Create a physical L-Server to install a VM host in the created resource folder.

For details on how to create a physical L-Server, refer to "[D.7 Creating an L-Server](#)".

Note

- Cloning images for a physical L-Server on which a VM host has been installed cannot be collected or deployed.
- Use the NIC for the public LAN of an L-Server with the status "not connected" without connecting network resources.

Point

If using Auto Deploy to create a VM host, perform the following procedures:

- Specify "Do not deploy" for "Image deployment".
- Specify "Network boot (PXE)" for "Boot mode".

4. Install a VM Host

Install a VM host on the created physical L-Server.

When using Auto Deploy to create a VM host, reserve the MAC address of the admin NIC and admin IP address for the physical L-Server on the DHCP server used with Auto Deploy and start the L-Server.

Specify the virtual MAC address configured on VIOM for the MAC address of the admin NIC.

For details, refer to the individual manuals of server virtualization software.

5. Install Agents

Install Resource Orchestrator agents and ServerView Agents on a VM host.

If using Auto Deploy to create a VM host, this procedure is not necessary.

For details on installing agents, refer to "2.2 Agent Installation" of the "Installation Guide CE".

Point

When using VMware ESX, install Resource Orchestrator agents and ServerView for VMware agents.

When using VMware ESXi, install ServerView ESXi CIM Provider agents.

6. Register a VM Host

Registers a VM host with VM management software.

For details, refer to the individual manuals of server virtualization software.

7. Register VM Management Software

Register VM management software in Resource Orchestrator.

For details, refer to "2.2 Registering VM Management Software" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

8. Register Agents

Register an agent on the physical L-Servers the VM host will be installed on. Execute the following procedure to register agents.

- a. Right-click the target L-Server in the orchestration tree, and select [Register]-[Agent] from the popup menu.
- b. In the displayed "Register Agent" dialog, click <OK>.

9. Register VM Pools

Register a VM host in a VM pool.

For details, refer to "7.1 VM Host Resources" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

F.2 Changing Configuration

Configuration of VM hosts can be changed the same way as physical L-Servers.

Refer to "11.2 Modifying an L-Server" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

F.3 Deletion

Execute the following procedure to delete a VM host.

1. Unregister the VM Host

Unregister the VM host from VM pools.

For details, refer to "Unregistration" in "12.3 Resource Operations" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

2. Stop the VM Host

Stop the VM host.

Refer to "11.1.2 Stopping an L-Server" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

3. Delete Physical L-Servers

Delete the physical L-Server used for installation of the VM host.

Refer to "11.4 Deleting an L-Server" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".

F.4 Advisory Notes for Installation of VM Hosts on Physical L-Servers

This section explains advisory notes when installing a VM host on a physical L-Server.

Collecting and Deploying Cloning Images

Cloning images cannot be collected or deployed.

When Using Auto Deploy to Create a VM Host

Backup and restore functions cannot be used for the created VM host.

When a VM Host is VMware vSphere(TM) 4 or Later

When installing a VMware vSphere(TM) 4 or later VM host on a physical L-Server, take note of the following points:

- Backup and restore functions cannot be used.
- When using L-Server redundancy, it is not possible to specify the same pool as that of a spare server between L-Servers on which Windows is operating.
- When performing physical server usage change, the same physical servers cannot be switched over between L-Servers on which Windows is operating.

Appendix G User Management Using Directory Service

This appendix explains how to manage users using the directory service.

G.1 Installation Method

This section explains the installation method of user management using the directory service.

The following directory service can be registered in Resource Orchestrator:

- Active Directory (Windows Server 2003 and Windows Server 2008)
- OpenDS provided with ServerView Operations Manager
- OpenDS configured by the user
- OpenLDAP V2.3 or later version (for the Basic mode)



- The directory server that can be used in Resource Orchestrator is only one specified during installation.

G.2 User Confirmation of Directory Service Server

Use the following procedure to confirm the user information of the directory service.

1. Check if there is necessary user information for operations using Resource Orchestrator in the directory service.

In order to log in the ROR console, user information for the administrator role configured during installation of Resource Orchestrator is necessary.

2. When there is no user information, register the user information in the directory service.

Register the user information in the directory service using the directory service client function.

Use the following object classes.

Table G.1 Object Class

Directory Service	Object Class	Attribute used for the Login user ID
Active Directory	user	samAccountName or cn
OpenDS	inetOrgPerson	uid or cn
OpenLDAP	inetOrgPerson	uid or cn

G.3 Importing Certificates

Import the directory server certificate into Resource Orchestrator.

Common Settings among Directory Servers

Use the following procedure to configure the common settings in the directory server.

1. Stop the manager.

For information on stopping managers, refer to "[7.2 Starting and Stopping the Manager](#)".

2. Copy the following files:

- Files to copy

[Windows]

Installation_folder\Manager\runtime\jre6\lib\security\cacerts

[Linux]

/opt/FJSVrcvnr/runtime/jre6/lib/security/cacerts

- Copy destination

[Windows]

Installation_folder\Manager\runtime\jre6\lib\security\cacerts.org

[Linux]

/opt/FJSVrcvnr/runtime/jre6/lib/security/cacerts.org

Configuration when Using Active Directory

When using Active Directory, it is necessary to import the server certificate.

Use the following procedure to import Active Directory server certificates. The server certificate format is the DER encoded binary X.509 (CER) format.

1. Execute the following commands, and import the Active Directory server certificate into Resource Orchestrator.

[Windows]

```
>"Installation_folder\Manager\runtime\jre6\bin\keytool.exe" -importcert -alias ror_ldap -trustcacerts -file Server_certificate_path -keystore "Installation_folder\Manager\runtime\jre6\lib\security\cacerts" <RETURN>
```

[Linux]

```
# /opt/FJSVrcvnr/runtime/jre6/bin/keytool -importcert -alias ror_ldap -trustcacerts -file Server_certificate_path -keystore /opt/FJSVrcvnr/runtime/jre6/lib/security/cacerts <RETURN>
```

For the -alias option, specify "ror_ldap". "changeit" is configured as the default password for keystores.

2. The confirmation message is displayed. Trust the server certificate, and enter one of the following:

- When adding a keystore

Enter "yes".

- When stopping operations

Enter "no".

```
Do you trust this certificate? [no]:
```



Example

```
>"C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe" -importcert -alias ror_ldap -trustcacerts -file c:\myserver.serverview.local_svsca.crt -keystore "C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\lib\security\cacerts"
Enter keystore password: changeit
Owner: CN=svsca, DC=serverview, DC=local
Issuer: CN=svsca, DC=serverview, DC=local
Serial number: 22646549ec7ac1994cc3a2b8eff66e27
Valid from: Mon Oct 04 11:19:47 JST 2010 until: Sun Oct 04 11:26:54 JST 2015
Certificate fingerprints:
MD5: 70:E3:CB:23:6F:D1:17:00:56:CA:E2:0D:30:73:14:A8
```



```
SHA1: 01:3C:06:81:2D:3F:6D:D9:C3:A6:D4:AA:7B:D5:5E:D5:5F:43:90:E5
Signature algorithm name: SHA1withRSA
Version: 3
...
Trust this certificate? [no]: yes
```

3. The following messages will be displayed, when addition to a keystore is successfully completed.

```
The certificate is added to the keystore.
```

4. Execute the following commands, and check if the server certificate has been correctly imported.

[Windows]

```
>"Installation_folder\Manager\runtime\jre6\bin\keytool.exe" -list -alias ror_ldap -keystore
"Installation_folder\Manager\runtime\jre6\lib\security\cacerts" <RETURN>
```

[Linux]

```
# /opt/FJSVrcvmr/runtime/jre6/bin/keytool -list -alias ror_ldap -keystore /opt/FJSVrcvmr/runtime/
jre6/lib/security/cacerts <RETURN>
```

For the -alias option, specify "ror_ldap".

5. The message will be displayed, when the server certificate confirmation is successfully completed.

Example

```
>"C:\Fujitsu\ROR\Manager\runtime\jre6\bin\keytool.exe" -list-alias rcve_ldap -keystore "C:\ Fujitsu\ROR
\SVROR\Manager\runtime\jre6\lib\security\cacerts"
Enter keystore password: changeit
rcve_ldap, 2010/10/05, trustedCertEntry,
Certificate fingerprints (MD5): 70:E3:CB:23:6F:D1:17:00:56:CA:E2:0D:30:73:14:A8
```

6. When performing Single Sign-On operations with ServerView Operations Manager, import the ServerView Operations Manager server certificate into Resource Orchestrator.

Import the server certificate, referring to "[OpenDS Provided with ServerView Operations Manager](#)".

OpenDS Provided with ServerView Operations Manager

Use the following procedure to import the ServerView Operations Manager server certificate into Resource Orchestrator.

1. Execute the following commands, and import the ServerView Operations Manager server certificate into Resource Orchestrator.

"changeit" is configured as the default password for keystores.

[Windows]

```
>"Installation_folder\Manager\runtime\jre6\bin\keytool.exe" -importkeystore -srckeystore "ServerView
Suite\Installation_folder\jboss\server\serverview\conf\pki\keystore" -destkeystore "Installation_folder
\Manager\runtime\jre6\lib\security\cacerts" <RETURN>
```

[Linux]

```
# /opt/FJSVrcvmr/runtime/jre6/bin/keytool -importkeystore -srckeystore /opt/fujitsu/ServerViewSuite/
jboss/server/serverview/conf/pki/keystore -destkeystore /opt/FJSVrcvmr/runtime/jre6/lib/security/
cacerts <RETURN>
```

2. A message will be displayed when import is successfully completed.

Check the "*Another name*" section.

Example

```
>"C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe" -importkeystore -srckeystore "C:\Program Files\Fujitsu\ServerView Suite\jboss\server\serverview\conf\pki\keystore" -destkeystore "C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\lib\security\cacerts"  
Enter destination keystore password: changeit  
Enter source keystore password: changeit  
Entry for Another name svs_cms successfully imported.  
Import command completed: 1 entries successfully imported. 0 entries failed or cancelled.
```

3. Execute the following commands, and check if the server certificate has been correctly imported.

[Windows]

```
>"Installation_folder\Manager\runtime\jre6\bin\keytool.exe" -list -alias Another_name -keystore  
"Installation_folder\Manager\runtime\jre6\lib\security\cacerts" <RETURN>
```

[Linux]

```
# /opt/FJSVrcvmr/runtime/jre6/bin/keytool -list -alias Another_name -keystore /opt/FJSVrcvmr/  
runtime/jre6/lib/security/cacerts <RETURN>
```

For the -alias option, specify the "*another name*" checked in 2.

4. The message will be displayed, when the server certificate confirmation is successfully completed.

Example

```
>"C:\Fujitsu\ROR\Manager\runtime\jre6\bin\keytool.exe" -list -alias svs_cms -keystore "C:\Fujitsu\ROR\  
\SVROR\Manager\runtime\jre6\lib\security\cacerts"  
Enter keystore password: changeit  
svs_cms, 2010/10/05, PrivateKeyEntry,  
Certificate fingerprints (MD5): C9:3C:8B:8B:C6:BA:67:92:89:70:D1:00:55:A3:CD:6
```

When Using OpenDS Configured Individually

When using an individually configured OpenDS, it is necessary to import the server certificate. Use the following procedure to import the server certificate of the individually configured OpenDS. The server certificate format is the JKS (Java Keystore) format.

1. Execute the following commands, and import the individually configured OpenDS server certificate into Resource Orchestrator.

"changeit" is configured as the default password for keystores.

[Windows]

```
>"Installation_folder\Manager\runtime\jre6\bin\keytool.exe" -importkeystore -srckeystore  
"OpenDSInstallation_folder\config\keystore" -destkeystore "Installation_folder\Manager\runtime\  
\jre6\lib\security\cacerts" <RETURN>
```

[Linux]

```
# /opt/FJSVrcvnr/runtime/jre6/bin/keytool -importkeystore -srckeystore
"OpenDSInstallation_folder/config/keystore" -destkeystore /opt/FJSVrcvnr/runtime/jre6/lib/
security/cacerts <RETURN>
```

2. A message will be displayed when import is successfully completed.

Check the "*Another name*" section.



Example

```
>"C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe" -importkeystore -srckeystore "C:
\win32app\OpenDS-2.2.0\config\keystore" -destkeystore "C:\Fujitsu\ROR\SVROR\Manager\runtime
\jre6\lib\security\cacerts"
Enter destination keystore password: changeit
Enter source keystore password: changeit
Entry for Another name server-cert successfully imported.
Import command completed: 1 entries successfully imported. 0 entries failed or cancelled.
```

3. Execute the following commands, and check if the server certificate has been correctly imported.

[Windows]

```
>"Installation_folder\Manager\runtime\jre6\bin\keytool.exe" -list -alias Another_name -keystore
"Installation_folder\Manager\runtime\jre6\lib\security\cacerts" <RETURN>
```

[Linux]

```
# /opt/FJSVrcvnr/runtime/jre6/bin/keytool -list -alias Another_name -keystore /opt/FJSVrcvnr/
runtime/jre6/lib/security/cacerts <RETURN>
```

For the `-alias` option, specify the "*another name*" checked in 2.

4. The message will be displayed, when the server certificate confirmation is successfully completed.



Example

```
>"C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe" -list -alias server -cert -keystore "C:
\Fujitsu\ROR\SVROR\Manager\runtime\jre6\lib\security\cacerts"
Enter keystore password: changeit
server-cert, 2010/10/05, PrivateKeyEntry,
Certificate fingerprints (MD5): 15:6F:61:8E:54:E3:57:99:8C:24:A5:76:1A:D4:4D:E0
```

5. When performing Single Sign-On operations with ServerView Operations Manager, import the ServerView Operations Manager server certificate into Resource Orchestrator.

Import the server certificate, referring to "[OpenDS Provided with ServerView Operations Manager](#)".

Configuration when using OpenLDAP

When using OpenLDAP, it is necessary to import the CA certificates for OpenLDAP. Import the certificate using the same procedure as in "[Configuration when Using Active Directory](#)".

G.4 Manager Configuration

1. Stop the manager.

For information on stopping managers, refer to "[7.2 Starting and Stopping the Manager](#)".

2. Register the directory service as an external authentication function of Resource Orchestrator.

To register the directory service, execute the `rcxadm authctl` command.

For details on the `rcxadm authctl` command, refer to "1.7.10 `rcxadm authctl`" of the "Reference Guide (Resource Management) CE".

Example

- When Using Active Directory

```
>rcxadm authctl register -ip 192.168.1.1 -port 636 -base dc=example,dc=local -bind
cn=Administrator,cn=Users,dc=example,dc=local -method SSL -passwd mypasswd -auth ldap
<RETURN>
```

- When using OpenDS

```
>rcxadm authctl register -ip 192.168.1.1 -port 1474 -base dc=fujitsu,dc=com -bind "cn=Directory
Manager" -method SSL -passwd admin -auth serverview <RETURN>
```

- When Using OpenLDAP

```
>rcxadm authctl register -ip 192.168.1.1 -port 636 -base dc=example,dc=local -bind
cn=manager,dc=example,dc=local -method SSL -passwd mypasswd -auth ldap <RETURN>
```

3. Start the manager.

For information on starting managers, refer to "7.2 Starting and Stopping the Manager".

4. Register the user information in Resource Orchestrator.

For details on how to register the user information, refer to "Appendix C User Management Using Directory Service" of the "Operation Guide CE".

G.5 Migration from Internal Authentication Function to Directory Service

This section explains how to migrate from an internal authentication function to user management using the directory service.

Migration to Active Directory

1. When using SSL encrypted communication between Active Directory and the manager, create an SSL communication environment.

An SSL communication environment is necessary to register user information using the `ldifde` command of Active Directory. An SSL certification environment is also necessary for performing Single Sign-On operations with ServerView Operations Manager. For details on how to import the server certificates of Active Directory, refer to "G.3 Importing Certificates".

2. Export the user information as files in LDIF format from the internal authentication function.

Example

```
>rcxadm user list -format ldif > myusers.ldif <RETURN>
```

3. Modify the user information exported as the ldif file in 2. for the actual environment.

Modify the base names of entries based on the base name of the Active Directory.

4. Execute the `ldifde` command to register the ldif file modified in 3. with Active Directory.

Example

```
>ldifde -i -e -k -t 636 -f myusers.ldif <RETURN>
```

For details on the `ldifde` command, refer to the Active Directory documentation.

Registered user passwords are reset as follows.

```
rcxuser@123
```

- Change the user passwords registered in 4. to appropriate values. Use the Active Directory functions, and change the password.
- Stop the manager.
For information on stopping managers, refer to "[7.2 Starting and Stopping the Manager](#)".
- Register the Active Directory as an external authentication function of Resource Orchestrator.

Example

```
>rcxadm authctl register -ip 192.168.1.1 -port 636 -base dc=example,dc=local -bind  
cn=Administrator,cn=Users,dc=example,dc=local -method SSL -passwd mypasswd -auth ldap <RETURN>
```

- Start the manager.
For information on starting managers, refer to "[7.2 Starting and Stopping the Manager](#)".
- When performing Single Sign-On operations with ServerView Operations Manager, user definitions are necessary for ServerView Operations Manager. For details on how to add user definitions for ServerView Operations Manager, perform settings for Single Sign-On referring to the following manual:
 - "Integrating ServerView User Management into Microsoft Active Directory" of the "ServerView Suite User Management in ServerView"

Migration to OpenDS or OpenLDAP

- Import the SSL server certificate.
 - When using OpenDS
Refer to "[G.3 Importing Certificates](#)".
 - When Using OpenLDAP
Import the OpenLDAP server certificate. Configure the SSL communication environment if necessary.

Example

[Windows]

```
>"Installation_folder\Manager\runtime\jre6\bin\keytool.exe" -importcert -alias ror_ldap -  
trustcacerts -file Server_certificate_path -keystore "Installation_folder\Manager\runtime\jre6\lib  
\security\cacerts" <RETURN>
```

[Linux]

```
# /opt/FJSVrcvmr/runtime/jre6/bin/keytool -importcert -alias ror_ldap -trustcacerts -file  
Server_certificate_path -keystore /opt/FJSVrcvmr/runtime/jre6/lib/security/cacerts <RETURN>
```

2. Export the user and user group information as files in LDIF format from the internal authentication function.

Example

```
>rcxadm user list -format ldif > myusers.ldif <RETURN>
```

The ldif file for the Active Directory is output.

3. Modify the user information exported as the ldif file in 2. for OpenDS and OpenLDAP.
 - a. Modify the base names of entries based on the base name of the directory service.
 - b. Delete the following attributes.
 - samAccountName
 - userAccountControl
 - unicodePwd
 - c. Add the following attributes to user entries.
 - sn
 - uid (same value as the cn attribute)
 - userPassword
 - d. Modify the values of the objectclass attribute.
 - Change "user" to "inetOrgPerson".
 - e. Change "cn=Users" in the "cn=*User_name*,cn=Users,dc=fujitsu,dc=com" to "ou=Users".

Example

- Before editing (ldif file for Active Directory)

```
# User
dn: cn=user01,cn=Users,dc=example,dc=local          # Change cn=Users to
ou=Users.
changetype: add
objectclass: user                                  # Change to objectclass:
inetOrgPerson.
cn: user01
samAccountName: user01                            # Delete this line.
userAccountControl: 512                           # Delete this line.
unicodePwd:: IgByAGMAeAB1AHMAZQBByAEAAMQAYADMAIga= # Delete this line.
                                                    # Add sn,uid, and
userPassword attributes.
```

- After editing (ldif file for OpenDS and OpenLDAP)

```
# User
dn: cn=user01,ou=Users,dc=example,dc=local
changetype: add
objectclass: inetOrgPerson
cn: user01
sn: user01
uid: user01
userPassword: mypassword
```

4. Use the directory service client function to register the ldif file modified in 3. with the directory service.

Set the Java SE 6 path for the environment variable JAVA_HOME, before executing the ldapmodify command of OpenDS.

For details on the command, refer to each directory service manual.

[Windows]

```
>"OpenDS_installation_folder\bat\ldapmodify.bat" -p Port_number -f ldif_file -D Administrator_user_DN  
-w Password <RETURN>
```

[Linux]

```
# "OpenDS_installation_folder/bin/ldapmodify" -p Port_number -f ldif_file -D Administrator_user_DN -w  
Password <RETURN>
```

Example

- When using OpenDS

```
>"C:\Program Files\Fujitsu\ServerView Suite\opens\bat\ldapmodify.bat" -p 1473 -f myusers.ldif -D  
"cn=Directory Manager" -w admin -c <RETURN>
```

- When Using OpenLDAP

```
>ldapadd -f myusers.ldif -x -D "cn=Manager,dc=example,dc=local" -w passwd <RETURN>
```

5. Stop the manager.

For information on stopping managers, refer to "[7.2 Starting and Stopping the Manager](#)".

6. Register OpenDS or OpenLDAP as an external authentication function of Resource Orchestrator.

Example

- When using OpenDS

```
>rcxadm authctl register -ip 192.168.1.1 -port 1474 -base dc=fujitsu,dc=com -bind "cn=Directory  
Manager" -method SSL -passwd admin -auth serverview <RETURN>
```

- When Using OpenLDAP

```
>rcxadm authctl register -ip 192.168.1.1 -port 636 -base dc=example,dc=local -bind  
cn=manager,dc=example,dc=local -method SSL -passwd mypasswd -auth ldap <RETURN>
```

7. Start the manager.

For information on starting managers, refer to "[7.2 Starting and Stopping the Manager](#)".

8. When performing Single Sign-On operations with ServerView Operations Manager in OpenDS, specify users who are defined in ServerView Operations Manager as the user information of Resource Orchestrator.

For details on how to register the user information, refer to "Appendix C User Management Using Directory Service" of the "Operation Guide CE".

9. When users of Resource Orchestrator log in to ServerView Operations Manager, user definitions are necessary for ServerView Operations Manager. For details on how to add user definitions for ServerView Operations Manager, perform settings for Single Sign-On referring to the following manual:

- "Integrating ServerView User Management into Microsoft Active Directory" of the "ServerView Suite User Management in ServerView"

For OpenDS, perform settings for Single Sign-On referring to the setting procedure of Active Directory.

Appendix H Basic Mode

This appendix explains Basic mode.

Basic mode can be used by configuring the Cloud Edition license after installing ROR VE.

For details on how to configure licenses, refer to ["License Setup"](#) in ["7.1 Login"](#).

H.1 Overview

Functions Available in Basic Mode

In Basic mode, the [Resource] tab and the [Home] tab can be used on the ROR console.

User Authentication Function for Basic Mode

The following two services are user authentication functions for Basic mode.

- Internal Authentication Function

Authenticates the user information of Resource Orchestrator. Decide the setting values for user accounts beforehand.

For details, refer to ["H.2 User Account Design Using the Internal Authentication Function"](#).

- Directory Service

Authenticates using the user information of the directory service. It is necessary to import the certificate and configure the manager beforehand.

For details, refer to ["Appendix G User Management Using Directory Service"](#).

H.2 User Account Design Using the Internal Authentication Function

This section explains the setting values for user accounts when using the internal authentication function.

For details on setting values for user accounts, refer to ["3.3 Defining User Accounts"](#).

It is necessary to set the following values for user accounts when using the internal authentication function.

Table H.1 Settings for User Accounts Created on Resource Orchestrator

Item	Description
User ID	The user ID must start with an alphanumeric character, and can contain up to 32 alphanumeric characters, underscores ("_"), hyphens ("-"), and periods (".").
Password	The string must be composed of alphanumeric characters and symbols, and can be up to 16 characters long.

For details on how to manage user accounts, refer to ["Chapter 9 Account"](#) of the ["User's Guide for Infrastructure Administrators CE"](#).

Appendix I Definition Files

This section explains how to configure definition files.

To use the functions of Resource Orchestrator, it is necessary to create definition files in advance.

Note

If you edit and save a UTF-8 text file using Windows Notepad, the Byte Order Mark (BOM) is stored in the first three bytes of the file, and the information specified on the first line of the file will not be analyzed correctly. When using Notepad, specify the information from the second line.

Location of the Definition File

Definition files are created in the following location.

[Windows]

Installation_folder\Manager\etc\customize_data

[Linux]

/etc/opt/FJSVrcvmr/customize_data

Functions Requiring a Definition File

The functions that require a definition file and the name of the definition file are indicated below.

Table I.1 List of Functions Requiring a Definition File (For Both Physical L-Servers and Virtual L-Servers)

Function	Definition File Name	Reference
When changing the location to back up configuration definition information	manager_backup.rcxprop	Refer to "8.2 Backup" of the "Operation Guide VE".
When configuring Thin Provisioning attributes on a storage pool	pool.rcxprop	Refer to "12.2 Resource Pool Operations" of the "User's Guide for Infrastructure Administrators (Resource Management) CE".
When configuring priority for resource selection on Thin Provisioning (*1)	storage.rcxprop	Refer to " D.5.1 Definition Files " and " E.1.1 Definition Files ".

*1: When there is both a storage pool with thin provisioning attributes set and a storage pool without thin provisioning attributes set.

Table I.2 List of Functions Requiring a Definition File (For Physical L-Servers)

Function	Definition File Name	Reference	
When using SAN storage	Settings required for all storage units	storage_portset.rcxprop	Refer to " 6.1.1 Creating Definition Files Combining Ports of SAN Storage ".
	Settings when using ETERNUS storage	storage.rcxprop	Refer to " D.5.1 Definition Files ".
	Settings when using dynamic LUN mirroring	storage_mirroring.rcxprop	Refer to " D.5.1 Definition Files ".
	When using configuration of priority for resource selection on	storage.rcxprop	Refer to " D.5.1 Definition Files ".

Function		Definition File Name	Reference
	Automatic Storage Layering		
	Settings when using EMC storage	emcpath.conf	Refer to " D.5.1 Definition Files ". Store the file in the following location: [Windows] <i>Installation_folder</i> \Manager\sys\usm\etc [Linux] /opt/FJSVrcvmr/sys/usm/etc
When changing the spare server switching policy and server model compatibility		spare_server_config.rcxprop	Refer to "14.1.1 L-Server High Availability" of the "Operation Guide CE".
When using IBP mode with LAN switch blades		vnetwork_ibp.rcxprop	Refer to " D.4 Pre-setup Preparations (Network) ".
When automatically specifying settings such as NIC redundancy and tagged VLAN while deploying OS images		net_info.conf	The file is automatically generated. For details, refer to " D.7.4 Network Redundancy and VLAN Settings of L-Servers ".
When creating a physical L-Server without specifying a model name in the L-Server template		server_spec.rcxprop	Refer to " D.5.1 Definition Files ".
When the number of FCs fitted and their position are different depending on the physical server		fc_connection_pattern	Refer to " D.5.1 Definition Files ".
When using L-Server alive monitoring		Physical.rcxprop Place the file directly under the alive_monitoring directory.	Refer to " D.5.1 Definition Files ".

Table I.3 List of Functions Requiring a Definition File (For Virtual L-Servers)

Function	Definition File Name	Reference
When simplifying the parameter settings for an OS	- For User Groups os_setting_user_group_name.rcxprop - Common on System os_setting.rcxprop	[VMware] Refer to " E.2.5 Setup ". [Hyper-V] Refer to " E.3.4 Setup ". [Oracle VM] Refer to " E.5.4 Setup ".
When using overcommit	pool.rcxprop	Refer to " E.1.1 Definition Files ".
When the VM host IP addresses in Resource Orchestrator do not match those in the VM management software	vmhost_ip_addresses.rcxprop	Refer to "2.2 Registering VM Management Software" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".
VM specific information definition file	- For User Groups vm_user_group_name_VM_type.rcxprop - Common on System vm_VM_type.rcxprop	Refer to " E.1.1 Definition Files ".

Function	Definition File Name	Reference
	Place the file directly under the vm_prop directory.	
When creating a virtual L-Server using a server which cannot use ServerView Agents	server_spec.rcxprop	Refer to " E.1.1 Definition Files ".
When using L-Server alive monitoring	[Windows] \alive_monitoring\vm_VM_type.rcxprop [Linux] \alive_monitoring\vm_VM_type.rcxprop	Refer to " E.1.1 Definition Files ".

Table I.4 List of Functions Requiring a Definition File (VMware)

Function	Definition File Name	Reference
When using a distributed virtual network (vDS) (port group and VLAN ID associations)	vnetwork_vmware.rcxprop	Refer to " E.2.2 Preparations ".
	vds_dc	Refer to " E.2.2 Preparations ". Store the file in the following location: [Windows] <i>Installation_folder\Manager\etc\vm</i>
When the Messages Notified by VM Management Software are Output in English	vm.rcxprop	Refer to " E.1.1 Definition Files ".
When configuring power control for VMware DRS and DPM	vm.rcxprop	Refer to " E.2.4 Configuration after Installation ".
When connecting to the virtual L-Server console from the admin client linking with the public LAN	vm_console.rcxprop	Refer to " E.2.4 Configuration after Installation ".

Table I.5 List of Functions Requiring a Definition File (Hyper-V)

Function	Definition File Name	Reference
When limiting the location to store cloning images for each user group	- For User Groups library_share_user_group_name_deny.conf - Common on System library_share_deny.conf	Refer to " E.3.4 Setup ".
When deleting cloning images and also deleting related files that have no dependencies with other templates	delete_image_all_files_scvm	Refer to " E.3.4 Setup ". Store the file in the following location: [Windows] <i>Installation_folder\Manager\etc\vm</i> [Linux] <i>/etc/opt/FJSVrcvmlr/vm</i>
When creating an L-Server specifying a cloning image collected from a client OS or localized version of Windows	- For User Groups image_admin_hyperv_user_group_name.rcxprop - Common on System image_admin_hyperv.rcxprop	Refer to " E.3.4 Setup ".
Configuring Network Resources when Using a	vnetwork_hyperv.rcxprop	Refer to " E.3.4 Setup ".

Function	Definition File Name	Reference
Physical Network Adapter Number that Differs from Configuration Patterns of VM Hosts which Support Automation of Network Configuration		

Table I.6 List of Functions Requiring a Definition File (RHEL5-Xen)

Function	Definition File Name	Reference
When changing the shared class configuration of PRIMECLUSTER GDS	storage_vmhost.rcxprop	Refer to " E.4.4 Setup ".
Relating the virtual bridge and VLAN ID	vnetwork_rhelxen.rcxprop	Refer to " E.4.4 Setup ".

Table I.7 List of Functions Requiring a Definition File (Oracle VM)

Function	Definition File Name	Reference
Relating the virtual bridge and VLAN ID	vnetwork_oraclevm.rcxprop	Refer to " E.5.4 Setup ".
Specifying SSL access for VM management software	ovmm.rcxprop	Refer to " E.5.5 Advisory Notes for Oracle VM Usage ".

Table I.8 List of Functions Requiring a Definition File (RHEL-KVM)

Function	Definition File Name	Reference
Relating the virtual bridge and VLAN ID	vnetwork_rhelkvm.rcxprop	Refer to " E.6.4 Setup ".

Appendix J Notes on Installation

This appendix explains points to keep in mind when setting up a Resource Orchestrator environment:

- The maximum of managed servers can be registered in Resource Orchestrator is limited, and depends on the Resource Orchestrator license purchased.

For details on the limit of managed servers, refer to license documentation.

An error will occur when trying to register more managed servers than the above limit. This limit includes the spare servers used by recovery settings. However, it does not include VM guests.

- Clustering software can be used on managed servers.

However, the following operations are not supported.

- Managed server switchover
- Backup and Restore
- Use of the Windows Server 2008 BitLocker drive encryption function (Windows BitLocker Drive Encryption) is not supported.

If the admin server or managed servers are running under Windows Server 2008, do not encrypt the system disk using the BitLocker drive encryption function.

[Linux]

When installing an operating system on a PRIMEQUEST server, use legacy boot.

Appendix K To Customize Dashboard

The dashboard provides an alert function for sending notifications via e-mail if the global pool use rate exceeds the threshold value.

The following settings can be customized by changing the alert information:

- E-mail send settings
- Threshold value
- Monitored pools

A dashboard development environment is required in order to customize alert information. This appendix explains how to build a dashboard development environment and how to change the alert information.



Alert information can be changed by copying and editing the sample alert information provided by this product. In the sample information, "90%" is set as the threshold value, and "All global pools" is set as the monitored pools.

K.1 Building the Dashboard Development Environment

The dashboard development environment is required to customize the cloud operation management dashboard. This section explains how to build the dashboard development environment.

The installation flow is shown as follows:

1. Installing the Dashboard Development Environment
2. Setting up the Dashboard Development Environment



The dashboard development environment can be built in the Windows environment only. If a Linux version is used, a separate Windows machine must be arranged for to build the dashboard development environment.

K.1.1 Installing the Dashboard Development Environment

This section explains the steps required to install the dashboard development environment.



- Use Interstage Business Process Manager Studio and Interstage Business Process Manager Analytics Studio bundled with this product when installing them. Studio bundled with Interstage Business Process Manager or Interstage Business Process Manager Analytics supplied as a standalone product cannot be used.
- If a Linux version is used, a Windows client machine that has been arranged for the dashboard development environment must be used to perform the tasks.

Firstly, insert the following DVD-ROM (Disk 3) into the DVD-ROM drive of the computer.

Follow the steps below to install.

Install JRE 5.0

Install JRE 5.0 in advance when installing the dashboard development environment to a machine other than the admin Server.

1. Execute the following file:

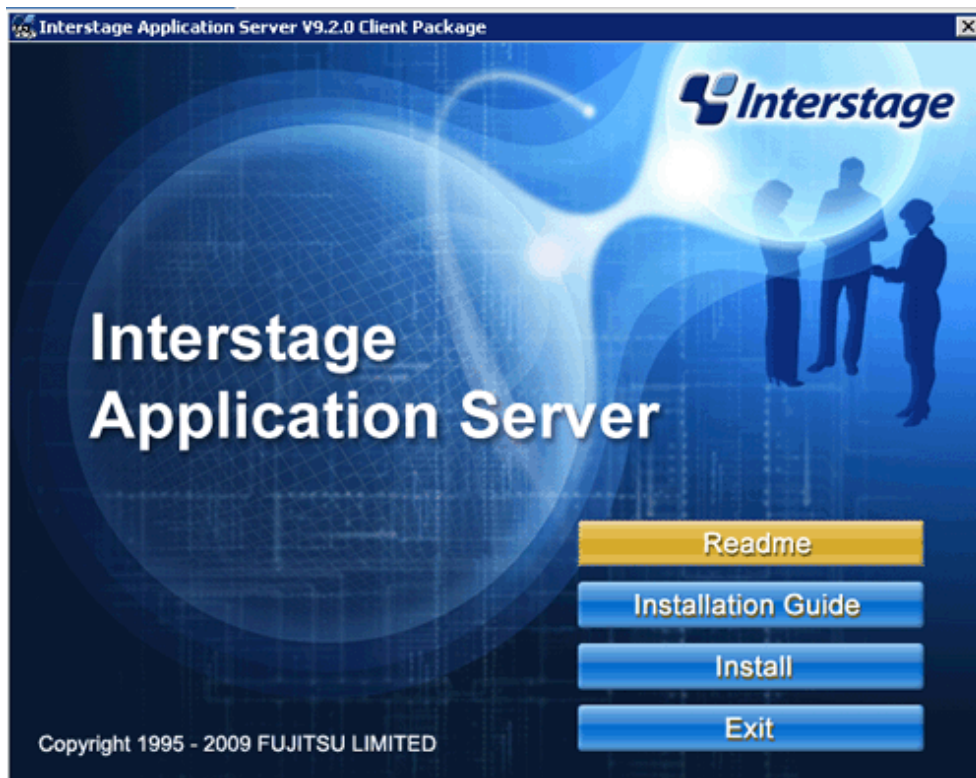
[Windows]

```
DVD-ROM drive:\DISK3\Studio\Windows\RCXCTMG\Disc1\en\autorun.exe
```

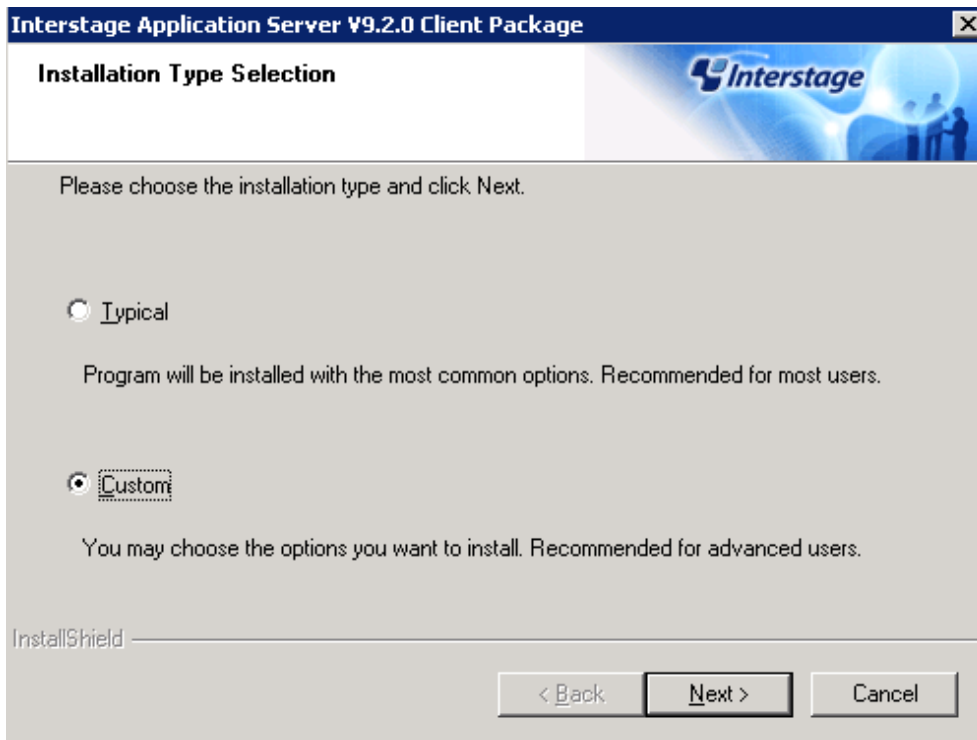
[Linux]

```
DVD-ROM drive:\DISK3\Studio\Windows\RCXCTMG\Disc1\en\autorun.exe
```

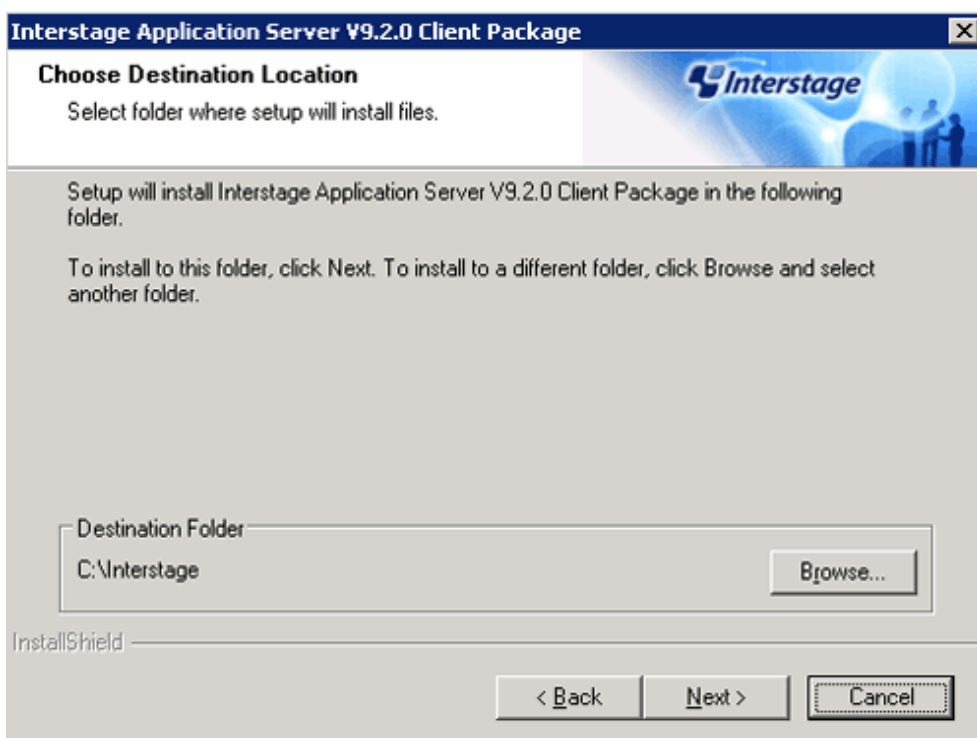
2. Click **Install**.



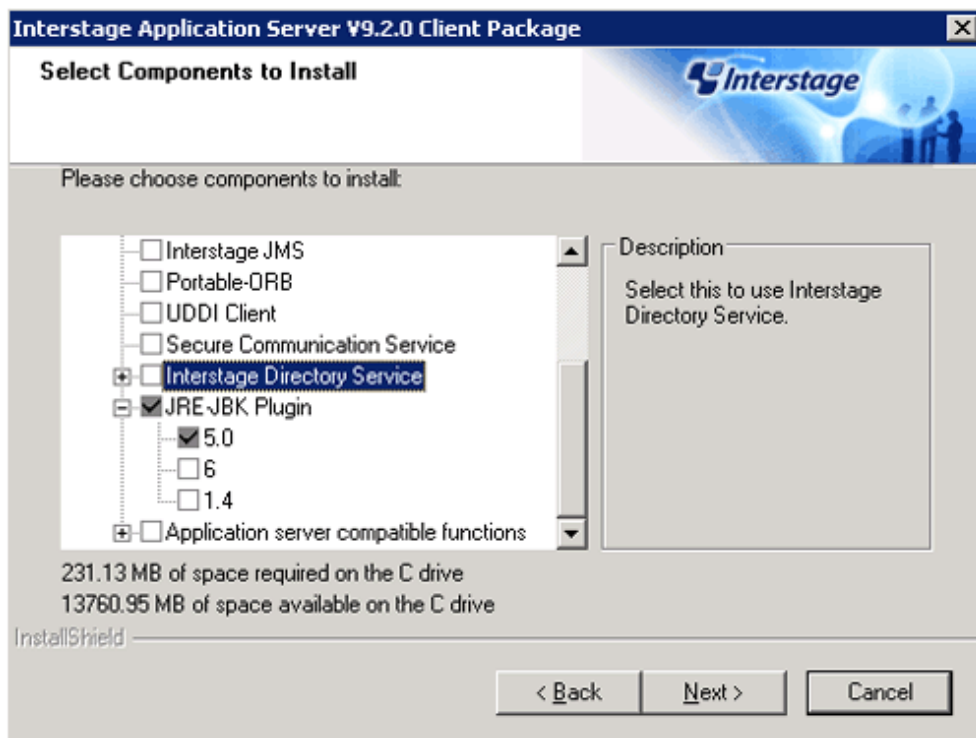
3. Select **Custom**, and click **Next**.



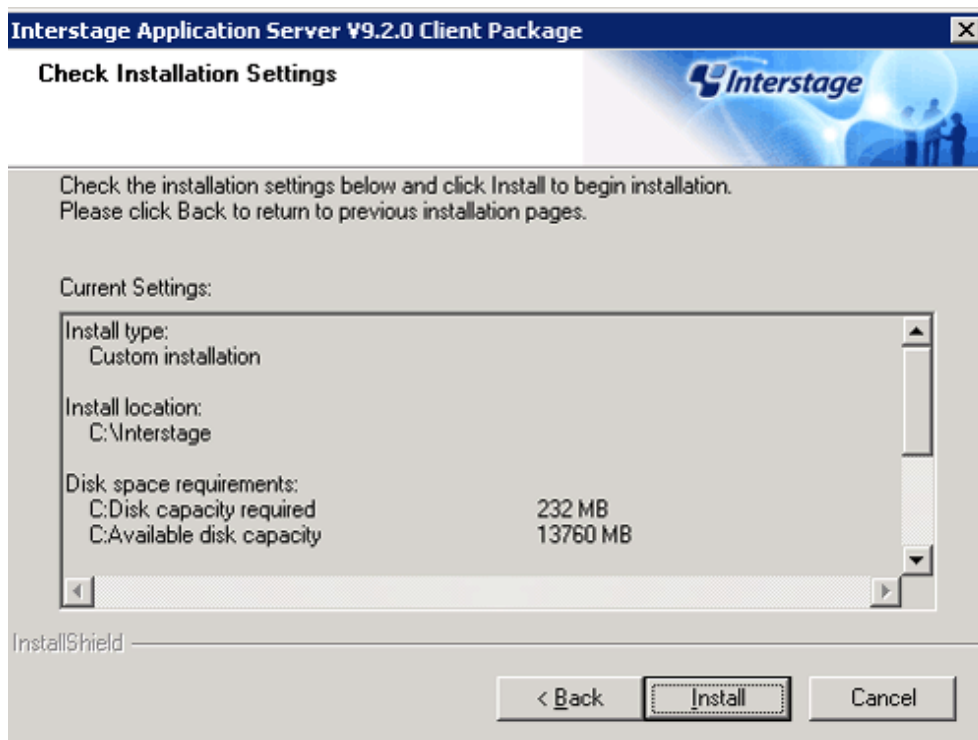
4. To select an installation folder other than the default folder, select **Destination Folder** displayed and select the installation folder. Click **Next**.



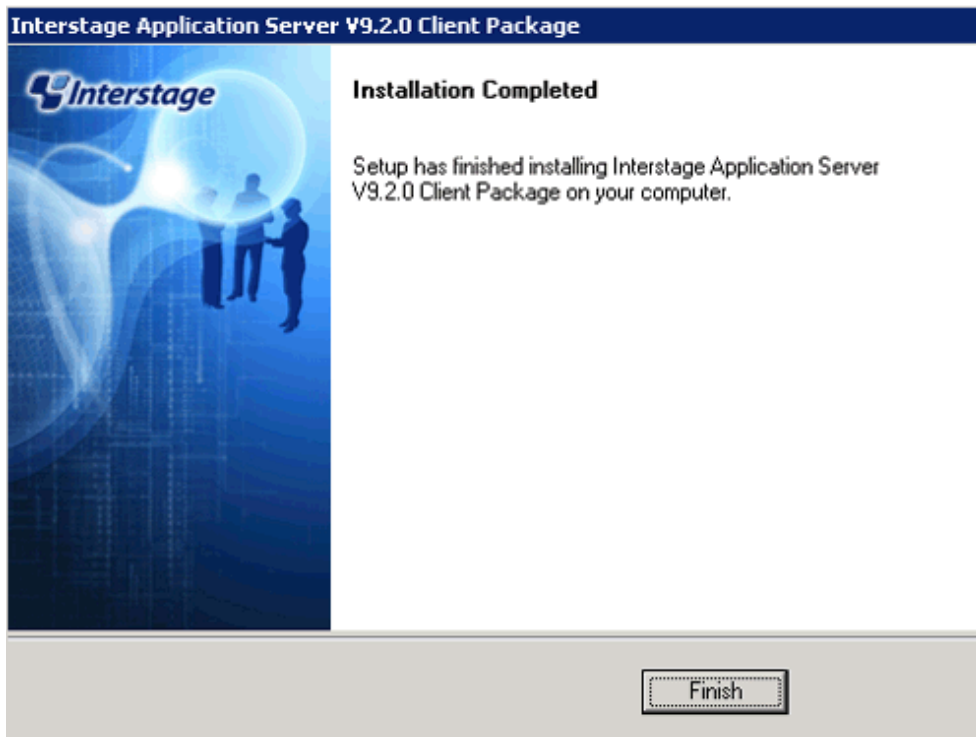
5. To select installation functions, select the **JRE-JBK Plugin** and **>> 5.0** checkboxes only. Clear all other checkboxes. Click **Next**.



6. Check the installation details and click **Install**.



7. Click **Finish** when installation is completed.



Install Interstage Business Process Manager Studio

Install BPM Studio.

1. Execute the following file:

[Windows]

```
DVD-ROM drive:\DISK3\Studio\Windows\RCXCTMG\Disc2\setup.exe
```

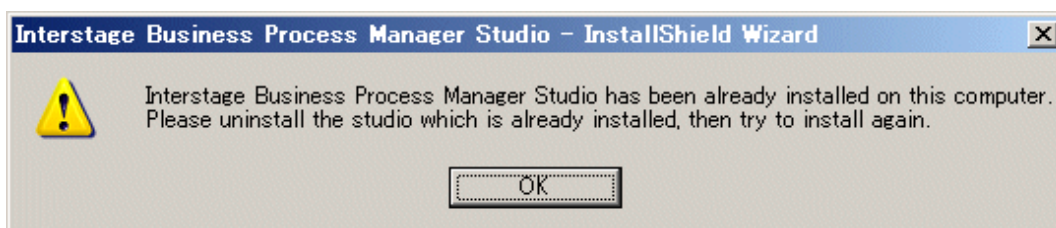
[Linux]

```
DVD-ROM drive:\DISK3\Studio\Windows\RCXCTMG\Disc2\setup.exe
```



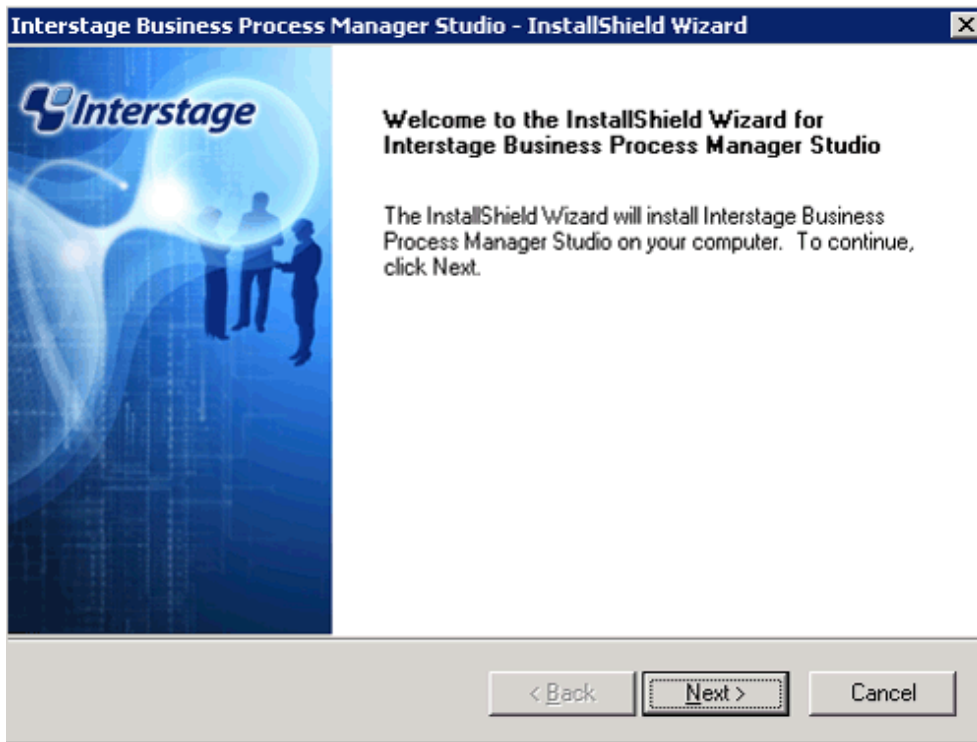
Note

The following dialog box will be displayed if exclusive software such as Systemwalker Runbook Automation Studio and Interstage BPM Studio for Systemwalker, or a standalone product such as Interstage BPM Studio has been installed.

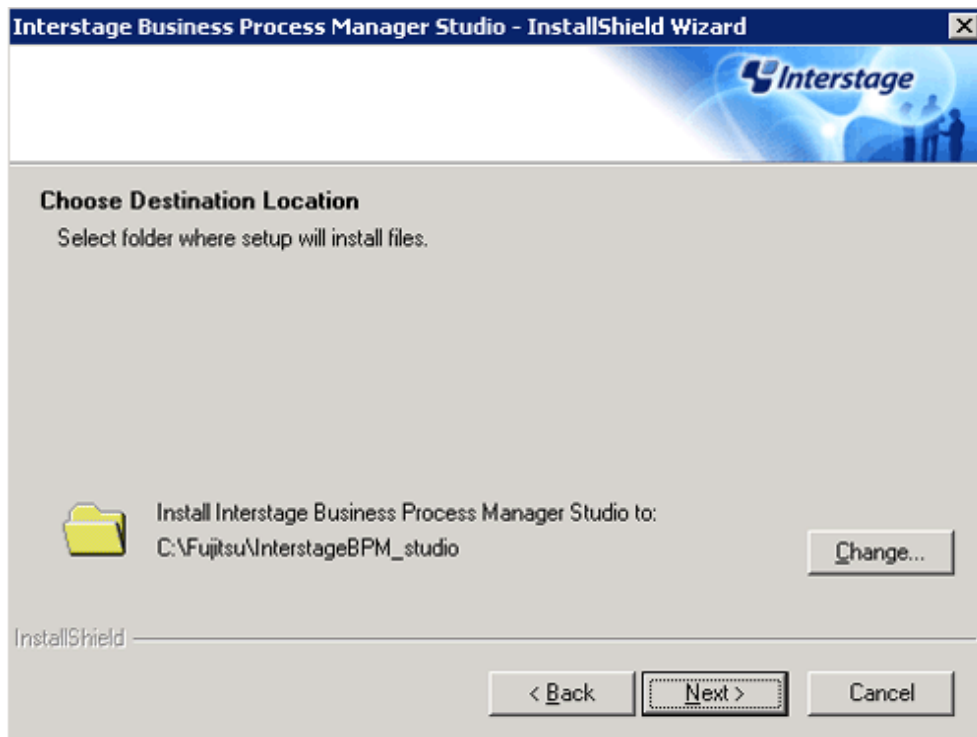


If exclusive software is installed, build the dashboard development environment after uninstalling the exclusive software or build the dashboard development environment on a separate Windows machine.

2. Click **Next**.

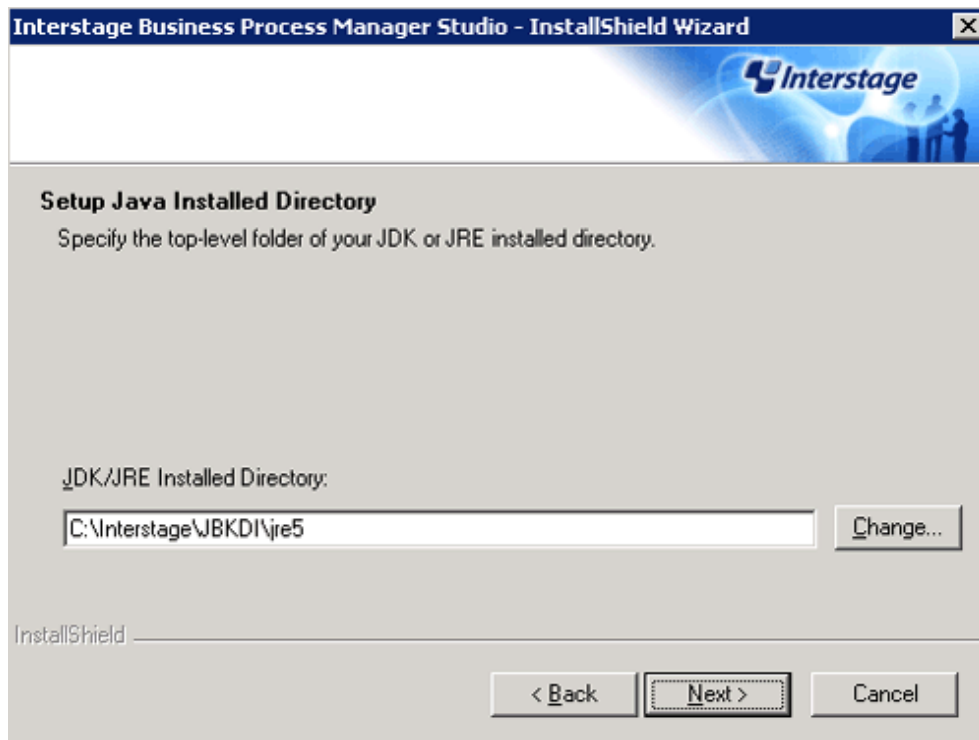


3. To change the installation folder, click **Change** and select the folder. Click **Next**.

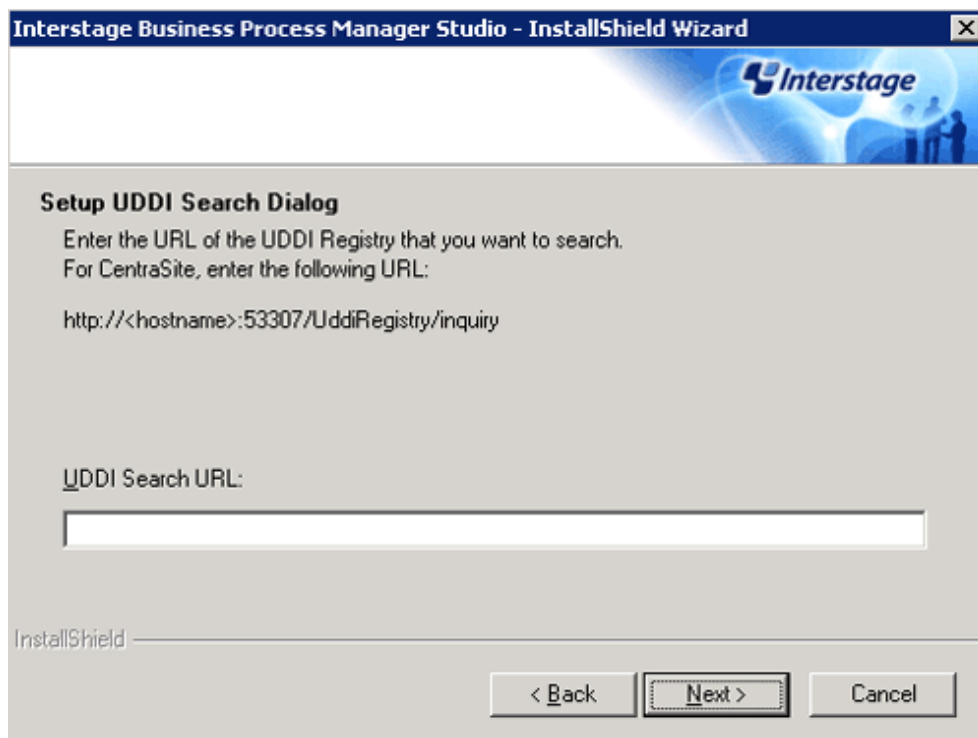


4. Check if the JDK or JRE folder is set correctly. If it is not set properly, set either one of the following and click **Next**:
 - *<Installation folder for this product>\IAPS\JDK5*

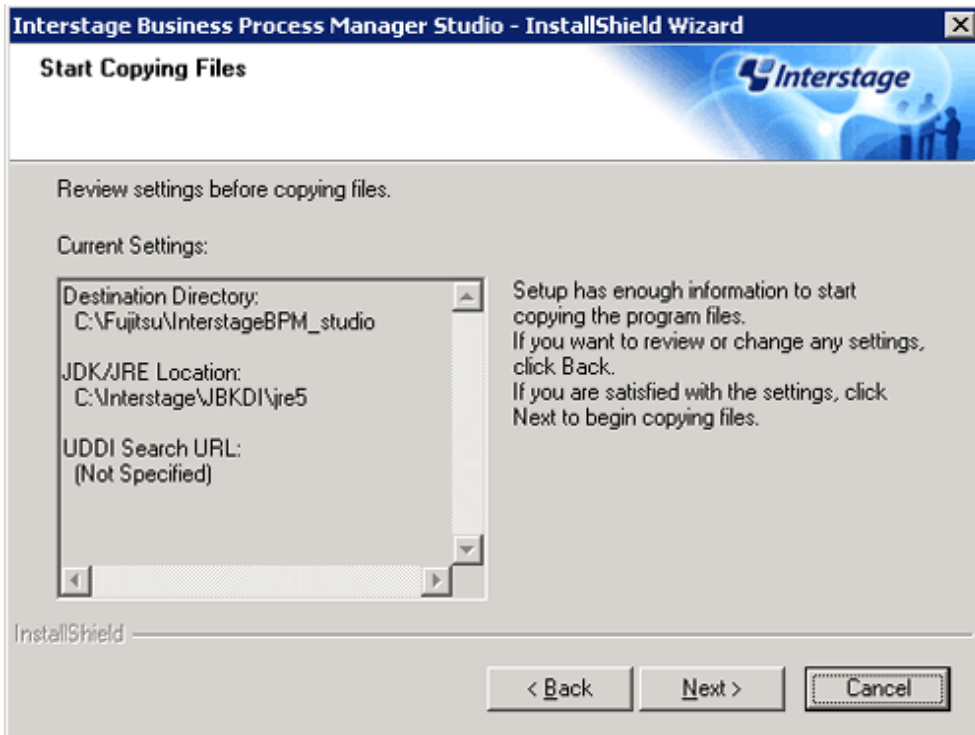
- <Installation folder specified when JRE5.0 was installed>\JBKDI\jre5



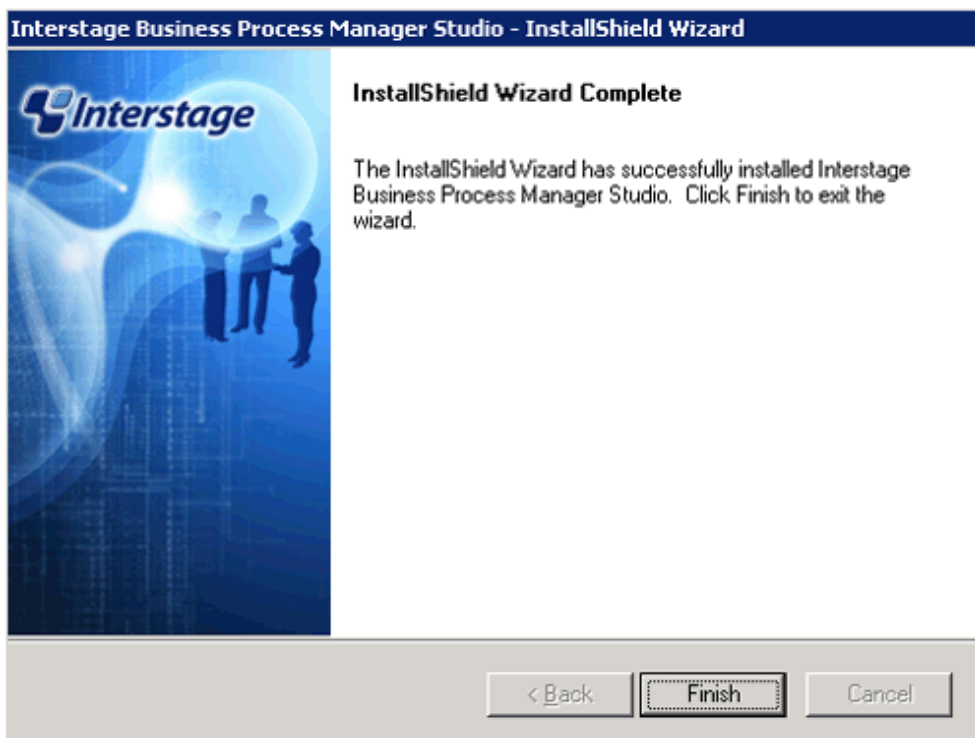
5. Do not enter anything in **UDDI Search URL** and click **Next**.



6. Click **Next**.



7. Click **Finish** when installation is completed.



Install Interstage BPM Analytics Studio

Install Analytics Studio.

1. Execute the following file:

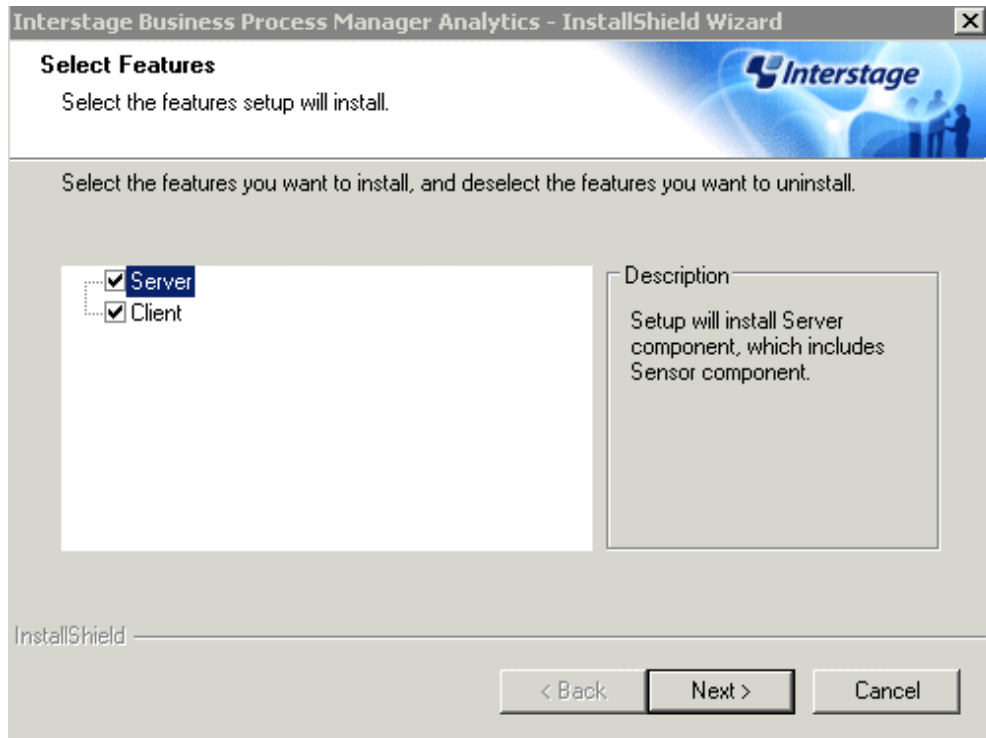
[Windows]

DVD-ROM drive:\DISK3\Manager_Extended\Windows\Install\RCXCTMG\Disc3\IBPMM\setup.exe

[Linux]

DVD-ROM drive:\unified\Disc5\ibpma\Client\IBPMM\setup.exe

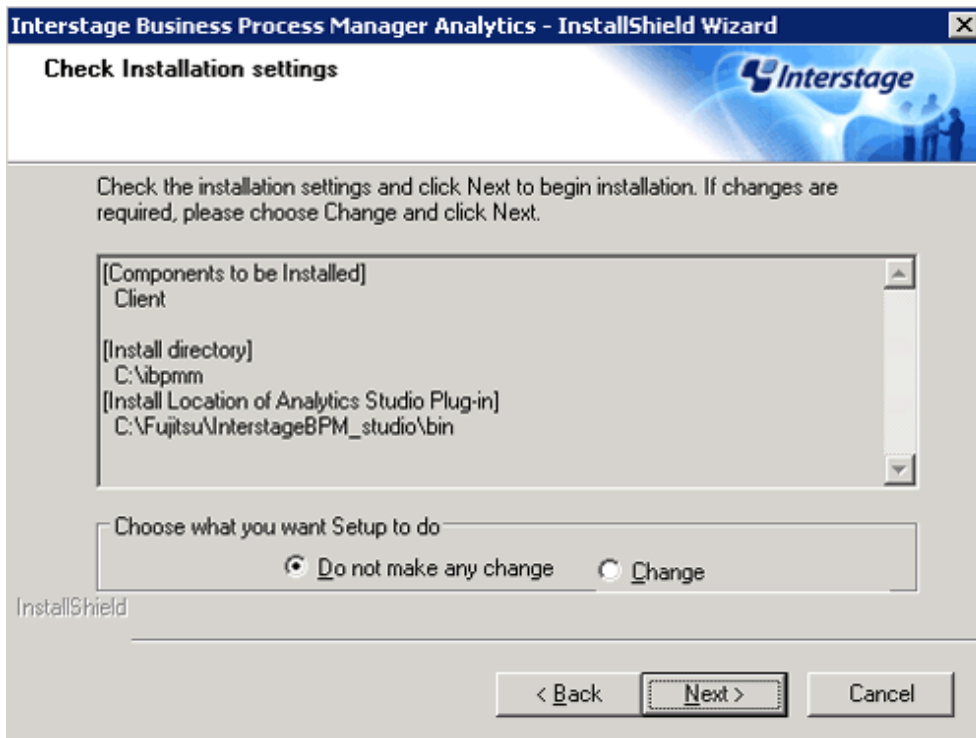
2. [Windows]Specify **Client**, and install the Interstage Business Process Manager Analytics client.



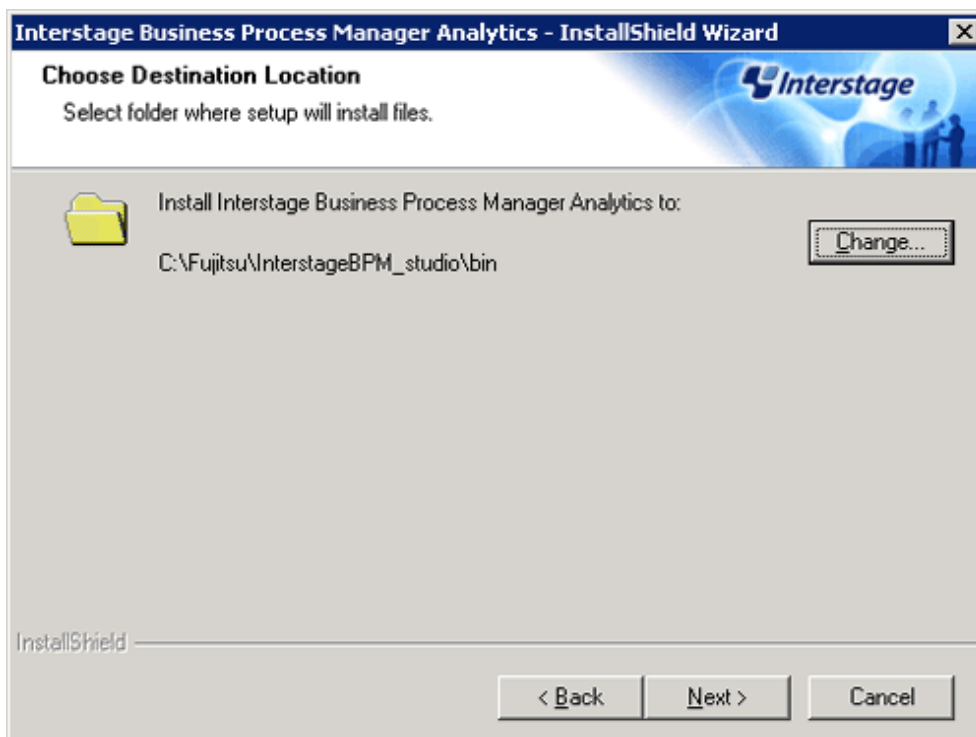
Note

When the environment is shared with the admin Server, the following window will be displayed. Select the client checkbox and click **Next**.

Do not remove the selection in **Server**.



3. The following window will be displayed, after confirming that *<BPM Studio installation folder>\bin* is specified as the **[Install Location of Analytics Studio Plug-in]**, keep the **Do not make any change** selection and click **Next**. Installation will start.

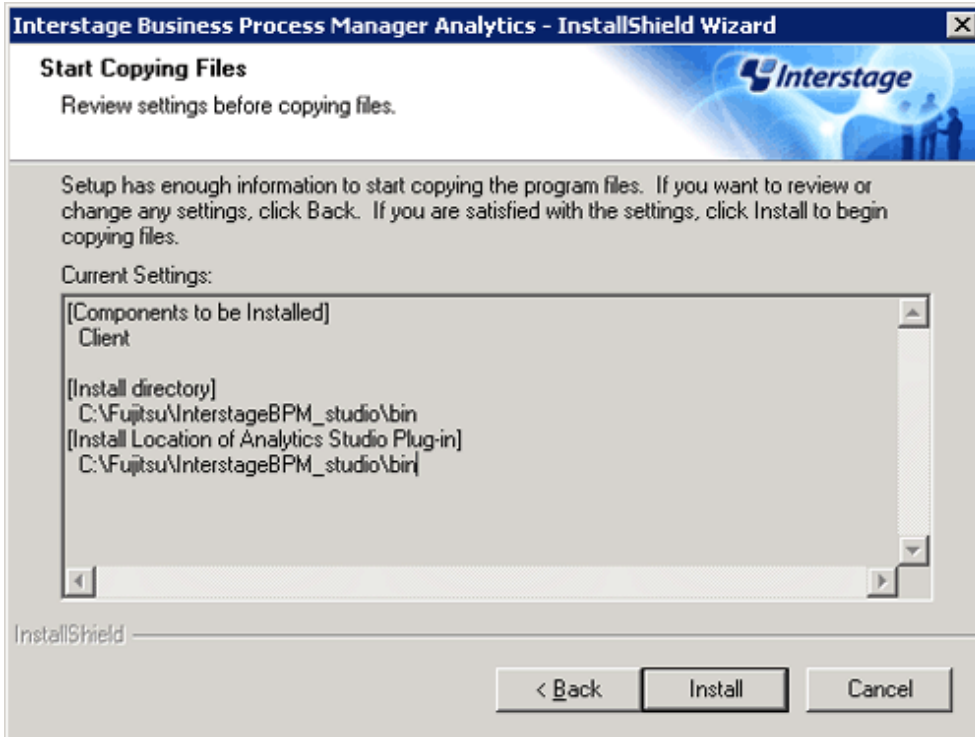


Point

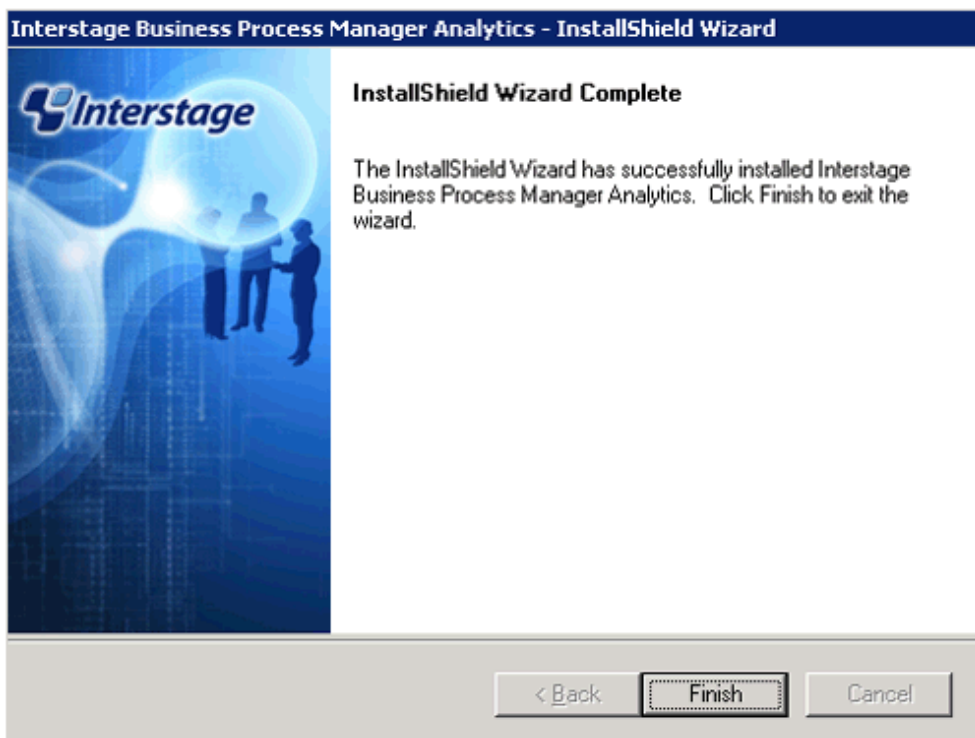
When the **[Install Location of Analytics Studio Plug-in]** is other than *<BPM Studio installation folder>\bin*, select **Change** and then click **Next**, and then select the correct installation folder.

 **Note**

The above screen will not be displayed if in the same environment as the admin server. The following screen will be displayed when proceeding with the wizard, so click the **Continue** button. Installation will start.

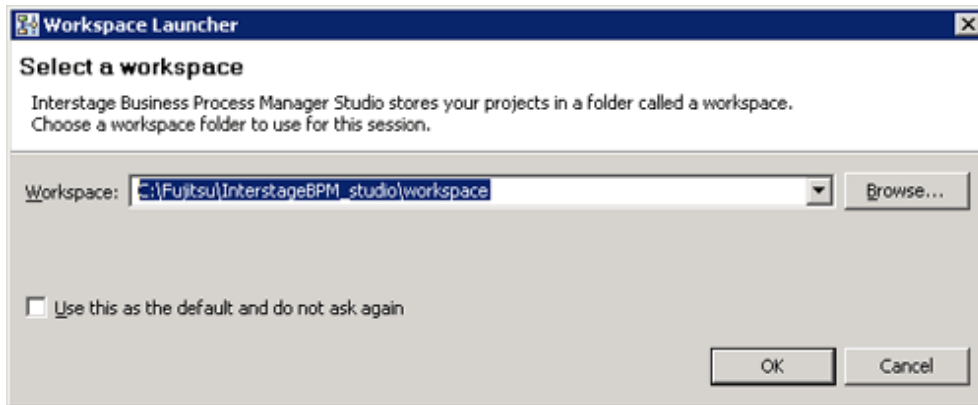


4. Click **Finish** when installation is completed.

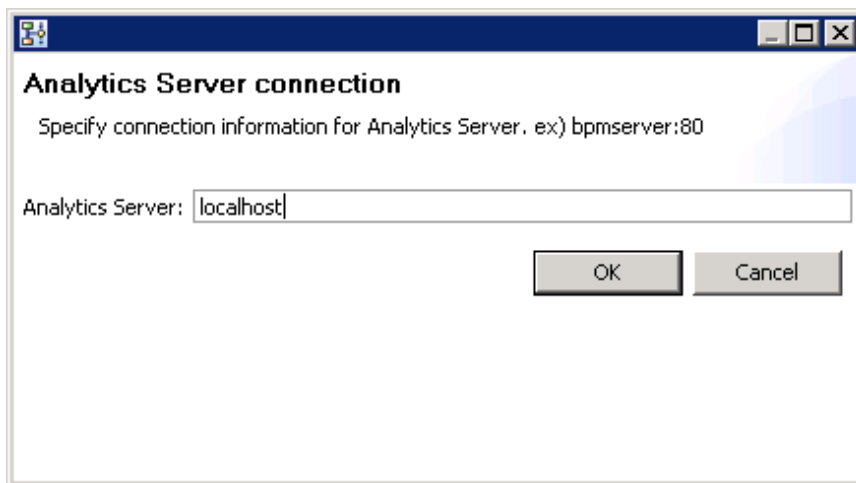


K.1.2 Setting up the Dashboard Development Environment

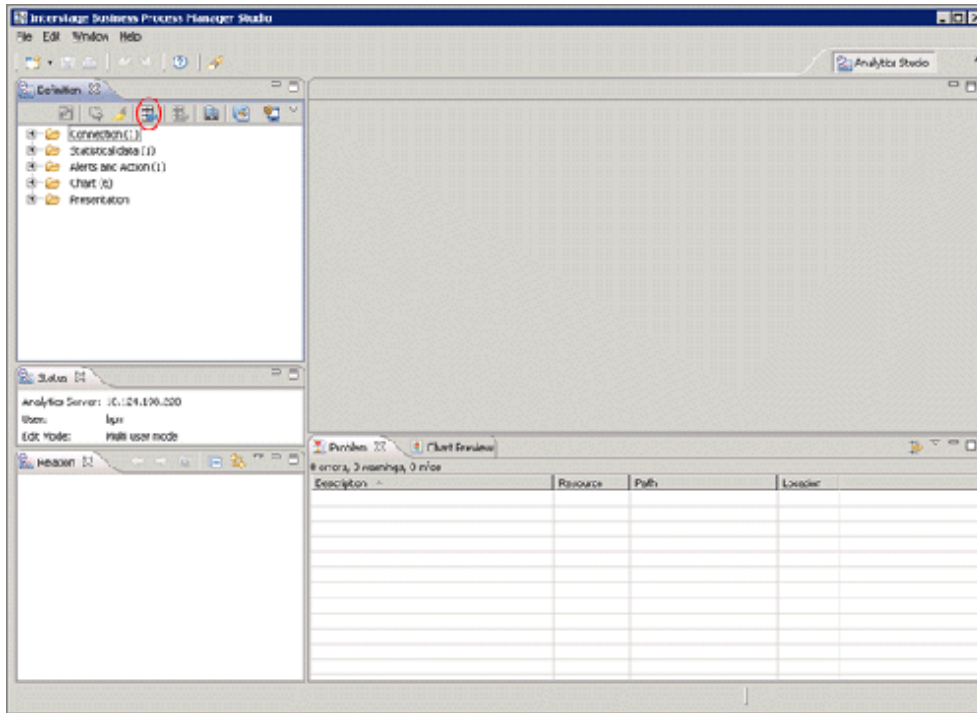
1. Perform the connection setting to the admin Server.
 - a. Select Windows **start** menu >> **Interstage Business Process Manager Studio** and then **Studio**.
 - b. The confirmation window for the work space folder will be displayed. Change the folder as required, and click the **OK** button.



- c. Select **Open Perspective** on the **Window** menu, and click **Analytics Studio**.
 - d. Enter the IP address and the port number of the admin Server in **Analytics Server**, and click the **OK** button. (If the admin Server is installed on the same machine, "localhost" may also be specified.)



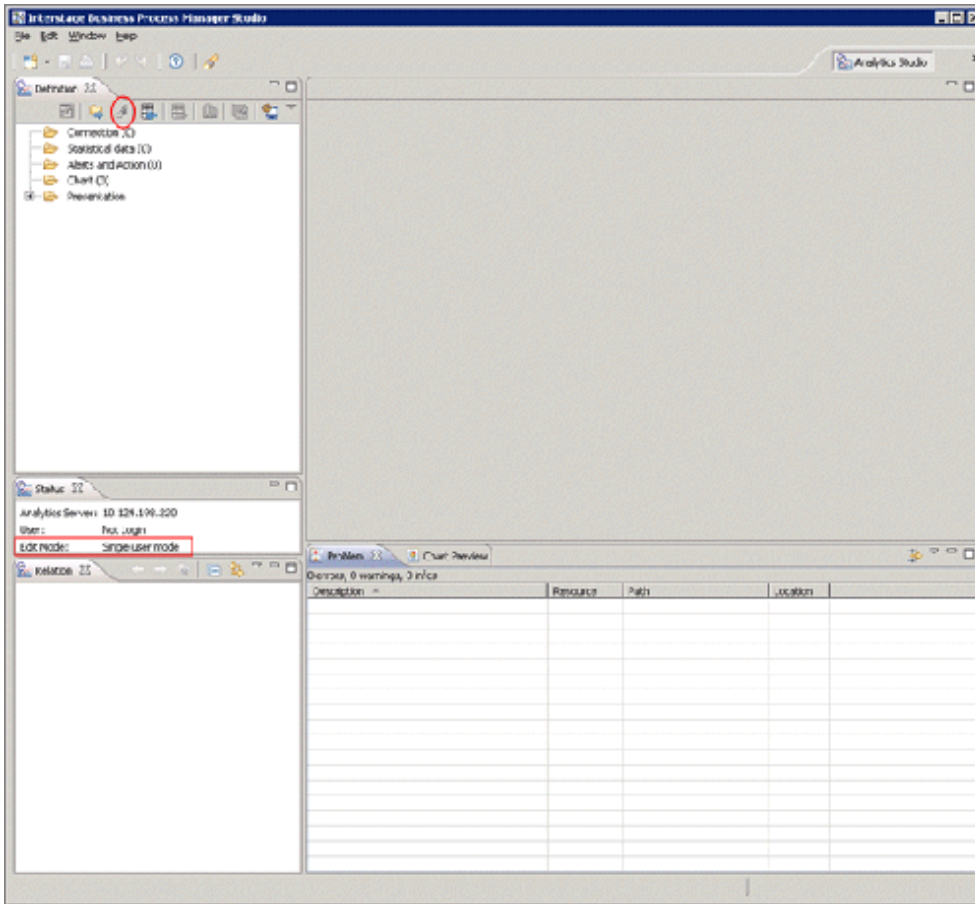
2. Click the **Reload from Server** button, and obtain the definition from the server (initial account and initial password: bpm)



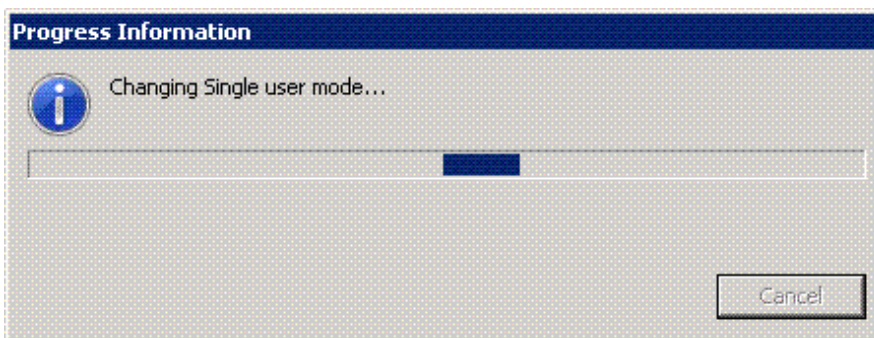
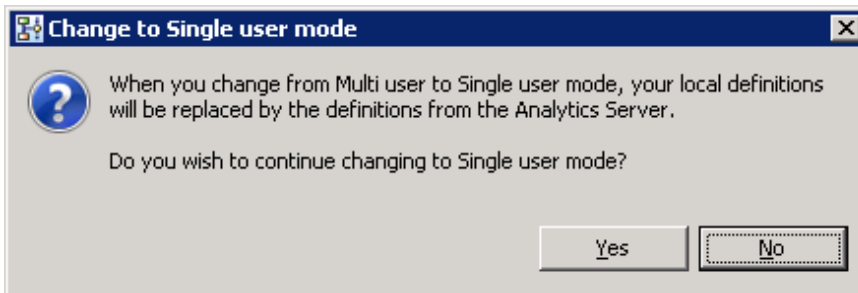
Note

The initial password must be changed. Login to the operation management console of Interstage Business Process Manager Analytics to change the initial password. Refer to Create Analytics Studio User under "1.1.1 After the first installation" in Chapter 1, "Interstage BPM Analytics Management Console" in the Interstage Business Process Manager Analytics V11.1 Management Console Guide for details.

3. If **Single user mode** is not specified in **Edit Mode**, click the **Edit Mode** icon located on the top left hand side of the window.



The processing starts by clicking the **Yes** button.



K.2 To Customize Dashboard

The following items can be customized:

- Email send settings

The send destination email address, the email subject, and the text can be set.

- Threshold values

The resource pool use rate threshold value can be set.

- Monitored pools

The resource pools to be monitored can be specified using any of the following specifications as conditions:

- Global pool for a specific resource pool

Specify any of the VM pool (CPU), the VM pool (memory), the storage pool, the network pool, the server pool, or the address pool.

- Global pool having a specific pool name

Specify any pool name.



The items above are the only customizations possible. Customization of charts or other dashboard definitions is not supported, and new definitions cannot be created.

Do not delete or modify the "@global" condition from the "Condition" of the editor view in "[K.2.3 Customizing Monitored Pools](#)".

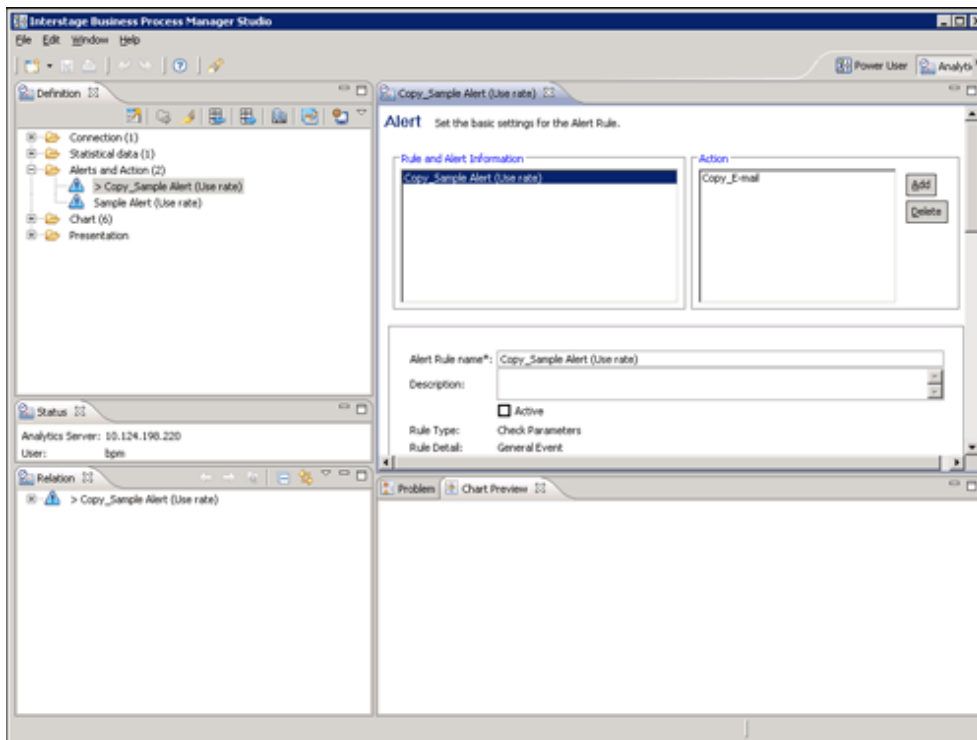
K.2.1 Customizing Email Send Settings

This section explains the procedure for customizing email send settings. It is necessary to customize email send settings. Customize threshold values and monitored pools as required.



Immediately after dashboard installation, the settings specify that email is not sent. Customize email send settings to send notifications via e-mail. Email send settings must be set in order to send alert information via email. Refer to "[6.4.6 Settings for Email Sent from the Dashboard](#)" for information on email setting for mail server.

1. Open "Alerts and Action" in the "Definition" view definition tree in the dashboard development environment.



2. From the displayed list of alert definitions, right-click "Sample Alert (Use rate)", and then select "Copy".
3. Double-click the copied "Copy_Sample Alert (Use rate)" to open the definition.
4. Change the alert rule name from "Copy_Sample Alert (Use rate)" to a suitable name.
5. Set the "Active" checkbox below the alert rule name to ON.
6. Customize threshold values as required. Refer to ["K.2.2 Customizing Threshold Values"](#) for information on changing threshold values.
7. Customize monitored Pools as required. Refer to ["K.2.3 Customizing Monitored Pools"](#) for information on changing monitored Pools.
8. Select "Copy Email" in Action at the upper-right of the editor view.
9. At **Email address**, specify the email address of the alert email send destination. Delete the email address "admin@localhost" specified as the default.

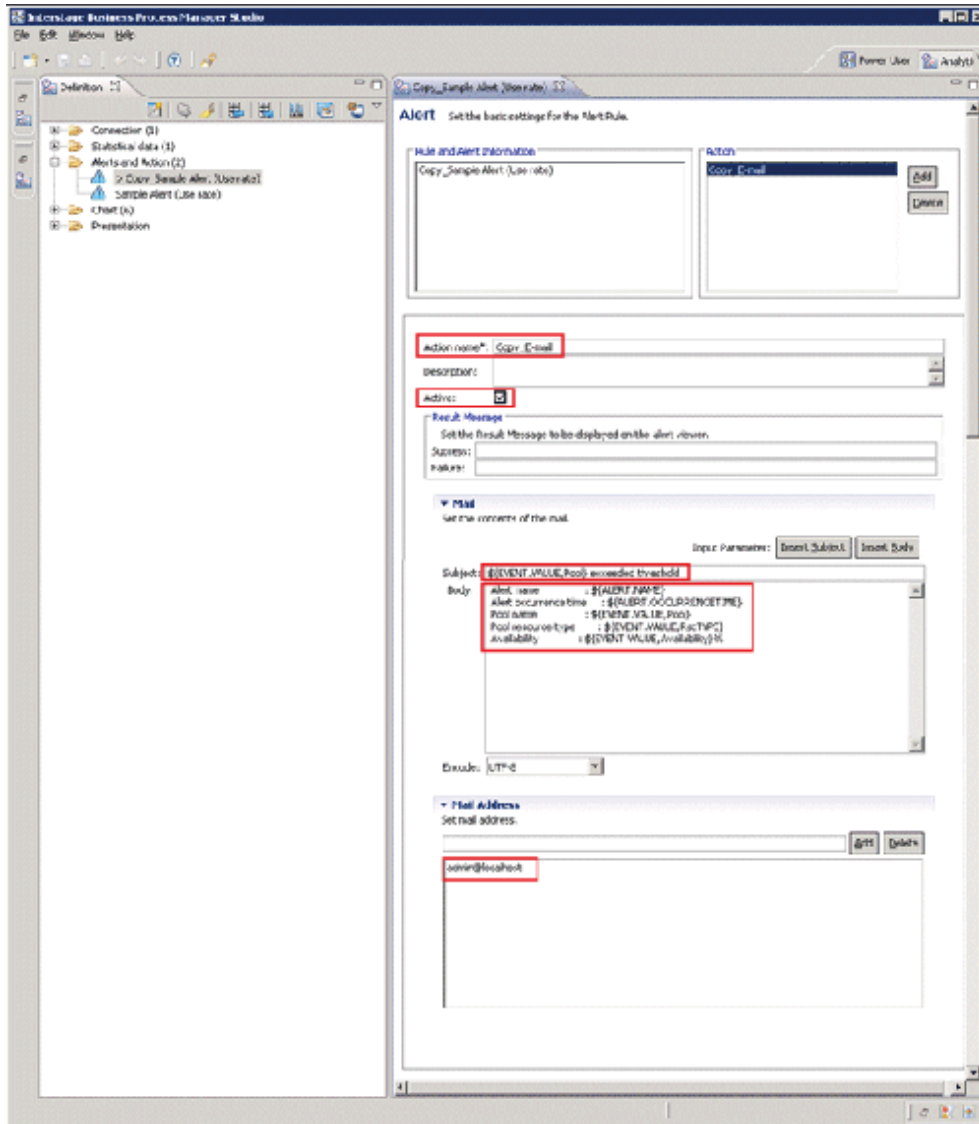
An alert email is sent as Bcc (Blind Carbon Copy), so the addresses of other addressees will not be seen by the recipient. Depending on the settings of the mail server, the "to address" (the recipient) may also be shown as "undisclosed-recipients;".

Modify the following items, as required:

- Action: Change from "Copy_Email" to a suitable name.
- Subject: "\${EVENT.VALUE,Pool} exceeded threshold" as default.
example: /VMHostPool exceeded threshold
- Body: the following items can be as default:
 - Alert name: \${ALERT.NAME}
 - Alert occurrence time: \${ALERT.OCCURRENCETIME}
 - Pool name: \${EVENT.VALUE,Pool}
 - Pool resource type: \${EVENT.VALUE,RscTYPE}
 - Availability: \${EVENT.VALUE,Availability}%

The alert parameter to be used in Subject and Body is as follows:

Variable	Description	Example
\${ALERT.NAME}	Alert Rule name	Alert (Use rate) CPU
\${ALERT.OCCURRENCETIME}	time when alerts occurred	October 14, 2011 13:05:45
\${EVENT.VALUE,Pool}	global pool name	/VMHostPool
\${EVENT.VALUE,RscTYPE}	resource type	CPU
\${EVENT.VALUE,Availability}	global pool use rate	35.5%



10. Click the **Save** icon.
11. Click the **Upload to Server** icon from the tool bar on the **Definition** view.
12. Do not select the **After uploading the Analytics Definition, replicate result in the system** checkbox but click the **OK** button.
13. Click **OK**.

- Follow the steps below to login to the operation management console of Interstage Business Process Manager Analytics, and restart the Analytics server.

- Connect to the operation management console, and login (initial password: bpm)

Access the following URL from the Web browser of the dashboard development environment, and start the operation management console of Interstage Business Process Manager Analytics.

```
http://[admin Server FQDN]/ibpmm/BPMAdminTool.do
```

- Select **BPM Analytics >> Server Management** and then **BPM Analytics Server** on the left hand side pane. Click **Stop** on the right hand side pane. After confirming **Status** has changed to **Stopped**, click **Start**.
- Confirm **Status** has changed to **Running**.

Note

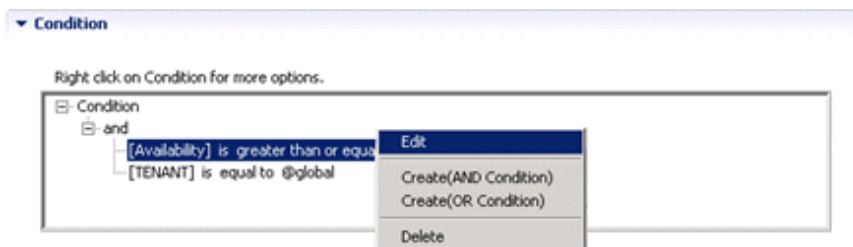
The initial password must be changed. Use the operation management console of Interstage Business Process Manager Analytics to change the initial password. Refer to "Change Administrator Password" under "1.1.1 After the first installation" in Chapter 1, "Interstage BPM Analytics Management Console" in the Interstage Business Process Manager Analytics V11.1 Management Console Guide for details.

Do not perform any operations from the operation management console other than setting passwords and the procedure described above for restarting the Interstage Business Process Manager Analytics server.

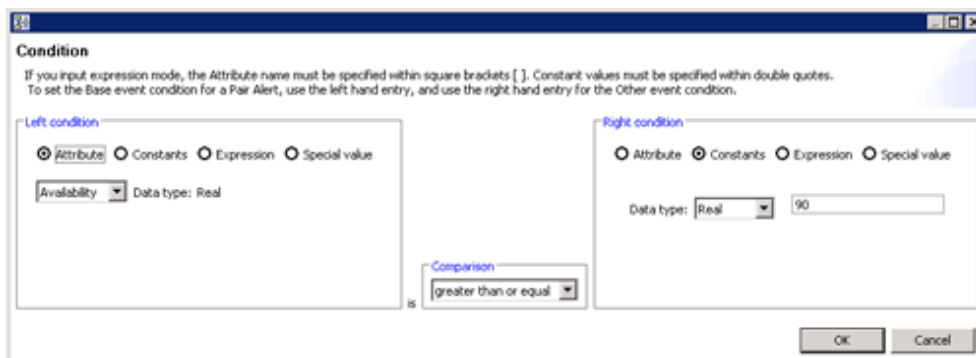
K.2.2 Customizing Threshold Values

This section explains the procedure for customizing threshold values.

- At "Condition" in the editor view, right-click a condition in the condition tree, and the select **Edit**. In the example below, "[Availability] is greater than or equal 90" is selected. The availability is the use rate.



- Use the "Right condition" radio buttons to select Constants. In the input field, enter the value to be used as the threshold value. The "Left condition" cannot be changed. In the Comparison drop-down list, select either "greater than or equal" or "greater than".

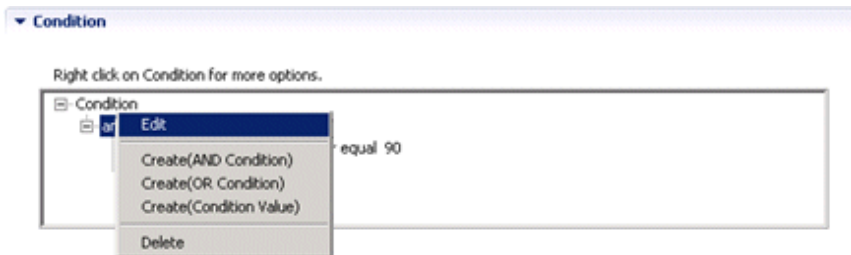


- Click the **OK** button.

K.2.3 Customizing Monitored Pools

This section explains the procedure for customizing the pools targeted for monitoring.

1. At "Condition" in the editor view right-click "and" in the condition tree, and then select "Create (Condition Value)".



2. Right-click the added "is equal to", and then select **Edit**.
3. Set the following in the conditions settings window:

- If the "Pool for a specific resource pool" alert is set:

Set the conditions below. Threshold values can be monitored for any of the VM pool (CPU), the VM pool (memory), the storage pool, the network pool, the server pool, and the address pool.

(Left-side conditions)

- Select the **Attribute** radio button.
- Select "RscTYPE" in the drop-down list.

(Right-side conditions)

- Select the "Constants" radio button.
- For the data type, select "String".
- Enter any of the following as resource types for which an alert is being set:

For VM pool (CPU) : CPU

For VM pool (memory) : MEMORY

For storage pool: STORAGE

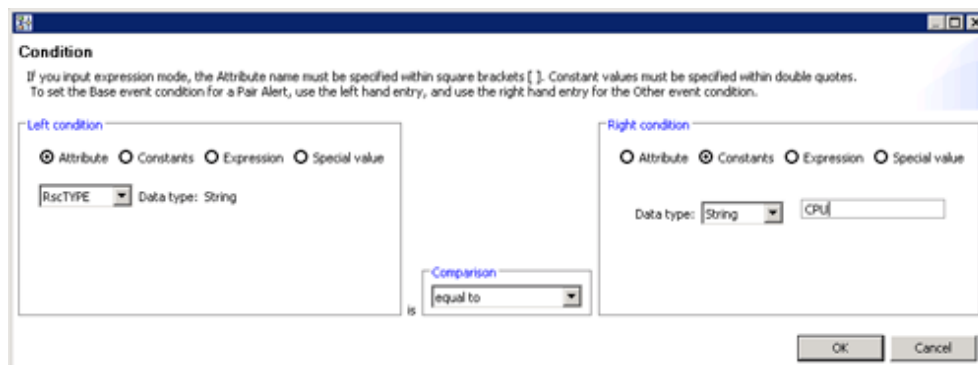
For network pool: NETWORK

For server pool: SERVERPOOL

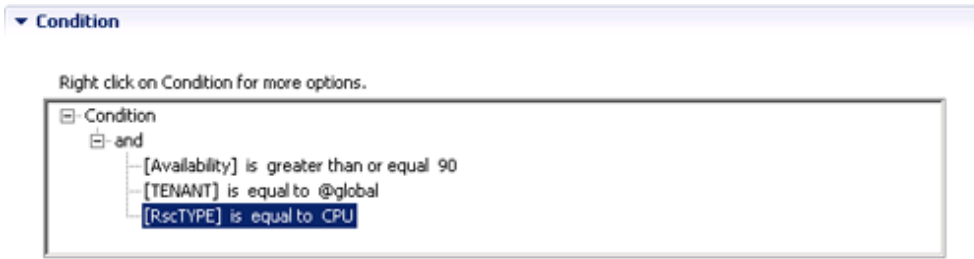
For address pool: ADDRESS

(Operator)

- In the drop-down list, select "equal to".



Set the above conditions, and then click the **OK** button. The conditions below are set.



- If the "Pool having a specific pool name" alert is set:

Set the conditions below. The pool names for which threshold values can be monitored can be specified.

(Left-side conditions)

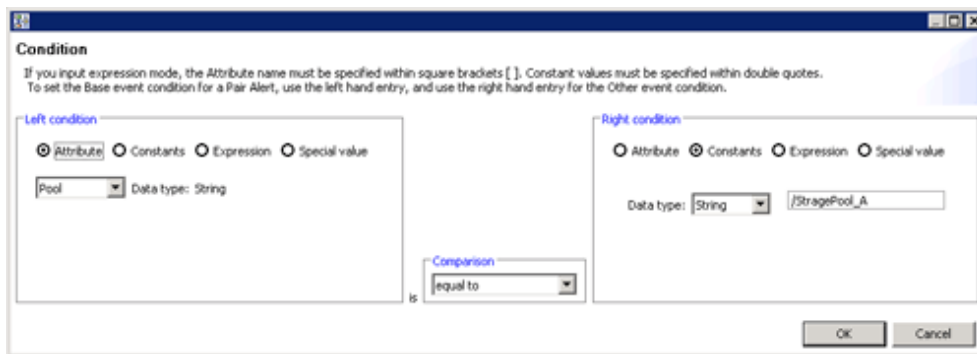
- Select the **Attribute** radio button.
- Select "Pool" in the drop-down list.

(Right-side conditions)

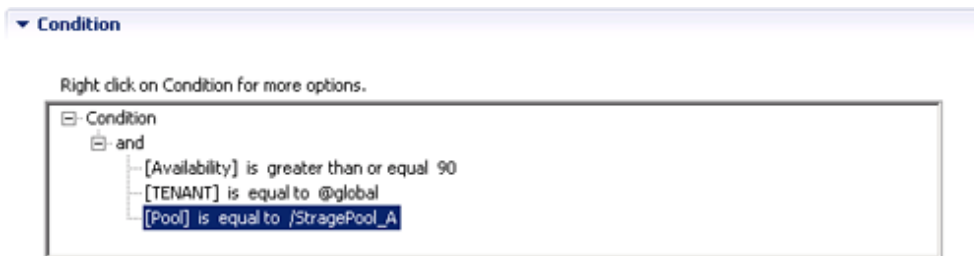
- Select the "Constants " radio button.
- For the data type, select "String".
- Specify (enter) the name of the pool for which the alert is being set.

(Operator)

- In the drop-down list, select "equal to".



Set the above conditions, and then click the **OK** button. The conditions below are set.



4. Click the **OK** button.

K.3 Backup and Restore the Dashboard Development Environment

Backup and restore of the dashboard development environment refers to the backup and restore of the definition information being edited in the dashboard development environment.

This section explains the procedure required to backup and restore the definition information.

K.3.1 Backup the Definition Information

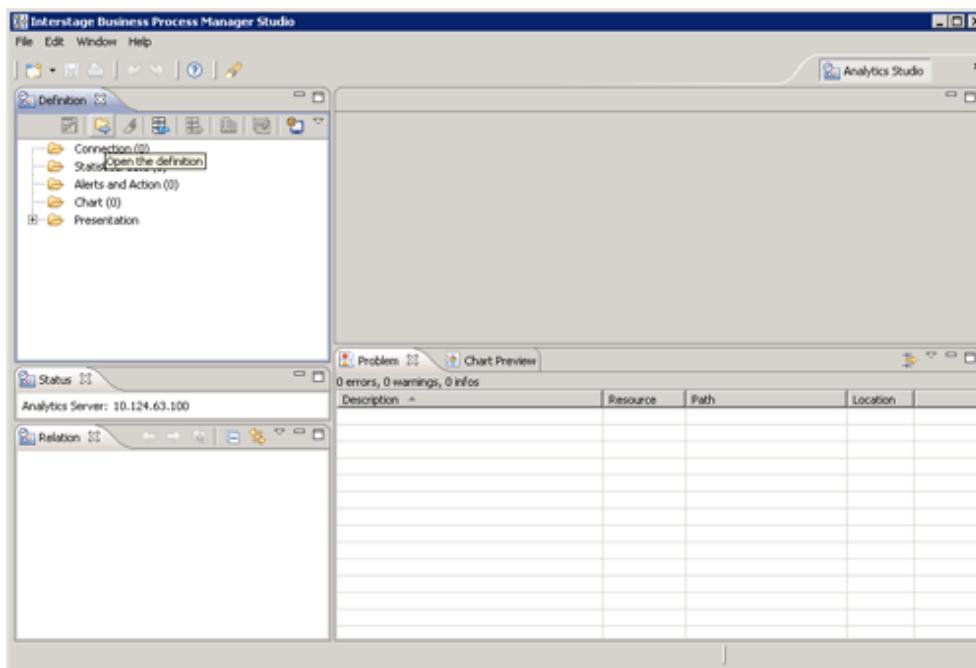
Follow the steps below to backup the definition information:

1. Close the dashboard development environment if it had been started.
2. Copy the workspace folder used in the dashboard development environment to another location without modifying it. The workspace folder that was copied becomes the backup.

K.3.2 Restore the Definition Information

Follow the steps below to restore the definition information:

1. Close the dashboard development environment if it had been started.
2. Delete the workspace folder used in the dashboard development environment if it exists.
3. Copy the backed-up workspace folder to the workspace folder used in the dashboard development environment.
4. Start the dashboard development environment.
5. Click the **Open the definition** icon.



K.4 Uninstalling the Dashboard Development Environment

Delete the dashboard development environment by uninstalling it. The uninstallation flow is shown as follows:

1. Uninstall the Interstage Business Process Manager Analytics Client
2. Uninstall Interstage Business Process Manager Studio
3. Uninstall JRE 5.0

K.4.1 Uninstall the Interstage Business Process Manager Analytics Client

[Windows]

If the dashboard development environment and the admin Server are installed on the same machine, follow the steps below to uninstall the dashboard development environment:

1. Select **Interstage Business Process Manager Analytics** from the list displayed on **Control Panel >> Uninstall or change a program**, and click the **Uninstall** button.
2. Deselect the **Client** checkbox on the **Select function** dialog box, and click **Next**.
3. A dialog box confirming the deletion of the **Client** function will be displayed. Click **Yes** and execute uninstallation.
4. After uninstallation is completed, delete the work area for the dashboard development environment. Delete the following directory:

```
<Workspace selected when BPM Studio was started>\Interstage BPM Analytics
```

When the dashboard development environment is installed on a different machine from where the admin Server is installed, uninstall the dashboard development environment by following the same procedure as that for [Linux].

[Linux]

1. Select **Interstage Business Process Manager Analytics** from the list displayed on **Control Panel >> Add or Remove Programs**, and click the **Remove** button.
2. Uninstall by following the confirmation dialog boxes.
3. After uninstallation is completed, delete the work area for the dashboard development environment. Delete the following directory:

```
<Workspace selected when BPM Studio was started>\Interstage BPM Analytics
```



Information

Refer to the following manual for details:

- Interstage Business Process Manager Analytics V11.1 Installation Guide



Note

When both the admin Server and the dashboard development environment are built on the same machine and both of these are to be uninstalled, the clients of Interstage Business Process Manager Analytics are also uninstalled when the admin Server is uninstalled. Tasks discussed in this section are therefore not required.

K.4.2 Uninstall Interstage Business Process Manager Studio

1. Select **Interstage Business Process Manager Studio** from the list displayed on **Control Panel >> Uninstall or change a program**, and click the **Uninstall** button.
2. Uninstall by following the confirmation dialog boxes.

K.4.3 Uninstall JRE 5.0

1. Select **Interstage Application Server V9.3.0 Client Package** from the list displayed on **Control panel >> Uninstall or change a program**, and click the **Uninstall/Change** button.
2. Uninstall by following the confirmation dialog boxes.

Appendix L Co-Existence with ServerView Deployment Manager

This appendix explains how to use both Resource Orchestrator and ServerView Deployment Manager on the same network.

L.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.

Figure L.1 System Configuration Example (Separate Server Installation)

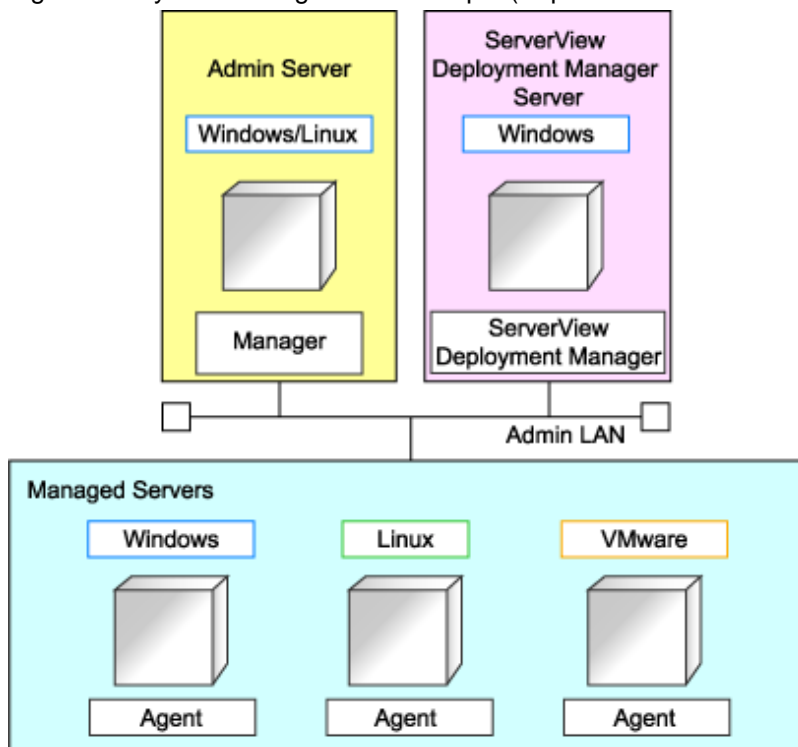
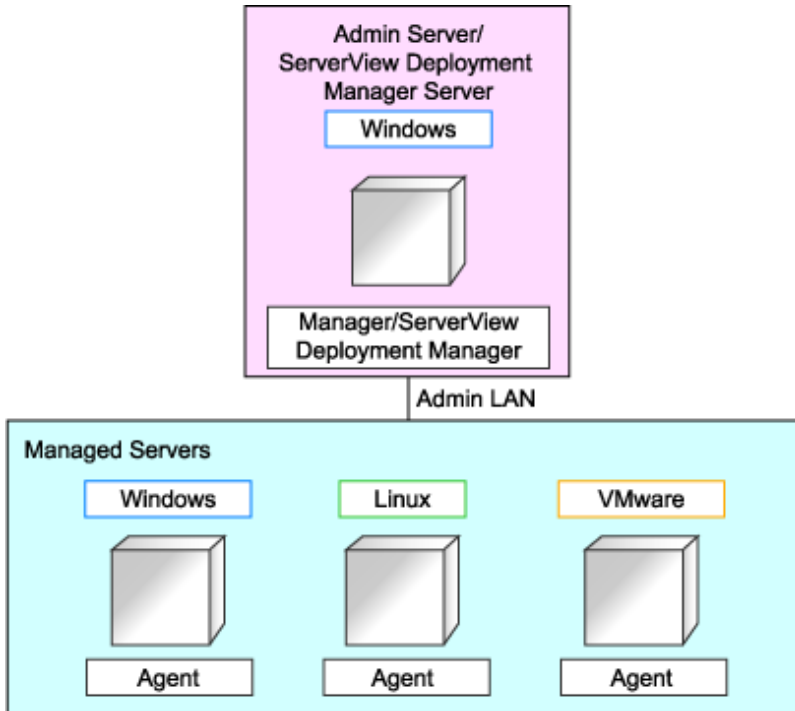


Figure L.2 System Configuration Example (Single Server Installation)



L.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)

In Resource Orchestrator, the switchover of VIOM 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 (for I/O virtualization)

Glossary

access path

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

active mode

The state where a managed server is performing operations.

Managed servers must be in active mode in order to use Auto-Recovery.

Move managed servers to maintenance mode in order to perform backup or restoration of system images, or collection or deployment of cloning images.

active server

A physical server that is currently operating.

admin client

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

admin LAN

A LAN used to manage resources from admin servers.

It connects managed servers, storage, and network devices.

admin server

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

affinity group

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

Equivalent to the LUN mapping of EMC.

agent

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

aggregate

A unit for managing storage created through the aggregation of a RAID group.

Aggregates can contain multiple FlexVols.

alias name

A name set for each ETERNUS LUN to distinguish the different ETERNUS LUNs.

Auto Deploy

A function for deploying VMware ESXi5.0 to servers using the PXE boot mechanism.

Automatic Storage Layering

A function that optimizes perform and cost by automatically rearranging data in storage units based on the frequency of access.

Auto-Recovery

A function which continues operations by automatically switching over the system image of a failed server to a spare server and restarting it in the event of server failure.

This function can be used when managed servers are in a local boot configuration, SAN boot configuration, or a configuration such as iSCSI boot where booting is performed from a disk on a network.

- When using a local boot configuration

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

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

The system is restored by having the spare server inherit the system image on the storage.

Also, when a VLAN is set for the public LAN of a managed server, the VLAN settings of adjacent LAN switches are automatically switched to those of the spare server.

backup site

An environment prepared in a different location, which is used for data recovery.

BACS (Broadcom Advanced Control Suite)

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

BASP (Broadcom Advanced Server Program)

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

blade server

A compact server device with a thin chassis that can contain multiple server blades, and has low power consumption.

As well as server blades, LAN switch blades, management blades, and other components used by multiple server blades can be mounted inside the chassis.

blade type

A server blade type.

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

BladeViewer

A GUI that displays the status of blade servers in a style similar to a physical view and enables intuitive operation.

BladeViewer can also be used for state monitoring and operation of resources.

BMC (Baseboard Management Controller)

A Remote Management Controller used for remote operation of servers.

boot agent

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

CA (Channel Adapter)

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

CCM (ETERNUS SF AdvancedCopy Manager Copy Control Module)

This is a module that does not require installation of the ETERNUS SF AdvancedCopy Manager agent on the server that is the source of the backup, but rather uses the advanced copy feature of the ETERNUS disk array to make backups.

chassis

A chassis used to house server blades and partitions.

Sometimes referred to as an enclosure.

cloning

Creation of a copy of a system disk.

cloning image

A backup of a system disk, which does not contain server-specific information (system node name, IP address, etc.), made during cloning.

When deploying a cloning image to the system disk of another server, Resource Orchestrator automatically changes server-specific information to that of the target server.

Cloud Edition

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

data center

A facility that manages client resources (servers, storage, networks, etc.), and provides internet connections and maintenance/operational services.

directory service

A service for updating and viewing the names (and associated attributes) of physical/logical resource names scattered across networks, based on organizational structures and geographical groups using a systematic (tree-shaped structure) management methodology.

disk resource

The unit for resources to connect to an L-Server. An example being a virtual disk provided by LUN or VM management software.

DN (Distinguished Name)

A name defined as a line of an RDN, which contains an entry representing its corresponding object and higher entry.

Domain

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

DR Option

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

Dual-Role Administrators

The administrators with both infrastructure administrator's and tenant administrator's role.

dynamic LUN mirroring

This is a feature whereby a mirror volume is generated at the remote site when a volume is generated at the local site, and copies are maintained by performing REC.

dynamic memory

A function that optimizes physical memory allocation for virtual machines, depending on their execution status on Hyper-V.

end host mode

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

environmental data

Measured data regarding the external environments of servers managed using Resource Orchestrator.

Measured data includes power data collected from power monitoring targets.

ESC (ETERNUS SF Storage Cruiser)

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

ETERNUS SF AdvancedCopy Manager

This is storage management software that makes highly reliable and rapid backups, restorations and replications using the advanced copy feature of the ETERNUS disk array.

Express

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

FC switch (Fibre Channel Switch)

A switch that connects Fibre Channel interfaces and storage devices.

Fibre Channel

A method for connecting computers and peripheral devices and transferring data.

Generally used with servers requiring high-availability, to connect computers and storage systems.

Fibre Channel port

The connector for Fibre Channel interfaces.

When using ETERNUS storage, referred to as an FC-CA port, when using NetApp storage, referred to as an FC port, when using EMC CLARiON, referred to as an SP port, when using EMC Symmetrix DMX or EMC Symmetrix VMAX, referred to as a DIRECTOR port.

fibre channel switch blade

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

FlexVol

A function that uses aggregates to provide virtual volumes.

Volumes can be created in an instant.

FTRP

The pool for physical disks created by Automatic Storage Layering for ETERNUS.

In Resource Orchestrator, FTRPs are used as virtual storage resources on which Thin Provisioning attributes are configured.

FTV

The virtual volumes created by Automatic Storage Layering for ETERNUS.

In Resource Orchestrator, FTVs are used as disk resources on which Thin Provisioning attributes are configured.

global pool

A resource pool that contains resources that can be used by multiple tenants.

It is located in a different location from the tenants.

By configuring a global pool with the attributes of a tenant, it becomes possible for tenant administrators to use the pool.

GLS (Global Link Services)

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

GSPB (Giga-LAN SAS and PCI_Box Interface Board)

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

GUI (Graphical User Interface)

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

HA (High Availability)

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

hardware initiator

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

hardware maintenance mode

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

HBA (Host Bus Adapter)

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

HBA address rename setup service

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

HBAAR (HBA address rename)

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

host affinity

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

Hyper-V

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

I/O virtualization option

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

IBP (Intelligent Blade Panel)

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

ICT governance

A collection of principles and practices that encourage desirable behavior in the use of ICT (Information and Communication Technology) based on an evaluation of the impacts and risks posed in the adoption and application of ICT within an organization or community.

ILOM (Integrated Lights Out Manager)

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

image file

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

infrastructure administrator

A user who manages the resources comprising a data center.

infra_admin is the role that corresponds to the users who manage resources.

Infrastructure administrators manage all of the resources comprising a resource pool (the global pool and local pools), provide tenant administrators with resources, and review applications by tenant users to use resources.

IPMI (Intelligent Platform Management Interface)

IPMI is a set of common interfaces for the hardware that is used to monitor the physical conditions of servers, such as temperature, power voltage, cooling fans, power supply, and chassis.

These functions provide information that enables system management, recovery, and asset management, which in turn leads to reduction of overall TCO.

IQN (iSCSI Qualified Name)

Unique names used for identifying iSCSI initiators and iSCSI targets.

iRMC (integrated Remote Management Controller)

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

iSCSI

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

iSCSI boot

A configuration function that enables the starting and operation of servers via a network.

The OS and applications used to operate servers are stored on iSCSI storage, not the internal disks of servers.

iSCSI storage

Storage that uses an iSCSI connection.

LAG (Link Aggregation Group)

A single logical port created from multiple physical ports using link aggregation.

LAN switch blades

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

LDAP (Lightweight Directory Access Protocol)

A protocol used for accessing Internet standard directories operated using TCP/IP.

LDAP provides functions such as direct searching and viewing of directory services using a web browser.

license

The rights to use specific functions.

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

link aggregation

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

By using this function, it becomes possible to use a band equal to the total of the bands of all the ports.

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

local pool

A resource pool that contains resources that can only be used by a specific tenant.

They are located in tenants.

logical volume

A logical disk that has been divided into multiple partitions.

L-Platform

A resource used for the consolidated operation and management of systems such as multiple-layer systems (Web/AP/DB) comprised of multiple L-Servers, storage, and network devices.

L-Platform template

A template that contains the specifications for servers, storage, network devices, and images that are configured for an L-Platform.

LSB (Logical System Board)

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

L-Server

A resource defined using the logical specifications (number of CPUs, amount of memory, disk capacity, number of NICs, etc.) of the servers, and storage and network devices connected to those servers.

An abbreviation of Logical Server.

L-Server template

A template that defines the number of CPUs, memory capacity, disk capacity, and other specifications for resources to deploy to an L-Server.

LUN (Logical Unit Number)

A logical unit defined in the channel adapter of a storage unit.

MAC address (Media Access Control address)

A unique identifier that is assigned to Ethernet cards (hardware).

Also referred to as a physical address.

Transmission of data is performed based on this identifier. Described using a combination of the unique identifying numbers managed by/assigned to each maker by the IEEE, and the numbers that each maker assigns to their hardware.

maintenance mode

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

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

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

managed server

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

management blade

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

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

Management Board

The PRIMEQUEST system management unit.

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

manager

The section (program) of Resource Orchestrator that operates on admin servers. It manages and controls resources registered with Resource Orchestrator.

master slot

A slot that is recognized as a server when a server that occupies multiple slots is mounted.

member server

A collective term that refers to a server in a Windows network domain that is not a domain controller.

migration

The migration of a VM guest to a different VM host. The following two types of migration are available:

- Cold migration
Migration of an inactive (powered-off) VM guest.
- Live migration
Migration of an active (powered-on) VM guest.

multi-slot server

A server that occupies multiple slots.

NAS (Network Attached Storage)

A collective term for storage that is directly connected to a LAN.

network device

The unit used for registration of network devices. L2 switches and firewalls fit into this category.

network map

A GUI function for graphically displaying the connection relationships of the servers and LAN switches that compose a network.

network view

A window that displays the connection relationships and status of the wiring of a network map.

NFS (Network File System)

A system that enables the sharing of files over a network in Linux environments.

NIC (Network Interface Card)

An interface used to connect a server to a network.

OS

The OS used by an operating server (a physical OS or VM guest).

overcommit

A function to virtually allocate more resources than the actual amount of resources (CPUs and memory) of a server. This function is used to enable allocation of more disk resources than are mounted in the target server.

PDU (Power Distribution Unit)

A device for distributing power (such as a power strip). Resource Orchestrator uses PDUs with current value display functions as Power monitoring devices.

physical LAN segment

A physical LAN that servers are connected to.

Servers are connected to multiple physical LAN segments that are divided based on their purpose (public LANs, backup LANs, etc.). Physical LAN segments can be divided into multiple network segments using VLAN technology.

physical network adapter

An adapter, such as a LAN, to connect physical servers or VM hosts to a network.

physical OS

An OS that operates directly on a physical server without the use of server virtualization software.

physical server

The same as a "server". Used when it is necessary to distinguish actual servers from virtual servers.

pin-group

This is a group, set with the end host mode, that has at least one uplink port and at least one downlink port.

Pool Master

On Citrix XenServer, it indicates one VM host belonging to a Resource Pool.

It handles setting changes and information collection for the Resource Pool, and also performs operation of the Resource Pool.

For details, refer to the Citrix XenServer manual.

port backup

A function for LAN switches which is also referred to as backup port.

port VLAN

A VLAN in which the ports of a LAN switch are grouped, and each LAN group is treated as a separate LAN.

port zoning

The division of ports of fibre channel switches into zones, and setting of access restrictions between different zones.

power monitoring devices

Devices used by Resource Orchestrator to monitor the amount of power consumed.

PDUs and UPSs with current value display functions fit into this category.

power monitoring targets

Devices from which Resource Orchestrator can collect power consumption data.

pre-configuration

Performing environment configuration for Resource Orchestrator on another separate system.

primary server

The physical server that is switched from when performing server switchover.

primary site

The environment that is usually used by Resource Orchestrator.

private cloud

A private form of cloud computing that provides ICT services exclusively within a corporation or organization.

public LAN

A LAN used for operations by managed servers.
Public LANs are established separately from admin LANs.

rack

A case designed to accommodate equipment such as servers.

rack mount server

A server designed to be mounted in a rack.

RAID (Redundant Arrays of Inexpensive Disks)

Technology that realizes high-speed and highly-reliable storage systems using multiple hard disks.

RAID management tool

Software that monitors disk arrays mounted on PRIMERGY servers.
The RAID management tool differs depending on the model or the OS of PRIMERGY servers.

RDM (Raw Device Mapping)

A function of VMware. This function provides direct access from a VMware virtual machine to a LUN.

RDN (Relative Distinguished Name)

A name used to identify the lower entities of a higher entry.
Each RDN must be unique within the same entry.

Remote Management Controller

A unit used for managing servers.
Used for gathering server data, failure notification, power control, etc.

- For Fujitsu PRIMERGY servers
iRMC2
 - For SPARC Enterprise
ILOM (T series servers)
XSCF (M series servers)
 - For HP servers
iLO2 (integrated Lights-Out)
 - For Dell/IBM servers
BMC (Baseboard Management Controller)
-

Remote Server Management

A PRIMEQUEST feature for managing partitions.

Reserved SB

Indicates the new system board that will be embedded to replace a failed system board if the hardware of a system board embedded in a partition fails and it is necessary to disconnect the failed system board.

resource

General term referring to the logical definition of the hardware (such as servers, storage, and network devices) and software that comprise a system.

resource folder

An arbitrary group of resources.

resource pool

A unit for management of groups of similar resources, such as servers, storage, and network devices.

resource tree

A tree that displays the relationships between the hardware of a server and the OS operating on it using hierarchies.

role

A collection of operations that can be performed.

ROR console

The GUI that enables operation of all functions of Resource Orchestrator.

ruleset

A collection of script lists for performing configuration of network devices, configured as combinations of rules based on the network device, the purpose, and the application.

SAN (Storage Area Network)

A specialized network for connecting servers and storage.

SAN boot

A configuration function that enables the starting and operation of servers via a SAN.

The OS and applications used to operate servers are stored on SAN storage, not the internal disks of servers.

SAN storage

Storage that uses a Fibre Channel connection.

script list

Lists of scripts for the automation of operations such as status and log display, and definition configuration of network devices.

Used to execute multiple scripts in one operation. The scripts listed in a script list are executed in the order that they are listed.

As with individual scripts, they can be created by the infrastructure administrator, and can be customized to meet the needs of tenant administrators.

They are used to configure virtual networks for VLANs on physical networks, in cases where it is necessary to perform auto-configuration of multiple switches at the same time, or to configure the same rules for network devices in redundant configurations.

The script lists contain the scripts used to perform automatic configuration.

There are the following eight types of script lists:

- script lists for setup
- script lists for setup error recovery
- script lists for modification
- script lists for modification error recovery
- script lists for setup (physical server added)
- script lists for setup error recovery (physical server added)
- script lists for deletion (physical server deleted)
- script lists for deletion

server

A computer (operated with one operating system).

server blade

A server blade has the functions of a server integrated into one board.
They are mounted in blade servers.

server management unit

A unit used for managing servers.
A management blade is used for blade servers, and a Remote Management Controller is used for other servers.

server name

The name allocated to a server.

server NIC definition

A definition that describes the method of use for each server's NIC.
For the NICs on a server, it defines which physical LAN segment to connect to.

server virtualization software

Basic software which is operated on a server to enable use of virtual machines. Used to indicate the basic software that operates on a PC server.

ServerView Deployment Manager

Software used to collect and deploy server resources over a network.

ServerView Operations Manager

Software that monitors a server's (PRIMERGY) hardware state, and notifies of errors by way of the network.
ServerView Operations Manager was previously known as ServerView Console.

ServerView RAID

One of the RAID management tools for PRIMERGY.

ServerView Update Manager

This is software that performs jobs such as remote updates of BIOS, firmware, drivers, and hardware monitoring software on servers being managed by ServerView Operations Manager.

ServerView Update Manager Express

Insert the ServerView Suite DVD1 or ServerView Suite Update DVD into the server requiring updating and start it.

This is software that performs batch updates of BIOS, firmware, drivers, and hardware monitoring software.

Single Sign-On

A system among external software which can be used without login operations, after authentication is executed once.

slave slot

A slot that is not recognized as a server when a server that occupies multiple slots is mounted.

SMB (Server Message Block)

A protocol that enables the sharing of files and printers over a network.

SNMP (Simple Network Management Protocol)

A communications protocol to manage (monitor and control) the equipment that is attached to a network.

software initiator

An initiator processed by software using OS functions.

Solaris Container

Solaris server virtualization software.

On Solaris servers, it is possible to configure multiple virtual Solaris servers that are referred to as a Solaris zone.

Solaris zone

A software partition that virtually divides a Solaris OS space.

SPARC Enterprise Partition Model

A SPARC Enterprise model which has a partitioning function to enable multiple system configurations, separating a server into multiple areas with operating OS's and applications in each area.

spare server

A server which is used to replace a failed server when server switchover is performed.

storage blade

A blade-style storage device that can be mounted in the chassis of a blade server.

storage management software

Software for managing storage units.

storage resource

Collective term that refers to virtual storage resources and disk resources.

storage unit

Used to indicate the entire secondary storage as one product.

surrogate pair

A method for expressing one character as 32 bits.

In the UTF-16 character code, 0xD800 - 0xDBFF are referred to as "high surrogates", and 0xDC00 - 0xDFFF are referred to as "low surrogates". Surrogate pairs use "high surrogate" + "low surrogate".

switchover state

The state in which switchover has been performed on a managed server, but neither fallback nor continuation have been performed.

System Board

A board which can mount up to 2 Xeon CPUs and 32 DIMMs.

system disk

The disk on which the programs (such as the OS) and files necessary for the basic functions of servers (including booting) are installed.

system image

A copy of the contents of a system disk made as a backup.

Different from a cloning image as changes are not made to the server-specific information contained on system disks.

tenant

A unit for the division and segregation of management and operation of resources based on organizations or operations.

tenant administrator

A user who manages the resources allocated to a tenant.

tenant_admin is the role for performing management of resources allocated to a tenant.

Tenant administrators manage the available space on resources in the local pools of tenants, and approve or reject applications by tenant users to use resources.

tenant folder

A resource folder that is created for each tenant, and is used to manage the resources allocated to a tenant.

L-Servers and local pools are located in tenant folders. Also, it is possible to configure a global pool that tenant administrators can use.

tenant user

A user who uses the resources of a tenant, or creates and manages L-Platforms, or a role with the same purpose.

Thick Provisioning

Allocation of the actual requested capacity when allocating storage resources.

Thin Provisioning

Allocating of only the capacity actually used when allocating storage resources.

tower server

A standalone server with a vertical chassis.

TPP (Thin Provisioning Pool)

One of resources defined using ETERNUS. Thin Provisioning Pools are the resource pools of physical disks created using Thin Provisioning.

TPV (Thin Provisioning Volume)

One of resources defined using ETERNUS. Thin Provisioning Volumes are physical disks created using the Thin Provisioning function.

UNC (Universal Naming Convention)

Notational system for Windows networks (Microsoft networks) that enables specification of shared resources (folders, files, shared printers, shared directories, etc.).



Example

.....
\\hostname\dir_name
.....

UPS (Uninterruptible Power Supply)

A device containing rechargeable batteries that temporarily provides power to computers and peripheral devices in the event of power failures.

Resource Orchestrator uses UPSs with current value display functions as power monitoring devices.

URL (Uniform Resource Locator)

The notational method used for indicating the location of information on the Internet.

VIOM (ServerView Virtual-IO Manager)

The name of both the I/O virtualization technology used to change the MAC addresses of NICs and the software that performs the virtualization.

Changes to values of WWNs and MAC addresses can be performed by creating a logical definition of a server, called a server profile, and assigning it to a server.

Virtual Edition

The edition that can use the server switchover function.

Virtual I/O

Technology that virtualizes the relationship of servers and I/O devices (mainly storage and network) thereby simplifying the allocation of and modifications to I/O resources to servers, and server maintenance.

For Resource Orchestrator it is used to indicate HBA address rename and ServerView Virtual-IO Manager (VIOM).

virtual server

A virtual server that is operated on a VM host using a virtual machine.

virtual storage resource

This refers to a resource that can dynamically create a disk resource.

An example being RAID groups or logical storage that is managed by server virtualization software (such as VMware datastores).

In Resource Orchestrator, disk resources can be dynamically created from ETERNUS RAID groups, NetApp aggregates, and logical storage managed by server virtualization software.

virtual switch

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

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

A function provided by server virtualization software in order to manage L-Server (VM) networks as virtual LAN switches.

Management of relationships between virtual L-Server NICs, and physical server NICs operating on VM hosts, can be performed using an operation similar to the connection of a normal LAN switch.

VLAN (Virtual LAN)

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

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

VLAN ID

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

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

VM (Virtual Machine)

A virtual computer that operates on a VM host.

VM guest

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

VM Home Position

The VM host that is home to VM guests.

VM host

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

VM maintenance mode

One of the settings of server virtualization software, that enables maintenance of VM hosts.

For example, when using high availability functions (such as VMware HA) of server virtualization software, by setting VM maintenance mode it is possible to prevent the moving of VM guests on VM hosts undergoing maintenance.

For details, refer to the manuals of the server virtualization software being used.

VM management software

Software for managing multiple VM hosts and the VM guests that operate on them.

Provides value adding functions such as movement between the servers of VM guests (migration).

VMware

Virtualization software from VMware Inc.

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

VMware DPM (VMware Distributed Power Management)

A function of VMware. This function is used to reduce power consumption by automating power management of servers in VMware DRS clusters.

VMware DRS (VMware Distributed Resource Scheduler)

A function of VMware. This function is used to monitor the load conditions on an entire virtual environment and optimize the load dynamically.

VMware Teaming

A function of VMware. By using VMware Teaming it is possible to perform redundancy by connecting a single virtual switch to multiple physical network adapters.

Web browser

A software application that is used to view Web pages.

WWN (World Wide Name)

A 64-bit address allocated to an HBA.

Refers to a WWNN or a WWPN.

WWNN (World Wide Node Name)

A name that is set as a common value for the Fibre Channel ports of a node. However, the definitions of nodes vary between manufacturers, and may also indicate devices or adapters. Also referred to as a node WWN.

WWPN (World Wide Port Name)

A name that is a unique value and is set for each Fibre Channel port (HBA, CA, fibre channel switch ports, etc.), and is the IEEE global MAC address.

As the Fibre Channel ports of the same WWPN are unique, they are used as identifiers during Fibre Channel port login. Also referred to as a port WWN.

WWPN zoning

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

Xen

A type of server virtualization software.

XSB (eXtended System Board)

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

XSCF (eXtended System Control Facility)

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

zoning

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