ServerView Resource Orchestrator Cloud Edition V3.1.0

Design Guide

Windows/Linux

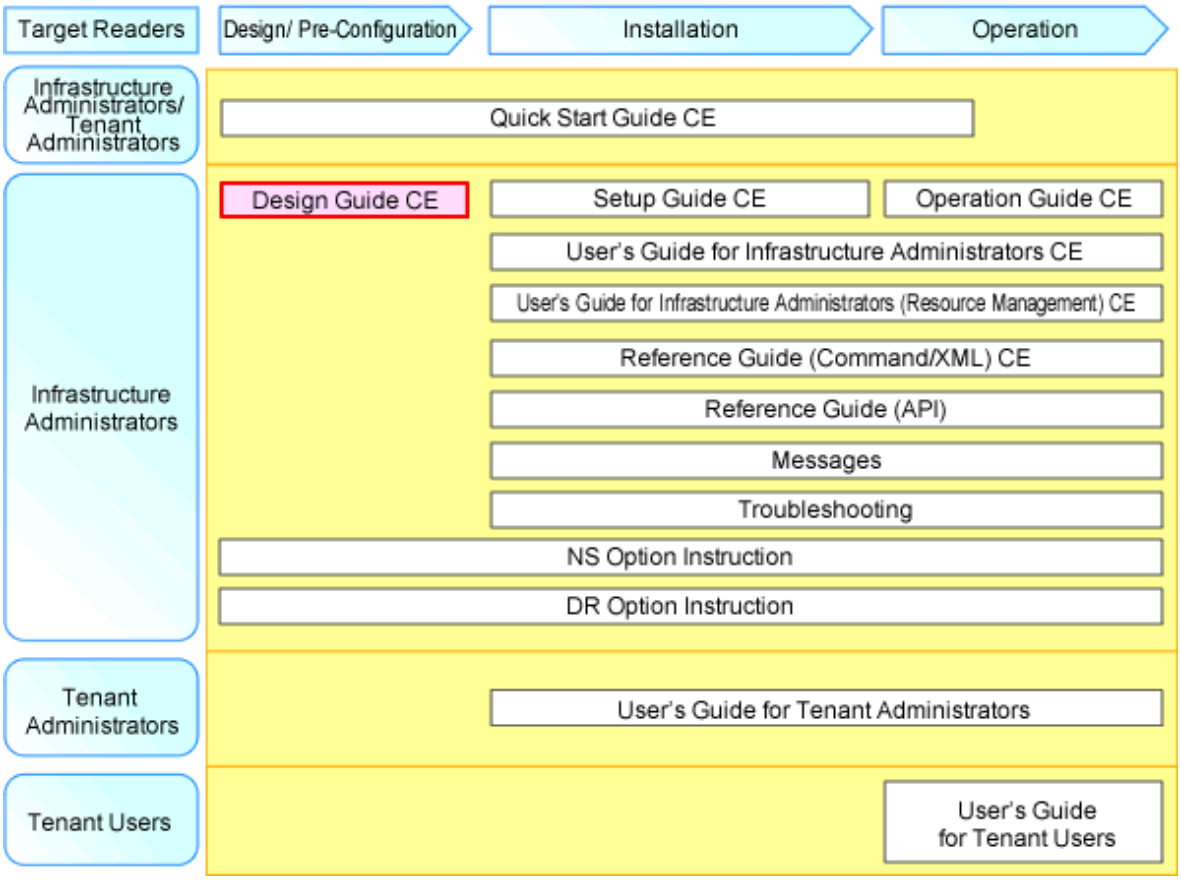
J2X1-7673-02ENZ0(01)
January 2014

Preface

Resource Orchestrator Documentation Road Map

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

Resource Orchestrator Documentation Road Map



Point

Refer to the user role manuals displayed in the table below for roles that are not in the diagram.

Roles that are not in the diagram	Roles that are in the diagram
Infrastructure operator Infrastructure monitor	Infrastructure administrator
Tenant operator Tenant monitor	Tenant administrator
(Dual-Role) Administrator (Dual-Role) Operator (Dual-Role) Monitor	Infrastructure administrator and Tenant administrator

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

Purpose

This manual provides an outline of ServerView Resource Orchestrator (hereinafter Resource Orchestrator) and the design and preparations 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:

Chapter 1 Documentation Road Map

Explains the documentation road map, and how to read it.

Chapter 2 Overview

Provides an overview of Resource Orchestrator.

Chapter 3 Flow of Resource Orchestrator Design and Preparations

Explains the flow of design and preparations for Resource Orchestrator.

Chapter 4 System Configuration Design

Explains points to keep in mind when setting up a Resource Orchestrator environment.

Chapter 5 Defining User Accounts

Explains the user accounts used in Resource Orchestrator.

Chapter 6 Defining Tenants and Resource Pools

Explains how to design tenants and resource pools.

Chapter 7 Defining High Availability and Disaster Recovery

High availability is realized by using the following functions.

Chapter 8 Defining and Configuring the Server Environment

Explains how to define and configure server environments.

Chapter 9 Defining and Configuring the Network Environment

Explains how to define and pre-configure the network environment.

Chapter 10 Deciding and Configuring the Storage Environment

Explains how to decide and configure the storage environment.

Chapter 11 Deciding and Configuring Server Virtualization Software

Explains how to decide and configure server virtualization software.

Chapter 12 Installing and Defining Single Sign-On

When installing Resource Orchestrator, a Single Sign-On environment can be configured. This section explains the necessary preparations.

Chapter 13 Deciding and Configuring the Power Monitoring Environment

Explains how to decide and configure the power monitoring environment.

Appendix A Port List

Explains the ports used by Resource Orchestrator.

Appendix B HTTPS Communications

Explains the HTTPS communication protocol used by Resource Orchestrator and its security features.

Appendix C Hardware Configuration

Explains how to configure hardware.

Appendix D Preparations for Creating a Physical L-Server

Explains how to perform design and configuration when creating a physical L-Server.

Appendix E Preparations for Creating a Virtual L-Server

Explains how to perform design and configuration when creating a virtual L-Server.

Appendix F Preparing for Automatic Configuration and Operation of Network Devices

Explains how to prepare for automatic configuration of network devices and operation.

Appendix G Sample Script for Automatic Configuration and Operation of Network Devices

Explains the sample scripts provided with Resource Orchestrator for performing automatic configuration of network devices and other operations.

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 Manager]	Sections related to Windows manager
[Linux Manager]	Sections related to Linux manager
[Windows]	Sections related to Windows (When not using Hyper-V)
[Linux]	Sections related to Linux
[Solaris]	Sections related to Solaris or Solaris Containers
[VMware]	Sections related to VMware
[Hyper-V]	Sections related to Hyper-V
[Xen]	Sections related to RHEL5-Xen
[KVM]	Sections related to RHEL-KVM
[Solaris Containers]	Sections related to Solaris containers
[Oracle VM]	Sections related to Oracle VM
[Physical Servers]	Sections related to physical servers
[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.
- Oracle Solaris may also be indicated as Solaris, Solaris Operating System, or Solaris OS.
- References and character strings or values requiring emphasis are indicated using double quotes (").
- Window names, dialog names, menu names, and tab names are shown enclosed by brackets ([ ]).
- Button names are shown enclosed by angle brackets (< >) or square brackets ([ ]).
- The order of selecting menus is indicated using [ ]-[ ].
- Text to be entered by the user is indicated using bold text.

- Variables are indicated using italic text and underscores.
- The ellipses ("...") in menu names, indicating settings and operation window startup, are not shown.
- The ">" used in Windows is included in usage examples. When using Linux, read ">" as meaning "#".
- The URLs in this manual were correct when the manual was written.

Menus in the ROR console

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

Regarding Installation Folder Paths

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

Replace it as shown below.

When using Windows 64-bit (x64)

C:\Program Files (x86)\Resource Orchestrator

When using Windows 32-bit (x86)

C:\Program Files\Resource Orchestrator

Abbreviations

The following abbreviations are used in this manual:

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

Abbreviation	Products
	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) Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.7 (for x86) Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.8 (for x86) Red Hat(R) Enterprise Linux(R) 5.8 (for Intel64) Red Hat(R) Enterprise Linux(R) 6.2 (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) 5.8 (for x86) Red Hat(R) Enterprise Linux(R) 5.8 (for Intel64) Red Hat(R) Enterprise Linux(R) 6.2 (for x86) Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64)

Abbreviation	Products
Red Hat Enterprise Linux 5	Red Hat(R) Enterprise Linux(R) 5 (for x86) Red Hat(R) Enterprise Linux(R) 5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.1 (for x86) Red Hat(R) Enterprise Linux(R) 5.1 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.2 (for x86) Red Hat(R) Enterprise Linux(R) 5.2 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.3 (for x86) Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.4 (for x86) Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.6 (for x86) Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.7 (for x86) Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.8 (for x86) Red Hat(R) Enterprise Linux(R) 5.8 (for Intel64)
Red Hat Enterprise Linux 6	Red Hat(R) Enterprise Linux(R) 6.2 (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
GLS	PRIMECLUSTER GLS
Navisphere	EMC Navisphere Manager
Solutions Enabler	EMC Solutions Enabler
MSFC	Microsoft Failover Cluster
Solaris	Solaris(TM) 10 Operating System
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 ESX	VMware(R) ESX(R)
VMware ESX 4	VMware(R) ESX(R) 4
VMware ESXi	VMware(R) ESXi(TM)
VMware ESXi 5.0	VMware(R) ESXi(TM) 5.0
VMware Tools	VMware(R) Tools
VMware vSphere 4.0	VMware vSphere(R) 4.0
VMware vSphere 4.1	VMware vSphere(R) 4.1
VMware vSphere 5	VMware vSphere(R) 5

Abbreviation	Products
VMware vSphere Client	VMware vSphere(R) Client
VMware vCenter Server	VMware(R) vCenter(TM) Server
VMware vClient	VMware(R) vClient(TM)
VMware FT	VMware(R) Fault Tolerance
VMware DRS	VMware(R) Distributed Resource Scheduler
VMware DPM	VMware(R) Distributed Power Management
VMware vDS	VMware(R) vNetwork Distributed Switch
VMware Storage VMotion	VMware(R) Storage VMotion
VIOM	ServerView Virtual-IO Manager
BladeLogic	BMC BladeLogic Server Automation
ServerView Agent	ServerView SNMP Agents for MS Windows (32bit-64bit) ServerView Agents Linux ServerView Agents VMware for VMware ESX Server
RCVE	ServerView Resource Coordinator VE
ROR	ServerView Resource Orchestrator
ROR VE	ServerView Resource Orchestrator Virtual Edition
ROR CE	ServerView Resource Orchestrator Cloud Edition
Resource Coordinator	Systemwalker Resource Coordinator 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

- 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
July 2012, First Edition	J2X1-7673-01ENZ0(00)
October 2012, Second Edition	J2X1-7673-02ENZ0(00)
January 2014, 2.1	J2X1-7673-02ENZ0(01)

Contents

Chapter 1 Documentation Road Map

For the documentation road map, refer to "Chapter1 Documentation Road Map" in the "ServerView Resource Orchestrator Cloud Edition V3.1.0 Quick Start Guide CE".

Chapter 2 Overview

This chapter provides an overview of Resource Orchestrator.

2.1 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 (*), as resource pools. By simplifying the launch, expansion, and change of business operations, this software provides quick support for evolving businesses.

* Note: 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

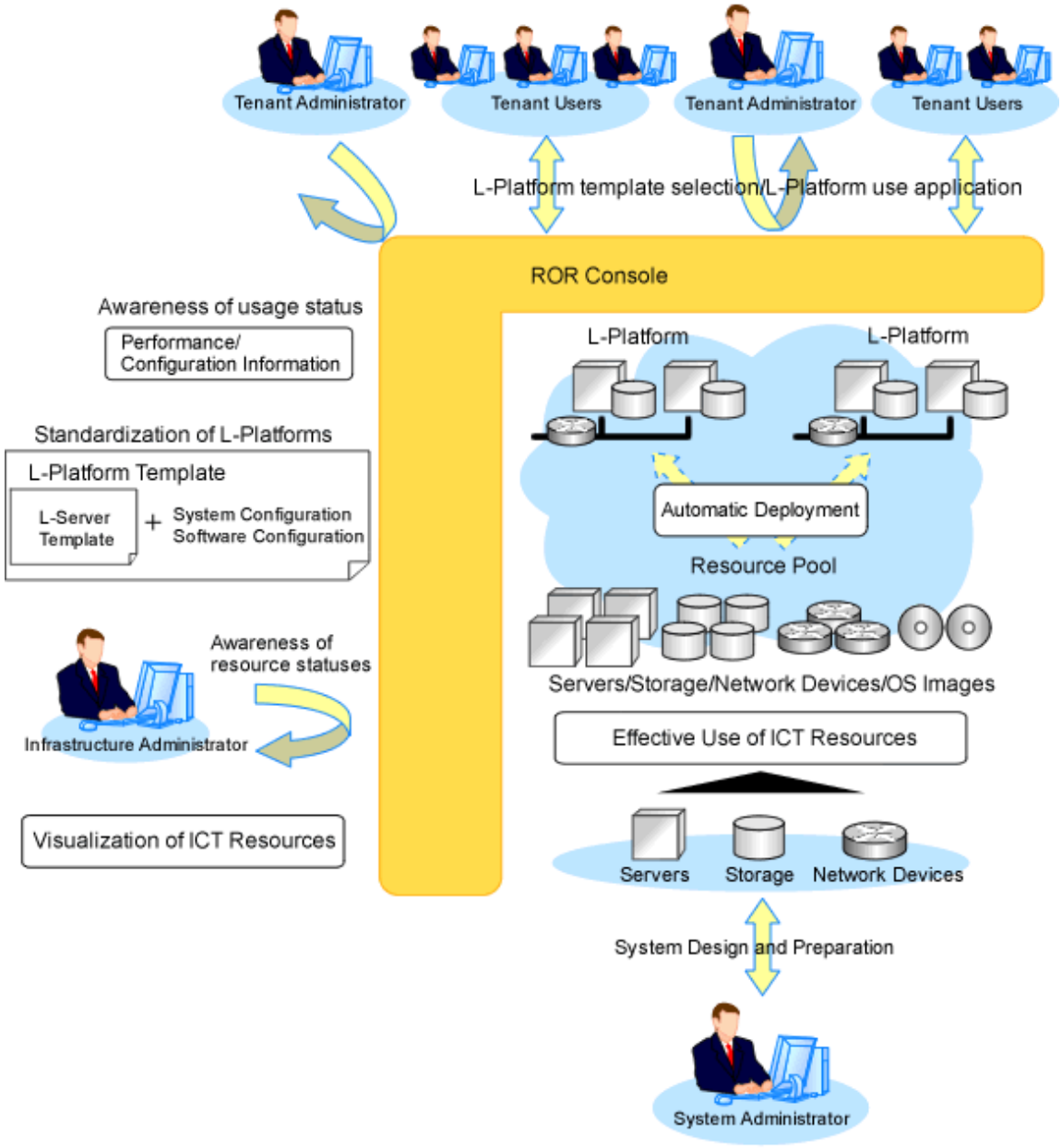
Even in environments with both physical and virtual resources, unified operations can be performed from one console for central management.

2.2 Resource Orchestrator User Roles and the Functions Available to Each User

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 2.1 Resource Orchestrator User Roles and the Functions Available to Each User



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 (platform) that connects two or more L-Servers on a network is called an L-Platform.

The infrastructure administrator manages the ICT resources (servers, storage, and networks) in a private cloud.
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.

System Operation Administrators

System operation administrators manage the operation of the entire system. System administrators install and configure systems. 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.

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.

The Functions Available to the Majority of Resource Orchestrator Users

For details on Resource Orchestrator user roles and the functions available for use, refer to "5.1.2 Roles and Available Operations".

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

Table 2.1 Available Functions

Main Function	Description	Target Users
Standardize L-Platforms (L-Platform templates)	Creates and publishes multiple logical configuration templates (L-Platform templates) for servers, storage, and networks.	Infrastructure Administrators or Tenant Administrators
Subscribe to an L-Platform	Search for and select L-Platform templates suitable for the purpose from amongst those published and subscribe.	Tenant Administrators or Tenant Users
Use L-Platforms	L-Platforms that meet one's needs can be used, as necessary.	Tenant Users
Viewing usage charges	L-Platform usage can be monitored as usage charge information. Usage charges are calculated based on the amount of L-Platform usage or charge information. The calculated usage charges can be viewed.	Infrastructure Administrators or 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. Also, it can display L-Server and L-Platform performance data configuration information, demand forecasting for resource pools and perform simulations of VM guest reallocations.	Infrastructure Administrators or Tenant Administrators

Function that ROR Console Offers

In Resource Orchestrator, the GUI provides the ROR Console.

The ROR Console provides the two following types of windows.

- Windows intended for tenant administrators and tenant users

  Windows intended for tenant administrators and tenant users are provided for L-Platform and user information operations.

  These windows are configured by tenant administrators themselves, and have been provided to reduce the infrastructure administrator workload.

- Windows intended for infrastructure administrators

  Operation windows and dashboard windows intended for infrastructure administrators are also provided for L-Platform and user information operations.

  These windows are provided to enable infrastructure administrators to display and operate all L-Platform and tenant information and to access important information quickly.

The table below shows the functions provided by the ROR Console.

Table 2.2 Function List Provided by ROR Console

Function	Overview	Infra Administrator	Tenants Administrator	Tenants users
Home	The window displayed immediately after login to the ROR Console. A function list and notifications are displayed.	Yes	Yes	Yes
Dashboard (Pool Conditions)	Displays the resource pool usage status.	Yes	Yes	-
Dashboard (System Conditions)	Displays L-Server performance information and configuration information	Yes	Yes	Yes
Dashboard (Capacity Planning)	Anticipate the demand for resource pools and perform simulations of VM guest reallocations.	Yes	Yes	-
Resource	A window for managing the resource pool and the relationship of resources to L-Server.	Yes	-	-
Template	A window for managing L-Platform Templates	Yes	Yes	-
L-Platform	A window for managing L-Platforms.	Yes	Yes	Yes
Request	A window for assessing and approving L-Platform usage applications and other applications from tenant users.	Yes	Yes	Yes
Tenants	A window for managing tenants and users belonging to tenants.	Yes	Yes	-
Usage Charges	Records of usage charges can be viewed.	Yes	Yes	-
Account	A window for changing a logged in user's information and password.	Yes	Yes	Yes
Help	Displays this product's manuals.	Yes	Yes	Yes

2.2.1 Resource Management

The following functions are provided by Resource Orchestrator.

For details on the operational environment for Resource Orchestrator, refer to "2.4 Software Environment" and "2.5 Hardware Environment".

Table 2.3 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 "2.2.2 Resource Pools".
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 "2.2.3 L-Server". For details on allocating and releasing resources to and from L-Servers, refer to "17.8 Allocating and Releasing Resources to L-Servers" in 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 "2.2.5 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 "2.2.6 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 "2.2.7 Simplifying Networks".
Simplifying storage settings	To use storage from a physical L-Server, configure storage units and storage networks.	For details, refer to "2.2.8 Simplifying Storage".
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 "17.9 Changing Physical Server Usage" in 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 18 Linking L-Servers with Configured Physical Servers or Virtual Machines" in 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, "Chapter 21 Resource Folder Operations" in 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 "5.1 Restricting Access Using Roles".

Function	Functional Overview	Remarks
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 "Chapter 6 Defining Tenants and Resource Pools" and "Chapter 4 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.	Refer to "Chapter 12 Installing and Defining Single Sign-On".
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.	Refer to "Chapter 7 Defining High Availability and Disaster Recovery".
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.	Refer to the "DR Option Instruction".
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 11 Monitoring Resources" in the "Operation Guide CE".
Power control	A function for turning servers ON or OFF.	Refer to "17.1 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 9 Hardware Maintenance" in the "Operation Guide CE".
Network device monitoring	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. - 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. - Network Map The following information is displayed in a comprehensive Network Map:	For details, refer to "11.4 Monitoring Networks" in the "Operation Guide CE" and "Appendix A User Interface" in the "User's Guide for Infrastructure Administrators (Resource Management) CE". For the specification of the monitoring method, refer to "14.6 Network Configuration Information" in the "Reference Guide (Command/XML) CE".

Function	Functional Overview	Remarks
	- 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	
Network maintenance	A function for maintaining network devices.	For details, refer to "Chapter 9 Hardware Maintenance" in 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 "17.3 Using the L-Server Console" in 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.

Table 2.4 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	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: - Managing unused physical servers as L-Servers by registering them with Resource Orchestrator - Managing configured physical servers by linking them to L-Servers VM hosts and physical OSs running on physical servers can be detected and registered as managed resources by Resource Orchestrator.
VM host	This refers to the server virtualization software running on a server to operate a virtual machine. For example, Windows Server 2008 R2 with Hyper-V roles added, VMware ESX for VMware, domain 0 for RHEL5-Xen, VM hosts for RHEL-KVM, Oracle VM Server, or VM hosts for Solaris Containers. VM hosts can be managed by monitoring their statuses, displaying their properties, and performing operations such as HBA address rename and server switchover. When a VM host is registered, any VM guests on the VM host are automatically detected and displayed in the server tree. The power operations and migration operations, etc. of VM guests can be performed from the server tree.
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.
Server management software	Software used for managing multiple servers. The target servers can be controlled.
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.

Resource	Description
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. The following usage methods are available for physical servers: - 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. For example, RAID groups of ETERNUS storage, aggregates of NetApp storage, and file systems for creating VM (VMware VMFS (datastore)).
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, server load balancers, 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. When a physical L-Server is created, a WWN and MAC address are necessary. When a virtual L-Server is created using KVM and RHEL5-Xen, a MAC address is necessary.
Virtual image resources	They are the following two images. - Cloning images collected from virtual L-Servers - Images using a template used for VM guest creation with VM management software
Physical image resources	Cloning images gathered from physical L-Servers.

2.2.2 Resource Pools

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

The resource pool management function allows you to effectively and efficiently use all resources.

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. When the resource pool is used, the time and trouble of requests for decision, arrangements, and environment construction, etc. that were necessary for individual systems becomes unnecessary because it is possible to prepare a server (including storage and network) simply by allocating an appropriate resource that

has been registered in the resource pool of this product. Preparation and operation of a premeditated infrastructure environment is possible. Moreover, it is possible to release resources when they become unnecessary, enabling re-assignment.

The types of resource pools are as described in "6.4 Resource Pool Types". For details, refer to "Chapter 20 Resource Pool Operations" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

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.

2.2.3 L-Server

Resource Orchestrator can be used to create L-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 "16.1 Creation Using an L-Server Template" in 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 "16.2 Creation of Physical L-Servers Using Parameters" or "16.3 Creation of Virtual L-Servers Using Parameters" in 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 "17.2 Modifying an L-Server" in 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 "17.7 Migration of VM Hosts between Servers" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

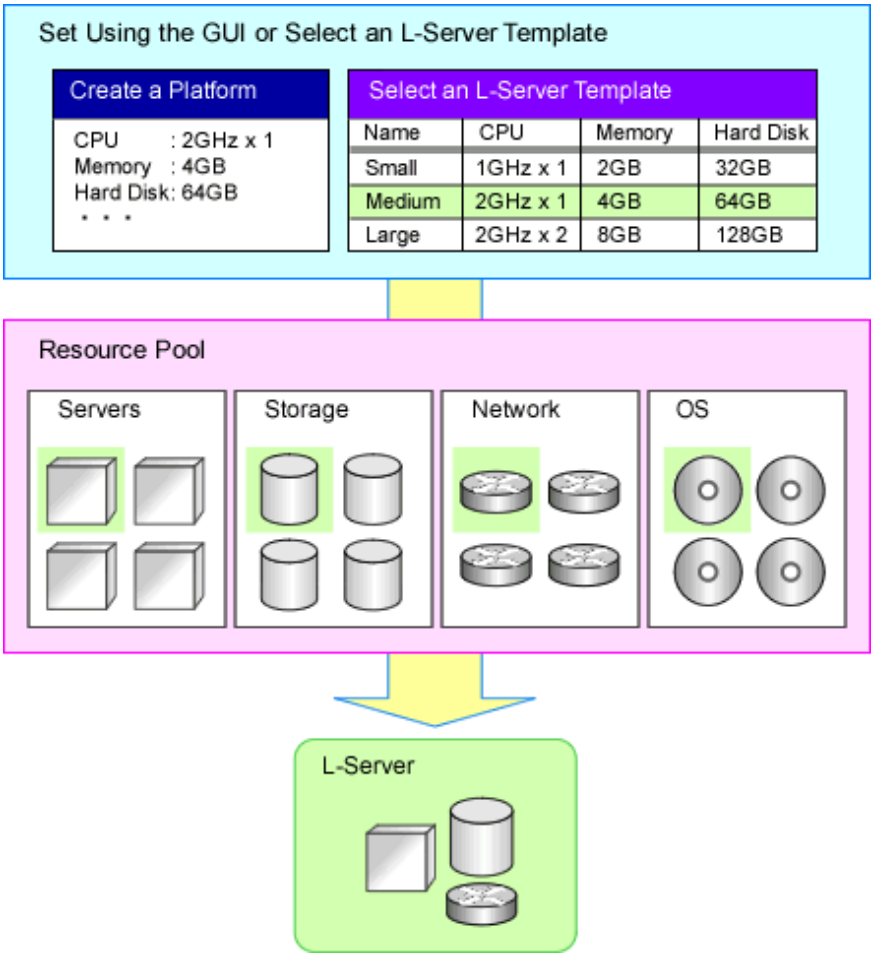
- Snapshot (For virtual L-Servers)

  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 "17.6.1 Snapshot" in 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 "17.6.2 Backup and Restore" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Figure 2.2 L-Server Creation



Selection of L-Server Deployment Location

Specify the resource pool and the server (the VM pool and VM host for a virtual L-Server, and the server pool and physical server for a physical L-Server) to deploy the L-Server to using one of the following methods.

When an L-Platform is created, only the resource pool can be specified.

- Resource pool automatic selection

  With this method, neither the resource pool nor the server are specified, and this product selects the resource pool automatically. The priority selected when L-Server is created can be set to the resource pool.

  When two or more pools that can be accessed exist, this product selects the resource pool with the higher priority as the deployment target (The smaller the value, the higher the priority). When two or more pools of the same priority exist, one is selected at random.

  After the resource pool is decided, the server is selected from the resource pool automatically.

  When the L-Server that use overcommit, use the following procedure to select location of an L-Server.

  - As for the selection location of an L-Server, VM host in VM pool of the overcommit setting that a user can access is select.
  - When two or more VM pools of overcommit exist, the VM host that disposes L-Server is selected regardless of the priority of the resource pool from among all VM host.

- Resource pool specification

  The server is selected from the specified resource pool automatically.

  In virtual L-Server, it is necessary to specify the resource pool according to the overcommit setting.

- Server specification

  The L-Server is deployed to the specified server.

  In virtual L-Server, it is necessary to specify VM host in the resource pool according to the overcommit setting.

The server that is the deployment target should meet the following requirements.

- The VM host is powered on
- Monitoring status is "normal"
- Maintenance mode is not set
- For details on maintenance mode, refer to "Appendix C Maintenance Mode" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".
- The maintenance mode of the server virtualization software is not set (For virtual L-Server)
- The conditions specified during L-Server creation are met

When creating a virtual L-Server, if the deployment target VM host in the VM pool is selected automatically, the VM host is selected using the conditions above, as shown below.

- 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.

  This enables reduction of waste by fragmenting the free space of VM hosts among all VM hosts.

  For L-Server templates that have overcommit enabled, if none of the searched VM hosts has sufficient space available, select a VM host and create an L-Server.

- When not using L-Server templates

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

- When the exclusion function of an L-Server has been set

  The L-Server is created on a VM host that other L-Servers do not use.
  The L-Servers on an L-Platform are configured for exclusive operation from all other L-Servers on the L-Platform.

- When the HA function or automatic re-installation function (examples: VMware HA or VMware DRS) of the VM product was enabled

  The VM host is selected by the VM product.

Simplifying Installing Using Cloning

Cloning is the function to distribute cloning images made from the content of the system disk of one server to another physical L-Server.

When a cloning image is created, network-specific settings such as host names and IP addresses are removed from the cloning image. This network-specific configuration is dynamically re-configured on the servers to which the cloning image is distributed.

This makes it possible to create duplicates of existing servers that will use the same operating system and software.

Simplifying Configuration Using by I/O Virtualization

I/O virtualization via HBA address rename (*) allows storage devices to be configured independently and prior to the rest of the server installation process. Servers can then be installed and set up without the involvement of storage administrators.

* Note: Refer to "2.2.9 I/O Virtualization".

L-Server for Infrastructure Administrator

The L-Server for the infrastructure administrator is an L-Server that cannot be used by the tenant administrator or tenant users. Only the tenant administrator and the tenant user can use a normal L-Server.

It is created for the following purpose.

- When the infrastructure administrator collects the cloning image

  The infrastructure administrator creates the cloning image, and releases it to the tenant administrator and tenant users.

  For details how to create an L-Server for an infrastructure administrator, refer to "Chapter 14 Creating an L-Server for an Infrastructure Administrator" in the "Setup Guide CE".

  For details how to collect cloning images, refer to "Chapter 15 Collecting and Registering Cloning Images" in the "Setup Guide CE".

- When installing a VM host on a physical L-Server

  The setting of the network and storage can be simplified using the functions of the physical L-Server when creating the VM host. Moreover, high availability operation and Disaster Recovery can be performed.

  For details how to set up, refer to the following:

  - Installing VM Hosts on Physical L-Servers

    Refer to "Appendix D Installing VM Hosts on Physical L-Servers" in the "Setup Guide CE".

  - Blade Chassis High Availability

    Refer to "17.1.2 Blade Chassis High Availability " in the "Operation Guide CE".

  - Disaster Recovery

    For details, refer to "Chapter 18 Disaster Recovery" in the "Operation Guide CE".

- When the software used on L-Server for the purpose of the infrastructure management of the VM management product etc. is installed, the simplification, the high availability operation, and Disaster Recovery of the construction of the VM management product can be operated.

Changing Physical Server Usage

The usage change of a physical server is a function to prepare more L-Servers than the number of physical servers, and to start the L-Server to be switched to. Because the usage of a physical server can be changed using to this function according to time zone and the situation, the resources of servers can be used effectively.

The boot disk and Internet Protocol address of an L-Server are retained while another L-Server uses a physical server.

This function can be used when an L-Server is actually a physical server. With virtual machines, as it is possible to deploy multiple L-Servers on a single VM host without making any settings, it is possible to get the same effect as changing the usage of a physical server by selecting the L-Server to start.

This function has the following two uses.

- One physical server used for the switchover of multiple L-Servers

  The physical server that starts an L-Server will always be the same server.

- An unused physical server in a server pool used for the switchover of multiple L-Servers

  The physical server allocated to an L-Server differs depending on the availability of the server pool.

For details, refer to "17.9 Changing Physical Server Usage" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Changing VM Guest Locations (Migration)

The operation (migration) that moves the VM guest between physical servers can be done from this product through coordination with the VM management product (VMware vCenter Server etc.) or the VM host (VM host of KVM).

Regrouping of all VM guests to a subset of servers and shut down of any unused servers or chassis to reduce overall power consumption.

When server maintenance becomes necessary, VM guests can be migrated to alternative servers and their applications kept alive during maintenance work.

2.2.4 L-Platform

This section explains L-Platforms.

An L-Platform is a logical resource used to collectively manage an entire system (platform) composed of two or more servers in a hierarchical system (Web/AP/DB), with a network.

The setting and the operation of two or more servers, storage, and networks can be simplified by the use of an L-Platform.
Resource Orchestrator can be used to deploy and operate L-Platforms.
An L-Platform defines the following combination of resources:

- L-Server

  An L-Platform is a logical server that manages physical servers and virtual servers (VM) together.
  For details on L-Servers, refer to "2.2.3 L-Server".

- Network resources

  This is a resource that expresses the network where it connects between L-Servers. Using network resources it is possible to automatically configure switches and virtual switches, and connect an L-Server to a network.
  For details, refer to "2.2.7 Simplifying Networks".

- Firewall resources

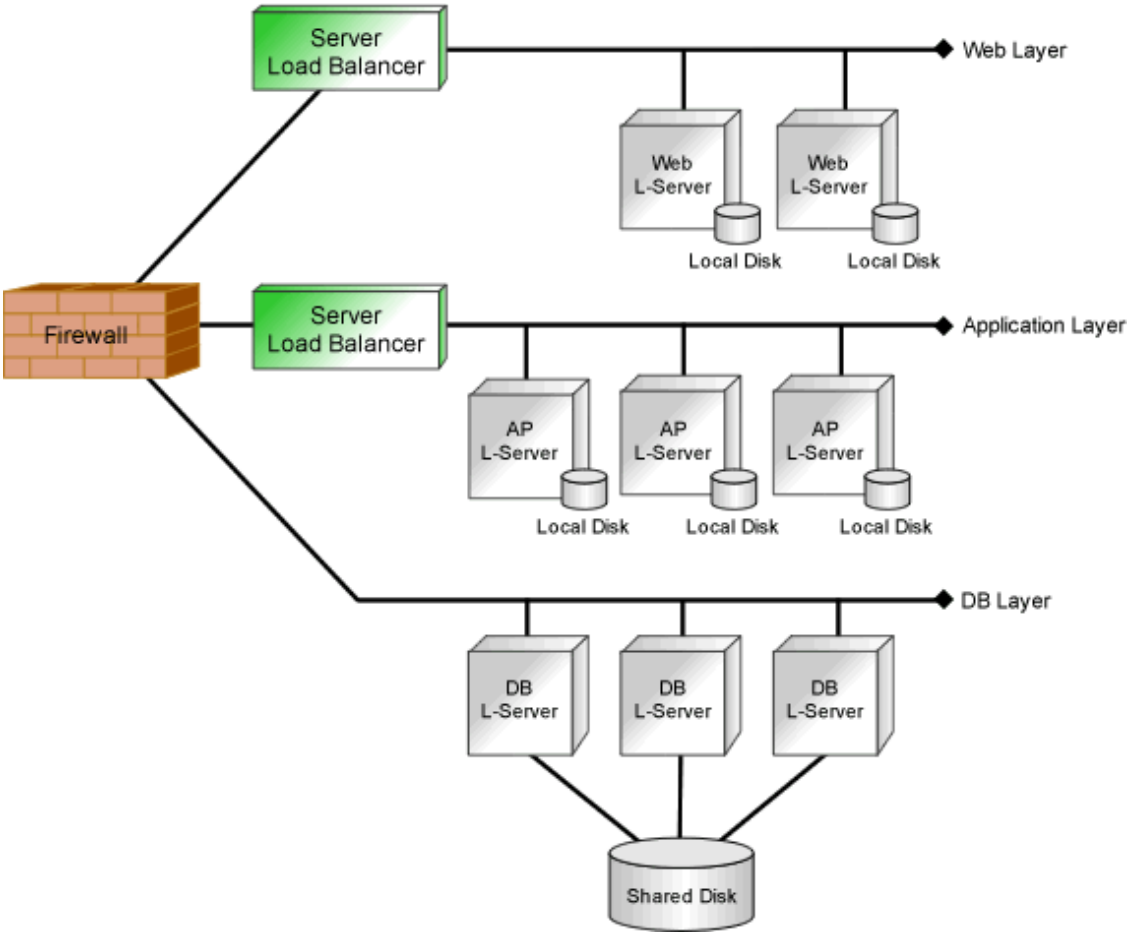
  In a hierarchical system, this resource ensures the security of each tier.

- Server load balancer resources

  This resource distributes the workload across multiple servers, reducing the delay in response when there is concentrated traffic or server failure.

The configuration of an L-Platform is shown below.

Figure 2.3 L-Platform Configuration



2.2.5 Templates

This section explains templates.

The following templates can be used with Resource Orchestrator:

- L-Platform Template
- L-Server Templates

L-Platform Template

An L-Platform template defines L-Platform specifications.

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

For how to create L-Platform templates, refer to "Chapter 8 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 "14.2 L-Server Template" in the "Reference Guide (Command/XML) CE".

For how to create L-Server templates, refer to "15.1.2 Creating a Template" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

2.2.6 Resource Visualization

Total capacity of resources in the resource pool and display of free space

The total capacity and the free space of the resources in the resource pool are displayed, and the availability can easily be checked from the [dashboard(Pool conditions)] tab of the ROR console.

For how to use the [dashboard (Pool Conditions)] tab of the ROR console, refer to "Chapter 4 dashboard (Pool Conditions)" in the "User's Guide for Infrastructure Administrators CE".

Display of the Number of L-Servers Each L-Server Templates can Create

The number of L-Servers that can be created for each L-Server template can be displayed for the specified L-Server template.

For details on the L-Server conversion view, refer to "20.6 Viewing a Resource Pool" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Relation Management of Physical Servers and Virtual Servers

Resource Orchestrator provides an integrated management console for environments composed of physical and virtual servers.

The [Resource] tab of the ROR console supports management of server configurations, monitoring of failures, and determination of the causes and range of effects of problems.

- Resource Orchestrator provides a tree-based view of chassis and server hardware and their operating systems (physical OS, VM host, or VM guest). This enables easy confirmation and tracking of relationships between chassis, servers, and operating systems.
- Resource Orchestrator monitors server hardware and displays icons representative of each server's status.

Resource Orchestrator also allows administrators to manage both physical and virtual servers in a uniform manner. Once registered, resources can be managed uniformly regardless of server models, types of server virtualization software, or differences between physical and virtual servers.

Easy Server Monitoring

When managing PRIMERGY BX servers, BladeViewer can be used to easily check server statuses and perform other daily operations. In BladeViewer, server statuses are displayed in a format similar to the physical configuration of a blade server system, making server management and operation more intuitive. BladeViewer provides the following features:

- Display of server blades' mount statuses.
- An intuitive way to monitor and control the power statuses of multiple server blades.
- Easier visualization of which applications are running on each server blade. This helps to quickly identify any affected applications when a hardware fault occurs on a server blade.

Monitoring of Power Consumption

By activating the power monitoring feature, it is possible to monitor trends in power consumption for resources equipped with power monitoring capabilities, or resources connected to a registered power monitoring device (PDU or UPS). The power consumption data regularly collected from the power monitoring environment can be output to a file in CSV format or as a graph.

2.2.7 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, firewalls, and server load balancers, configuring, modifying, or deleting the definitions that include VLAN settings is automatically performed using scripts. Scripts are prepared for each model of the network devices by infrastructure administrators.

2.2.7.1 Timing of Automatic Network Settings

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

Table 2.5 Timing of Automatic Network Settings Execution

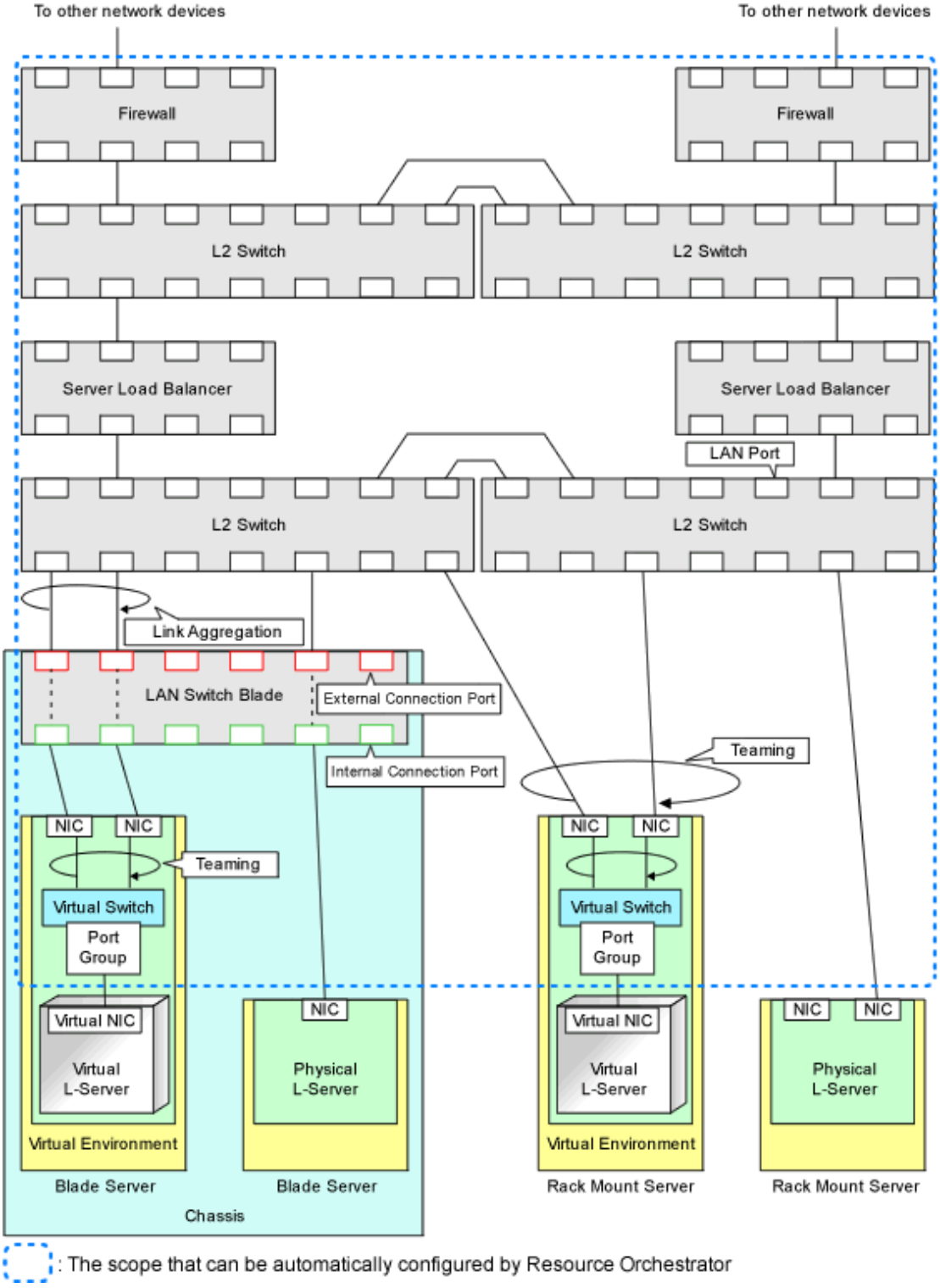
Target	Operation	L-Server (IP Address Settings for OS)	Virtual Switch (Creation/VLAN Settings)	LAN Switch Blade (VLAN Settings)		L2 Switches (Overall Settings)	Firewall (Overall Settings)	Server Load Balancer (Overall Settings)
				Internal Connection Port	External Connection Port			
Network resources	Creation	-	-	-	Yes (*1)	Yes	-	-
	Modification	-	-	-	Yes (*1)	Yes	-	-
	Deletion	-	Yes	-	-	Yes	-	-
Virtual L-Server	Creation	Yes	Yes	Yes	-	-	-	-
	Modification	-	-	-	-	-	-	-
	Deletion	-	-	-	-	-	-	-
Physical L-Servers	Creation	Yes	-	Yes	-	Yes (*2)	-	-
	Modification	-	-	Yes	-	-	-	-
	Deletion	-	-	Yes	-	Yes (*2)	-	-
L-Platform	Creation	Yes	Yes (*3)	Yes	-	Yes (*5)	Yes	Yes
	Modification	-	Yes (*3)	Yes (*4)	-	Yes (*5)	Yes	Yes
	Deletion	-	-	Yes (*4)	-	Yes (*5)	Yes	Yes

Yes: Available
-: Not Available
*1: When automatic network settings and automatic VLAN settings for uplink ports are enabled, network settings are automatically configured.
*2: Available when using rack mount servers.
*3: Available when using virtual L-Servers.
*4: Available when using physical L-Servers.
*5: Available when using rack mount servers and physical L-Servers.

2.2.7.2 Scope of Automatic Network Settings

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

Figure 2.4 Scope of Automatic Network Settings Execution



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 C Configuration when Creating Virtual L-Servers" in the "Setup Guide CE".

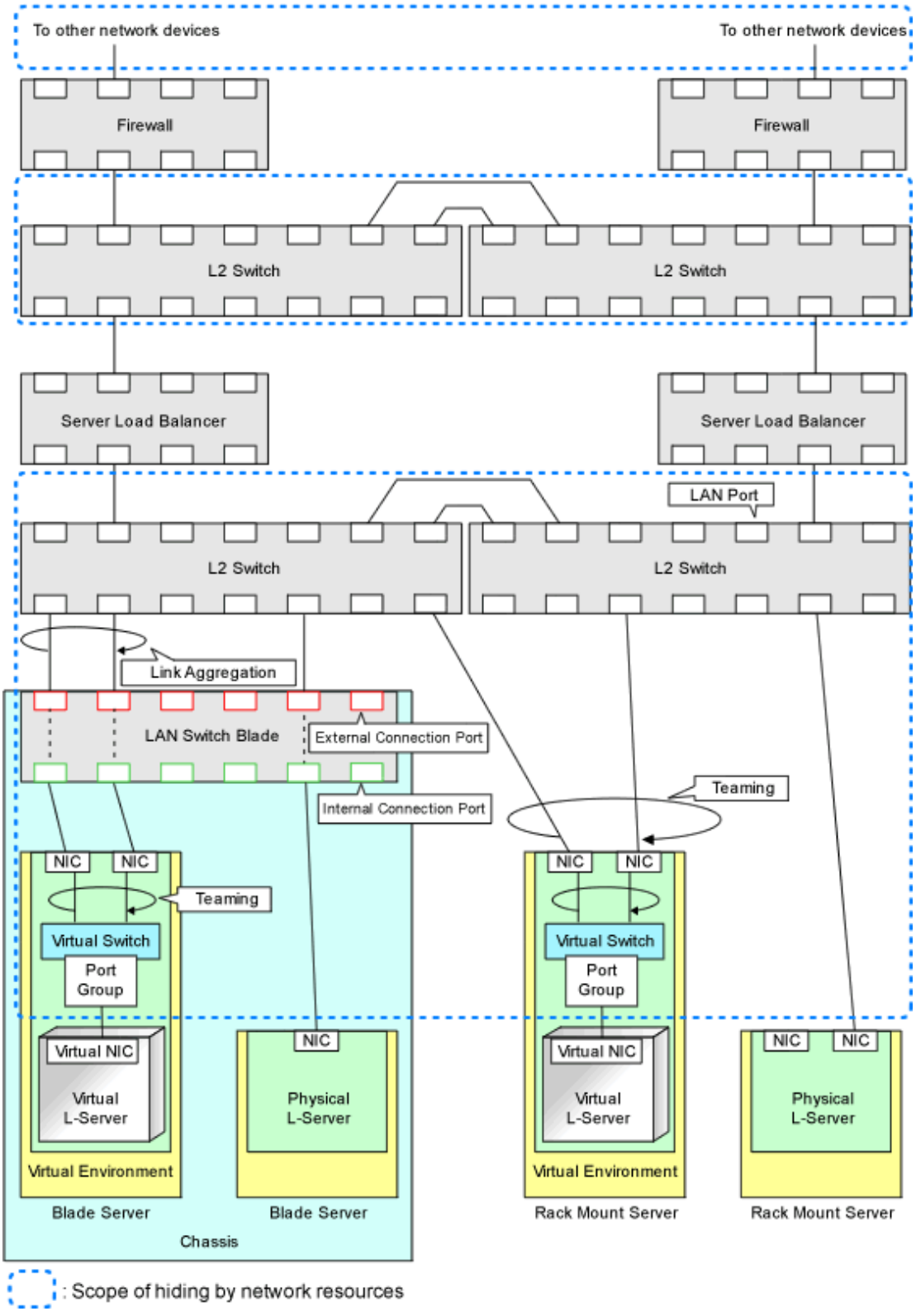
2.2.7.3 Hiding Network Information

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

- Virtual Switches

- Port Groups
- LAN Switch Blades
- L2 Switches

Figure 2.5 Hiding of Network Device Information



2.2.7.4 Network Device Automatic Configuration

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

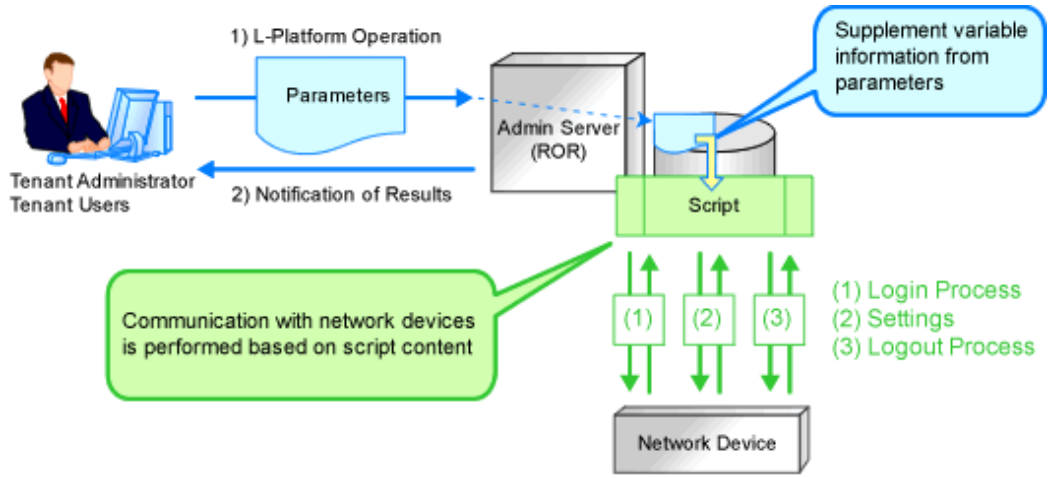
- Automatic configuration of firewalls and server load balancers when creation, modification, or deletion of an L-Platform is performed

  The detailed timing is as follows:

  - When an L-Platform is created from an L-Platform template that includes a network device (firewall or server load balancer)
  - When L-Server addition or deletion is performed for an L-Platform
  - When the settings of a network device (firewall or server load balancers) in an L-Platform are modified
  - When an L-Platform created from an L-Platform template that includes a network device (firewall or server load balancer) is deleted

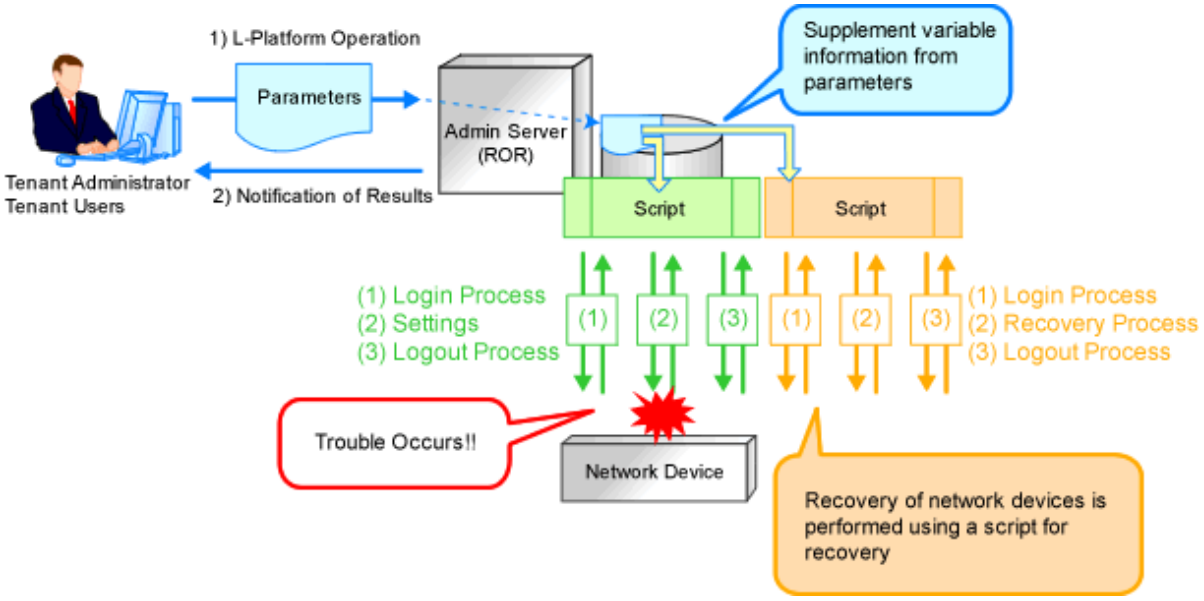
- Automatic configuration for L2 switches when creation, modification, or deletion of an network resource is performed
- Automatic configuration for L2 switches when creation or modification of a physical L-Server is performed on rack mount servers

Figure 2.6 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 2.7 Network Device Automatic Configuration Image (Recovery Process)



2.2.7.5 Network Device Configuration File Management

The following files are available as network device (firewall, server load balancer and L2 Switch) configuration files.

- Network device configuration files

  A configuration file containing settings related to communication, such as address and VLAN information of devices and interfaces, and rules for firewalls and server load balancers

- Network device environment files

  Files required for the operation of devices such as CA certificates, user authentication databases and user customized information (excluding network device configuration files)

In this product, a function which manages device configuration files using generations is offered. Using this function modification changes can be checked and restoration of configurations can be performed easily when network devices are exchanged.

The following features are provided by the network device configuration file management function.

- Backing up and restoration of configuration files

  Network device configuration files can be backed up by this product and managed using generations.
  Further, the latest configuration files which already backed up can be restored to network devices.

- Export of configuration files

  The files that are backed up and managed using generations can be exported from the manager.

- Backing up and restoration of environment files

  Network device configuration files can be backed up to this product.
  Further, backed up environment files can be restored to network devices.

- Export of environment files

  The backed up files can be exported to the infrastructure admin's terminal.

- Registration of external server information

  For network devices which do not have an ftp server, the information of an external ftp server, which is used for backing up and restoration of network devices, can be registered.

  Specify this external server in the network configuration information (XML definition) file when registering the network device.

2.2.7.6 Easy Network Monitoring

This section provides a brief overview of easy network monitering.

Visualize networks (network map function)

For PRIMERGY BX servers, Resource Orchestrator provides a Network Map function, which helps visualize and relate physical networks (between servers and LAN switches) together with virtualized networks (from VLANs or virtual switches used in server virtualization software). The Network Map provides the following features:

- Automatic detection and display of network connections (topology) and link statuses between heterogeneous network resources.
- Facilitates overall network consistency diagnostics and identification of the resources (physical and virtual) affected by a network issue.
- Displays comprehensive content that can be used in communication between server and network administrators, thus smoothing out coordination between the two parties.

Status monitoring

Resource Orchestrator monitors status of network devices (Firewalls, server load balancers, and L2 switches) to automatic network settings for them.

2.2.8 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.

In this product, the following two storage resources are managed.

- Virtual Storage Resources

  Virtual storage resource indicates the following 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. Virtual storage resources do not need to be individually registered as resources.

  The resources can be managed as virtual storage resources using the same operations.

  - For physical servers

    An original resource used to create LUN such as ETERNUS RAID groups or NetApp aggregates on storage units

  - For VM

    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

- Disk Resources

  A disk resource refers to a disk resource allocated to a server.

  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.

  - For physical servers

    - 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

    Virtual Disk

Allocation of Storage to an L-Server

In Resource Orchestrator, use the following procedure to allocate a disk resource to an L-Server:

- Method involving allocation of disk resources with specified sizes that have been automatically created by this product from storage resources (Automatic generation from virtual storage)
- Method involving allocation of disk resources that have been created in advance using storage management software to L-Servers (Creation of disk resources in advance)

The allocation strategy on storage differs depending on the type of the L-Server and the storage device used.

- Allocating Storage to a Physical L-Server

  For details, refer to "Allocating Storage to a Physical L-Server".

  The following storage allocation methods and storage types are available for physical L-Servers.

Table 2.6 Storage Allocation Methods and Storage Types for Physical L-Servers

Allocation Method	Storage Type
Allocate disk resources automatically created from virtual storage resources	- ETERNUS Storage - NetApp FAS Storage
Allocate disk resources that were created in advance	- ETERNUS Storage - NetApp FAS Storage - EMC CLARiiON Storage - EMC Symmetrix DMX Storage - EMC Symmetrix VMAX Storage

- Allocating Storage to a Virtual L-Server

  For details, refer to "Allocating Storage to a Virtual L-Server".

  Storage Allocation Methods and Storage Types and Server Virtualization Types for Virtual L-Servers are as follows.

Table 2.7 Storage Allocation Methods and Storage Types and Server Virtualization Types for Virtual L-Servers

Allocation Method	Storage Type
Allocate disk resources automatically created from virtual storage resources	- VMware - Hyper-V - Oracle VM - RHEL5-Xen
Allocate disk resources that were created in advance	- KVM - Solaris Containers

Supported Storage Configurations

For the storage units that can be connected with physical L-Servers, refer to "Table 2.67 Storage Units that can be Connected with L-Servers on Physical Servers" in "2.5 Hardware Environment".

For supported storage for Virtual L-Servers, refer to the following:

[VMware]
Refer to "Supported Storage Configurations" in "E.1.3 Storage Preparations".

[Hyper-V]
Refer to "Supported Storage Configurations" in "E.2.3 Storage Preparations".

[Xen]
Refer to "Supported Storage Configurations" in "E.3.3 Storage Preparations".

[Oracle VM]
Refer to "Supported Storage Configurations" in "E.4.3 Storage Preparations".

[KVM]

Refer to "Supported Storage Configurations" in "E.5.3 Storage Preparations".

[Solaris Containers]
Refer to "Supported Storage Configurations" in "E.6.3 Storage Preparations".

Effective Utilization of Storage Using Thin Provisioning

Thin provisioning is technology for virtualizing storage capacities.

In Resource Orchestrator, efficient use of storage is achieved by the following two methods.

- Method using the thin provisioning of a storage unit
- Method using the thin provisioning of server virtualization software

For details, refer to "Effective Utilization of Storage Using Thin Provisioning".

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, refer to "Effective Utilization of Storage Using Automatic Storage Layering".

2.2.9 I/O Virtualization

I/O adapters (HBA) for servers are shipped with an assigned physical address that is unique across the world. This World Wide Name (WWN) is used by the storage network to identify servers. Until now, the WWN settings on storage networks needed to be updated whenever servers were added, replaced, or switched over. Resource Orchestrator uses I/O virtualization technology that makes server-side I/O control possible. It does this by replacing physically-bound WWNs with virtual WWNs assigned to each server based on its role in the system. Resource Orchestrator can handle two different I/O virtualization technologies (HBA address rename and VIOM).

With VIOM, the ability to re-define MAC addresses of network interfaces, boot configuration, and network configuration means that it is no longer necessary to re-configure network devices or applications that depend on Mac address values.

Note

- The "I/O virtualization option" is required when using HBA address rename.
- ServerView Virtual-IO Manager should be installed on the admin server when integrating Resource Orchestrator with VIOM.

2.2.10 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 "Chapter 6 Defining Tenants and Resource Pools".

For creating, modifying, and deleting tenants, refer to "Chapter 11 Tenants" in the "User's Guide for Infrastructure Administrators CE".

2.2.11 High Availability of Managed Resources

The function allows failed applications to automatically be recovered onto an available spare server by pre-allocating spare servers to managed servers.

Depending on the server's boot method, one of the three following switchover methods can be used to recover applications on a spare server:

- HBA address rename

  This method is used in SAN boot environments where servers start from boot disks located in SAN storage arrays. If the primary server fails, its World Wide Name (WWN) is inherited by the spare server, which then automatically starts up from the same SAN

disk. This is made possible by the I/O virtualization (*) capabilities of the HBA address rename function, which is able to dynamically re-configure the WWN of an I/O adapter (HBA).

* Note: Refer to "2.2.9 I/O Virtualization".

- VIOM server profile exchange method

  This method is used in environments where servers start from boot disks located in SAN storage arrays or on a storage device connected to the LAN. If the primary server fails, the World Wide Name (WWN) and MAC address, boot configuration, and network configuration set in its server profile are inherited by the spare server, which then automatically starts up from the same boot disk. This is made possible by the I/O virtualization (*) capabilities of the HBA address rename function, which is able to dynamically re-configure the WWN of an I/O adapter (HBA).

  For details on server profiles, refer to the ServerView Virtual-IO Manager manual.

  * Note: Refer to "2.2.9 I/O Virtualization".

- Storage Affinity Switchover Method

  This method is used in environments where SPARC Enterprise servers start from boot disks located in SAN storage arrays. When a primary server fails in a SAN boot environment, changing the following configuration using storage management software enables access and startup from the same boot disk. When HBA WWNs are fixed, reconfiguring storage devices enables continuation of operations.

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

  * Note: Refer to "8.1.6 Settings when Switching Over SPARC Enterprise Servers".

The following LAN switch settings can also be exchanged between primary and spare servers during server switchover.

- VLAN
- Port groups (For PRIMERGY BX900/BX400 LAN switch blades operating in IBP mode)

Several servers can share one or more common spare servers, irrespective of the kind of servers used (physical or virtual), or the applications that are running on them.

Spare servers can also be shared between physical and virtual servers. This is done by combining Auto-Recovery with the high availability feature provided with the server virtualization software used.

Note that the Auto-Recovery function differs from clustering software (such as PRIMECLUSTER) in the following respect:

- Server failure detection

  The Auto-Recovery function can detect hardware failures using server management software (such as ServerView Agents) and server management devices (management blades, management boards, or remote management controllers). It cannot detect system slowdowns.

2.2.12 Disaster Recovery

Resource Orchestrator provides simple and highly reliable Disaster Recovery.

For details, refer to the "DR Option Instruction".

2.3 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 2.8 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 [Physical Servers]	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
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
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
Network device monitoring	Network monitoring is a function which monitors status of resources such as firewalls and displays them using a GUI as normal, abnormal etc.	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 (*2)
NS Appliance	NS Appliance is a function which ensures network security by separating a multi-tier system into individual layers. This runs as a virtual appliance on Physical L-Servers.	No	Yes (*3)

*1: Available for physical servers registered in the server tree. For details, refer to "Chapter 18 Server Switchover Settings" in the "User's Guide VE".
*2: Available when the DR option is purchased.
*3: Available when the NS 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 2.9 Managed Server Hardware Differences Depending on Product

Software	Hardware	ROR VE	ROR CE (*)
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	Yes

* Note: For details, refer to "2.5 Hardware Environment".

Table 2.10 Server Virtualization Software Differences Depending on Product

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

* Note: For details, refer to "2.4.2.1 Required Basic Software".

2.4 Software Environment

Resource Orchestrator is composed of the following DVD-ROM.

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

2.4.1 Software Organization

Resource Orchestrator is composed of the following software.

Table 2.11 Software Organization

Software	Functional Overview
ServerView Resource Orchestrator V3.1.0 Manager (hereinafter manager)	- Used to control managed servers and neighboring network devices - Manages resource pools and L-Servers - Operates on the admin server
ServerView Resource Orchestrator V3.1.0 Agent (hereinafter agent)	- Performs pre-configuration during deployment, monitors operating servers, and controls backup and cloning - Operates on managed servers (*1)
ServerView Resource Orchestrator V3.1.0 HBA address rename setup service (hereinafter HBA address rename setup service)	- Realization of high availability of the HBA address rename setup used by the admin server (*2)

Software	Functional Overview
	- 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 "10.1 Deciding the Storage Environment".

2.4.2 Software Requirements

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

2.4.2.1 Required Basic Software

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

Required Basic Software

Table 2.12 [Windows Manager]

Basic Software (OS)	Remarks
Microsoft(R) Windows Server(R) 2008 Standard (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 2.13 [Linux Manager]

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) 5.8 (for x86) Red Hat(R) Enterprise Linux(R) 5.8 (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. For required packages, refer to "Table 2.36 Required Packages of Manager [Linux Manager]". The Linux Kernel version depending on the hardware corresponds to the version supported by Fujitsu.

Table 2.14 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 2.15 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 2.16 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) 5.8 (for x86) Red Hat(R) Enterprise Linux(R) 5.8 (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) 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)	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 2.37 Required Packages of Agent [Linux]". The Linux Kernel version depending on the hardware corresponds to the version supported by Fujitsu.

Basic Software (OS)	Remarks
SUSE(R) Linux Enterprise Server 11 for x86 SUSE(R) Linux Enterprise Server 11 for EM64T	

Table 2.17 Agent [Solaris]

Basic Software (OS)	Remarks
Solaris(TM) 10 Operating System	Supported after 05/09 (Update7). When using SAN boot, refer to the manual for Fibre Channel card driver, "SPARC Enterprise - ETERNUS SAN Boot Environment Build Guide".

Table 2.18 Agent [VMware]

Basic Software (OS)	Remarks
VMware vSphere 4.0 VMware vSphere 4.1 VMware vSphere 5	Install Resource Orchestrator on the VMware ESX host. (*)

* Note: VMware ESXi of VMware vSphere 4.0 or earlier cannot be used for managed servers.
VMware ESXi of the version of VMware vSphere 4.1 or later can be used for managed servers, but there is no need to install Resource Orchestrator on VMware ESXi.

Table 2.19 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) 5.8 (for x86) Red Hat(R) Enterprise Linux(R) 5.8 (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 2.20 Agent [Oracle VM]

Basic Software (OS)	Remarks
Oracle VM 3.0	-

Table 2.21 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	-

* Note: This is necessary when creating physical L-Servers using rack mount or tower servers.

Table 2.22 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) 5.8 (for x86) Red Hat(R) Enterprise Linux(R) 5.8 (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 2.38 Required Packages of HBA address rename Setup Service [Linux]". The Linux Kernel version depending on the hardware corresponds to the version supported by Fujitsu.

* Note: This is necessary when creating physical L-Servers using rack mount or tower servers.

Note

[VMware]
The free version of VMware ESXi cannot be used for managed servers.
When using VMware ESXi for managed servers, purchase the appropriate license.

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 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 2.23 List of Functions with no Support of Combined Use

Server Virtualization Software	Functions with no Support of Combined Use
VMware vSphere 4.0 VMware vSphere 4.1 VMware vSphere 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 2.24 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.

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.

Required Patches

Table 2.25 [Windows Manager]

Basic Software (OS)	Patch ID/Bundle Update
Microsoft(R) Windows Server(R) 2003 R2 Standard x64 Edition	Hotfix KB942589 (*)
Microsoft(R) Windows Server(R) 2003 R2 Enterprise x64 Edition	Hotfix KB942589 (*)

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

Table 2.26 [Linux Manager]

Basic Software (OS)	Patch ID/Bundle Update (*)
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)

* Note: Necessary when upgrading.

Table 2.27 Agent [Windows]

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

Table 2.28 Agent [Hyper-V]

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

Table 2.29 Agent [Linux]

Basic Software (OS)	Patch ID/Bundle Update (*)
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)

Basic Software (OS)	Patch ID/Bundle Update (*)
	Bundle Update U09091 (5.4 compatible) Bundle Update U10041 (5.5 compatible)

Table 2.30 Agent [Solaris]

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

Table 2.31 Agent [VMware]

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

Table 2.32 Agent [Xen] [KVM]

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

Table 2.33 Agent [Oracle VM]

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

Table 2.34 HBA address rename setup service [Windows]

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

Table 2.35 HBA address rename Setup Service [Linux]

Basic Software (OS)	Patch ID/Bundle Update (*)
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)

* Note: Necessary when upgrading.

[Hyper-V]
For the manager, agents, SCVMM, SCVMM agents, and Windows guest OSs, 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 2.36 Required Packages of Manager [Linux Manager]

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)

Basic Software (OS)	Required Packages
	audit-libs(i686) (*1) cloog-ppl compat-expat1(i686) compat-libtermcap(i686) compat-openldap(i686) compat-readline5(i686) cpp cracklib(i686) (*1) cyrus-sasl-lib(i686) db4(i686) elfutils-libelf(i686) (*1) expat(i686) file gcc gcc-c++ gdb(i686) (*2) 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) (*1) libXp(i686) libXt(i686) libXtst(i686) make mpfr ncurses (*2) ncurses-libs(i686) (*1) net-snmp net-snmp-utils nspr (*3) nss (*3) nss-softokn-freebl(i686) nss-util (*3) openldap (*3) openssl(i686)

Basic Software (OS)	Required Packages
	openssl098e(i686) pam(i686) (*1) perl perl-libs perl-Module-Pluggable perl-Pod-Escapes perl-Pod-Simple perl-version ppl readline(i686) (*1) redhat-lsb sqlite(i686) strace(i686) (*2) sysstat tcsh unixODBC(i686) X-Window (*4) zlib(i686)
Red Hat(R) Enterprise Linux(R) 5.8 (for x86) Red Hat(R) Enterprise Linux(R) 5.8 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.7 (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) (*1) 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 (*4) zlib(i386)

*1: Necessary when the OS architecture is Intel64.
*2: Necessary when the OS architecture is x86.
*3: Necessary when managing a managed server within a separate subnet to the admin server.
*4: Install an OS, specifying a package.

Table 2.37 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) (*2)

Basic Software (OS)	Required Packages
	libXt(i686) libXtst(i686) ncurses (*1) (*3) ncurses-libs(i686) net-snmp-utils readline(i686) sqlite(i686) sysfsutils sysstat (*1) unixODBC(i686)
Red Hat(R) Enterprise Linux(R) 5.8 (for x86) Red Hat(R) Enterprise Linux(R) 5.8 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.7 (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) 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)	alsa-lib(i686) glibc(i686) libgcc(i686) libICE(i686) libselinux(i686) libsepol libSM(i686) libstdc++(i686) libX11(i686) libXau(i686) libXdmcp libXext(i686) libXi(i686) libXt(i686) libXtst(i686) ncurses-libs(i686) net-snmp-utils readline(i686) sqlite(i686) sysstat (*1)

*1: Necessary when installing an agent (dashboard functions).
*2: Necessary when the OS architecture is Intel64.
*3: Necessary when the OS architecture is x86.

Table 2.38 Required Packages of HBA address rename Setup Service [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) libXt(i686) libXtst(i686) ncurses-libs(i686) readline(i686)

Basic Software (OS)	Required Packages
	sqlite(i686) unixODBC(i686)
Red Hat(R) Enterprise Linux(R) 5.8 (for x86) Red Hat(R) Enterprise Linux(R) 5.8 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.7 (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)	alsa-lib(x86_64) e2fsprogs-libs glibc(x86_64) libgcc(i686) libICE(x86_64) libSM(x86_64) libstdc++(i686) libX11(x86_64) libXau(x86_64) libXdmcp libXext(i686) libXi(i686) libXt(i686) libXtst(i686) ncurses(i686) readline(i686) sqlite(i686)

2.4.2.2 Required Software

The software listed below is required when using Resource Orchestrator.

Required Software (Windows Manager)

The required software for Windows manager is as follows:

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

When the ROR console is started on Windows manager, the required software of the admin client is also necessary.

Table 2.39 [Windows Manager]

Required Software	Version	Remarks
ServerView Operations Manager for Windows (*1)	V5.30 - V6.00.09	Necessary for Single Sign-On.
Microsoft(R) LAN Manager module	-	Used when performing backup and restore, or cloning for physical servers. Obtain it from the Microsoft FTP site. (*2)
BACS or Intel PROSet or PRIMECLUSTER GLS for Windows or OneCommand NIC Teaming and Multiple VLAN Manager	-	Necessary when performing redundancy of the admin LAN for admin servers. When using PRIMECLUSTER GLS, the following patches are required. - TP002714XP-06
ServerView Virtual-IO Manager	2.6 or later	Necessary when creating physical L-Servers using blade servers. When BX920 S3 or BX924 S3 is a managed server, it corresponds to ServerView Virtual-IO Manager V3.0.4 or later.

Required Software	Version	Remarks
VMware vCenter Server	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 Service	-	Necessary for ServerView Operations Manager.
SNMP Trap Service (Standard OS service)	-	Necessary for ServerView Operations Manager. Necessary when receiving SNMP Trap from the server.
DHCP Server (Standard OS service)	-	Necessary when managing a managed server within a separate subnet to the admin server.
Microsoft(R) System Center Virtual Machine Manager 2008 R2 or Microsoft(R) System Center 2012 Virtual Machine Manager	-	[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.2.4 Network 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	2.0	[Hyper-V] Necessary for management of VM guest and VM host.
ETERNUS SF Storage Cruiser Manager	14.2 or later	Necessary when using the storage affinity switchover method for server switchover. Necessary when connecting an ETERNUS LUN to a physical L-Server. Apply one of the following: - 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: - 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	15.0 or later	Necessary when using dynamic LUN mirroring on ETERNUS storage.
NavisecCLI	7.30 or later	Necessary when connecting an EMC CLARiiON LUN to a physical L-Server.

Required Software	Version	Remarks
SymCLI	-	Necessary when connecting an EMC Symmetrix DMX or EMC Symmetrix VMAX device to a physical L-Server.
Solutions Enabler	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.
Oracle VM Manager	3.0	[Oracle VM] Necessary for management of VM guest and VM host.
BMC BladeLogic Server Automation	8.2 or later	Necessary when creating an L-Server in a Solaris Container. Can be placed on the same server as the manager (recommended) or on another server. When operating managers in clusters, place it on a different server.
BMC BladeLogic Server Automation Console	8.2 or later	Necessary when creating an L-Server in a Solaris Container. Install it on the same server as the manager.

*1: When installing managers in cluster environments, installation on both the primary and secondary nodes is necessary.
*2: Obtain it from the following Microsoft FTP site.

Microsoft FTP site

URL: ftp://ftp.microsoft.com/bussys/clients/msclient/dsk3-1.exe

Required Software (Linux Manager)

Required Software for Linux Manager is as follows.

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

Table 2.40 [Linux Manager]

Required Software	Version	Remarks
ServerView Operations Manager for Linux	V5.30 - V6.00.09	Necessary for Single Sign-On.
Microsoft(R) LAN Manager module	-	Necessary when using backup and restore, or cloning. Obtain it from the Microsoft FTP site. (*)
ServerView Virtual-IO Manager	2.6 or later	Necessary when creating physical L-Servers using blade servers. When BX920 S3 or BX924 S3 is a managed server, it corresponds to ServerView Virtual-IO Manager V3.0.4 or later.
PRIMECLUSTER GLS	-	Necessary when performing redundancy of the admin LAN for admin servers.
VMware vCenter Server	4.0 4.1 5.0	Necessary for management of VM guest and VM host.

Required Software	Version	Remarks
ETERNUS SF Storage Cruiser Manager	14.2 or later	Necessary when using the storage affinity switchover method for server switchover. Necessary when connecting an ETERNUS LUN to a physical L-Server. Apply one of the following: - 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	In the following cases, ETERNUS SF Storage Cruiser manager must be version 15.0 or later: - 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	15.0 or later	Necessary when using dynamic LUN mirroring on ETERNUS storage.
NavisecCLI	7.30 or later	Necessary when connecting an EMC CLARiiON LUN to a physical L-Server.
SymCLI	-	Necessary when connecting an EMC Symmetrix DMX or EMC Symmetrix VMAX device to a physical L-Server.
Solutions Enabler	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.
Oracle VM Manager	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.
BMC BladeLogic Server Automation	8.2 or later	Necessary when creating an L-Server in a Solaris Container. Can be placed on the same server as the manager (recommended) or on another server. When operating managers in clusters, place it on a different server.
BMC BladeLogic Server Automation Console	8.2 or later	Necessary when creating an L-Server in a Solaris Container. Install it on the same server as the manager.

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

Microsoft FTP site

URL: ftp://ftp.microsoft.com/bussys/clients/msclient/dsk3-1.exe

Table 2.41 Agent [Windows]

Required Software	Version	Remarks
ServerView Agents for Windows	V4.50.05 or later	Required for collecting and managing server information of PRIMERGY and PRIMEQUEST.
"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. (*) 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 or OneCommand NIC Teaming and Multiple VLAN Manager	-	Necessary when performing redundancy of the admin LAN and public LAN for managed servers. When using PRIMECLUSTER GLS, the following patches are required. - TP002714XP-06
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.

*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

URL(x64):
http://www.microsoft.com/downloads/details.aspx?familyid=C2684C95-6864-4091-BC9A-52AEC5491AF7&displaylang=en

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" in the "Setup Guide CE".
The module is not necessary after installation of agents.

Table 2.42 Agent [Linux]

Required Software	Version	Remarks
ServerView Agents for Linux	V4.90.14 or later	Required for collecting and managing server information of PRIMERGY and PRIMEQUEST.

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

Table 2.43 Agent [Red Hat Enterprise Linux]

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

Table 2.44 Agent [Solaris]

Required Software	Version	Remarks
PRIMECLUSTER GLS	4.2 or later	Necessary when performing redundancy of the admin LAN and public LAN for managed servers.
ETERNUS SF Storage Cruiser	14.2 or later	Necessary on the primary server of the managed server when using the storage affinity switchover method for server switchover.
RSCD Agent	8.2 or later	Required when using the global zone of Solaris Containers for the agent, and creating an L-Server.

Table 2.45 Agent [VMware]

Required Software	Version	Remarks
ServerView Agents for VMware	V4.30-20 or later	Required for collecting and managing server information of PRIMERGY and PRIMEQUEST. Not necessary when using VMware ESXi for the agent.
ServerView ESXi CIM Provider	1.10.01 or later	Necessary when using VMware ESXi as a managed server.

Table 2.46 Agent [Hyper-V]

Required Software	Version	Remarks
ServerView Agents for Windows	V4.50.05 or later	Required for collecting and managing server information of PRIMERGY and PRIMEQUEST.
"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. (*) 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: - Virtual network creation and NIC connection

Required Software	Version	Remarks
		- 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: - When not performing network redundancy for L-Servers using blade servers - When using servers other than blade servers
PRIMECLUSTER GLS for Windows (*1)	-	After configuring redundancy for blade servers using PRIMECLUSTER GLS, it is necessary to perform the following configurations automatically: - 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: - When not performing network redundancy for L-Servers using blade servers - When using servers other than blade servers For details, refer to "2.2.7 Simplifying Networks".

*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

URL(x64):
http://www.microsoft.com/downloads/details.aspx?familyid=C2684C95-6864-4091-BC9A-52AEC5491AF7&displaylang=en

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" in the "Setup Guide CE".
The module is not necessary after installation of agents.

Table 2.47 Agent [Xen]

Required Software	Version	Remarks
ServerView Agents for Linux	V4.81-14 or later	Necessary when using PRIMEQUEST series servers.
PRIMECLUSTER GDS	-	Necessary when using RHEL5-Xen servers.

Table 2.48 Agent [KVM]

Required Software	Version	Remarks
ServerView Agents for Linux	V5.1 or later	Required for collecting and managing server information of PRIMERGY and PRIMEQUEST.

Table 2.49 Agent [Oracle VM]

Required Software	Version	Remarks
ServerView Agents for Linux	5.0 or later	Required for collecting and managing server information of PRIMERGY and PRIMEQUEST.

Table 2.50 HBA address rename setup service [Windows]

Required Software	Version	Remarks
Windows(R) Internet Explorer(R)	8 9	Necessary for displaying the online help.

Table 2.51 HBA address rename Setup Service [Linux]

Required Software	Version	Remarks
Firefox	3	Necessary for displaying the online help.

Required Software: Admin Clients

The following software is necessary for admin clients.

Table 2.52 List of Required Software for Admin Clients

Required Software	Version	Remarks
Windows(R) Internet Explorer(R)	8 9 (*1)	Required for display of the ROR console.
Adobe Flash Player	10.3.183.5 or higher	Used for displaying the ROR console and the dashboard on admin clients.
Java(TM) 2 Runtime Environment Standard Edition	(*2)	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. Operation on Windows 2003 x64 Edition is not supported.

*1: When connecting with the ROR Console, use Compatibility View Settings.
*2: To display the management window of ServerView Operations Manager, please refer to the ServerView Operations Manager manual. To display the VM management console or the console window, version 1.5 or later is necessary.

2.4.2.3 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 2.53 [Manager]

Operating System Type	Product Name	Version and Level	Remarks
Windows	INTERSTAGE	All versions	Here "INTERSTAGE" includes the following products: - INTERSTAGE - INTERSTAGE Standard Edition - INTERSTAGE Enterprise Edition
	Interstage Apcoordinator	All versions	-
	Interstage Application Server	All versions	Here "Interstage Application Server" includes the following products: - 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: - Interstage Business Application Server Standard Edition - Interstage Business Application Server Enterprise Edition
	Interstage Business Process Manager	All versions	-
	Interstage Business Process Manager Analytics	All versions	-
	Interstage BPM Flow	All versions	-
	Interstage Service Integrator	All versions	-

Operating System Type	Product Name	Version and Level	Remarks
	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	Here "Systemwalker Centric Manager" includes the following products: - 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	Here "Systemwalker IT Change Manager" includes the following products: - 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	Here "Systemwalker Operation Manager" includes the following products: - SystemWalker/OperationMGR Global Enterprise Edition - SystemWalker/OperationMGR Enterprise Edition - SystemWalker/OperationMGR Standard Edition - SystemWalker OperationMGR Global Enterprise Edition - SystemWalker OperationMGR Enterprise Edition - SystemWalker OperationMGR Standard Edition - Systemwalker Operation MGR Global Enterprise Edition - Systemwalker OperationMGR Enterprise Edition - Systemwalker OperationMGR Standard Edition

Operating System Type	Product Name	Version and Level	Remarks
	Systemwalker PKI Manager	All versions	-
	Securecrypto Library	All versions	-
	Systemwalker Resource Coordinator	All versions	Here "Systemwalker Resource Coordinator" includes the following products: - Systemwalker Resource Coordinator - Systemwalker Resource Coordinator Base Edition - Systemwalker Resource Coordinator Virtual server Edition
	Systemwalker Runbook Automation (Admin Server)	15.0.0 or earlier 15.1.0 (*5)	-
	Systemwalker Runbook Automation (Linked Server/Relay Server/ Business Server)	All versions	-
	Systemwalker Service Quality Coordinator	V13.5 or earlier V15.0 (*2)	-
	Systemwalker Service Catalog Manager	V14g	-
	Systemwalker Software Configuration Manager	V14.0.0	-
	Systemwalker Software Configuration Manager (Admin Server)	V14.1.0 (*1)	-
	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	-
	ServerView Resource Orchestrator	All versions	-
	ServerView Deployment Manager (*4)	All versions	-
	Premeo Premium Agent	All versions	-

Operating System Type	Product Name	Version and Level	Remarks
	TeamWARE Office Server	All versions	-
	TRADE MASTER	All versions	-
Linux	Interstage Application Server	All versions	Here "Interstage Application Server" includes the following products: - 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: - 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: - 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: - SystemWalker/CentricMGR - SystemWalker/CentricMGR-M - SystemWalker/CentricMGR GEE - SystemWalker/CentricMGR EE - SystemWalker/CentricMGR SE - Systemwalker Centric Manager Global Enterprise Edition

Operating System Type	Product Name	Version and Level	Remarks
			- Systemwalker Centric Manager Enterprise Edition - Systemwalker Centric Manager Standard Edition
	Systemwalker IT Process Master	All versions	-
	Systemwalker IT Change Manager	All versions	Here "Systemwalker IT Change Manager" includes the following products: - Systemwalker IT Change Manager Enterprise Edition - Systemwalker IT Change Manager Standard Edition
	Systemwalker Operation Manager	V13.3 or earlier	Here "Systemwalker Operation Manager" includes the following products: - Systemwalker Operation Manager Enterprise Edition - Systemwalker Operation Manager Standard Edition
	Systemwalker Resource Coordinator	All versions	Here "Systemwalker Resource Coordinator" includes the following products: - Systemwalker Resource Coordinator - Systemwalker Resource Coordinator Base Edition - Systemwalker Resource Coordinator Virtual server Edition
	Systemwalker Runbook Automation (Admin Server)	15.0.0 or earlier 15.1.0 (*5)	-
	Systemwalker Runbook Automation (Linked Server/Relay Server/ Business Server)	All versions	-
	Systemwalker Service Quality Coordinator	V13.5 or earlier V15.0 (*2)	-
	Systemwalker Service Catalog Manager	V14g	-
	Systemwalker Software Configuration Manager (Admin Server)	V14.1.0 (*1)	-
	Systemwalker Software Configuration Manager (Linked Server/Public Server)	All versions	-
	Cloud Infrastructure Management Software	All versions	-
	ServerView Resource Coordinator VE	All versions	-
	ServerView Resource Orchestrator	All versions	-
	Premeo Premium Agent	All versions	-

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

*2: When Systemwalker Service Quality Coordinator is used, the media and a license for Systemwalker Service Quality Coordinator are necessary.
*3: Because the manager of Resource Orchestrator contains a PXE server, it cannot be used together with the PXE server that is required for the remote installation function of ServerView Installation Manager.
*4: ServerView Deployment Manager can be installed after this product has been installed.
*5: Systemwalker Runbook Automation can be installed after this product has been installed.

Table 2.54 [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	-
Solaris containers	Server System Manager (Manager only)	All versions	-
	Systemwalker Service Quality Coordinator	V13.5 or earlier V15.0 (*2)	-
	ETERNUS SF Disk Space Monitor	All versions	-

*1: ServerView Deployment Manager can be installed after this product has been installed.

Operating System Type	Product Name	Version and Level	Remarks
Windows	Systemwalker Service Quality Coordinator	V13.5 or earlier V15.0 (*2)	-
	Systemwalker Service Catalog Manager	V14g	-
	ETERNUS SF Disk Space Monitor	All versions	-
Linux	Systemwalker Service Quality Coordinator	V13.5 or earlier V15.0 (*2)	-
	Systemwalker Service Catalog Manager	V14g	-
	ETERNUS SF Disk Space Monitor	All versions	-
Solaris	Server System Manager (Manager only)	All versions	-
	Systemwalker Service Quality Coordinator	V13.5 or earlier V15.0 (*2)	-
	ETERNUS SF Disk Space Monitor	All versions	-

*2: When Systemwalker Service Quality Coordinator is used, the media and a license for Systemwalker Service Quality Coordinator are necessary.

Basic Mode

Exclusive software in Basic mode are as follows:

Table 2.55 List of Exclusive Software

Software	Product Name
[Windows Manager]	ServerView Installation Manager (*1)
	ServerView Deployment Manager
[Linux Manager]	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)
Agent [Solaris Containers]	Server System Manager (Manager only)
Agent [Solaris]	Server System Manager (Manager only)

*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 this product has been installed. For details on installation, refer to "2.2 Installing Agents" in the "Setup Guide CE".

Note

- Resource Orchestrator managers contain some components of SystemcastWizard Professional. Therefore, they cannot be placed and operated on the same subnet as SystemcastWizard.
  Furthermore, take caution regarding the following points when placing SystemcastWizard Professional (hereinafter ScwPro) or SystemcastWizard Lite (hereinafter ScwLite) on the same subnet.
  - Operate ScwPro and ScwLite in non-aggressive mode on a simple DHCP server. Make sure that the IP address scope allocated to the simple DHCP server does not conflict with the IP addresses for Resource Orchestrator managed servers.
  - Resource Orchestrator managed servers cannot be managed simultaneously by ScwPro and ScwLite.
    Do not register servers already registered with Resource Orchestrator on ScwPro or ScwLite.
  - To simultaneously operate multiple servers, change the multicast IP address settings for ScwPro so that they do not conflict with the Resource Orchestrator managers.
- 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 (*)
  - ServerStart (when using the remote installation function)

- ServerView Installation Manager
- Solaris JumpStart

* Note: 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 B Co-Existence with ServerView Deployment Manager" in the "Setup Guide VE".

[Windows]

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

Table 2.56 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)
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.

[Physical Servers]

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

2.4.2.4 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 2.57 Static Disk Space

Software	Folder	Required Disk Space (Unit: MB)
[Windows Manager]	*Installation_folder* (*)	4000
[Linux Manager]	/opt	3525
	/etc/opt	255
	/var/opt	768
Agent [Windows] [Hyper-V]	*Installation_folder* (*)	300
Agent [Linux]	/opt	250
	/etc/opt	55
	/var/opt	105
Agent [VMware] [Xen] [KVM] [Oracle VM]	/opt	95
	/etc/opt	5
	/var/opt	5
Agent [Solaris]	/opt	350
	/etc/opt	15

Software	Folder	Required Disk Space (Unit: MB)
	/var/opt	5

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

- When using a 64-bit (x64) OS

  Default value: C:\Program Files (x86)\Resource Orchestrator

- When using a 32-bit (x86) OS

  Default value: C:\Program Files\Resource Orchestrator

2.4.2.5 Dynamic Disk Space

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

Table 2.58 Dynamic Disk Space

Software	Folder	Required Disk Space (Unit: MB)
[Windows Manager]	*Installation_folder* (*1)	9080 + *Number_of_managed_servers* * 4
		Environmental_data_storage_area
		Performance_display_information_storage_area(*8)
		Metering log_storage_area(*9)
	Image_file_storage_folder (*2)	*Image_file_storage_area* (*3)
	Backup_storage_folder_for_configuration_definition_information	*Backup_storage_area_for_configuration_definition_inf*
	L-Server_restoration_log_storage_folder	*L-Server_restoration_log_storage_folder* (*4)
	Network_device_configuration_file_storage_folder (*10)	*Network_device_configuration_file_storage_area* (*11)
[Linux Manager]	/etc	2
	/var/opt	9080 + *Number_of_managed_servers* * 4
		Environmental_data_storage_area
		Performance_display_information_storage_area(*8)
		Metering log_storage_area(*9)
	Image_file_storage_directory (*2)	*Image_file_storage_area* (*3)
	Backup_storage_folder_for_configuration_definition_information	*Backup_storage_area_for_configuration_definition_inf*
	L-Server_restoration_log_storage_folder	*L-Server_restoration_log_storage_folder* (*4)
	Network_device_configuration_file_storage_folder (*10)	*Network_device_configuration_file_storage_area* (*11)
Agent [Windows]	*Installation_folder* (*1)	60
		Log_data(*5)
Agent [Hyper-V]	*Installation_folder* (*1)	60
		Log_data(*6)
Agent [Linux]	/etc	1
	/var/opt	1
		Log_data(*7)
Agent [VMware] [Xen]	/etc	1
	/var/opt	1

Software	Folder	Required Disk Space (Unit: MB)
[KVM] [Oracle VM]		
Agent [Solaris]	/etc	1
	/var/opt	1
		Log_data(*7)
HBA address rename setup service [Windows]	*Installation_folder* (*1)	60
HBA address rename Setup Service [Linux]	/etc	1
	/var/opt	60

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

- When using a 64-bit (x64) OS

  Default value: C:\Program Files (x86)\Resource Orchestrator

- When using a 32-bit (x86) OS

  Default value: C:\Program Files\Resource Orchestrator

*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:

- When using a 64-bit (x64) OS

  Default value: C:\Program Files (x86)\Resource Orchestrator\SVROR\ScwPro\depot

- When using a 32-bit (x86) OS

  Default value: C:\Program Files\Resource Orchestrator\SVROR\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 "Image File for Physical Servers Storage Area".
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 the disk capacity and content of the backup storage area for configuration definition information and the L-Server restoration log storage area, refer to "10.1 Backup and Restoration of Admin Servers" in 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 the "How to estimate the amount of space required for the log data ("Troubleshoot" directory)" section 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 2.59 Formula of Disk Space Necessary for Information Storage Area for Performance Display

Target Resource	Required Disk Space
Dashboard information	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. When the number of tenants is 100, 6.6 GB of capacity is required. Disk Space = (67.0 + (55.5 * number of tenants)) * 1.2 (MB)
Usage condition information	The size will increase and decrease depending on the numbers of VM hosts and VM guests. The capacity differs depending on the VM management software. 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. Disk space = ((N1 * host number) + (N2 * guest number)) *1.2(MB) [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 2.60 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 2.61 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		- The following operations are executed every day
		  - 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		- Execute monthly base backup (every 30 days) - Execute hourly difference backup.

Table 2.62 Formula for Metering Logs per Day

- Target capacity for metering logs

- 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

  (A) * operation number for L-Platforms per day
  + (B) * operation number for other than L-Platforms per day
  + (C) * number of operating L-Platforms

  = 2.3 KB * 20 + 0.6 KB * 2000 + 2.3 KB * 1000
  = 3.5MB

*10: The name of the storage folder (directory) specified for network device configuration files.

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

- When using a 64-bit (x64) OS

  C:\Program Files (x86)\Resource Orchestrator\SVROR\Manager\var\netdevice

- When using a 32-bit (x86) OS

  C:\Program Files\Resource Orchestrator\SVROR\Manager\var\netdevice

[Linux]
The default is as follows:
/var/opt/FJSVrcvmr/netdevice

*11: Size increases or decreases depending on the number of network devices managed by the network device file management function, and the number of generations of the network device configuration file of each network device.
The size required for each network device is equal to the number of generations of the network device configuration file * 512 KB.
The maximum number of network devices that can be managed by the network device configuration file management function is 72.

Environmental_data_storage_area

The environmental data storage area is the area necessary when using power monitoring.
The environmental data storage area is located in the installation folder of the admin server, and is used to store environmental data collected from power monitoring targets and aggregate data.
The amount of space that is necessary for the environmental data storage area can be determined from the number of power monitoring targets being registered, the polling interval, and the period the environmental data is to be stored for.
For details on each setting, refer to "13.1.1 Settings for the Power Monitoring Environment".
Estimate the necessary space using the following formula.

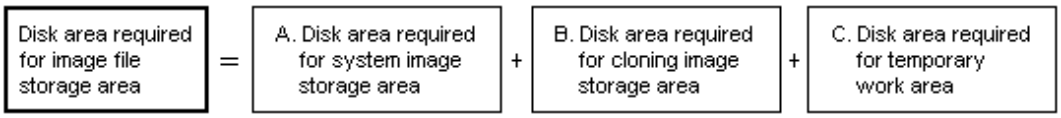
Necessary disk space (MB) = (*detail_storage_period_(months)* * 6 / *polling_interval_(minutes)* + 10) * 3 * *number_of_power_monitoring_targets*

Image File for Physical Servers Storage Area

The image file storage area for physical servers is necessary when performing backup and cloning.
The image file storage area is secured on an admin server as an area to store the image files (system images and cloning images) collected through the backup and cloning of managed servers.

Create the image file storage area on the local disk of the admin server, or SAN storage. It is not possible to specify folders on network drives, shared folders (NFS, SMB, etc.) on other machines on a network, or UNC format folders.

The space necessary for the image file storage area is the total amount of disk space necessary for the "system image storage area", the "cloning image storage area", and the "temporary work area".
Estimate the necessary space based on the disk space required for each storage area using the following formula.



Estimate the necessary space for the image file storage area using the following procedure.

1. **Calculate the size of image files.**

   Calculate the image file sizes as base data for estimating the required disk space for A, B, and C indicated above.
   The calculation method is given below.

   File size of image files = *disk_space_per_managed_server* * *compression_ratio*

   Disk_space_per_managed_server

   When system construction using the same software configuration has been performed before, use the consumed disk space of that system (the sum of the disk space for each partition when dividing one disk into multiple partitions).
   Check the consumed disk space using the relevant OS function.
   When system construction using the same software configuration has not been performed before, calculate the disk space from the required disk space indicated in the installation guide for each piece of software.
   For the OS, refer to "Examples of Calculation".

   Compression_ratio

   The compression ratio involved when storing the consumed disk space of managed servers as an image file on the admin server. Compression ratio is dependent on file content, and usually a compression ratio of around 50% can be expected. When there are many files that have already been compressed (installation media of software, image data, or other media), the overall compression ratio is lower.
   For the OS, refer to "Examples of Calculation".

   An example of the calculation of disk space and the compression ratio directly after OS installation is given below.

   Example

   Examples of Calculation

   - For Windows Server 2003

     Used disk space: 1.9 GB -> After compression: 0.9 GB Compression ratio: 0.9/1.9 = 47%

2. **Calculate the space required for the system image storage area.**

   The system image storage area is the area necessary when performing backup. Secure space for each managed server for which backup system images are made.
   This is not necessary when not performing backup.

   Calculate the size of the system image storage area based on the image file size of step 1. Estimate the area for each managed server for which system images are backed up using the following formula, and use the total as the estimated size.

   Disk space required for the system image storage area = *file_size_of_image_files* * *number_of_versions*

   Number_of_versions

   The number of versions of system images. By default, up to three versions of system images can be managed.

Point

By reducing the number of versions of system images saved it is possible to reduce the amount of space required for the system image storage area.
For details of how to change the number of system images saved, refer to "5.9 rcxadm imagemgr" in the "Reference Guide (Command/XML) CE".

The following is an example when three managed servers, A, B, and C are performing backup of system images, and the used disk space and compression ratios are expected to be the following values.

Example

Example of Estimation
Server A - *Image_file_size*: 3.0 GB (Used disk space: 6.0 GB, Compression ratio 50%)
Server B - *Image_file_size*: 1.6 GB (Used disk space: 4.0 GB, Compression ratio 40%)
Server C - *Image_file_size*: 1.6 GB (Used disk space: 4.0 GB, Compression ratio 40%)

(3.0 * 3) + (1.6 * 3) + (1.6 * 3) = 18.6 (GB)

3. **Calculate the space required for the cloning image storage area.**

   The cloning image storage area is the area necessary when performing cloning. Secure space for each managed server for which cloning images are collected.
   This is not necessary when not performing cloning.

   Calculate the size of the cloning image storage area based on the image file size of step 1. Estimate the area for each managed server from which cloning images are collected using the following formula, then set the total as the estimated size.

Disk space required for the cloning image storage area = *file_size_of_image_files* * *number_of_versions*

   Number_of_versions

   The number of versions of cloning images. By default, up to three versions of cloning images can be managed.

Point

By reducing the number of versions of cloning images saved it is possible to reduce the amount of space required for the cloning image storage area.
For details of how to change the number of cloning images saved, refer to "5.9 rcxadm imagemgr" in the "Reference Guide (Command/XML) CE".

The following is an example when managed servers A and B are used to collect cloning images, and the used disk space and compression ratios are expected to be the following values.

Example

Example of Estimation
Server A - *Image_file_size*: 3.0 GB (Used disk space: 6.0 GB, Compression ratio 50%)
Server B - *Image_file_size*: 1.6 GB (Used disk space: 4.0 GB, Compression ratio 40%)

(3.0 * 3) + (1.6 * 3) = 13.8 (GB)

4. **Calculate the space required for the temporary work area.**

   When collecting system images or cloning images, the temporary work area is necessary to keep the former version of images until collection of new system images or cloning images is completed.
   This is not necessary when not performing backup or cloning.

Calculate the size of the temporary work area based on the image file size of step 1.
Estimate the largest size of the image files of all managed servers, and determine the necessary area using the following formula.

Disk space required for the temporary work area = *largest_image_file_size* * *image_file_collection_multiplicity*

Estimate image file collection multiplicity using operational designs in which image file collection (system image backup and cloning image collection) is simultaneously performed at the limit of multiplicity for multiple managed servers under management of an admin server. However, as Resource Orchestrator is designed not to exceed four multiplicities in order to reduce the load on the admin servers, the maximum multiplicity is 4.

The following is an example when three managed servers, A, B, and C are used to collect system images or cloning images, and the file size of each image file is as below. In this example, the image file collection multiplicity is 3.

Example

Example of Estimation
Server A - *Image_file_size*: 3.0 GB (Used disk space: 6.0 GB, Compression ratio 50%)
Server B - *Image_file_size*: 1.6 GB (Used disk space: 4.0 GB, Compression ratio 40%)
Server C - *Image_file_size*: 1.6 GB (Used disk space: 4.0 GB, Compression ratio 40%)

3.0 * 3 = 9.0 (GB)

5. **Calculate the space necessary for the image file storage area based on the disk space calculated in 2. to 4.**

   Calculate the total amount of required space for A, B, and C calculated in steps 2 to 4. (A: Disk area required for system image storage area, B: Disk area required for cloning image storage area, C: Disk area required for temporary work area).

2.4.2.6 Memory Size

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

Table 2.63 Memory Size

Software	Memory Size (Unit: MB)
[Windows Manager]	6656
[Linux Manager]	10752
Agent [Windows] [Hyper-V]	512
Agent [Linux]	256
Agent [Solaris]	64
Agent [VMware]	32
Agent [Xen] [KVM]	32
Agent [Oracle VM]	32

2.5 Hardware Environment

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

Required Hardware Conditions for Managers and Agents

Table 2.64 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. For details on the amount of memory necessary for Resource Orchestrator, refer to "2.4.2.6 Memory Size".

Software	Hardware	Remarks
		Please consider the amount of memory necessary for required software as well as the amount of memory necessary for Resource Orchestrator.
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 RX200 S7 PRIMERGY RX300 S4 PRIMERGY RX300 S5 PRIMERGY RX300 S6 PRIMERGY RX300 S7 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	- 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: - 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 (PY-SWB104(PG-SW109) or PY-SWB101(PG-SW201)) are mounted in CB1 and CB2, only NIC1 and NIC2 can be used. - When PRIMERGY BX920 S3 or BX924 S3 is used, Resource Orchestrator can only use Function 0 of each port.
	SPARC Enterprise M series	- Virtual L-Servers can be deployed. For details, refer to "E.6 Solaris Containers" and "C.7 Solaris Containers" in the "Setup Guide CE". - Configured virtual machines can be used by associating them with virtual L-Servers. - Configured physical servers can be used by associating them with physical L-Servers. For details, refer to "Chapter 18 Linking L-Servers with Configured Physical Servers or Virtual Machines" in the "User's Guide for Infrastructure Administrators (Resource Management) CE". - Servers can be managed. For details, refer to the manuals for Virtual Edition. - To use power consumption monitoring, the XCP version should be 1090 or later.
	SPARC Enterprise T5120 SPARC Enterprise T5140 SPARC Enterprise T5220	- Configured physical servers can be used by associating them with physical L-Servers. For details, refer to "Chapter 18 Linking L-Servers with

Software	Hardware	Remarks
	SPARC Enterprise T5240 SPARC Enterprise T5440	Configured Physical Servers or Virtual Machines" in the "User's Guide for Infrastructure Administrators (Resource Management) CE". - Servers can be managed. For details, refer to the manuals for Virtual Edition. - The ILOM version should be version 3.0 or later.
HBA address rename setup service	Personal computers (*3) PRIMERGY RX series servers PRIMERGY BX series servers PRIMERGY TX series servers PRIMEQUEST Other PC servers	-

*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).

Note

The functions that agents can use differ depending on the hardware being used.

Table 2.65 Function Availability List

Function		PRIMERGY Series Servers		PRIMEQUEST	SPARC Enterprise	Other PC servers
		Blade Models	Rack Mount/Tower Models			
Status monitoring		Yes	Yes	Yes	Yes	Yes (*1)
Power operations		Yes	Yes	Yes	Yes	Yes
Backup and restore (*2)		Yes	Yes	Yes	No	Yes
Hardware maintenance		Yes	Yes (*3)	Yes (*3)	No	Yes (*3)
Maintenance LED		Yes	No	No	No	No
External management software		Yes	Yes	Yes	Yes	No
Server switchover	Backup and restore method	Yes	Yes	No	No	Yes
	HBA address rename method (*4)	Yes	Yes	No	No	No
	VIOM server profile exchange method	Yes (*5)	No	No	No	No
	Storage affinity switchover method	No	No	No	Yes (*6)	No
Cloning (*2, *7)		Yes	Yes	Yes (*11)	No	Yes
HBA address rename (*4)		Yes	Yes	No	No	No
VIOM coordination		Yes (*5)	No	No	No	No
VLAN settings		Yes	No	No	No	No
Pre-configuration		Yes	Yes	Yes	Yes	Yes
Power consumption monitoring		Yes (*8)	Yes (*9)	No	Yes (*10)	No

Yes: Use possible.
No: Use not possible.

*1: Server monitoring in coordination with server management software is not possible.
*2: When agents are operating on iSCSI disks, image operations are not possible for the following disk configurations.
Perform operation using a single iSCSI disk configuration.

- iSCSI disk + internal disk
- iSCSI disk + SAN disk

*3: Maintenance LEDs cannot be operated.
*4: When using HBA address rename, the mounted HBA must be compatible with HBA address rename.
*5: ServerView Virtual-IO Manager is required.
*6: Only M3000 servers, SPARC Enterprise Partition Models and T5120/T5140/T5220/T5240/T5440 servers with undivided areas are supported. SPARC Enterprise Partition Models with divided areas are not supported.
*7: Cloning of Linux agents operating on iSCSI disks is not possible.
*8: Only BX900 S1 chassis and BX920 S1, BX920 S2, BX922 S2, BX924 S2, and BX960 S1 servers are supported.
*9: Only rack mount models (RX200/300/600) are supported.
*10: Only M3000 servers are supported.
*11: Cloning is available only when Legacy boot is specified for the boot option. When UEFI is specified, cloning is unavailable.

Required Hardware for Admin Clients

The following hardware is required for admin clients:

Table 2.66 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	-

Hardware Condition of Storage that can be Connected with Physical L-Server

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

Table 2.67 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: - 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. - ETERNUS DX8000 S2 series - ETERNUS DX400 S2 series - ETERNUS DX90 S2 - ETERNUS DX80 S2

Hardware	Remarks
	- 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. - 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 Dynamic LUN mirroring can be used with Resource Orchestrator with the following apparatuses. - ETERNUS DX8000 S2 series - ETERNUS DX410 S2 - ETERNUS DX440 S2 - ETERNUS DX90 S2 When using the target units for the following options, Automatic Storage Layering can be used with Resource Orchestrator. - 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.

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

Table 2.68 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

Hardware Conditions of Storage that can be Connected to Virtual L-Servers

When connecting storage units to virtual L-Servers, the following storage units can be used:

[VMware]
Refer to "Supported Storage Configurations" in "E.1.3 Storage Preparations".

[Hyper-V]
Refer to "Supported Storage Configurations" in "E.2.3 Storage Preparations".

[Xen]
Refer to "Supported Storage Configurations" in "E.3.3 Storage Preparations".

[Oracle VM]
Refer to "Supported Storage Configurations" in "E.4.3 Storage Preparations".

[KVM]
Refer to "Supported Storage Configurations" in "E.5.3 Storage Preparations".

[Solaris Containers]
Refer to "Supported Storage Configurations" in "E.6.3 Storage Preparations".

Network Hardware Conditions When Using Simplifying of Network Settings:

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

- Physical L-Server

  "B.3.1 Automatic Network Configuration" in the "Setup Guide CE"

- Virtual L-Server

  - "C.2.4 Automatic Network Configuration" in the "Setup Guide CE"
  - "C.3.4 Automatic Network Configuration" in the "Setup Guide CE"

Table 2.69 Supported Network Devices

Hardware		Version
L2 switches (*)	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	IOS 12.2 or later

Hardware		Version
	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	
	Cisco Nexus 2000 series (*3) Cisco Nexus 5000 series (*3)	NX-OS V4.1 or later
	Brocade VDX 6710 series (*3) Brocade VDX 6720 series (*3) Brocade VDX 6730 series (*3)	NOS 2.0 or later
Firewall (*2)	Fujitsu IPCOM EX IN series Fujitsu IPCOM EX SC series	E20L10 or later
	Fujitsu NS Appliance (*4)	-
	Cisco ASA 5500 series (*5)	ASASoftware-8.3 or later
Server load balancer (*2)	Fujitsu IPCOM EX IN series Fujitsu IPCOM EX LB series (*3)	E20L10 or later
	F5 Networks BIG-IP Local Traffic Manager series	BIG-IP V11.2

* Note: L2 switches are essential 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
- When placing an L2 switch between a firewall and server load balancer
- When placing an L2 switch between a server load balancer and a rack mount or tower server

*2: Necessary when placing a firewall or a server load balancer on an L-Platform.

*3: Network device monitoring is supported but sample scripts for automatic configuration are not offered.

*4: This is not a hardware product but a virtual appliance.

*5: Cisco ASA5505 is not supported.

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

Hardware Conditions of Power Monitoring Devices

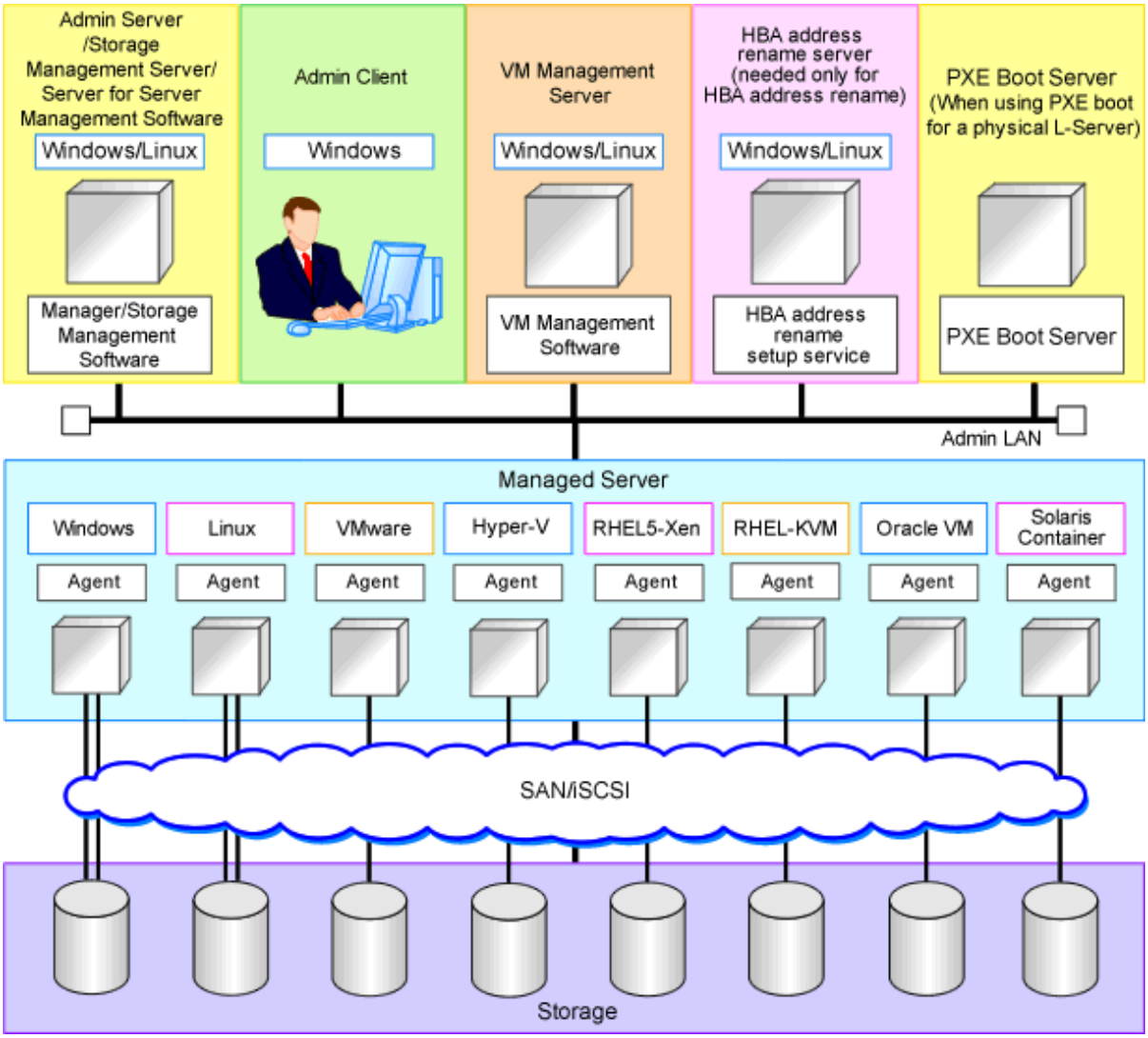
Table 2.70 Supported Power Monitoring Devices

Hardware	Remarks
Symmetra RM 4000VA PG-R1SY4K/PG-R1SY4K2	The firmware version of the network management card is v2.5.4 or v3.0 or higher
Smart-UPS RT 10000 PY-UPAR0K/PG-R1SR10K	-
Smart-UPS RT 5000 PY-UPAC5K	-

2.6 System Configuration

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

Figure 2.8 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]
Register VMware ESXi as the target in ServerView Operations Manager when using 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.

Note

When using VMware ESXi, Resource Orchestrator agents cannot be installed.
Install ServerView ESXi CIM Provider agents.

When using other vendor's servers, perform "C.1.5 Configuration when Creating a Virtual L-Server using VMware ESXi on other Vendor's Servers" in the "Setup Guide CE".

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.

Install Web browsers on admin clients.
If a server virtualization software client is installed on an admin client, the software can be started from the client screen of Resource Orchestrator.

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 no server is necessary for storage management software, as Navisphere operates on the Storage Processor (hereinafter 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.

Server Management Server

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

- When using BMC BladeLogic Server Automation
  - Necessary when creating an L-Server in a Solaris Container.
  - Can be placed on the same server as the manager (recommended) or on another server.

    When operating managers in clusters, place it on a different server.

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 online 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 "10.1.3 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

Note

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 "5.4.2 Registering Blade Servers" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

iSCSI LAN

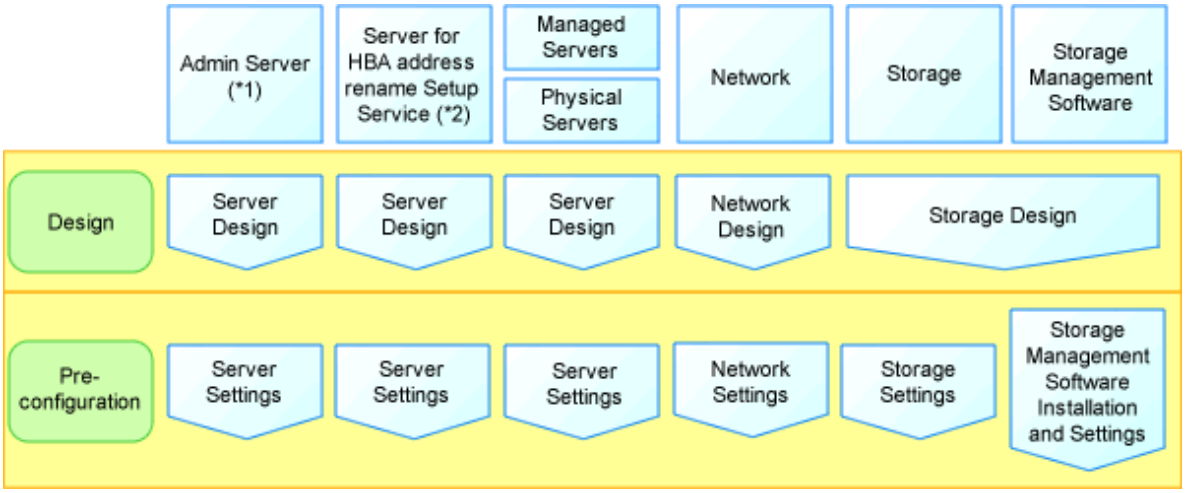
Refer to "9.1.3 Physical Network Design for the Public LAN and iSCSI LAN".

Chapter 3 Flow of Resource Orchestrator Design and Preparations

This chapter explains the flow of Resource Orchestrator Design and Preparation.

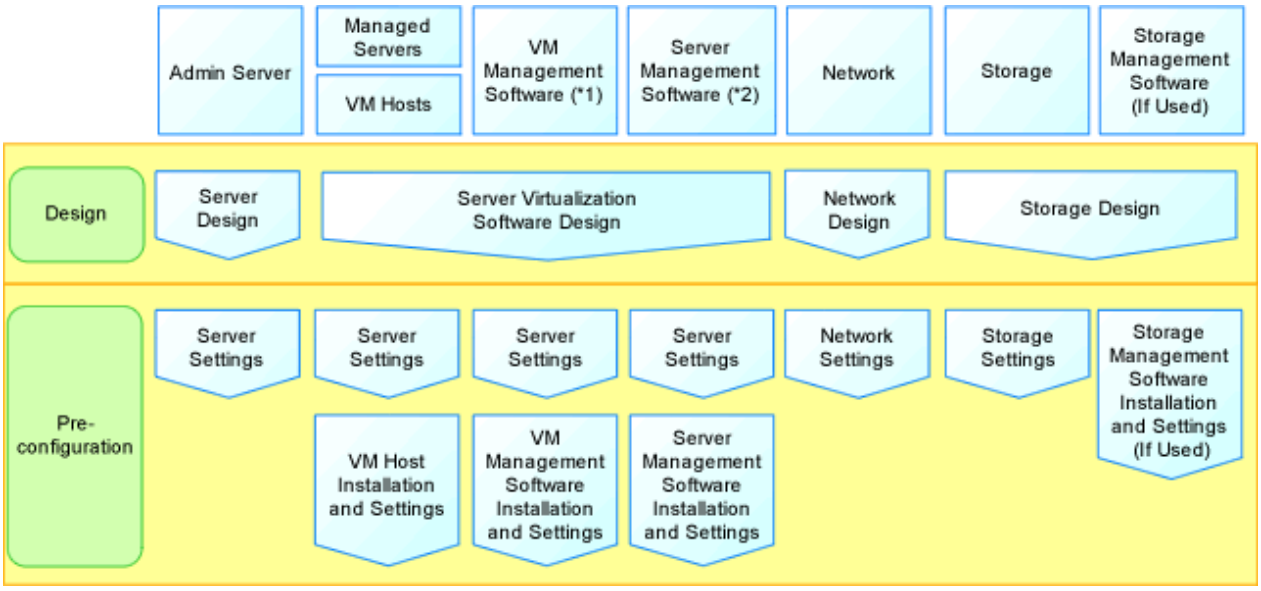
The flows for physical L-Servers and virtual L-Servers are different.

Figure 3.1 Preparations for Resource Orchestrator Installation (Physical L-Server)



*1: When creating a physical L-Server using a blade server, installation of VIOM is necessary.
*2: Necessary when creating a physical L-Server using a rack mount or tower server.

Figure 3.2 Preparations for Resource Orchestrator installation (Virtual L-Server)



*1: When using RHEL-Xen, KVM or Solaris Containers, VM Management Software is not necessary.
*2: When using Solaris Containers, Server Management Software is necessary.

Resource Orchestrator Setup Design

Design the following content when installing this product.

- System Configuration Design

  For details, refer to "Chapter 4 System Configuration Design".

- Defining User Accounts

  For details, refer to "Chapter 5 Defining User Accounts".

- Defining Tenant and Resource Pools

  For details, refer to "Chapter 6 Defining Tenants and Resource Pools".

- Defining High Availability and Disaster Recovery

  Refer to "Chapter 7 Defining High Availability and Disaster Recovery".

- Defining the Server Environment

  Define the server environment to manage with the admin server and this product.

  For details, refer to "8.1 Defining the Server Environment".

- Define the Network Environment

  For details, refer to "Chapter 9 Defining and Configuring the Network Environment".

- Deciding the Storage Environment

  For details, refer to "10.1 Deciding the Storage Environment".

- Deciding Server Virtualization Software

  Decide the server virtualization software to manage with this product.

  For details, refer to "11.1 Deciding Server Virtualization Software".

- Installing and Defining Single Sign-On

  decide the single sign-on environment.

  For details, refer to "Chapter 12 Installing and Defining Single Sign-On".

- Deciding the Power Monitoring Environment

  For details, refer to "13.1 Deciding the Power Monitoring Environment".

Pre-setup Preparations

The advance preparation is necessary before the manager of this product is installed.

Perform it according to the following procedure.

- Defining the Server Environment

  The server environment managed with the admin server and this product is set.

  Refer to "8.2 Configuring the Server Environment".

- Configure the Network Environment

  For details, refer to "Chapter 9 Defining and Configuring the Network Environment".

- Configuring the Storage Environment

  For details, refer to "10.2 Configuring the Storage Environment".

- Defining the Server Environment

  Set the server virtualization software managed with this product.

  For details, refer to "11.2 Settings for Server Virtualization Software".

- Installing and Defining Single Sign-On

  set the single sign-on environment.

  For details, refer to "Chapter 12 Installing and Defining Single Sign-On".

- Configuring the Power Monitoring Environment

  For details, refer to "13.2 Configuring the Power Monitoring Environment".

Chapter 4 System Configuration Design

This section explains how to design a system configuration.

L-Server Design

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

For details, refer to the following:

- For Physical L-Servers

  For details, refer to "D.1 System Configuration".

- For Virtual L-Servers

  [VMware]
  For details, refer to "E.1.1 System Configuration".

  [Hyper-V]
  For details, refer to "E.2.1 System Configuration".

  [Xen]
  For details, refer to "E.3.1 System Configuration".

  [Oracle VM]
  For details, refer to "E.4.1 System Configuration".

  [KVM]
  For details, refer to "E.5.1 System Configuration".

  [Solaris Containers]
  For details, refer to "E.6.1 System Configuration".

L-Platform Network Design

For details on L-Platform Network design, refer to "9.1 Defining the Network Environment".

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.

Chapter 5 Defining User Accounts

This chapter explains the user accounts used in Resource Orchestrator.

Defining 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.

For details on the resources which can be operated for each role, refer to "5.1 Restricting Access Using Roles".

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 1 and 32 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 12.1 Object Class" in "12.3 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.

5.1 Restricting Access Using Roles

This section explains the control of access using roles.

5.1.1 Overview

Resource Orchestrator can limit the available operations and resources based on the user.

- Collections of possible operations

  These are referred to as roles.

- Resources that can be operated

  These are referred to as access scope.
  The access scope of a user who was assigned the tenant administrator role or the tenant user role is a tenant that they manage and use.

Privileges can be controlled by configuring the roles and access scope based on users.

The following names are used for roles. For details on the detailed operation privileges for each role, refer to "Operation Scopes of Roles" in "5.1.2 Roles and Available Operations".

Table 5.1 Role Types

Role Types	Role Names	Description
Infrastructure Administrative Role	Infrastructure administrator (infra_admin)	An infrastructure administrator manages the ICT resources of a private cloud (servers, storage, network), and OSs running on an L-Platform. An infrastructure administrator performs consolidated management of pooled ICT resources using Resource Orchestrator, confirms load status and when necessary, adds ICT resources, and performs switchover and maintenance. The role of the infrastructure administrator is cannot perform operations when L-Platforms and an L-Servers are operating. Use this role to limit the privileges of users managing the infrastructure in regards to L-Platform and L-Servers, in order to prevent the accidental operation of said L-Platforms and L-Servers. The only operations that can be performed for an L-Platform, are monitoring and backup, and for an L-Server, monitoring and the operations given in "17.7 Migration of VM Hosts between Servers" in the "User's Guide for Infrastructure Administrators (Resource Management) CE". However, all operations can be performed for the other resources.
	Infrastructure operator (infra_operator)	An infrastructure operator can only monitor an L-Platform. Power operations and backup for resources in a resource pool can also be executed by an infrastructure operator.
	Infrastructure monitor (monitor)	A monitor can only monitor all resources.
Tenant Management Roles	Tenant administrator (tenant_admin)	Tenant administrators perform L-Server template management, user management of tenant users, and approval of L-Platform creation applications from tenant users. Use a tenant administrator, when another administrator manages an L-Platform, such as when performing cloud-type operations to borrow an L-Platform.
	Tenant operator (tenant_operator)	Tenant operator can only perform the following operations from the operations which tenant administrators can perform. - Resource backup - L-Platform power operation - Resource monitoring of all tenants - Tenant and local pool monitoring
	Tenant monitor (tenant_monitor)	A tenant monitor can only monitor L-Platforms and L-Servers.
Multiple Roles	Administrator (administrator)	An administrator is both an infrastructure administrator and a tenant administrator.
	Operator (operator)	An operator is both an infrastructure operator and a tenant operator.
	Monitor (monitor)	A monitor can only monitor all resources.
Tenant Use Roles	Tenant user (tenant_user)	Tenant users can create L-Platforms inside tenants. Tenant users apply to tenant administrators to create and use L-Platforms. When an application is approved and an L-Platform created, the user who applied is automatically assigned the role of L-Platform User (lplatform_user).

Role Types	Role Names	Description
	L-Platform User (lplatform_user)	L-Platform User is the role to enable tenant users (tenant_user) to use L-Platforms. L-Platform users can operate, change, and delete L-Platforms. This role is automatically assigned when an L-Platform is created. When the L-Platform is deleted, the assigned role is deleted automatically. Addition and deletion is not necessary.

User groups are the function for executing batch management of multiple users. By configuring roles and access scopes in the same way as for users, user privileges for all users belonging to the user group can be configured as a batch operation.

For user groups, only "supervisor" and "monitor" are defined by default.

For the "supervisor" user group, the access scope and role of "all=administrator" are configured.
"all=administrator" is the role for administrators (administrators who are both infrastructure administrators and tenant administrators) with unlimited access scopes.

For the "monitor" user group, the access scope and role of "all=monitor" are configured.
"all=monitor" is the role for monitors (monitors who are both infrastructure monitors and tenant monitors) with unlimited access scopes.

When a tenant is created, the user group corresponding to a tenant will be created. When the tenant administrator and tenant users are created, they belong to a user group corresponding to the tenant.

If no user group is specified when creating a user, the user group will be the same as the user who performed creation. Therefore, it is not necessary to consider the existence of user groups, when using a user within the same department.

When resource folders and resources specified in the access scope of a user and a user group are deleted, they are also deleted from the access scope and the role settings.

For details on the relations on access scope and role settings of a user and a user group, refer to "Table 5.2 Relations on Access Scope and Role Settings of Users and User Groups".

Table 5.2 Relations on Access Scope and Role Settings of Users and User Groups

Users	User Groups	Access Scope and Roles
Configured	Configured	User configurations are valid
Configured	Not configured	User configurations are valid
Not configured	Configured	User group configurations are valid
Not configured	Not configured	All resources are inaccessible

5.1.2 Roles and Available Operations

This section explains roles.

For details on how to configure roles and access scopes for users and user groups, refer to "Chapter 3. Configuring Users for Infrastructure Administrators" in the "User's Guide for Infrastructure Administrators (Resource Management)".

By specifying a combination of role and access scope for the target user or user group, the access privileges are restricted. The access scope is restricted by specifying resource folders, resource pools, or resources in the orchestration tree.

Among the users with the infrastructure admin role, those users who have had their scope of access limited can only refer to certain resources. For this reason, only an orchestration tree can be used among the trees of a resource tab. Switchover to other trees is not possible.

For details on trees, refer to "A.1 ROR Console" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Operation Scopes of Roles

- Infrastructure Administrative Role
- Tenant Management Roles

- Tenant Users
- Multiple Roles

Table 5.3 Infrastructure Administrative Role

Type	Operation	Operator (Role)		
		Infrastructure Administrators infra_admin	Infrastructure Operator infra_operator	Infrastructure Monitor monitor
Application Process	Approval	No	No	No
	Evaluation	Yes	No	No
L-Server/L-Platform	Creation	No	No	No
	Modification/ Movement/Deletion	No	No	No
	Power Operation (Usage Change) (*1)	No	No	No
	Console Screen Acquisition	No	No	No
	Snapshot/Backup	No	No	No
	Image Collection	No	No	No
	Monitoring	Yes	Yes	Yes
	System Conditions	Yes	Yes	Yes
	Capacity Planning	Yes	Yes	Yes
	Network Device Operation	No	No	Yes (*6)
Maintenance of L-Servers	Migration	Yes	No	No
	Conversion/Reversion	Yes	No	No
L-Server Templates	Import/Modification/ Deletion	Yes	No	No
	Export	Yes	Yes	No
	Viewing	Yes	Yes	Yes
L-Platform Template	Create new templates	Yes	No	No
	Copying/Modification/ Deletion	Yes	No	No
	Viewing	Yes	Yes (*2)	Yes (*2)
L-Server for infrastructure administrator	Creation/Modification/ Movement/Deletion	Yes	No	No
	Power operation (Usage change)	Yes	Yes	No
	Console Screen Acquisition	Yes	Yes	No
	Snapshot/Backup	Yes	Yes	No
	Image Collection	Yes	Yes	No
	Monitoring	Yes	Yes	Yes
Maintenance of the L-Server for the	Migration	Yes	No	No

Type	Operation	Operator (Role)		
		Infrastructure Administrators infra_admin	Infrastructure Operator infra_operator	Infrastructure Monitor monitor
infrastructure administrator				
Resource Pool	Creation/Modification/ Movement/Deletion	Yes	No	No
	Resource registration/ deletion (*3)	Yes	No	No
	Migration of resources between resource pools	Yes	No	No
	Monitoring	Yes	Yes	Yes
	Pool Conditions	Yes	Yes	Yes
	Capacity Planning	Yes	Yes	Yes
Physical Server	Registration/Deletion	Yes	No	No
	Power control (*4)	Yes	Yes	No
	Console Screen Acquisition	Yes	Yes	No
	Maintenance Mode Settings	Yes	No	No
	Monitoring	Yes	Yes	Yes
	System Conditions	Yes	Yes	Yes
VM Hosts	Registration/Deletion	Yes	No	No
	Power Operations	Yes	Yes	No
	Maintenance Mode Settings	Yes	No	No
	Monitoring	Yes	Yes	Yes
	System Conditions	Yes	Yes	Yes
	Capacity Planning	Yes	Yes	Yes
Storage management software	Creation/Modification/ Deletion	Yes	No	No
	Monitoring	Yes	Yes	Yes
Disk	Registration/Deletion (*3)	Yes	No	No
	Modification	Yes	No	No
	Monitoring	Yes	Yes	Yes
Network	Creation/Modification/ Deletion	Yes	No	No
	Monitoring	Yes	Yes	Yes
Address	Creation/Modification/ Deletion	Yes	No	No
	Monitoring	Yes	Yes	Yes
Image	Modification	Yes	No	No

Type	Operation	Operator (Role)		
		Infrastructure Administrators infra_admin	Infrastructure Operator infra_operator	Infrastructure Monitor monitor
	Deletion	Yes	No	No
	Monitoring	Yes	Yes	Yes
Chassis	Creation/Modification/ Deletion	Yes	No	No
	Power Operations	Yes	Yes	No
	Monitoring	Yes	Yes	Yes
Power Monitoring Device	Creation/Modification/ Deletion	Yes	No	No
	Monitoring	Yes	Yes	Yes
Network Devices	Creation/Modification/ Deletion	Yes	No	No
	Monitoring	Yes	Yes	Yes
	Management of Device Configuration Files	Yes	No	No
File Server	Viewing	Yes	No	No
Network Configuration Information	Import	Yes	No	No
	Export	Yes	No	No
Server NIC Definitions	Reflect/Display	Yes	No	No
Pre-configuration	Download	Yes	No	No
Tenants	Creation/Modification/ Movement/Deletion	Yes	No	No
	Monitoring	Yes	Yes	Yes
Resource Folders	Creation/Modification/ Movement/Deletion	Yes	No	No
	Monitoring	Yes	Yes	Yes
	L-Server batch power operations under resource folders (*5)	Yes	Yes	No
Users	Modification of individual information	Yes	Yes	Yes
	Addition/Modification/ Deletion of users in the user group the user belongs to	Yes	No	No
	Addition/Modification/ Deletion of users in other user groups	Yes	No	No
	Viewing	Yes	Yes	Yes
User Groups	Creation/Modification/ Deletion	Yes	No	No

Type	Operation	Operator (Role)		
		Infrastructure Administrators infra_admin	Infrastructure Operator infra_operator	Infrastructure Monitor monitor
	Viewing	Yes	Yes	Yes
L-Platform Template Software Information	Creation	Yes	No	No
	Copying	Yes	No	No
	Modification/Deletion	Yes	No	No
	Viewing	Yes	Yes (*2)	Yes (*2)
L-Platform Template Image Information	Creation	Yes	No	No
	Copying	Yes	No	No
	Modification/Deletion/ Display Modification	Yes	No	No
	Viewing	Yes	Yes (*2)	Yes (*2)
L-Platform Template Segment Information	Creation	Yes	No	No
	Modification/Deletion	Yes	No	No
	Viewing	Yes	Yes (*2)	Yes (*2)
L-Platform Template Template Information	Creation	Yes	No	No
	Copying	Yes	No	No
	Modification/Deletion/ Display Modification	Yes	No	No
	Viewing	Yes	Yes (*2)	Yes (*2)
Usage Charges	Search by tenant	Yes	No	No
	Search by L-Platform	Yes	No	No

*1: Usage changes are only possible when L-Server attributes have been configured in advance.
*2: Information about L-Platform templates can only be obtained using the L-Platform API.
*3: Users whose access scopes are not restricted should perform resource registration.
*4: The power operations are also available from BladeViewer.
*5: Power operations are only carried out for the L-Server for the infrastructure administrator.
*6: It is possible to use rulesets for operations which infrastructure administrator prepare for displaying information of network devices.

Table 5.4 Tenant Management Roles

Type	Operation	Operator (Role)		
		Tenant Administrators tenant_admin	Tenant Operator tenant_operator	Tenant Monitor tenant_monitor
Application Process	Approval	Yes (*1)	No	No
	Evaluation	No	No	No
L-Server/L-Platform	Creation	Yes	No	No
	Modification/ Movement/Deletion	Yes	No	No
	Power Operation (Usage Change) (*2)	Yes	Yes	No
	Console Screen Acquisition	Yes	Yes	No

Type	Operation	Operator (Role)		
		Tenant Administrators tenant_admin	Tenant Operator tenant_operator	Tenant Monitor tenant_monitor
	Snapshot/Backup	Yes	Yes	No
	Image Collection	Yes	Yes	No
	Monitoring	Yes	Yes	Yes
	System Conditions	Yes	Yes	Yes
	Capacity Planning	Yes	Yes	Yes
	Network Device Operation	Yes	Yes	Yes (*5)
L-Server Templates	Import/Modification/ Deletion	No	No	No
	Export	No	No	No
	Viewing	Yes	No	No
L-Platform Template	Create new templates	No	No	No
	Copying/Modification/ Deletion	Yes (*3)	No	No
	Viewing	Yes	Yes (*4)	Yes (*4)
	Modification of L-Servers	No	No	No
Resource Pool	Monitoring	Yes	Yes	No
	Pool Conditions	Yes	Yes	Yes
	Capacity Planning	Yes	Yes	Yes
Physical Server	Monitoring	Yes	Yes	No
	System Conditions	Yes	Yes	Yes
VM Hosts	Monitoring	Yes	Yes	No
Image	Modification	Yes	No	No
	Deletion	Yes	No	No
	Monitoring	Yes	Yes	No
Network Devices	Monitoring	Yes	Yes	No
Users	Modification of individual information	Yes	Yes	Yes
	Addition/Modification/ Deletion of users in the tenant the user belongs to	Yes	No	No
	Addition/Modification/ Deletion of users in another tenant	No	No	No
	Viewing	Yes	Yes	Yes
L-Platform Template Software Information	Creation	Yes	No	No
	Copying	Yes	No	No
	Modification/Deletion	Yes	No	No

Type	Operation	Operator (Role)		
		Tenant Administrators tenant_admin	Tenant Operator tenant_operator	Tenant Monitor tenant_monitor
	Viewing	Yes	Yes (*4)	Yes (*4)
L-Platform Template Image Information	Creation	Yes	No	No
	Copying	Yes	No	No
	Modification/Deletion/ Display Modification	Yes	No	No
	Viewing	Yes	Yes (*4)	Yes (*4)
L-Platform Template Segment Information	Creation	Yes	No	No
	Modification/Deletion	Yes	No	No
	Viewing	Yes	Yes (*4)	Yes (*4)
L-Platform Template Template Information	Creation	No	No	No
	Copying	Yes	No	No
	Modification/Deletion/ Display Modification	Yes	No	No
	Viewing	Yes	Yes (*4)	Yes (*4)
Usage Charges	Search by tenant	No	No	No
	Search by L-Platform	Yes	No	No

*1: Tenant administrators approve L-Platform applications submitted by tenant users or other tenant administrators.
*2: Usage changes are only possible when L-Server attributes have been configured in advance.
*3: Only the data that the user copied can be changed or deleted.
*4: Information about L-Platform templates can only be obtained using the L-Platform API.
*5: It is possible to use rulesets for operations which infrastructure administrator prepare for displaying information of network devices.

Table 5.5 Tenant Users

Type	Operation	Tenant Users tenant_user	L-Platform User lplatform_user
Application Process	Approval	No	No
	Evaluation	No	No
L-Server/L-Platform	Creation	Yes	No
	Modification/Movement/Deletion	No	Yes
	Power Operation (Usage Change) (*)	No	Yes
	Console Screen Acquisition	No	Yes
	Snapshot/Backup	No	Yes
	Image Collection	No	No
	Monitoring	No	Yes
	System Conditions	No	Yes
	Network Device Operation	No	Yes
L-Server Templates	Import/Modification/Deletion	No	No
	Export	No	No
	Viewing	Yes	Yes

Type	Operation	Tenant Users tenant_user	L-Platform User lplatform_user
L-Platform Template	Create new templates	No	No
	Copying/Modification/Deletion	No	No
	Viewing	Yes	Yes
Resource Pool	Monitoring	Yes	Yes
Physical Server	Monitoring	Yes	Yes
	System Conditions	Yes	Yes
VM Hosts	Monitoring	Yes	Yes
Image	Modification	No	No
	Deletion	No	No
	Monitoring	Yes	Yes
Network Devices	Monitoring	Yes	Yes
Users	Modification of individual information	Yes	Yes
	Viewing	Yes	Yes
L-Platform Template Software Information	Creation	No	No
	Copying	No	No
	Modification/Deletion	No	No
	Viewing	Yes	No
L-Platform Template Image Information	Creation	No	No
	Copying	No	No
	Modification/Deletion/Display Modification	No	No
	Viewing	Yes	No
L-Platform Template Segment Information	Creation	No	No
	Modification/Deletion	No	No
	Viewing	Yes	No
L-Platform Template Template Information	Creation	No	No
	Copying	No	No
	Modification/Deletion/Display Modification	No	No
	Viewing	Yes	No
Usage Charges	Search by tenant	No	No
	Search by L-Platform	No	No

* Note: Usage changes are only possible when L-Server attributes have been configured in advance.

Table 5.6 Multiple Roles

Type	Operation	Administrator administrator	Operator operator	Monitor monitor
Application Process	Approval (*1)	Yes	No	No
	Evaluation	Yes	No	No

Type	Operation	Administrator administrator	Operator operator	Monitor monitor
L-Server/L-Platform	Creation	Yes	No	No
	Modification/ Movement/Deletion	Yes	No	No
	Power Operation (Usage Change) (*2)	Yes	Yes	No
	Console Screen Acquisition	Yes	Yes	No
	Snapshot/Backup	Yes	Yes	No
	Image Collection	Yes	Yes	No
	Monitoring	Yes	Yes	Yes
	System Conditions	Yes	Yes	Yes
	Capacity Planning	Yes	Yes	Yes
	Network Device Operation	Yes	Yes	Yes (*6)
Maintenance of L-Servers	Migration	Yes	No	No
	Conversion/Reversion	Yes	No	No
L-Server Templates	Import/Modification/ Deletion	Yes	No	No
	Export	Yes	Yes	No
	Viewing	Yes	Yes	Yes
L-Platform Template	Create new templates	Yes	No	No
	Copying/Modification/ Deletion	Yes	No	No
	Viewing	Yes	Yes (*5)	Yes (*5)
L-Server for infrastructure administrator	Creation/Modification/ Movement/Deletion	Yes	No	No
	Power operation (Usage change)	Yes	Yes	No
	Console Screen Acquisition	Yes	Yes	No
	Snapshot/Backup	Yes	Yes	No
	Image Collection	Yes	Yes	No
	Monitoring	Yes	Yes	Yes
Maintenance of the L-Server for the infrastructure administrator	Migration	Yes	No	No
Resource Pool	Creation/Modification/ Movement/Deletion	Yes	No	No
	Resource registration/ deletion (*3)	Yes	No	No
	Migration of resources between resource pools	Yes	No	No

Type	Operation	Administrator administrator	Operator operator	Monitor monitor
	Monitoring	Yes	Yes	Yes
	Pool Conditions	Yes	Yes	Yes
	Capacity Planning	Yes	Yes	Yes
Physical Server	Registration/Deletion	Yes	No	No
	Power control (*4)	Yes	Yes	No
	Console Screen Acquisition	Yes	Yes	No
	Maintenance Mode Settings	Yes	No	No
	Monitoring	Yes	Yes	Yes
	System Conditions	Yes	Yes	Yes
VM Hosts	Registration/Deletion	Yes	No	No
	Power Operations	Yes	Yes	No
	Maintenance Mode Settings	Yes	No	No
	Monitoring	Yes	Yes	Yes
	System Conditions	Yes	Yes	Yes
	Capacity Planning	Yes	Yes	Yes
Storage management software	Creation/Modification/ Deletion	Yes	No	No
	Monitoring	Yes	Yes	Yes
Disk	Registration/Deletion (*3)	Yes	No	No
	Modification	Yes	No	No
	Monitoring	Yes	Yes	Yes
Network	Creation/Modification/ Deletion	Yes	No	No
	Monitoring	Yes	Yes	Yes
Address	Creation/Modification/ Deletion	Yes	No	No
	Monitoring	Yes	Yes	Yes
Image	Modification	Yes	No	No
	Deletion	Yes	No	No
	Monitoring	Yes	Yes	Yes
Chassis	Creation/Modification/ Deletion	Yes	No	No
	Power Operations	Yes	Yes	No
	Monitoring	Yes	Yes	Yes
Power Monitoring Device	Creation/Modification/ Deletion	Yes	No	No
	Monitoring	Yes	Yes	Yes

Type	Operation	Administrator administrator	Operator operator	Monitor monitor
Network Devices	Creation/Modification/ Deletion	Yes	No	No
	Monitoring	Yes	Yes	Yes
	Management of Device Configuration Files	Yes	No	No
File Server	Viewing	Yes	No	No
Network Configuration Information	Import	Yes	No	No
	Export	Yes	No	No
Server NIC Definitions	Reflect/Display	Yes	No	No
Pre-configuration	Download	Yes	No	No
Tenants	Creation/Modification/ Movement/Deletion	Yes	No	No
	Monitoring	Yes	Yes	Yes
Resource Folders	Creation/Modification/ Movement/Deletion	Yes	No	No
	Monitoring	Yes	Yes	Yes
	L-Server batch power operations under resource folders	Yes	Yes	No
Users	Modification of individual information	Yes	Yes	Yes
	Addition/Modification/ Deletion of users in the user group the user belongs to	Yes	No	No
	Addition/Modification/ Deletion of users in other user groups	Yes	No	No
	Viewing	Yes	Yes	Yes
User Groups	Creation/Modification/ Deletion	Yes	No	No
	Viewing	Yes	Yes	Yes
L-Platform Template Software Information	Creation	Yes	No	No
	Copying	Yes	No	No
	Modification/Deletion	Yes	No	No
	Viewing	Yes	Yes (*5)	Yes (*5)
L-Platform Template Image Information	Creation	Yes	No	No
	Copying	Yes	No	No
	Modification/Deletion/ Display Modification	Yes	No	No
	Viewing	Yes	Yes (*5)	Yes (*5)

Type	Operation	Administrator administrator	Operator operator	Monitor monitor
L-Platform Template Segment Information	Creation	Yes	No	No
	Modification/Deletion	Yes	No	No
	Viewing	Yes	Yes (*5)	Yes (*5)
L-Platform Template Template Information	Creation	Yes	No	No
	Copying	Yes	No	No
	Modification/Deletion/ Display Modification	Yes	No	No
	Viewing	Yes	Yes (*5)	Yes (*5)
Usage Charges	Search by tenant	Yes	No	No
	Search by L-Platform	Yes	No	No

*1: Dual-role administrators approve L-Platform applications submitted by dual-role administrators.
*2: Usage changes are only possible when L-Server attributes have been configured in advance.
*3: Users whose access scopes are not restricted should perform resource registration.
*4: The power operations are also available from BladeViewer.
*5: Information about L-Platform templates can only be obtained using the L-Platform API.
*6: It is possible to use rulesets for operations which infrastructure administrator prepare for displaying information of network devices.

Operate resources registered in a resource pool, by selecting the resource in the resource pool after selection from the orchestration tree. To operate resources which are not registered in resource pool or resources which are unable to be registered, use a user with full operation access scope.

5.2 Customizing Access Authority for L-Platform Operations

Authorization (access authority) to operate the L-Platform Management window can be customized in accordance with the user role (tenant administrator, tenant user).

Operations for the L-Platform Management window, from which access authority can be customized, are as follows.

- L-Platform subscription
- L-Platform cancellation
- L-Platform reconfiguration
- Server startup / shutdown
- Take, restore and deletion of virtual server snapshots
- Event log reference
- Image collection
- Backup, restore and deletion of physical servers
- Firewall settings
- Server load balancer settings

The access authority customize commands are used to customize access authority. Refer to "Chapter 11 Access Authority Customize Commands" in the "Reference Guide (Command/XML) CE" for information on the access authority customize commands.

Chapter 6 Defining Tenants and Resource Pools

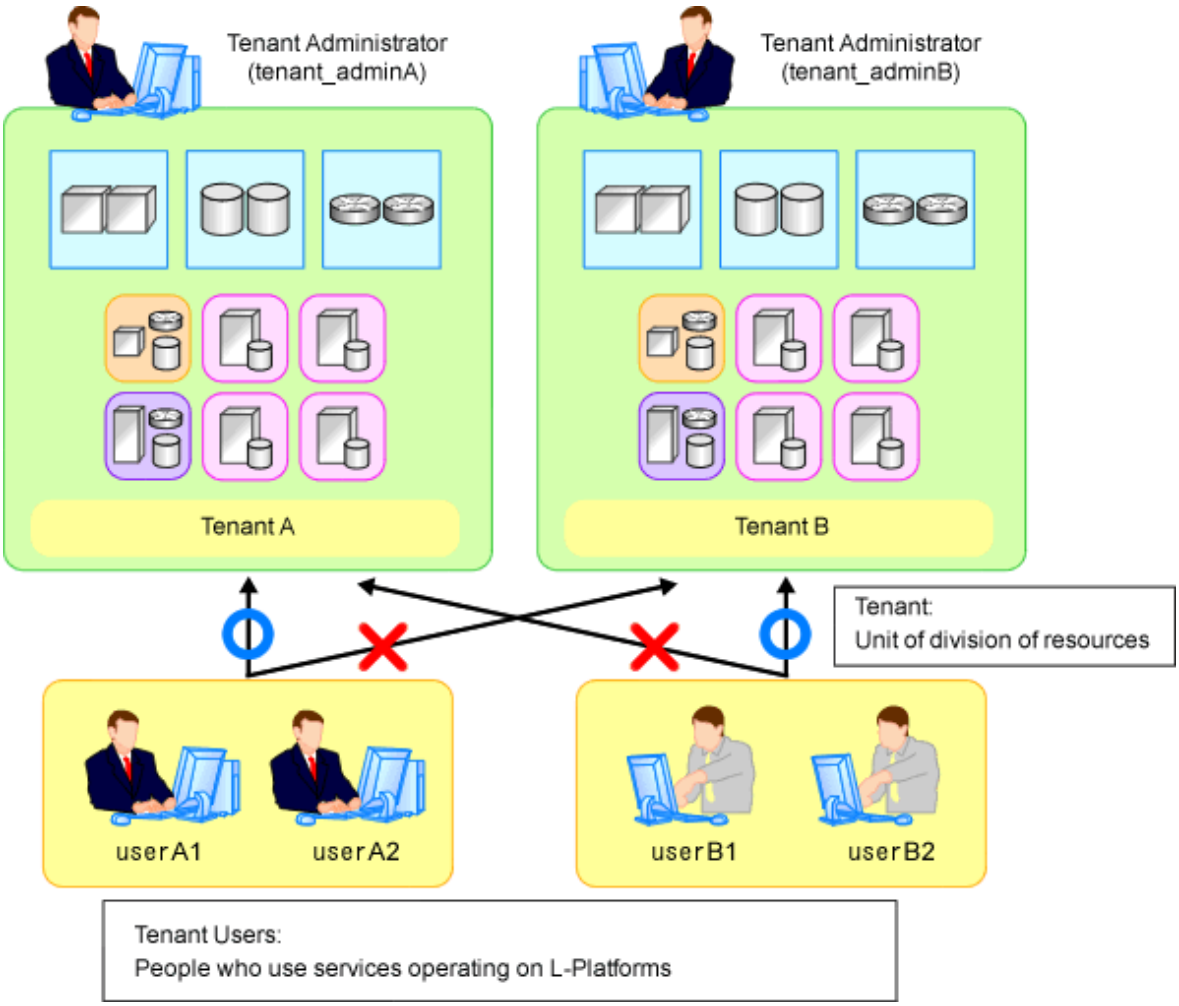
This section explains how to design tenants and resource pools.

6.1 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 6.1 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

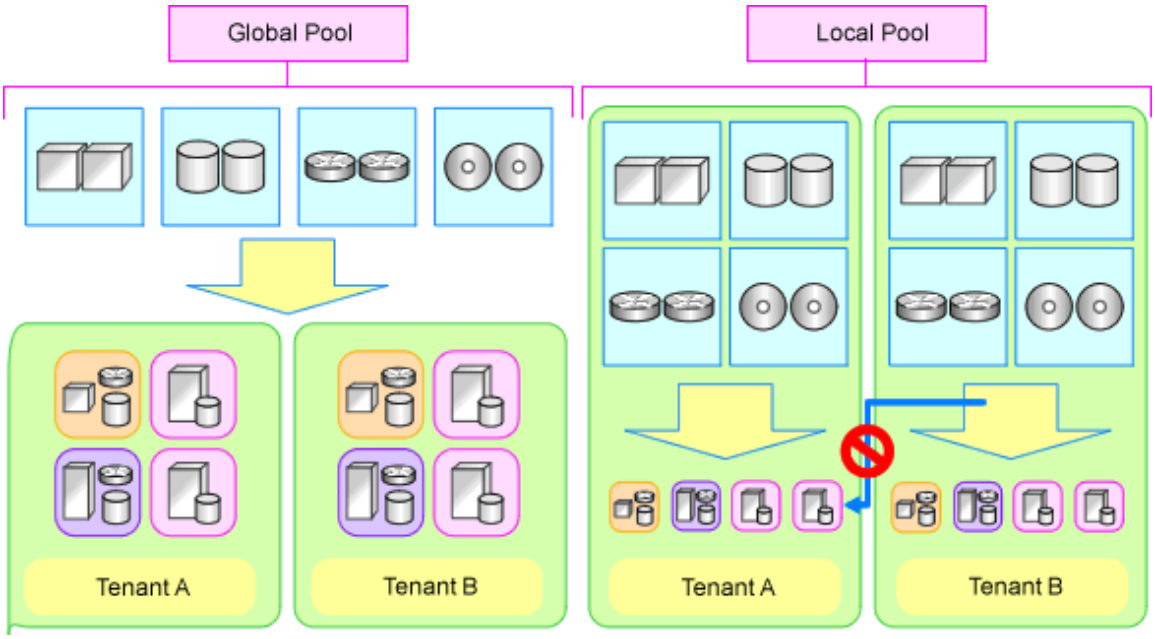
  Resource pools for each tenant.

- 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 6.2 Global Pools and Local Pools



6.2 Tenant Operation

This section explains how to operate tenants.

The following five patterns of tenant operation are available.

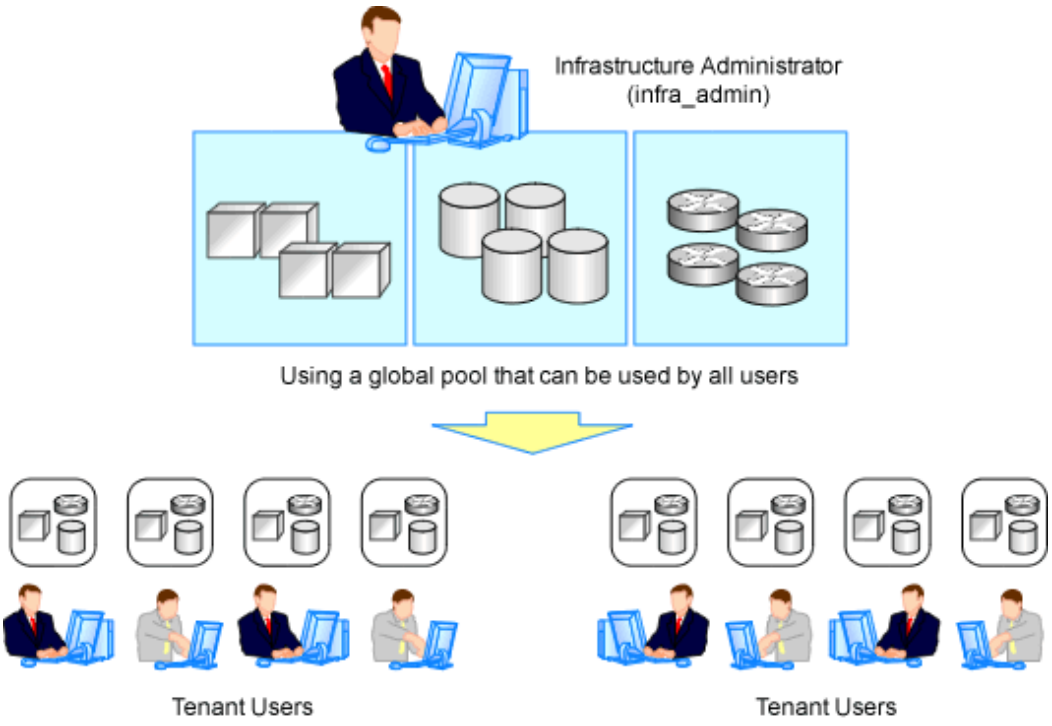
Table 6.1 Tenant Operation

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	Divide in tenant	Use local pools only
D	Divide in tenant	Use both global pools and local pools Use local pools as a priority
E	Divide in tenant	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 6.3 Pattern A

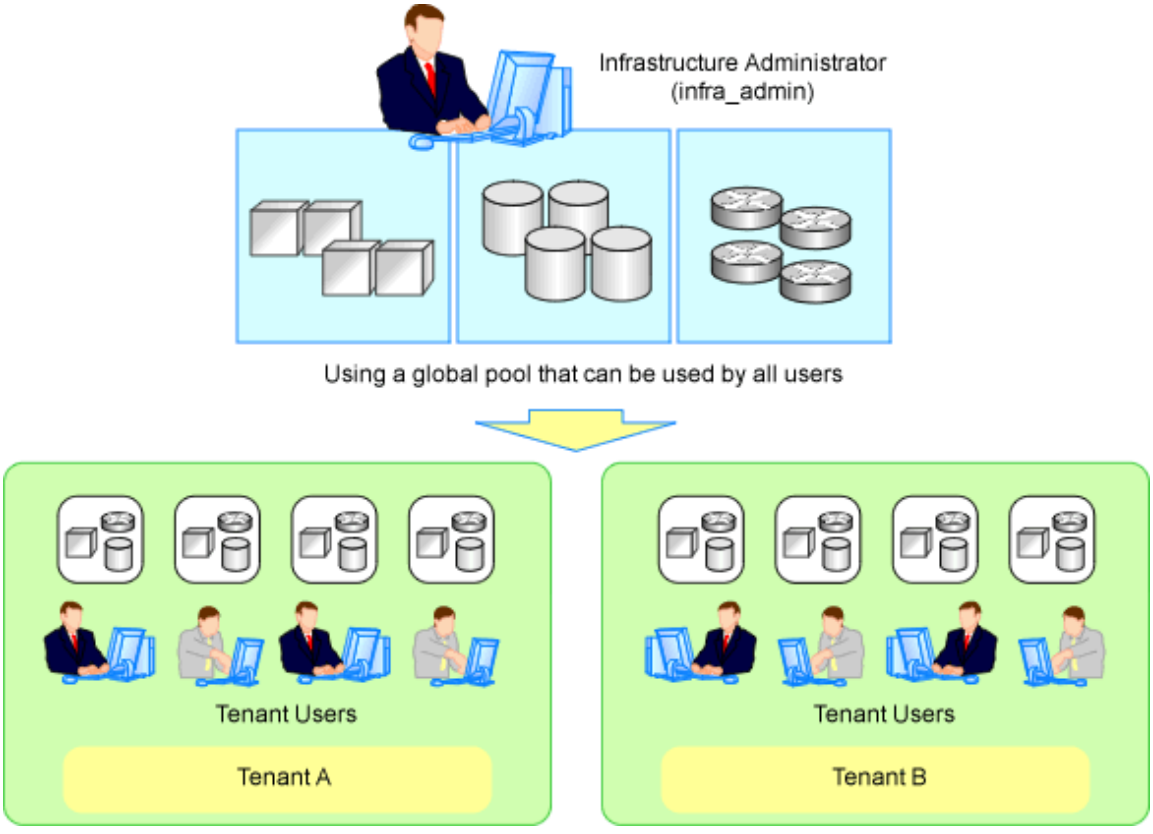


(Pattern B) Divide for Each Tenant (Global Pools Only)

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

This enables public cloud-conscious tenant operation.

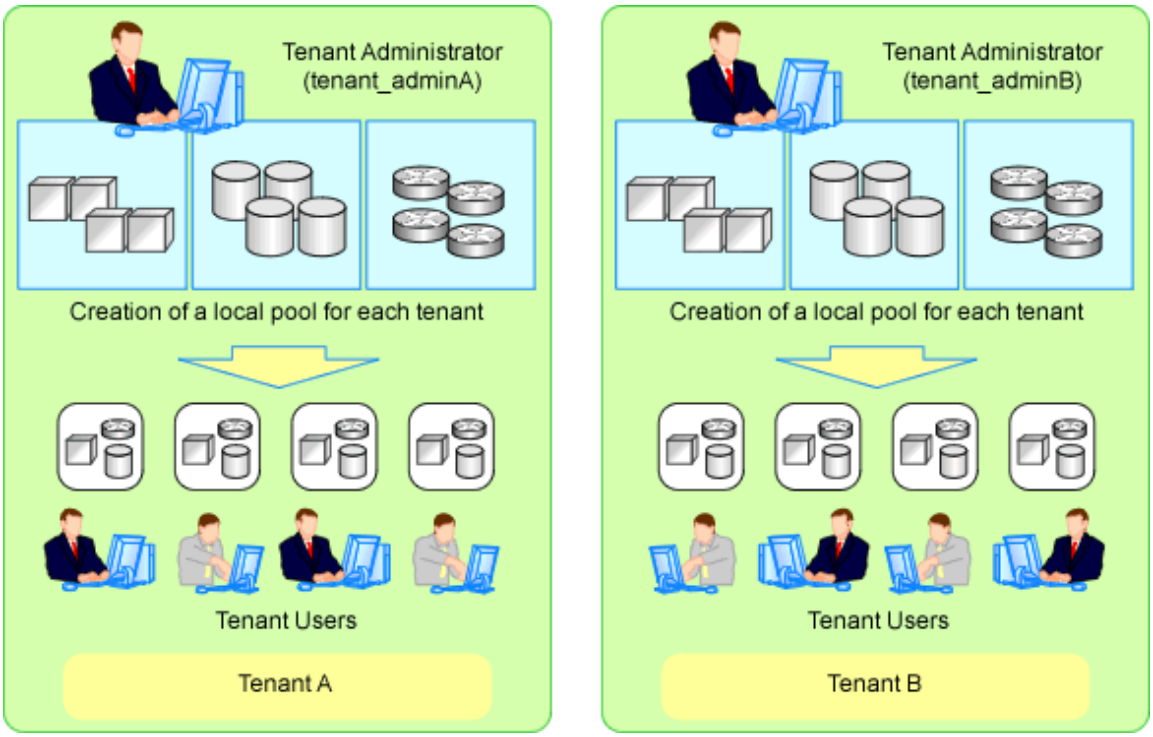
Figure 6.4 Pattern B



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

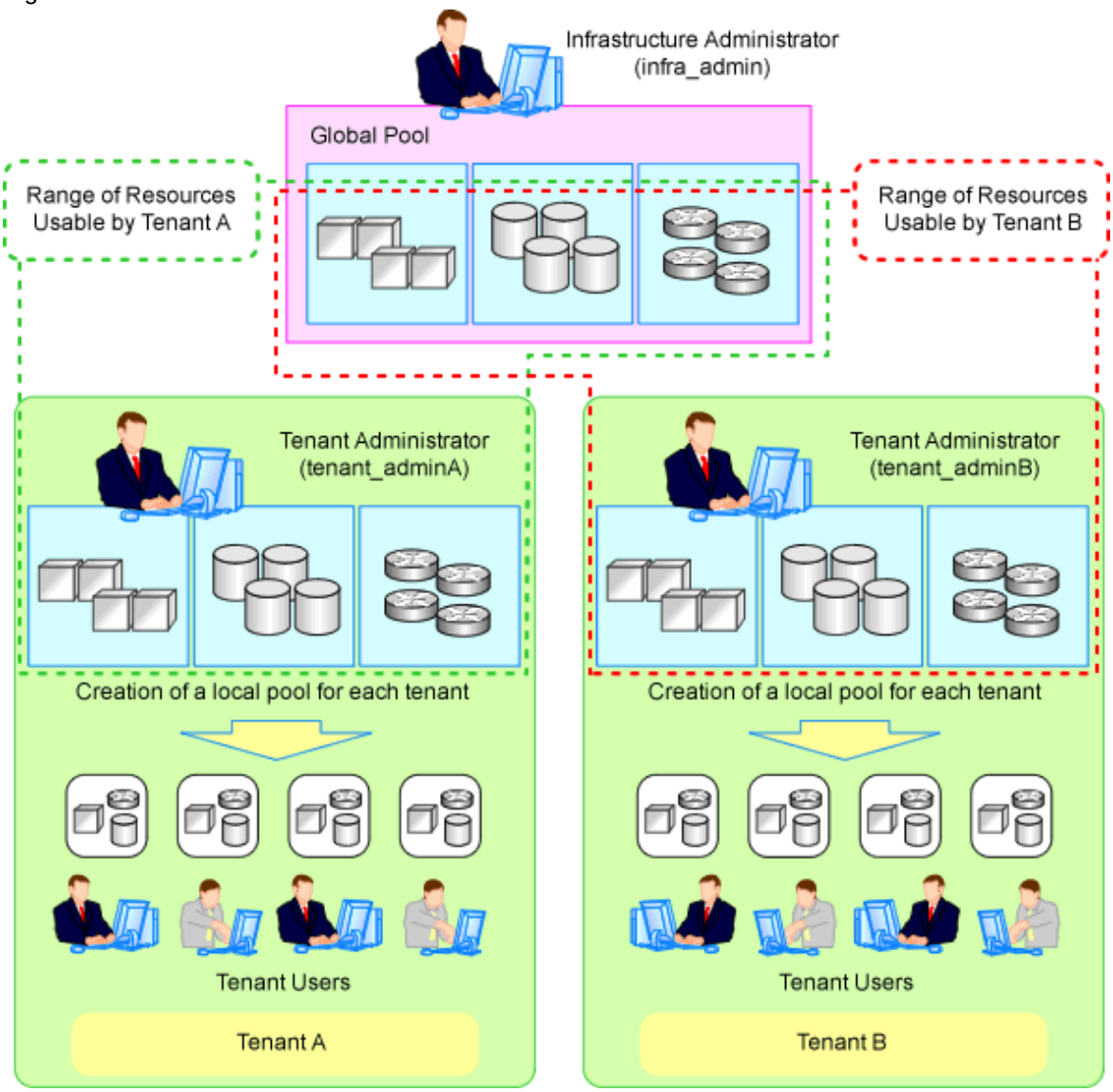
Create a local pool for each tenant. This pattern is a similar operation to allocating resources to each tenant.

Figure 6.5 Pattern C



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

Figure 6.6 Pattern D

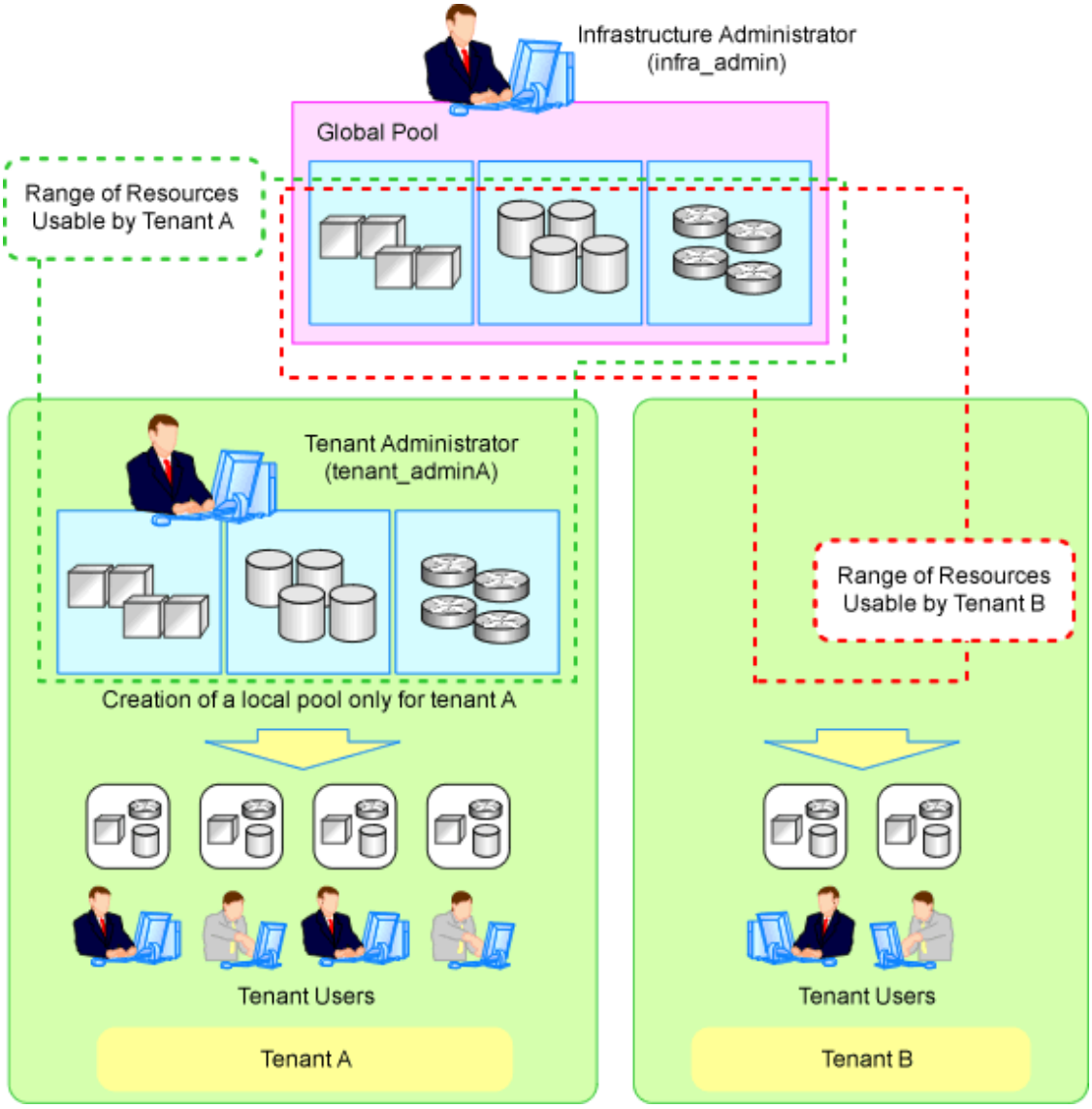


Only spare resources are placed in global pools. These spare resources are used when there is an increased workload.

(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 6.7 Pattern E



6.3 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 6.2 Global Pool and Local Pool Selection Policy

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

The existence of a local pool and the global pool used by a tenant can be specified as an initial value at the time of tenant creation. To change the initial value at the time of tenant creation, modify the tenant creation default definition file.

For details of the tenant creation default definition file, refer to "14.10 Tenants" in the "Reference Guide (Command/XML) CE".

6.4 Resource Pool Types

This section explains the types of resource pools.

Resource pools are categorized as indicated below.

Table 6.3 Resource Pool Types

Resource Pool Types	Overview
VM Pool	A resource pool for storing VM hosts used when creating new servers (VM). VM hosts of different server virtualization software can be stored. 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. 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.
Server Pool	A resource pool for storing the physical servers used when creating new servers.
Storage Pool	Resource pools containing the following resources: - Virtual storage resources (RAID groups, aggregates, VM file systems) - Disk resources (LUNs, FlexVol, virtual disks) The following resources can be stored together: - Virtual storage resources - Disk resources - Resources of differing storage devices
Network Pool	Resource pools containing the following resources: - Network resource (VLAN ID and an external connection port, etc. are defined). - Network devices (Firewalls) - Network devices (Server load balancers)
Address Pool	Resource pools containing the following resources: - MAC address (Media Access Control address) - WWN
Image Pool	Resource pools containing the following resources: - 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

6.5 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.

6.6 Concept for Separating Tenants by Resource Pool

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

6.6.1 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.

6.6.2 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.
- This section explains the concept for separating tenants (necessity of local pool creation) for each resource pool.

6.6.3 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.

- 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

6.6.4 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.

6.6.5 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, as the required resources differ based on the types of servers and server virtualization software, when managing different servers, division of the access pool simplifies management. The method of division should be matched to that of the server pool.

Table 6.4 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

Yes: Necessary

No: Not necessary

Table 6.5 Address Set Resources Required for Each Server Virtualization Software

	MAC address (Media Access Control address)	WWN
RHEL5-Xen, KVM	Yes	No
Excluding RHEL5-Xen, KVM	No	No

Yes: Necessary

No: Not necessary

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.

6.6.6 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.
Images gathered after configuration of tenant-specific applications should be managed in the local pool of the relevant tenant.

Chapter 7 Defining High Availability and Disaster Recovery

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

- L-Server redundancy

  L-Server redundancy is possible with Resource Orchestrator.

  On physical L-Servers, by specifying a spare server pool, an operating server can be switched to a spare server when server failure occurs.
  On virtual L-Servers, settings differ according to the server virtualization software being used.
  For details, refer to "17.1.1 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 "17.1.2 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 D Installing VM Hosts on Physical L-Servers" in the "Setup Guide CE".

- 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 "7.2 Storage Chassis High Availability Design".

  For details on operation methods, refer to "17.1.3 Storage Chassis High Availability" in the "Operation Guide CE".

  In the case of VM hosts, failover of disks from the primary site to the backup site can also be performed by building VM hosts on physical L-Servers.

  For details, refer to "Appendix D Installing VM Hosts on Physical L-Servers" in the "Setup 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 "17.2 Admin Server High Availability" in the "Operation Guide CE".

- Disaster Recovery

  Disaster recovery can be done in a simple and reliable way by exporting and importing the following information between managers of Resource Orchestrator.

  - L-Platform Templates
  - L-Platform Configuration Information
  - Resource Information
  - Accounting Information
  - Metering Log

  For details on prerequisites, refer to "Chapter 2 Design" in the "DR Option Instruction".

  For details on installing and operating Disaster Recovery, refer to "Chapter 3 Installation" and "Chapter 4 Operation" in the "DR Option Instruction".

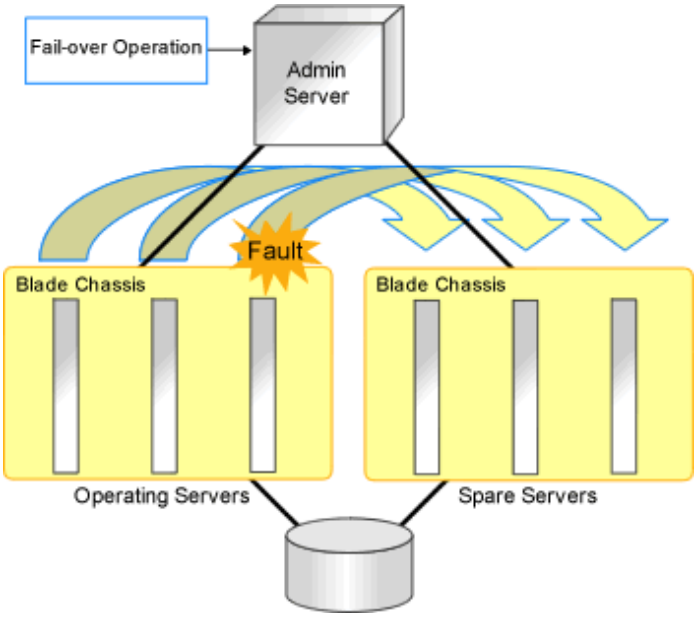
7.1 Blade Chassis High Availability Design

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 D Installing VM Hosts on Physical L-Servers" in the "Setup Guide CE".

Figure 7.1 Server Switchover when a Chassis Fails



7.2 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 CLARiiON, 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.

- 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.

7.3 Admin Server High Availability Design

Redundancy for managers is possible with Resource Orchestrator.

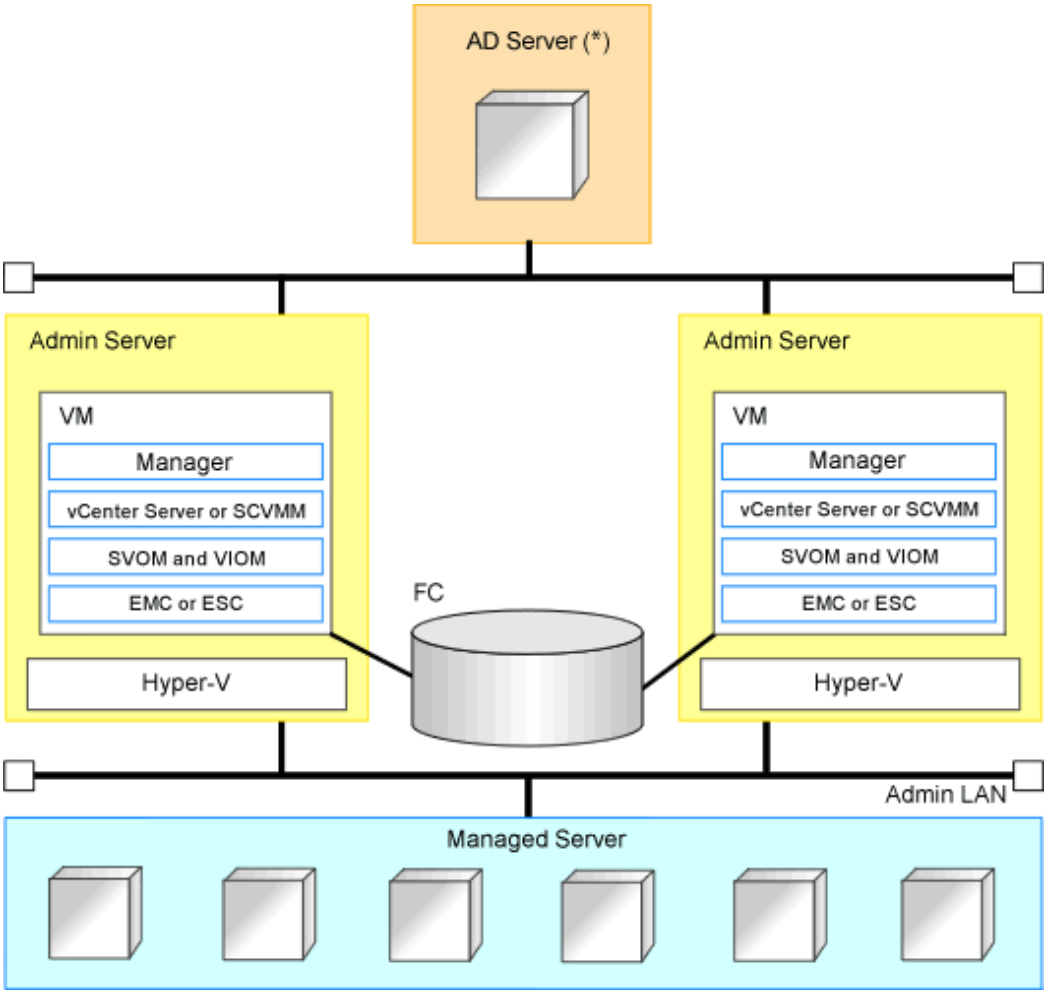
High availability configuration of admin servers can be performed as follows.

- Operating the manager on a virtual machine and using the redundancy function of the virtual machine
  - Managers operate on a Windows guest OS of a Hyper-V virtual machine environment.
  - 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.

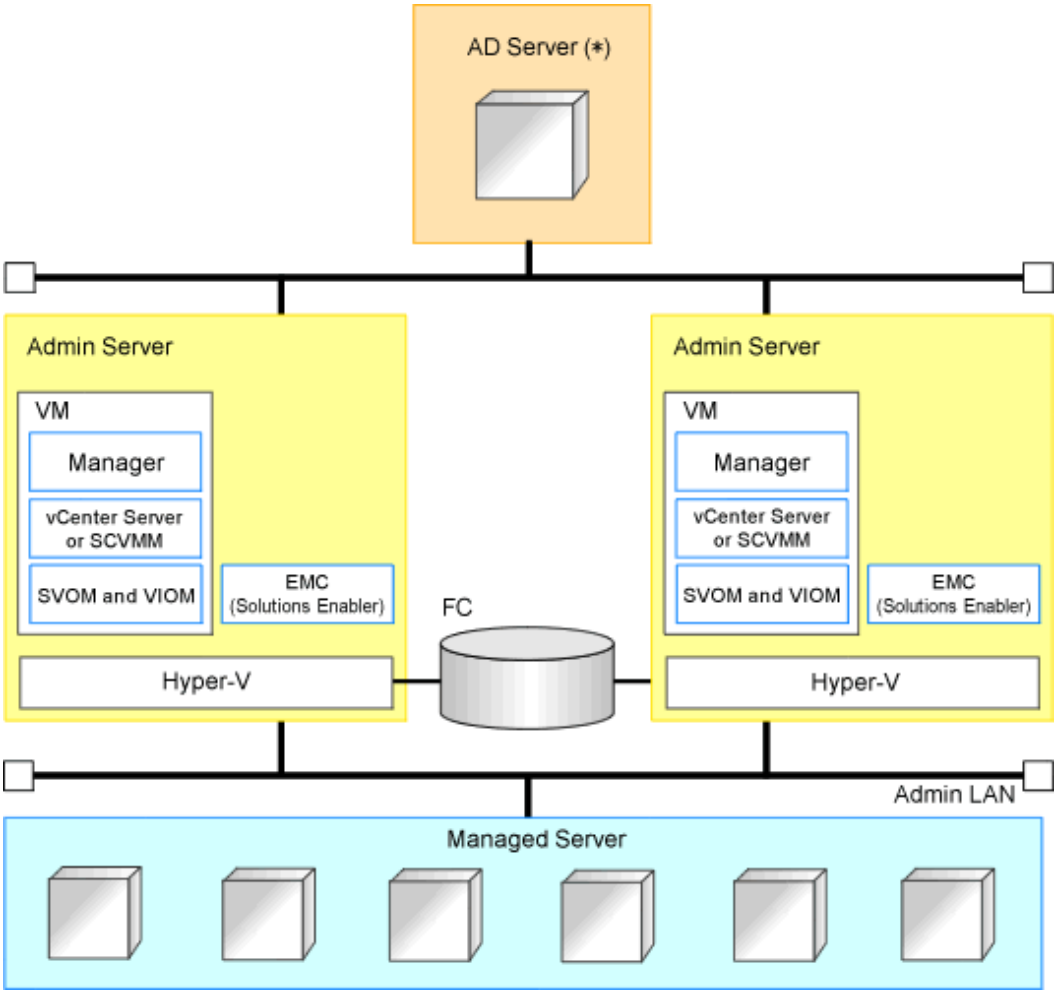
The configurations are shown below.

Figure 7.2 Storage other than EMC (Symmetrix)



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

Figure 7.3 EMC (Symmetrix) Storage



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

Chapter 8 Defining and Configuring the Server Environment

This section explains how to define and configure server environments.

8.1 Defining the Server Environment

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

In this product, it corresponds to the following kind of servers. Decide the value set to the server according to the kind of the server.

- Blade Servers

  For details, refer to "8.1.1 Settings for Blade Servers".

- Rack Mount and Tower Servers

  For details, refer to "8.1.2 Settings for Rack Mount and Tower Servers".

- PRIMEQUEST

  For details, refer to "8.2.3 Configuring PRIMEQUEST".

- SPARC Enterprise M3000/T Series

  For details, refer to "8.1.4 Settings for SPARC Enterprise (M3000/T Series)".

  When switching over SPARC Enterprise servers, refer to "8.1.6 Settings when Switching Over SPARC Enterprise Servers".

- SPARC Enterprise M4000/M5000/M8000/M9000

  For details, refer to "8.1.5 Settings for SPARC Enterprise M4000/M5000/M8000/M9000".

  When switching over SPARC Enterprise servers, refer to "8.1.6 Settings when Switching Over SPARC Enterprise Servers".

Servers that do not use the server management software will be treated as "Rack Mount and Tower Server".

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

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.

For details, refer to "D.3.1 Deciding the Storage Environment" in "D.3.1 Deciding the Storage Environment".

8.1.1 Settings for Blade Servers

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.

8.1.2 Settings for Rack Mount and 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 ("-").

Note

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

8.1.3 Settings 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.

Note

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

8.1.4 Settings for SPARC Enterprise (M3000/T Series)

Resource Orchestrator is able to manage SPARC Enterprise servers by using their XSCF interface for the M3000 series and the ILOM interface for the T series as a remote management controller.

For M3000

For M3000, choose values for the following XSCF settings according to the criteria listed below.

IP address

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

User name

Name of the user account used to log into XSCF and gain control over the managed server.
A user account with "platadm" privileges within XSCF must be specified.
The user name must start with an alphabet character, and can contain up to 31 alphanumeric characters, underscores ("_"), and hyphens ("-").

Password

Password used to log into the remote management controller with the above user name.
The user password can contain up to 32 alphanumeric characters, blank spaces (" "), and any of the following characters.
"!", "@", "#", "$", "%", "^", "&", "*", "[", "]", "{", "}", "(", ")", "-", "+", "=", "~", ",", ">", "<", "/", "'", "?", ";", ":"

SNMP trap destination

The destination for SNMP traps sent by XSCF should be set to the admin server's IP address.

SNMP community name

Name of the SNMP community used to communicate with XSCF.
This community name can contain up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

For T Series

For the T series, choose values for the following ILOM settings according to the criteria listed below.

IP address

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

User name

The name of the user account used to log into ILOM and gain control over the managed server.
A user account with Admin privileges within ILOM must be specified.
The user name must start with an alphabet character, and can contain between 4 and 16 alphanumeric characters, underscores ("_"), and hyphens ("-").

Password

Password used to log into the remote management controller with the above user name.
The user password can contain between 8 and 16 alphanumeric characters, blank spaces (" "), and any of the following characters.
"!", "@", "#", "$", "%", "^", "&", "*", "[", "]", "{", "}", "(", ")", "-", "+", "=", "~", ",", ">", "<", "/", "'", "?", ";", ":"

SNMP trap destination

The destination for SNMP traps sent by ILOM should be set to the admin server's IP address.

SNMP community name

Name of the SNMP community used to communicate with ILOM.
This community name can contain up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

8.1.5 Settings for SPARC Enterprise M4000/M5000/M8000/M9000

Resource Orchestrator is able to manage SPARC Enterprise servers by using their XSCF interface as a remote management controller. Choose values for the following XSCF settings according to the criteria listed below.

Chassis name

This name is used to identify the chassis for SPARC Enterprise M4000/M5000/M8000/M9000 servers 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

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

User name

Name of the user account used to log into XSCF and gain control over the managed server.
A user account with "platadm" privileges within XSCF must be specified.
This name can contain up to 31 alphanumeric characters, hyphens ("-"), and underscores ("_").

Password

Password used to log into the remote management controller with the above user name.
The user password can contain up to 32 alphanumeric characters, blank spaces (" "), and any of the following characters.
"!", "@", "#", "$", "%", "^", "&", "*", "[", "]", "{", "}", "(", ")", "-", "+", "=", "~", ",", ">", "<", "/", "'", "?", ";", ":"

SNMP trap destination

The destination for SNMP traps sent by XSCF should be set to the admin server's IP address.

SNMP community name

Name of the SNMP community used to communicate with XSCF.
This community name can contain up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

8.1.6 Settings when Switching Over SPARC Enterprise Servers

When integrating with ESC, it should be configured first. Register the Fibre Channel switches and storage units connected to primary servers and managed servers on ESC.

Note

When integrating with ESC, do not register servers used as spare server for Resource Orchestrator on ESC.

After registration, collect WWNs of HBAs set on physical servers or WWNs of CAs set on storage units.

Collection of WWNs of HBA Set on Physical Servers

From the client window of ESC, collect the WWNs for HBAs contained in the registered servers.
For servers that are not registered on ESC, collect WWNs from the seals, drivers, and utilities provided with HBA cards.
Refer to the storage device manual of each storage device for details.

Collection of WWNs of CA Set on Storage Units

From the client window of ESC, collect the WWNs for HBAs contained in the registered storage.
Refer to the storage device manual of each storage device for details.

Collected WWNs are reflected in the relationship between physical servers and HBA WWNs from the perspective of the server, and in the relationship between the storage CA and WWNs from the perspective of storage devices.
System configuration requires that the relationship between HBA WWNs, storage CA WWNs, and volumes from the perspective of storage devices be defined clearly.
When using a multi-path configuration, design the values to match the order of HBAs configured as primary servers or spare servers with those of the corresponding CAs.

Information

For integration with ESC, Resource Orchestrator supports configurations where managed servers have up to eight HBA ports mounted.

8.2 Configuring the Server Environment

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

Set it according to the value decided in "8.1 Defining the Server Environment" as follows.

- Settings for Blade Servers

  For details, refer to "8.2.1 Configuring Blade Servers".

- Settings for Rack Mount and Tower Servers

  For details, refer to "8.2.2 Configuring Rack Mount and Tower Servers".

- Settings for PRIMEQUEST

  For details, refer to "8.2.3 Configuring PRIMEQUEST".

- Settings for SPARC Enterprise M3000

  Please refer to the following.

  "8.2.4 Configuring SPARC Enterprise M3000 Series"

  "8.2.9 Configuring OBP (Open Boot Prom) Settings (SPARC Enterprise)"

- Settings for SPARC Enterprise M4000/M5000/M8000/M9000

  Please refer to the following.

  "8.2.5 Configuring SPARC Enterprise M4000/M5000/M8000/M9000"

  "8.2.9 Configuring OBP (Open Boot Prom) Settings (SPARC Enterprise)"

- Settings for SPARC Enterprise T Series

  Please refer to the following.

  "8.2.6 Configuring SPARC Enterprise T Series"

  "8.2.9 Configuring OBP (Open Boot Prom) Settings (SPARC Enterprise)"

On the following servers, configure the settings as described in "8.2.7 Configuring BIOS Settings of Managed Servers".

- Blade Servers (not using VIOM)
- Rack Mount and Tower Servers
- PRIMEQUEST

When an OS has been installed on the managed server, configure the settings as described in "8.2.8 Configuring OS Settings of Managed Servers".

When VMware ESXi has been installed on the managed server, configure the settings as described in "8.2.10 Configuring ServerView Operations Manager (VMware ESXi)".

8.2.1 Configuring Blade Servers

Refer to the management blade manual to apply the settings chosen in "8.1.1 Settings for Blade Servers" 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 ServerView Agents installed.

8.2.2 Configuring Rack Mount and Tower 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.

8.2.3 Configuring PRIMEQUEST

Refer to the management board manual to apply the settings chosen in "8.1.3 Settings 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

8.2.4 Configuring SPARC Enterprise M3000 Series

Refer to the management controller (XSCF) manual to apply the settings chosen in "8.1.4 Settings for SPARC Enterprise (M3000/T Series)" to the management controller.

- IP address
- User name
- Password
- SNMP community name
- SNMP trap destination

  This must be the IP address of the admin server.

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

- SNMP Agent
- SSH Service
- HTTPS Service

Note

When assigning multiple IP addresses to multiple network interfaces on a XSCF module, ensure that the IP address used by Resource Orchestrator is assigned to the first of those network interfaces.

Set as follows to automatically start up the OS when powering on.

- Set the "Autoboot" of the Domain Mode to "on".
- Set the mode switch of the operator panel to "Locked" in OpenBoot configurations.

8.2.5 Configuring SPARC Enterprise M4000/M5000/M8000/M9000

Refer to the management controller (XSCF) manual to apply the settings chosen in "8.1.5 Settings for SPARC Enterprise M4000/M5000/M8000/M9000" to configure the following on the IPMI controller.
Note that the SNMP community must be set to Write (read and write) access.

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

  This must be the IP address of the admin server.

Refer to the instructions given in the XSCF manual and enable the following functions.

- SNMP Agent
- SSH Service
- HTTPS Service
- Domain Autoboot

Set as follows to automatically start up the OS when powering on.

- Set the "Autoboot" of the Domain Mode to "on".
- Set the mode switch of the operator panel to "Locked" in OpenBoot configurations.

8.2.6 Configuring SPARC Enterprise T Series

Refer to the management controller (ILOM) manual to apply the settings chosen in "8.1.4 Settings for SPARC Enterprise (M3000/T Series)" to configure the following on the IPMI controller.

- IP address
- User name
- Password
- SNMP community name
- SNMP trap destination

  This must be the IP address of the admin server.

Refer to the instructions given in the ILOM manual and enable the following functions.

- SNMP Agent
- SSH Configuration
- HTTPS Configuration
- IPMI Status

8.2.7 Configuring 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 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".
- Set PXE VLAN Support to "Disabled" when the server switchover method is HBA address rename.

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 "5.4.2 Registering Blade Servers" and "5.5.1 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/

- **When Using VIOM (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

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 "7.3.2 Registering Blade Servers" or "7.4.1 Registering Rack Mount or Tower Servers" in the "User's Guide VE".

FC-HBA BIOS

Apply the same settings as those described in the above "When using HBA address rename for SAN boot" section.

- **When Using VIOM (iSCSI Boot)**

System BIOS

Enable iSCSI boot for the NIC which is used for the iSCSI LAN.

Use the VIOM server profile for the iSCSI boot parameter settings.

For details on server profile setup, refer to the ServerView Virtual-IO Manager manual.

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 the network interface used for the iSCSI LAN (NIC3(Index3))
4. Boot from the network interface used for the iSCSI LAN (NIC4(Index4))

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 "7.3.2 Registering Blade Servers" or "7.4.1 Registering Rack Mount or Tower Servers" in the "User's Guide VE".
- When using NIC3 or NIC4 for the admin LAN, use NICs other than NIC3 and NIC4 for the iSCSI LAN. In this case, switch the order of step 3. and step 4.

FC-HBA BIOS

Disable the function.

8.2.8 Configuring OS Settings of 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)

8.2.9 Configuring OBP (Open Boot Prom) Settings (SPARC Enterprise)

When managing SPARC Enterprise servers from Resource Orchestrator, set the "auto-boot?" option to "true" in the OBP configuration. Otherwise, the operating system will not automatically start up when powering on SPARC Enterprise servers.

- SAN Boot Settings

  Configure the following settings on OBP for automatic boot from SAN storage devices.

  - auto-boot?

    Set to "true".

  - boot-device

    Set with a boot disk identifier at the beginning.

  Configure the following settings on OBP for HBAs connected to the boot disk.

  - HBA boot

    Enable the function.

  - Topology

    Set to NPORT connection.

  - Target devices

    Configure based on the values set in "8.1.6 Settings when Switching Over SPARC Enterprise Servers".

For details, refer to "SPARC Enterprise SAN Boot Environment Build Guide" of the Fibre Channel card driver manual.

8.2.10 Configuring 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.

Chapter 9 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.

9.1 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, server load balancers, and L2 switches) to provide services over internal or external networks (such as intranets or the Internet).

- The network for the iSCSI LAN

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

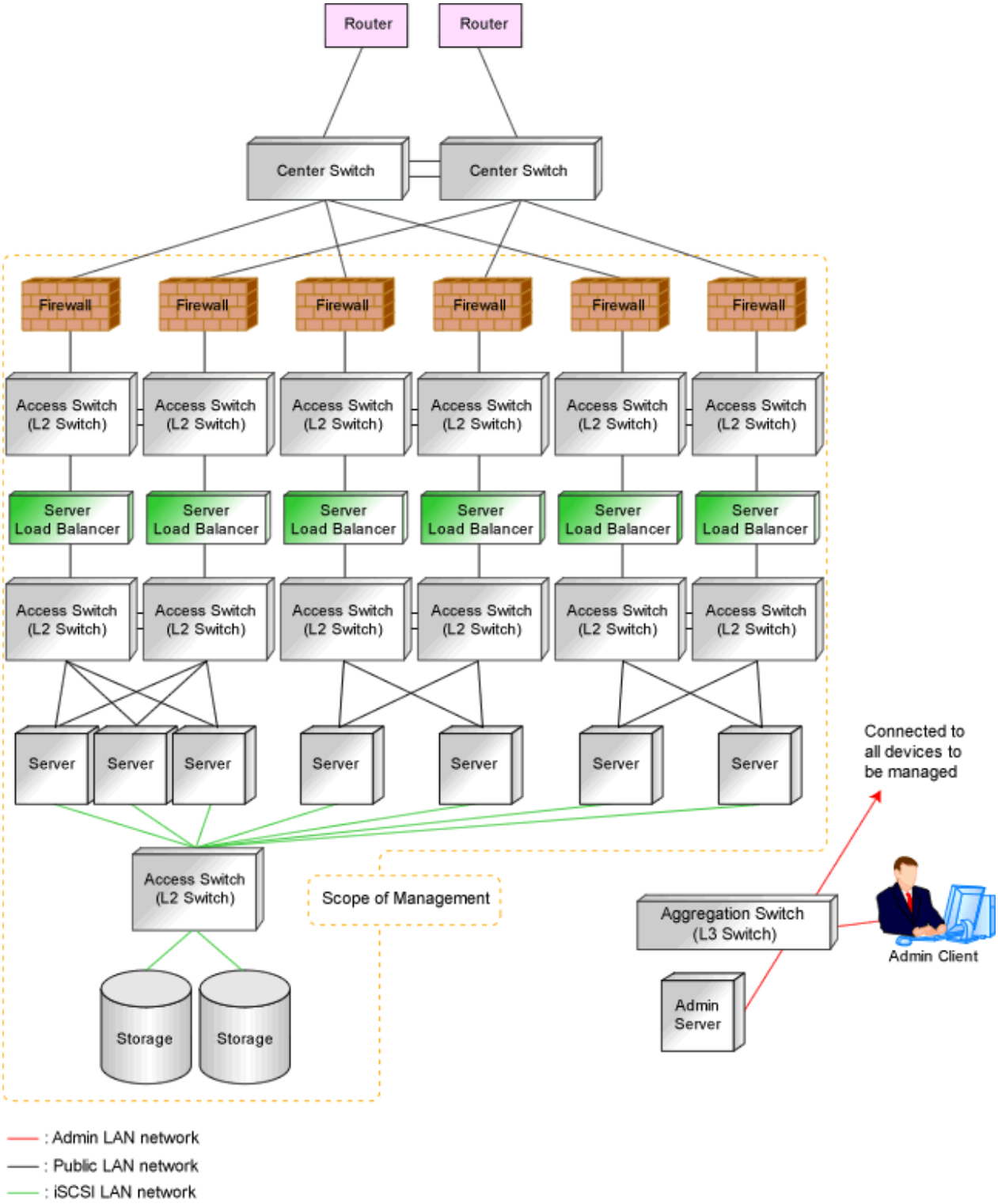
For keeping operations secure, it is recommended to physically configure each network separately.

The maximum value of the subnet mask of the network that Resource Orchestrator supports is 255.255.255.255 (32-bit mask). The minimum value is 255.255.0.0 (16-bit 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 9.1 Network Environment Example



9.1.1 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.

9.1.1.1 Information Necessary for Design

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

- The number of tenants
- 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.
- The scope of VLAN IDs for use on the admin LAN

  As the 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.
- The IP address range of the admin LAN
- Whether to configure admin route redundancy

9.1.1.2 Admin LAN for Servers

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

- Network interface 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 "9.1.1.5 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 "5.4 When using Blade Servers" and "5.5 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.

- Whether to use Admin LAN redundancy

  Perform the redundancy of the admin LAN as below.

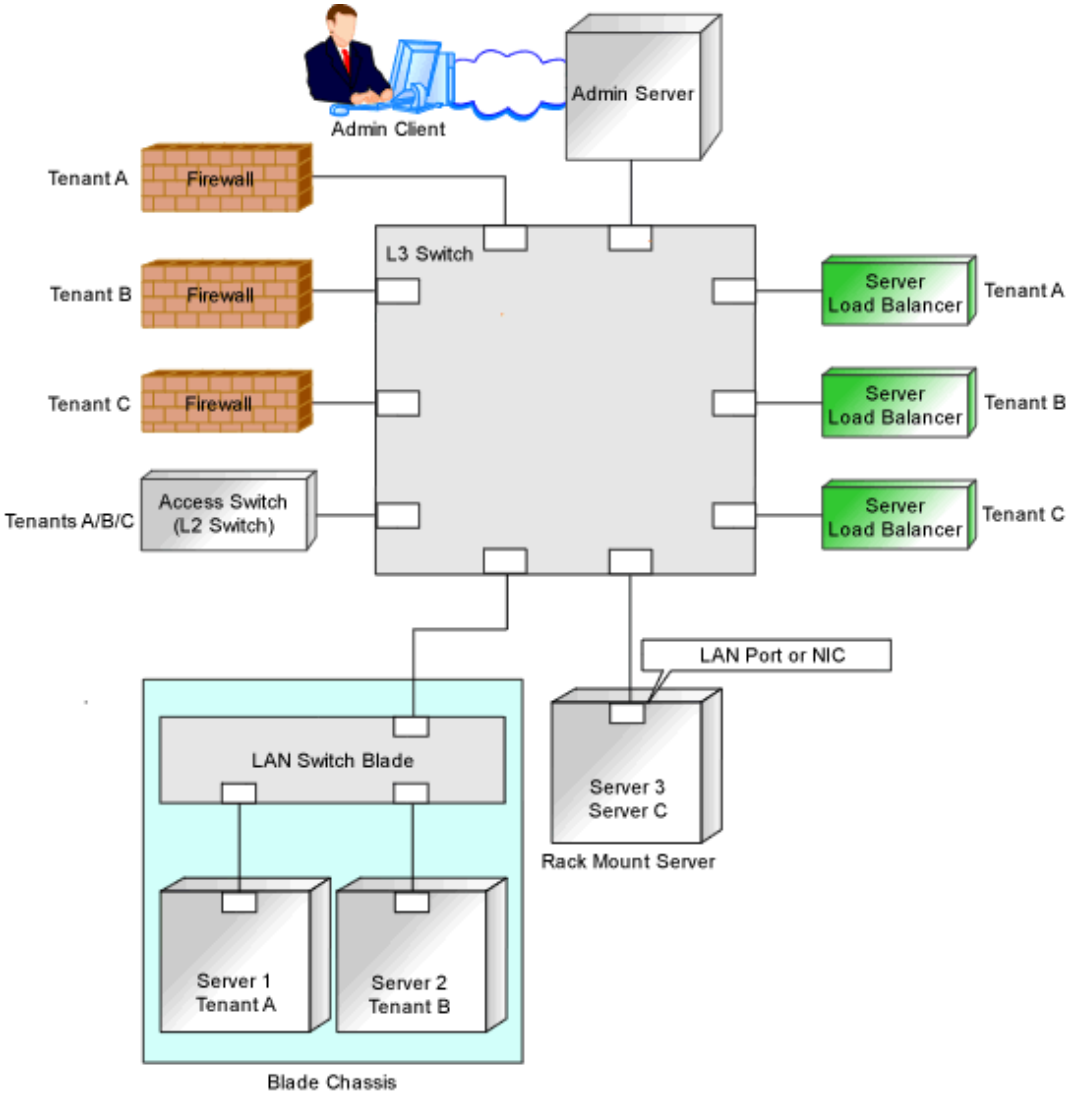
  - For physical L-Servers, use Intel PROSet, PRIMECLUSTER GLS, or Linux bonding.
  - For VM hosts, perform redundancy according to the server virtualization software used.

- The network configuration for LAN switch blades

9.1.1.3 Admin LAN for Network Devices

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

Figure 9.2 Admin LAN Connection Example



See

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

9.1.1.4 Safer Communication

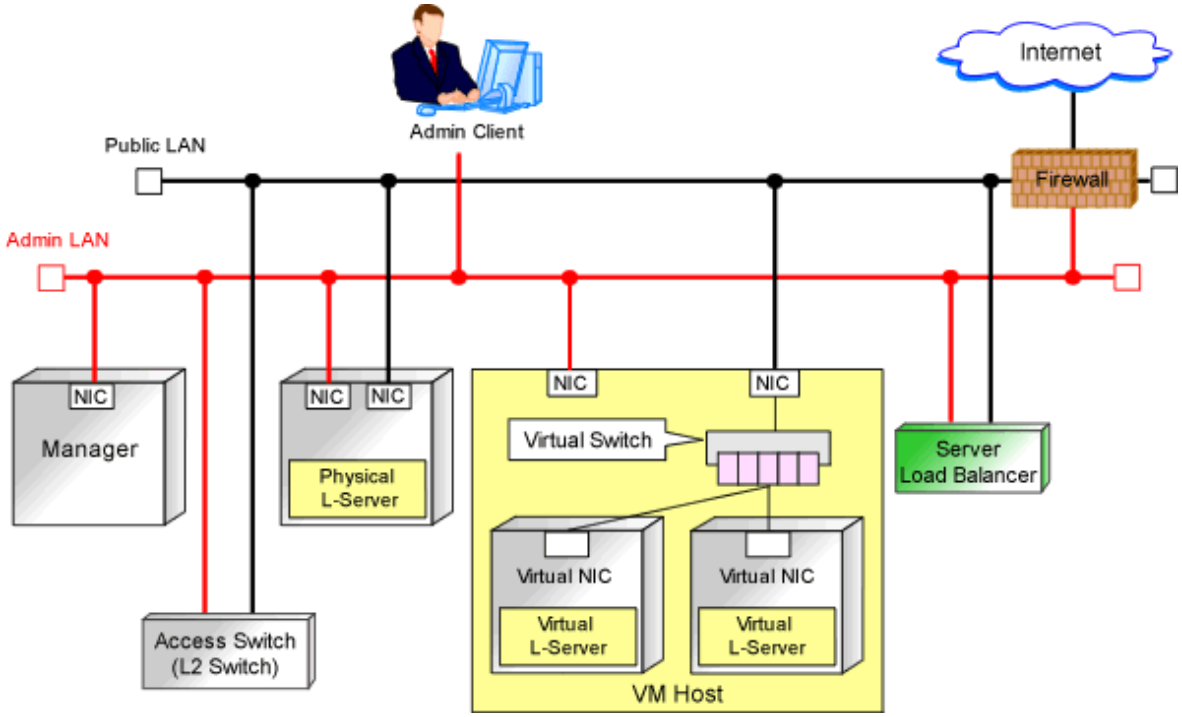
For environments where virtual L-Servers and the admin server (manager) communicate, it is recommended to perform the following configuration to improve security:

- 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 9.3 Network Configuration Example



9.1.1.5 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 configured as follows.

- A 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 of HBA address rename setup service, refer to "Chapter10 Settings for the HBA address rename Setup Service" in the "Setup Guide CE".

- 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.

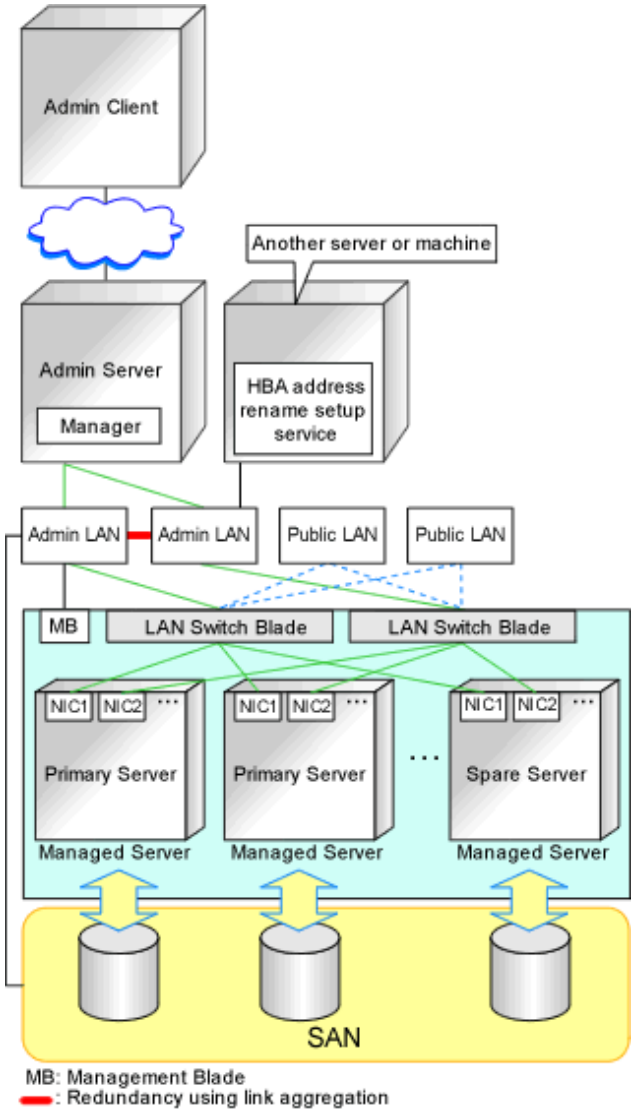
  For details, refer to "5.4 When using Blade Servers" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".
- This service periodically obtains information about managed servers from the admin server and operates using this information. For this reason, it should be installed 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.

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



- 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.

9.1.2 Virtual System Design

Design virtual systems for users.

9.1.2.1 Information Necessary for Design

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

- Resource requirements
  - 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.
  - Whether to use server load balancers

    If server load balancing needs to be performed for each virtual system, deploy server load balancers.
  - Server type (physical L-Server or virtual L-Server)
  - Whether to use iSCSI (Storage)

Information

When deploying both a firewall and a server load balancer, an L2 switch may be necessary between the firewall and server load balancer depending on device specifications. Therefore, check the specifications of the firewall and server load balancer beforehand.

- Communication route configuration

  It is normal to use a redundant configuration for communication routes.

- Communication performance assumption (throughput)

  Define the assumed communication performance for each system.

Figure 9.5 Example of Virtual System Configuration Elements

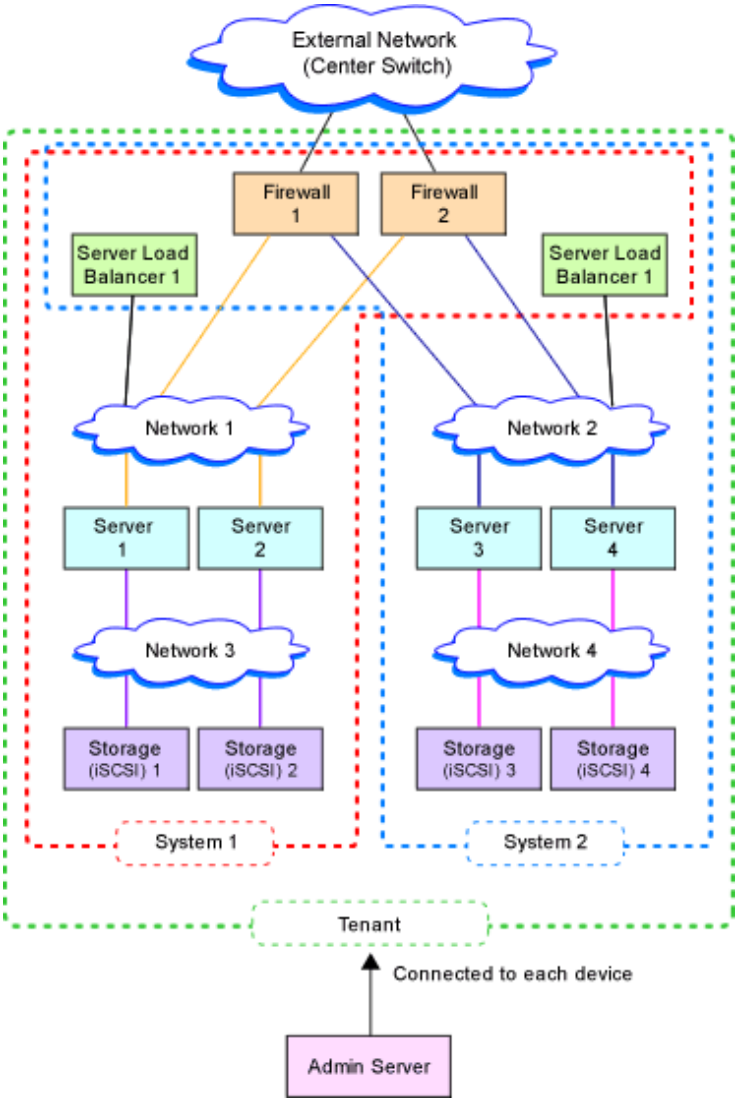
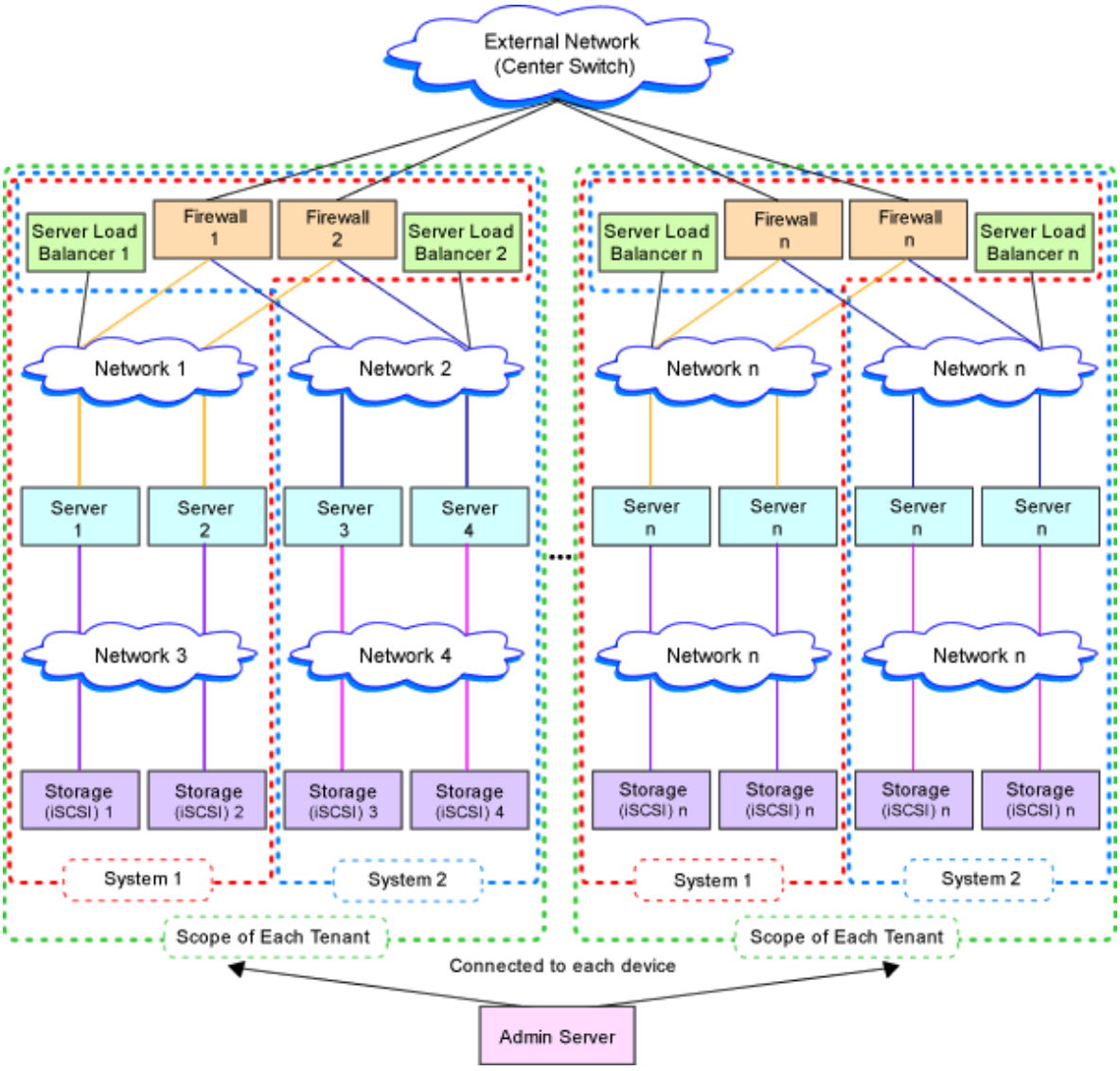


Figure 9.6 Example of Overall Configuration of a Virtual System (A Collective of Virtual System Configuration Elements)



9.1.3 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.

9.1.3.1 Information Necessary for Designing a Public LAN

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

- 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

- Specifications (including supported functions) required for the devices
- 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.

- 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.

- The IP address range of the public LAN

  Design the address architecture allocated by virtual system, and define the required IP address range

  - When deploying firewall

    When using address conversion function, define the virtual IP address.

  - When deploying server load balancer

    Define the virtual IP address using server load balancer

  IP address on the public LAN, that designed and defined by the infrastructure administrator, is used by the virtual system configured for tenant.
  Therefore, the infrastructure administrator must nofity the tenant administrator.of the IP address on the public LAN allocated to a tenant.

- Whether to configure communication route redundancy

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

- 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.

9.1.3.2 Information Necessary for Designing an iSCSI LAN

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

- The NIC on the server used for an iSCSI LAN

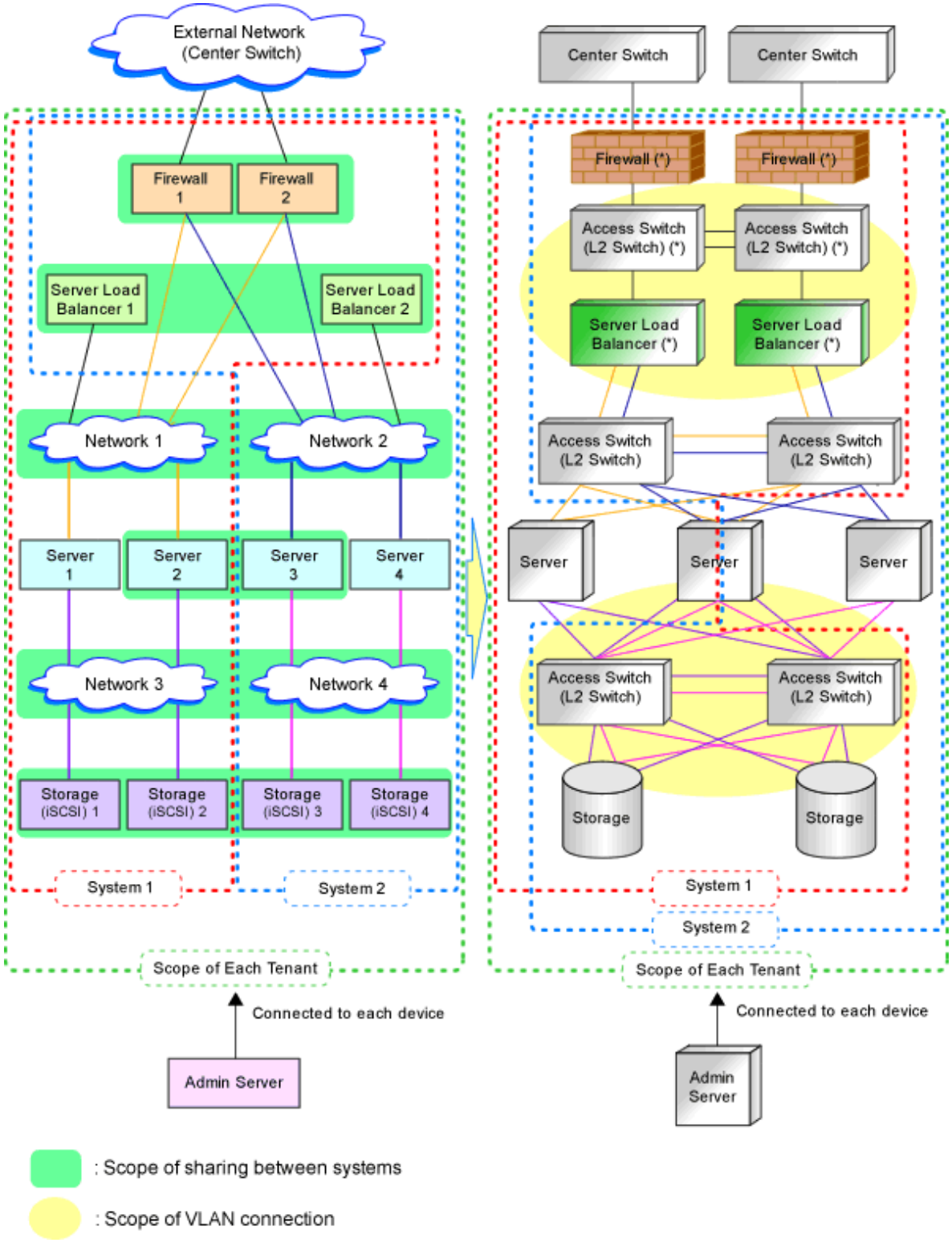
  Both single and multi-path configurations are available.

- The network address and a VLAN ID for use on the iSCSI LAN for each tenant
- Whether to connect external switches between ETERNUS storage and LAN switch blades, or NetApp storage and LAN switch blades
- Whether to use multi-tenant functions on ETERNUS storage or NetApp storage
- The IQN to be used for the NIC of the server
- The Network address to be used for the port of the storage
- The IQN set for storage (The IQN used for the NIC on the server side is used.)
- Whether to use authentication for iSCSI communication (When using authentication, 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 9.7 Sample Image of Virtual Systems and the Corresponding Physical Network Configuration

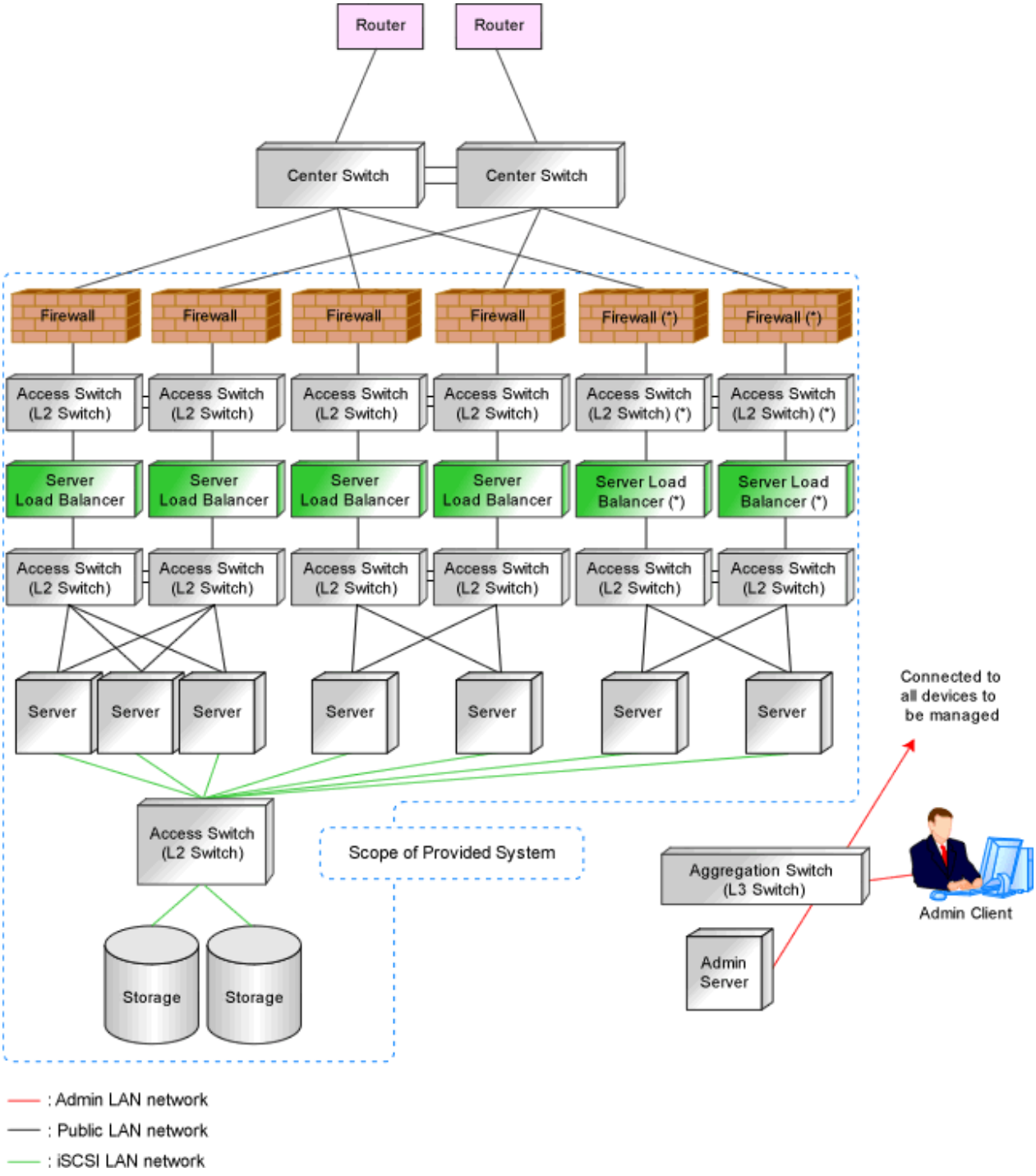


*1: Some types of network devices have both firewall functions and server load balancer functions. (In this case, there is no access switch between the firewall and server load balancer.)

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 9.8 Example of Overall Physical Network Configuration



*1: Some types of network devices have both firewall functions and server load balancer functions. (In this case, there is no access switch between the firewall and server load balancer.)

9.1.4 Relationship between Physical Network Configuration and Resources

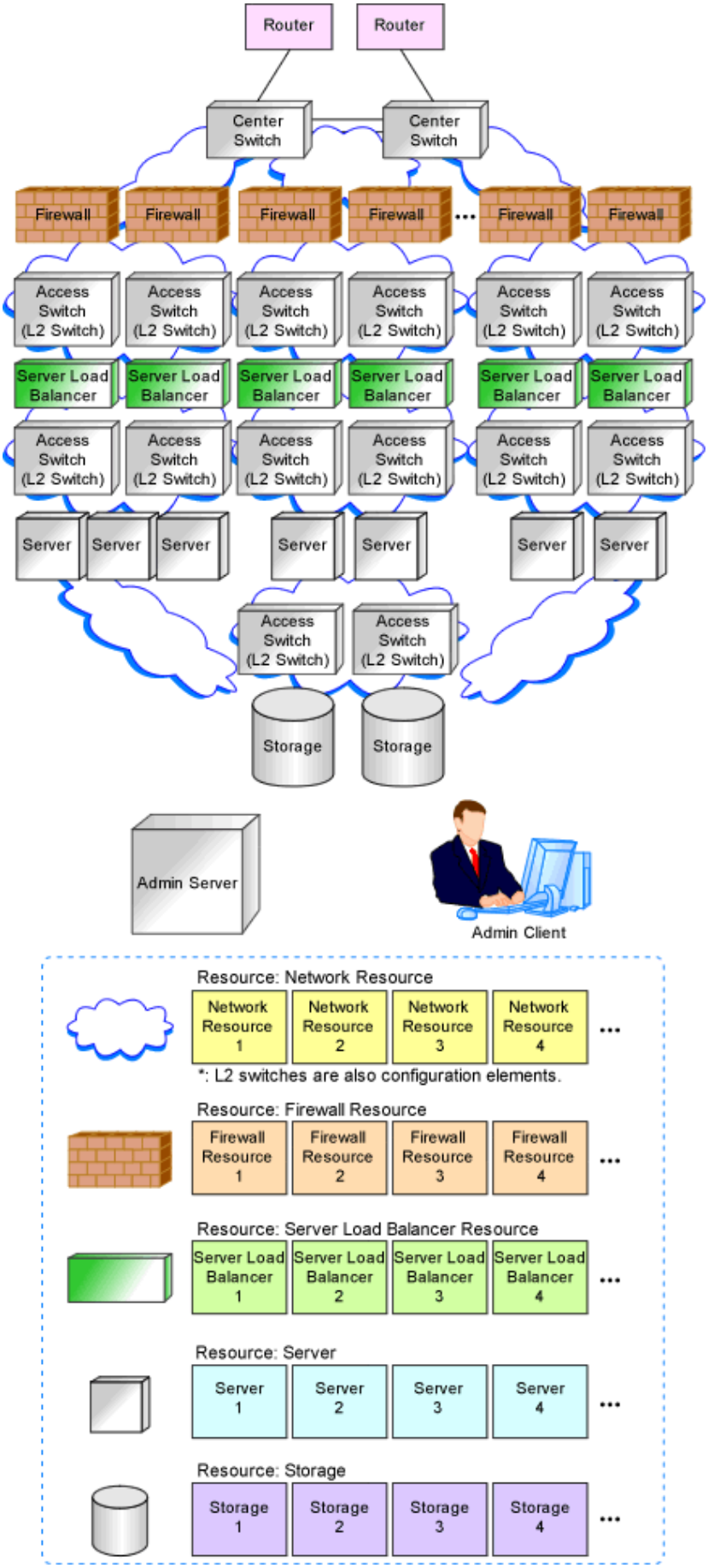
This section explains the relationship between the defined physical system and the resources managed by Resource Orchestrator.

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 9.8 Example of Overall Physical Network Configuration" as an example.

Figure 9.9 Relationship between Physical Network Configuration and Resources

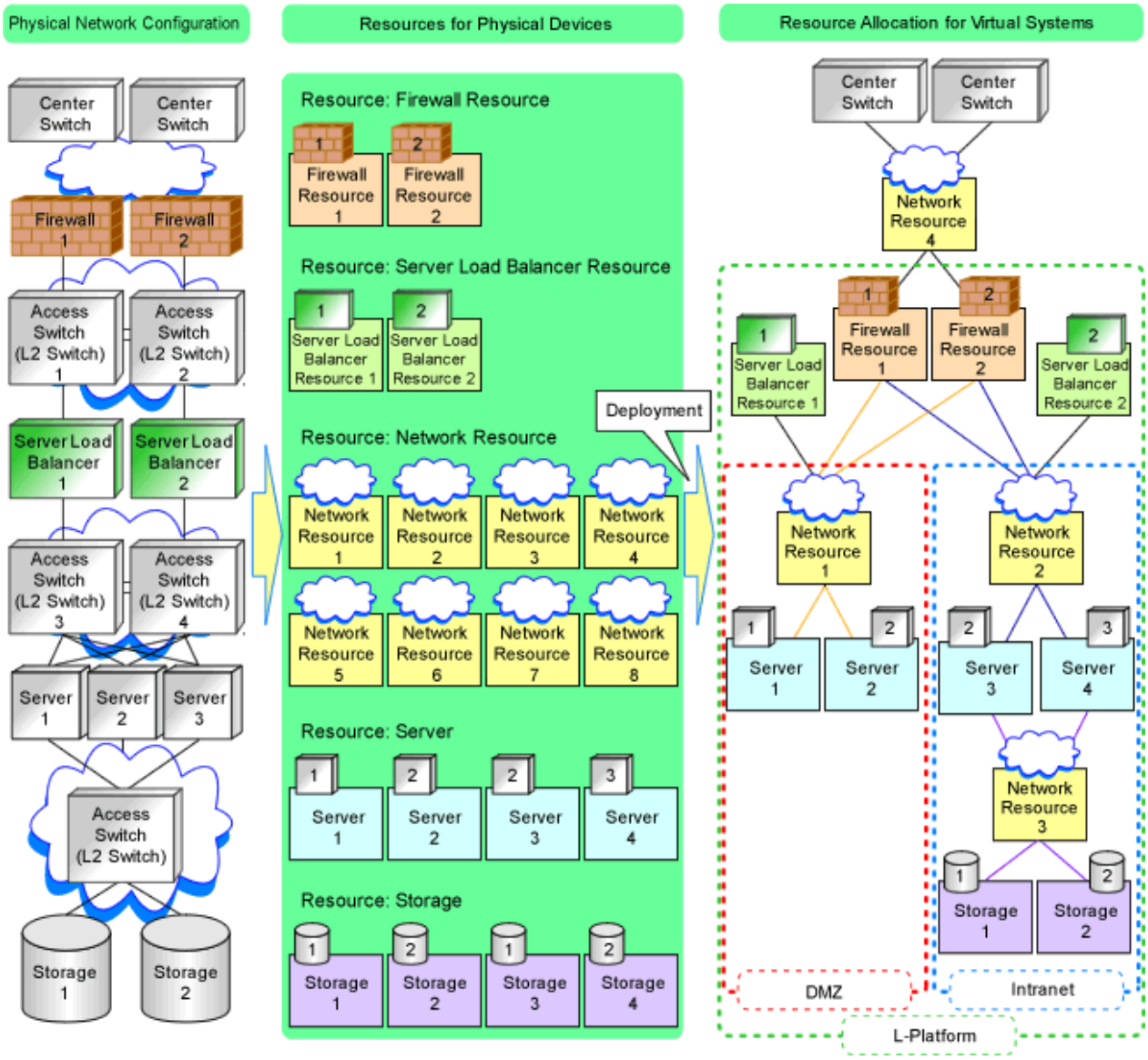


The following figure shows a sample image when physical devices and resources are allocated for a single virtual system (L-Platform).

In this sample image, resources are allocated for firewalls, server load balancers 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 9.10 Virtual System and Resource Allocation Example



9.2 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.

9.2.1 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.

9.2.2 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.

9.2.3 Settings for Managed Network Devices

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

9.2.3.1 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)
  - Login User Name

    Define the login user name to be used for login to the network device.
    This user name can contain up to 32 alphanumeric characters (upper or lower case), underscores ("_"), and hyphens ("-").

  - Password

    Define the password for the login user name to be used for direct login to 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.

9.2.3.2 Settings for Pre-configuration

Define settings necessary for pre-configuration.

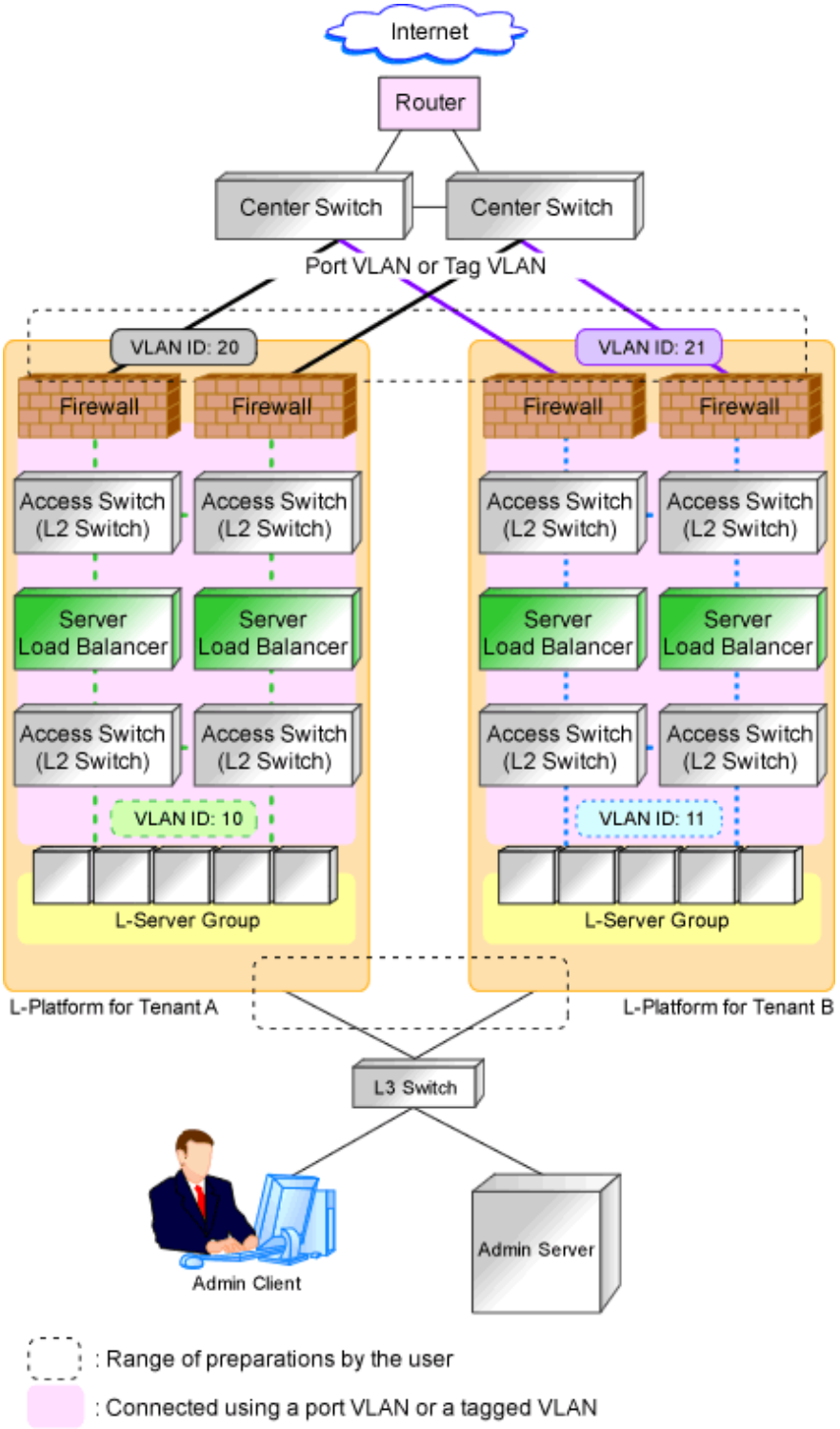
- Public LAN Pre-configuration Settings

  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 9.11 Managed Device Pre-configuration Scope



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.

9.2.3.3 Settings for Automatically Configured Devices

The sample scripts provided with Resource Orchestrator are not for defining all definitions of network devices. When using the sample scripts, define the information necessary for auto-configuration of network devices.

Regarding the configuration provided by the sample scripts, refer to "Table G.2 Units for which Sample Scripts are Provided".

Firewalls

In the sample scripts, only the network settings within the range of Resource Orchestrator management and firewall rules are auto-configured.
Define the following settings for firewalls:

- Networks not managed by Resource Orchestrator (external interfaces etc.)
- Basic information (system definitions, redundant devices, interfaces, communication routes, etc.)

Server Load Balancers

In the sample scripts, only load balancing rules and SSL accelerator settings are auto-configured.
Therefore, define the following settings for server load balancers:

- Basic information (system definitions, redundant devices, interfaces, communication routes, etc.)
- Register the server certificate, error web page response file, etc.
- In case of the device which has needed configuration according to server certificate registration, configure security policy such as SSL connection protocol, cipher suite, etc.

L2 Switches

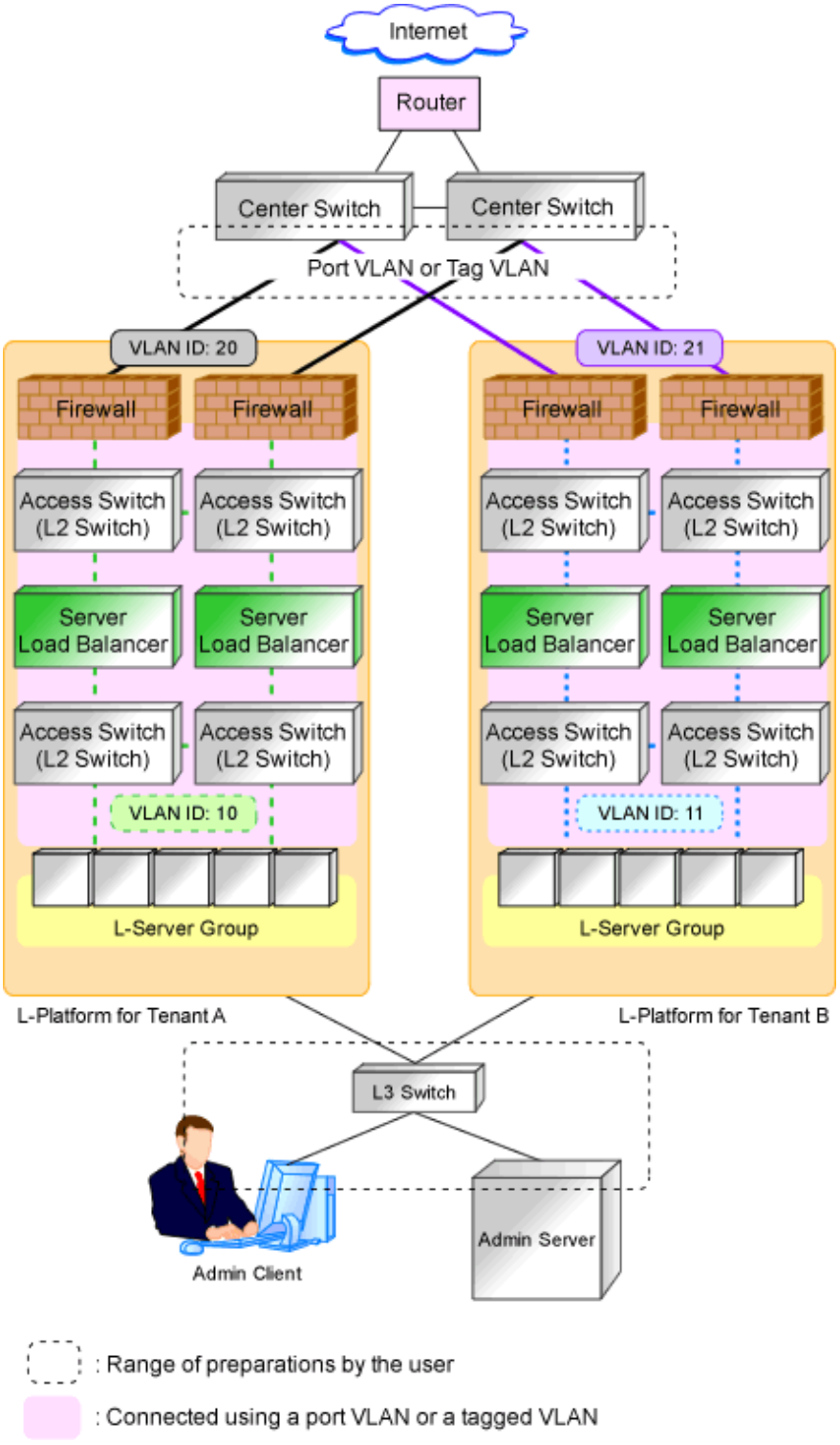
In the sample scripts, only the VLAN IDs specified for network resources are auto-configured.
Define the following settings for L2 switches:

- The definition of the interface to perform VLAN definition for
- The VLAN operation mode
- Cascade ports, etc

9.2.4 Settings for Unmanaged Network Devices

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

Figure 9.12 Example of the Configuration Scope of Unmanaged Network Devices



9.2.4.1 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.

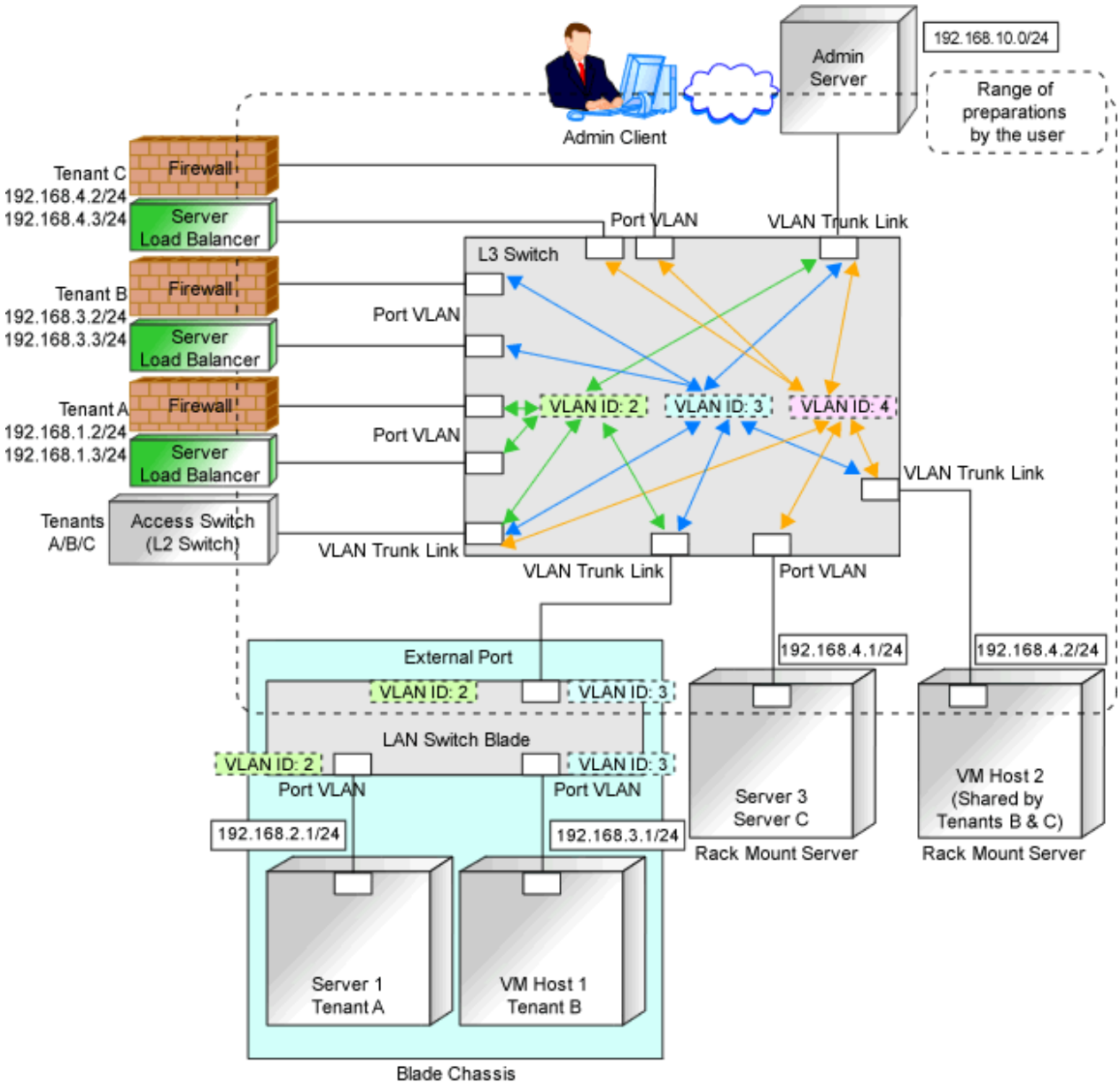
- Redundancy Information

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

9.2.4.2 Admin LAN Settings

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

Figure 9.13 Admin LAN Network Configuration



- 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.

9.2.5 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 used 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.

- When a physical L-Server uses the iSCSI storage, ensure that all of the IP addresses configured here are on the same subnet.

9.2.6 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)
  - Login User Name

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

  - Password

    Define the password of the login user name to be used for direct login to 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.

9.2.7 Network 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.
- When a physical L-Server uses the iSCSI storage, ensure that all of the IP addresses configured here are on the same subnet.

9.2.8 Network 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.

9.3 Pre-configuring Devices

Configure defined setting information.

9.3.1 Pre-configuring Admin Servers

Configure the information defined in "9.2.1 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.

9.3.2 Pre-configuring Admin Clients

Configure the information defined in "9.2.2 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.

9.3.3 Pre-configuring Managed Network Devices

Configure the information defined in "9.2.3 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.

9.3.4 Pre-configuring Unmanaged Network Devices

Configure the information defined in "9.2.4 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.

9.3.5 Pre-configuring Managed Servers

Configure the information defined in "9.2.5 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 "9.1.1.2 Admin LAN for Servers" of "9.1.1 Admin LAN Network Design".

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

9.3.6 Pre-configuring LAN Switch Blades on Managed Blade Systems

Configure LAN switch blades on the managed blade systems using the information defined in "9.2.6 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 "5.4.4 Configuring VLANs on LAN Switch Blades" in 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 on how to back up the configuration definition information of a switch blade, refer to the manual of the LAN switch blade.
- Resource Orchestrator uses telnet or SSH to log into LAN switch blades and automate settings.

  When telnet or SSH (version 2) 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 or SSH is unavailable, the following features are also unavailable.
  - Registration of LAN switch blades
  - Changing of LAN switch blade settings
  - Changing and setting the VLAN for LAN switch blades (internal and external connection ports)
  - Restoration of LAN switch blades
  - Server switchover (changing network settings while a server is switched over)
- SSH connection (SSH version 2) can be selected for the following LAN switch blades.
  - LAN switch blade PY CB Eth Switch/IBP 10Gb 18/8 (1.00 or later version)
  - LAN switch blade PY CB Eth Switch/IBP 1Gb 36/8+2 (4.16 or later version)
  - LAN switch blade PY CB Eth Switch/IBP 1Gb 36/12 (3.12 or later version)
  - LAN switch blade PY CB Eth Switch/IBP 1Gb 18/6 (3.12 or later version)

- 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.
  This setting is not necessary, since there are no pin-group or AVS functions for SBAX2.

- 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.

  LAN switch blades

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

  Configuration

  - LLDP (Link Layer Discovery Protocol)
    When setting LLDP, disable the setting for [VLAN name information].
    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 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. It may be necessary to enable LLDP depending on the LAN switch blade.
  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 of physical servers. 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
    - Deactivated (depends on LAN switch blade model)
- Each port VLAN configuration must meet the conditions below.
  - Do not configure more than one port VLAN.
  - Do not configure the same VLAN ID for the port VLAN and the tagged VLAN.
- Mount the following LAN switch blades in the connection blade slots except for CB5/6 when using a PRIMERGY BX900 chassis.
  - LAN switch blade PY CB Eth Switch/IBP 1Gb 36/8+2
  - LAN switch blade PY CB Eth Switch/IBP 1Gb 36/12

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)

Information

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 9.14 With Port VLANs

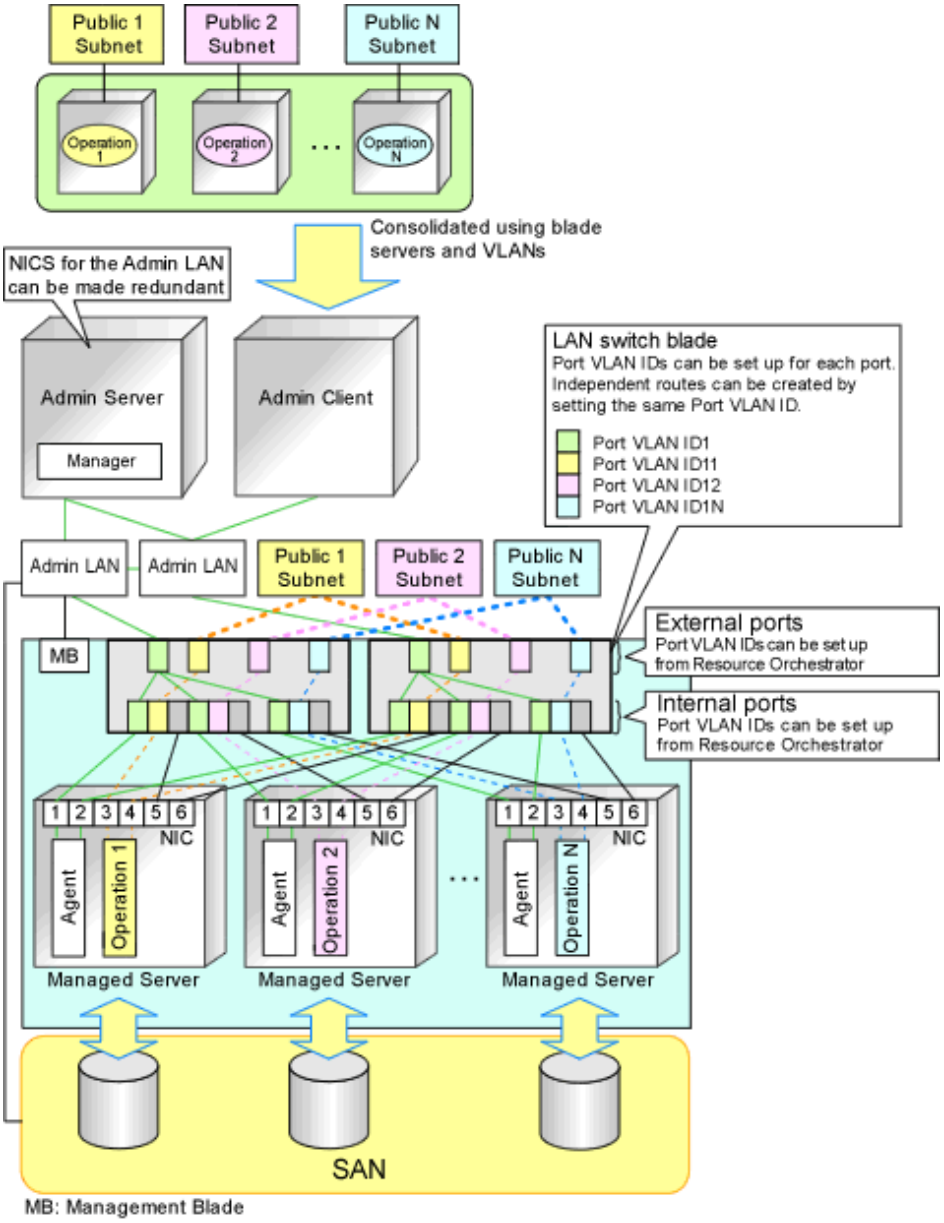
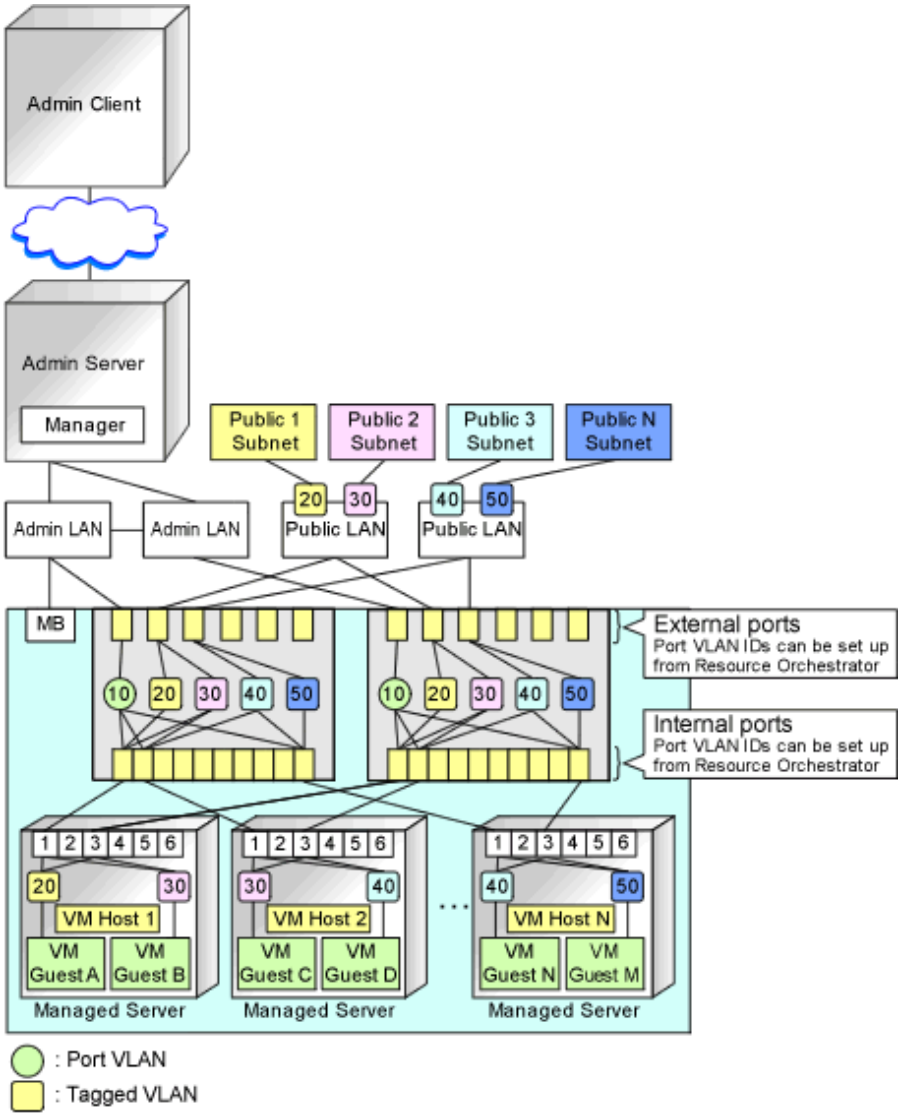


Figure 9.15 With Tagged VLANs



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.

9.3.7 Pre-configuring Managed Storage Units

Configure the information defined in "9.2.7 Network 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.

9.3.8 Pre-configuring Networks for Other Managed Hardware

Configure the information defined in "9.2.8 Network 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.

9.3.9 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

  Set the following items necessary for the connection with the server.

  - Information of hosts that access the LUN
  - CHAP authentication
  - Mutual CHAP authentication

9.4 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

Conditions	Necessary Preparations
When managing network devices as resources	Create network resources
	Configure definitions of the network device file management function
	Register external FTP servers
When using the automatic configuration and operation function for network devices registered as network device resources	Create model definitions for the network devices
	Create a folder for registering rulesets
	Register sample scripts

9.4.1 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 manager 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 series servers
  - PRIMERGY BX900 series servers

  Switch Blade
  - PY CB Eth switch/IBP 10Gb 18/8
  - PY CB Eth switch/IBP 1Gb 36/8+2
  - PY CB Eth switch/IBP 1Gb 36/12
  - PY CB Eth switch/IBP 1Gb 18/6

See

For details on how to create network resources which automatically configure VLANs for LAN switch blade uplink ports, refer to "7.4.2 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 9.1 Network Configurations for Blade Servers".

  For details on the timing of automatic configuration, refer to "Table 2.5 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 "B.3.1 Automatic Network Configuration" in the "Setup Guide CE".

  - For Virtual L-Servers

    [VMware]
    Refer to "Physical Server (Blade Server) Configuration to Support Automation of Network Configuration in Resource Orchestrator" in "C.2.4 Automatic Network Configuration" in the "Setup Guide CE".

    [Hyper-V]
    Refer to "Physical Server (Blade Server) Configuration to Support Automation of Network Configuration in Resource Orchestrator" in "C.3.4 Automatic Network Configuration" in the "Setup Guide CE".

See

- For details on the rcxadm nicdefctl command, refer to "5.15 rcxadm nicdefctl" in the "Reference Guide (Command/XML) CE".
- For details on the server NIC definitions, refer to "14.11 Server NIC Definitions" in the "Reference Guide (Command/XML) CE".

Figure 9.16 Automatic Network Configuration for Blade Servers

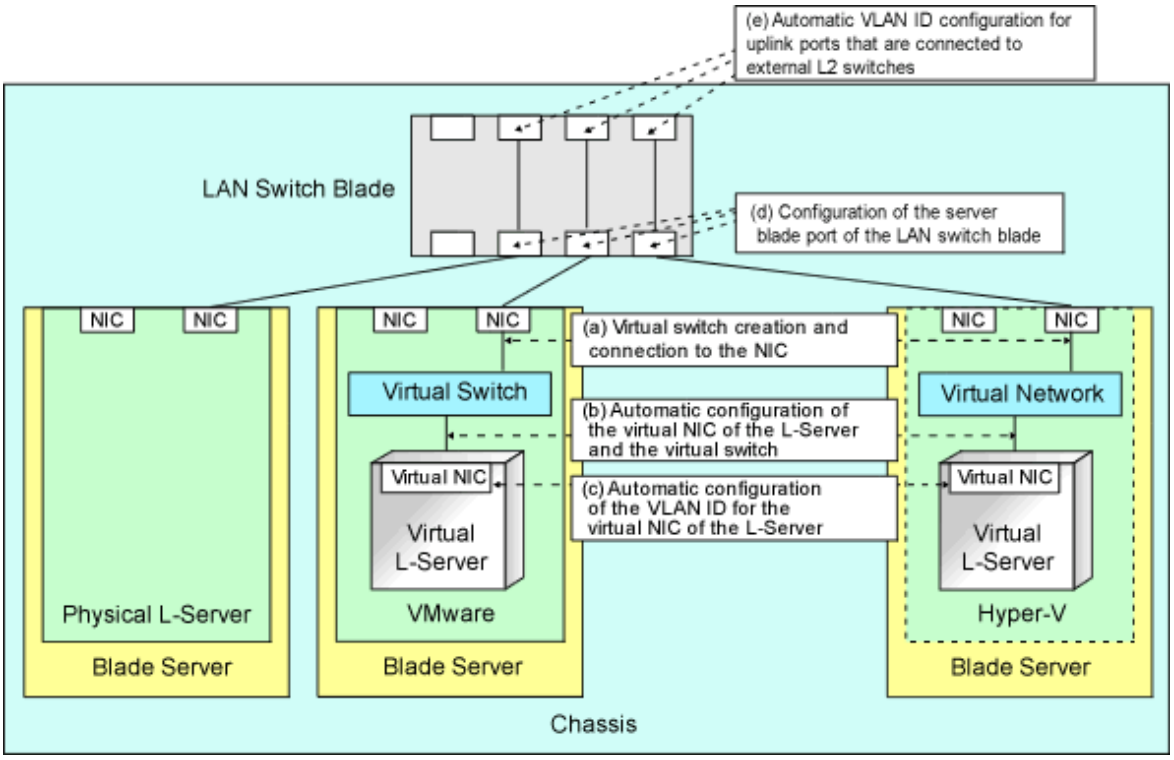


Table 9.1 Network Configurations for Blade Servers

		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)	
		Without	With	Without	With	Without	With	Without	With	Without	With	Without	With
A	Creating virtual switches and connecting to NICs (*2)	-	-	Yes (*3)	Yes	Yes (*3)	Yes (*4)	No	No	No	No	No	No
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 9.2 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 "14.11 Server NIC Definitions" in the "Reference Guide (Command/XML) CE".
For details on the rcxadm nicdefctl command, refer to "5.15 rcxadm nicdefctl" in the "Reference Guide (Command/XML) 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 9.3 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 "14.12 VMware Exclusion Port Group Definition Files" in the "Reference Guide (Command/XML) CE".

*6: Configure a port VLAN or a tagged VLAN. For details on how to configure VLANs, refer to "5.4.6 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 "B.3.2 Manual Network Configuration" in the "Setup Guide CE".

- For Virtual L-Servers

  [VMware]
  Refer to "C.2.5 Manual Network Configuration" in the "Setup Guide CE".

  [Hyper-V]
  Refer to "C.3.5 Manual Network Configuration" in the "Setup Guide CE".

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 9.17 Network Configuration for Rack Mount or Tower Servers

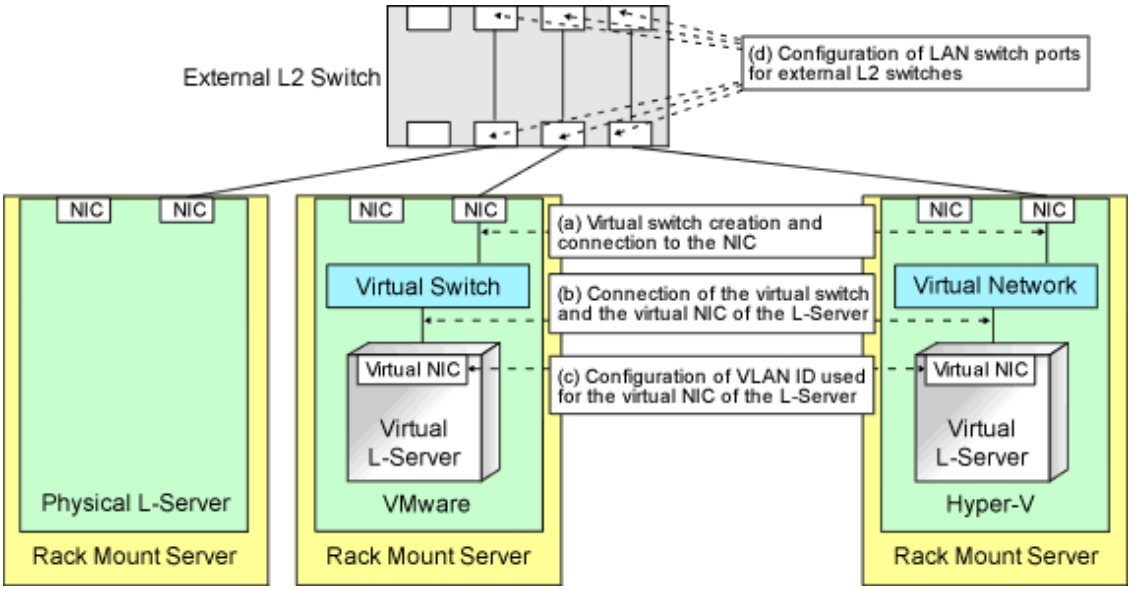


Table 9.4 Network Configurations for Rack Mount or Tower Servers

		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)	
		Without	With	Without	With	Without	With	Without	With	Without	With	Without	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 rcxadm nicdefctl commit command in advance.
For details on the server NIC definitions, refer to "14.11 Server NIC Definitions" in the "Reference Guide (Command/XML) CE".
For details on the rcxadm nicdefctl command, refer to "5.15 rcxadm nicdefctl" in the "Reference Guide (Command/XML) CE".

Replace as follows for each server virtualization software.

Table 9.5 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 9.6 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 "14.12 VMware Exclusion Port Group Definition Files" in the "Reference Guide (Command/XML) CE".

*4: Configured by network device automatic configuration.

IP Address Auto-Configuration (Virtual L-Servers)

[Physical Servers] [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 OSs 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 "16.3.4 [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 "B.3.2 Manual Network Configuration" in the "Setup Guide CE".
  - For Virtual L-Servers

    Settings differ according to the server virtualization software being used.

[VMware]
Refer to "C.2.5 Manual Network Configuration" in the "Setup Guide CE".

[Hyper-V]
Refer to "C.3.5 Manual Network Configuration" in the "Setup Guide CE".

[Xen]
Refer to "C.4.4 Manual Network Configuration" in the "Setup Guide CE".

[KVM]
Refer to "C.6.4 Manual Network Configuration" in the "Setup Guide CE".

[Oracle VM]
Refer to "C.5.4 Manual Network Configuration" in the "Setup Guide CE".

- Redundant Configuration

  - For Physical L-Servers

    Refer to "B.3.1 Automatic Network Configuration" and "B.8 Network Redundancy and VLAN Settings of L-Servers" in the "Setup Guide CE".

  - For Virtual L-Servers

    Settings differ according to the server virtualization software being used.

    [VMware]
    Refer to "C.2.4 Automatic Network Configuration" in the "Setup Guide CE".

    [Hyper-V]
    Refer to "Automatic Network Configuration for Blade Servers" in "C.3.4 Automatic Network Configuration" in the "Setup Guide CE".

    [Xen]
    Refer to "C.4.4 Manual Network Configuration" in the "Setup Guide CE".

    [KVM]
    Refer to "C.6.4 Manual Network Configuration" in the "Setup Guide CE".

    [Oracle VM]
    Refer to "C.5.4 Manual Network Configuration" in the "Setup Guide CE".

PRIMERGY Rack Mount Servers, PRIMERGY Tower Servers, or PRIMEQUEST Servers

- Non-Redundant Configuration

  - For Physical L-Servers

    Refer to "B.3.2 Manual Network Configuration" in the "Setup Guide CE".

  - For Virtual L-Servers

    Settings differ according to the server virtualization software being used.

    [VMware]
    Refer to "C.2.5 Manual Network Configuration" in the "Setup Guide CE".

    [Hyper-V]
    Refer to "C.3.5 Manual Network Configuration" in the "Setup Guide CE".

    [Xen]
    Refer to "C.4.4 Manual Network Configuration" in the "Setup Guide CE".

    [KVM]
    Refer to "C.6.4 Manual Network Configuration" in the "Setup Guide CE".

    [Oracle VM]
    Refer to "C.5.4 Manual Network Configuration" in the "Setup Guide CE".

- Redundant Configuration

  - For Physical L-Servers

    Refer to "B.3.1 Automatic Network Configuration" in the "Setup Guide CE".

  - For Virtual L-Servers

    Settings differ according to the server virtualization software being used.

    [VMware]
    Refer to "C.2.4 Automatic Network Configuration" in the "Setup Guide CE".

    [Hyper-V]
    Refer to "C.3.5 Manual Network Configuration" in the "Setup Guide CE".

    [Xen]
    Refer to "C.4.4 Manual Network Configuration" in the "Setup Guide CE".

    [KVM]
    Refer to "C.6.4 Manual Network Configuration" in the "Setup Guide CE".

    [Oracle VM]
    Refer to "C.5.4 Manual Network Configuration" in the "Setup Guide CE".

Point

- When Creating Physical L-Servers

  For details on the network configuration example, refer to "Appendix D Preparations for Creating a Physical L-Server".

- When Creating Virtual L-Servers

  For details on the network configuration example, refer to "Appendix E Preparations for Creating a Virtual L-Server".

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 "B.8 Network Redundancy and VLAN Settings of L-Servers" in the "Setup Guide CE".

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 "7.5 Modifying Network Resource Specifications" in the "User's Guide for Infrastructure Administrators (Resource Management) CE", and "14.5.2 Modification" in the "Reference Guide (Command/XML) CE".

9.4.2 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

  For details, refer to "D.4 Network Preparations".

- 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.

9.4.3 When Using an iSCSI LAN for iSCSI Boot

[Physical Servers]
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 "14.4.2 iSCSI Boot Information" in the "Reference Guide (Command/XML) CE" beforehand.

Storage Location of the Definition File

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

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

Definition File Name

- 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.

```
Variable = Value
```

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

Definition File Items

Table 9.7 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.	Specify the items in the following format.

Variable	Meaning	Value
	The following models can be specified: - BX620 - BX920 - BX922 - BX924 - BX960 When setting the default, specify an asterisk ("*").	*NIC*[*index*] *index* 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
```

- 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 ("*").

9.4.4 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".

9.4.5 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 "14.11 Server NIC Definitions" in the "Reference Guide (Command/XML) CE".
For details on the rcxadm nicdefctl commit command, refer to "5.15 rcxadm nicdefctl" in the "Reference Guide (Command/XML) CE".

9.4.6 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 "14.11 Server NIC Definitions" in the "Reference Guide (Command/XML) CE".
For details on the rcxadm nicdefctl commit command, refer to "5.15 rcxadm nicdefctl" in the "Reference Guide (Command/XML) CE".

9.4.7 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 "14.12 VMware Exclusion Port Group Definition Files" in the "Reference Guide (Command/XML) CE".

9.4.8 When Registering Network Devices as Resources

Preparation required in advance to manage network devices as resources is explained in this section.

9.4.8.1 Creation of Network Configuration Information (XML definition)

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.
- When connection information is already registered

  When link information is already registered, if you register several network devices at once with link information defined in network configuration information, already registered link information is processed according to the mode of the link information registration.
  - When "add" is specified

    The same link information is not overwritten.
  - When "modify" is specified

    Already registered link information is deleted, and then defined link information is registered.

  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 of state 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.

  When "telnet" has been specified in the protocol element, 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)	*Arbitrary string*#
			Arbitrary string>
Cisco	Catalyst ASA	Login prompt	Username:
		Password prompt	Password:
		Command prompt (*1)	*Arbitrary string*#
			Arbitrary string>
	Nexus	Login prompt	login:
		Password prompt	Password:
		Command prompt (*1)	*Arbitrary string*#
			Arbitrary string>
Brocade	VDX	Login prompt	Login:
		Password prompt	Password:
		Command prompt (*1)	*Arbitrary string*#
			Arbitrary string>
F5 Networks	BIG-IP (*2)	Login prompt Password prompt Command prompt	There are no restrictions.

  *1: The "#" or ">" following *arbitrary string* is used as a prompt character for the command prompt.
  *2: The model name for the BIG-IP LTM series is handled as "BIG-IP".

- 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.

- When register connection information of BIG-IP

  When register connection information of BIG-IP, please register in the following order.

  1. Registering network configuration information that is excepted connection information.
  2. Please confirm port information is displayed in screen for resource details of registered BIG-IP in ROR console.
  3. Registering network configuration information that is included connection information.
     In that case, please omit or specify "add" to registration mode of network device (value of Mode tag under the Netdevices tag)

Information

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.

See

- For details on network configuration information (XML definitions), refer to "14.6 Network Configuration Information" in the "Reference Guide (Command/XML) CE".
- For details on the rcxadm netconfig command, refer to "3.7 rcxadm netconfig" in the "Reference Guide (Command/XML) CE".
- For details on releasing maintenance mode, refer to "22.1 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 "14.13 Network Device Model Definitions" in the "Reference Guide (Command/XML) CE".

9.4.8.2 When using Network Device File Management Function

Preparation required beforehand to use network device file management function is explained in this section.

Configure definitions of the network device file management function

When using network device file management function, it is necessary to configure the function to be used and the number of generation files in the definition file beforehand.

For details on the configuration of network device management function, refer to "9.4.8.3 Network Device Management Function Definition File".

Register external FTP servers

When managing network device files, for network devices without FTP server function, an external FTP server is necessary.

- Backup the network device file
- Transfer the backed up the network device file to admin server as the manager
- Transfer the backed up the network device file from admin server as the manager
- Restore the network device file transferred from admin server to target network device

Excute the rcxadm netconfig import command and register external ftp server.

For details on the rcxadm netconfig command, refer to "3.7 rcxadm netconfig" in the "Reference Guide (Command/XML) CE".

Point

When using Nexus 5000 series, it is necessary to set the following settings for external ftp server in advance.

1. Set the change route.
2. Change the route directory("/") of account to home directory.

Set the login information of network device

When registering or changing network device, register the login information in the network configuration information(XML definition).

- Case of "SR-X series"
  - LoginInfo protocol: ftp
  - User: Need to specify
  - Password: Need to specify
  - Tenant: Do not specify
- Case of "BIG-IP Local Traffic Manager series"
  - LoginInfo protocol: ssh

  - LoginInfo authority: admin
  - User: Need to specify
  - Password: Need to specify
  - Tenant: Do not specify
- Case of "Nexus 5000 series"
  - LoginInfo protocol: telnet
  - LoginInfo authority: admin
  - User: Need to specify
  - Password: Need to specify
  - Tenant: Do not specify
- Case of the other support device
  - LoginInfo protocol: telnet
  - LoginInfo authority: user
  - User: Need to specify
  - Password: Need to specify
  - PrivilegedPassword: Need to specify
  - Tenant: Do not specify

Note

Explains points to keep in mind when using this function.

- When using "IPCOM EX series"
  - When restoring the network device file without initializing the authentication information

    Excute the rcxadm netdevice cfexport command and export the network device environment file in advance, and then configure IPCOM EX manually.

    For details on configuration, refer to the IPCOM EX manuals.
  - When deleting, changing or deleting the account information registered in this product

    Excute the rcxadm netdevice cfbackup command and backup the network device configuration file.

    When restoring without backing up, due to account information inconsistency restore may fail.
  - When using automatic updating function of the authentication information

    When excuting the rcxadm netdevice cfrestore command and restoring the network device environment file, authentication information may initialize.

    #### Point

    The automatic updating function as follows.

    - When "skey" in accout authentication type is specifyed
    - When the authentication in SSL-VPN client or L2TP/IPsec client is performed "local database operation"
- When using "BIG-IP Local Traffic Manager series"
  - The user specified in login information must operate the network device with tmsh immediately after login.

- Do not create the following files.
  - /var/local/ucs/environment.ucs
  - /var/local/scf/config.scf

- When using "Nexus 5000 series"
  - When restoring "Nexus 5000 series", perform the following.
    - When not connecting Nexus 2000 series

      (1) Log in to the target Nexus, and confirm the management IP address and SNMP community name.
      (2) Clear startup-config using write erase command.
      (3) Restart the target Nexus.
      (4) After restarting, log in to the target Nexus again.
      (5) Set the management IP address and SNMP community name which confirmed in (1).
      (6) After log out of the target Nexus, performed to restore.

    - When connecting Nexus 2000 series

      (1) Log in to the target Nexus, and confirm the management IP address and SNMP community name.
      (2) Clear startup-config using write erase command.
      (3) Restart the target Nexus.
      (4) After restarting, log in to the target Nexus again.
      (5) Set the FEX.
      (6) Set the management IP address and SNMP community name which confirmed in (1).
      (7) After log out of the target Nexus, performed to restore.

- When using "Cisco ASA 5500 series"

  When using redundancy configurations and only one device is fault, do not need to excute the rcxadm netdevice cfrestore command.
  By the function in "Cisco ASA 5500 series", reflect the configurations from the network device in active status automatically.
  For details, refer to "Cisco ASA 5500 series" manuals.

- When using "Catalyst series"

  If executing restoration to "Catalyst series", please export network device file in rcxadm netdevice cfexport command and log in directly to network device to execute restoration manually.
  For logging in to network device and restoration order, please refer to manual of network devices.

  When executing restoration using rcxadm netdevice cfrestore command, the command may fail.
  When message is displayed with code "08" after rcxadm netdevice cfrestore command failed displaying 62786 message, please execute deal that is described in "Messages".

9.4.8.3 Network Device Management Function Definition File

The definition of the configuration management of the network device can be changed by setting the value to the following definition files beforehand.

Storage Location of the Definition File

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

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

Definition File Name

unm_mon.rcxprop

Definition File Format

Specify variables in the definition file in the following format.

Parameter = *Value*

Parameter

Specify variables for network device configuration file management.

Parameter	Meaning and Value
CONFIG_BACKUP	Specify whether to enable network device file management function. - true Network device file management is enabled. - false Network device file management is disabled. If left blank, "true" is specified.
CONFIG_AUTO_MASTER	Specify whether to collect a master configuration file when registering a network device as a resource. - true A master configuration file is collected. - false A master configuration file is not collected. If left blank, "false" is set.
CONFIG_AUTO_BACKUP	Specify whether to back up configuration files when network device auto-configuration is performed. - true Network device configuration file backup is performed. - false Network device configuration file backup is not performed. If left blank, "false" is set.
CONFIG_RETRY_COUNT	Specify the retry count using a value between 0 and 10 for the network device connection when configuration backup is performed. If left blank, "3" is set.
CONFIG_TIMEOUT	Specify the time out value using a value between 10 and 60 for the network device connection when configuration backup is performed. If left blank, "30" is set.
CONFIG_NOTIFY_COMMAND	Specify whether to output a notification message if a change is detected in the backed up configuration when the rcxadm netdeivce cfbackup command is executed (On demand collection). - true A message is output. - false No message is output. If left blank, "false" is set.
CONFIG_NOTIFY_AUTO	Specify whether to output a notification message if a change is detected in the backed up network device configuration file when network device autoconfiguration is performed. - true

	Message is ouput. - false Message is not ouput. If left blank, "false" is specified.

Example

```
CONFIG_BACKUP=true
CONFIG_AUTO_MASTER=true
CONFIG_AUTO_BACKUP=true
CONFIG_RETRY_COUNT=3
CONFIG_TIMEOUT=30
CONFIG_NOTIFY_COMMAND=true
CONFIG_NOTIFY_AUTO=false
```

9.4.9 When Automatically Configuring and operating Network Devices

This section explains how to prepare to use the function for automatically configuring and operating network devices.

Information

Automatic configuration and operation of firewalls and server load balancer is not possible if they are not registered in a network pool.

The following operations are necessary to automatically configure and operate network devices.

- Creating Model Definitions for Network Devices
- Create a folder for registering rulesets
- Create rulesets for automatic configuration and operations

  The virtual IP address which is set at firewall rule or server load balance rule is IP address for use on the public LAN.

  For details on virtual IP address, refer to "9.1.3.1 Information Necessary for Designing a Public LAN".

Ruleset is the generic name for scrips and required files for scripts which prepared per device name or model name to automatically configure and operate network devices.

This product provides sample of scripts and required files.

For details on preparation,refer to "Appendix F Preparing for Automatic Configuration and Operation of Network Devices".

For details on sample, refer to "Appendix G Sample Script for Automatic Configuration and Operation of Network Devices".

9.5 When Providing an 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 9.8 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.
	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.

* Note: 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

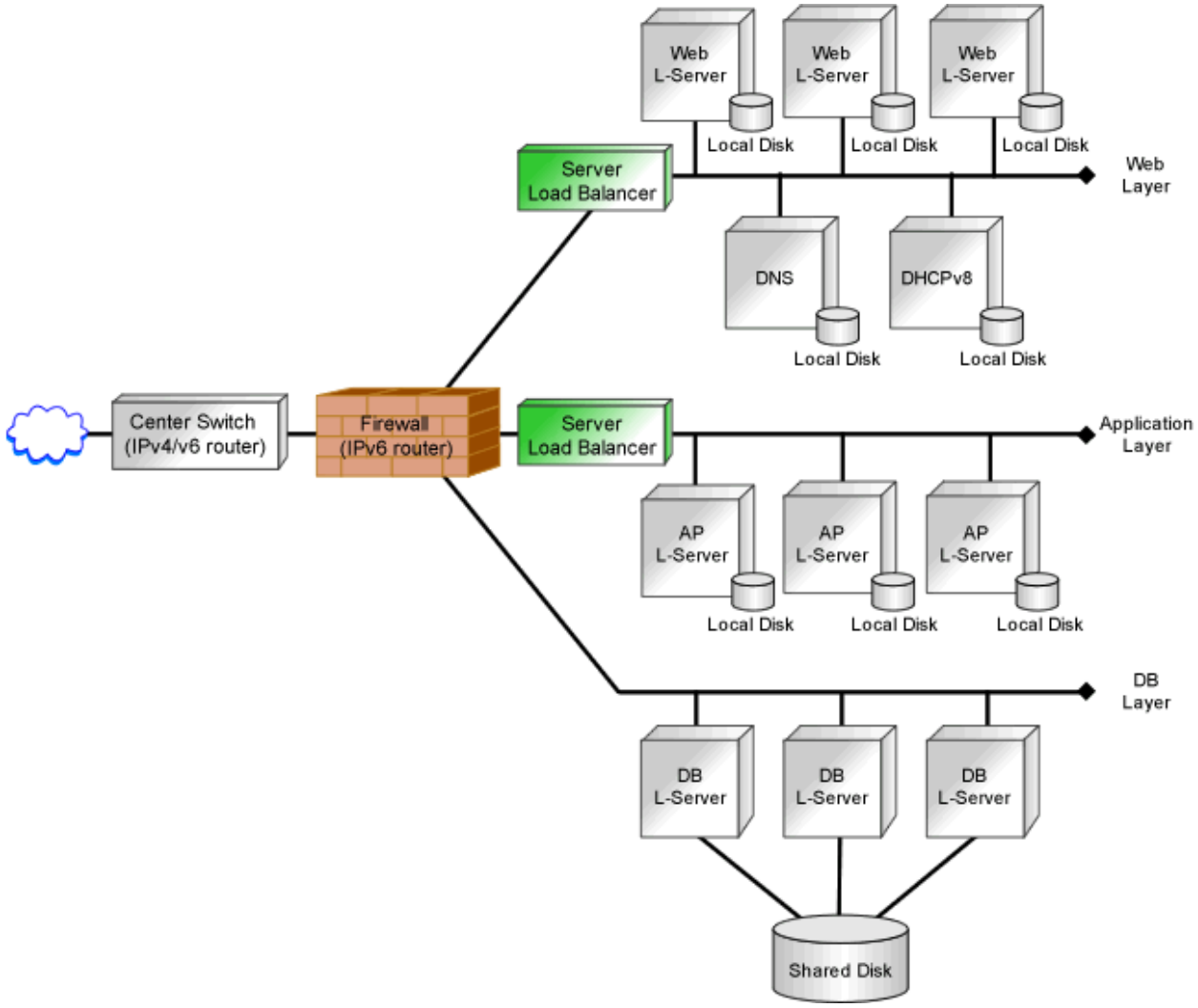
An example of designing the IPv6 address range (prefix and network ID) to be allocated to each public LAN based on the assigned GUA is given below:

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 9.18 Example of Public LAN Configuration Using an IPv6 Network



Chapter 10 Deciding and Configuring the Storage Environment

This section explains how to define and configure the storage environment.

10.1 Deciding the Storage Environment

This section explains how to define the storage environment settings required for a Resource Orchestrator setup.

10.1.1 Allocating 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.

     (Virtual storage resources registered in a storage pool where the priority level is high and virtual storage resources with a high capacity are selected by priority.)

  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] [Solaris Containers]

  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 virtual L-Server disk.

  2. Make the VM host (In [Solaris Containers], the global zone) recognize the LUNs created in 1. as raw devices.

     When migrating VM guests (In [Solaris Containers], the non-global zone) 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 virtual L-Server 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.

For details on storage allocation methods and storage types and server virtualization types for virtual L-Servers, refer to "Table 2.7 Storage Allocation Methods and Storage Types and Server Virtualization Types for Virtual L-Servers".

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.

     (Virtual storage resources registered in a storage pool where the priority level is high and virtual storage resources with a high capacity are selected by priority.)
  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.

For detail on storage allocation methods and storage types for physical L-Servers, refer to "Table 2.6 Storage Allocation Methods and Storage Types for Physical L-Servers".

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.

  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.

- Method for using the thin provisioning of server virtualization software

  Resource Orchestrator can be coordinated 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 how to set storage pool has thin provisioning attributes, refer to "20.2 Creating a Resource Pool" in 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.

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 "10.1.2 Storage Configuration".

- 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 "Effective Utilization of Storage Using Thin Provisioning".

Note

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.

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.

10.1.2 Storage Configuration

This section provides an overview of storage configurations.
The storage configurations supported by Resource Orchestrator are as follow:

- When Using Physical L-Servers

  Refer to "D.3 Storage Preparations" and "D.3 Storage Preparations" in "D.3 Storage Preparations".

- When Using Virtual L-Servers

  [VMware]
  Refer to "Supported Storage Configurations" in "E.1.3 Storage Preparations".

  [Hyper-V]
  Refer to "Supported Storage Configurations" in "E.2.3 Storage Preparations".

  [Xen]
  Refer to "Supported Storage Configurations" in "E.3.3 Storage Preparations".

  [Oracle VM]
  Refer to "Supported Storage Configurations" in "E.4.3 Storage Preparations".

  [KVM]
  Refer to "Supported Storage Configurations" in "E.5.3 Storage Preparations".

  [Solaris Containers]
  Refer to "Supported Storage Configurations" in "E.6.3 Storage Preparations".

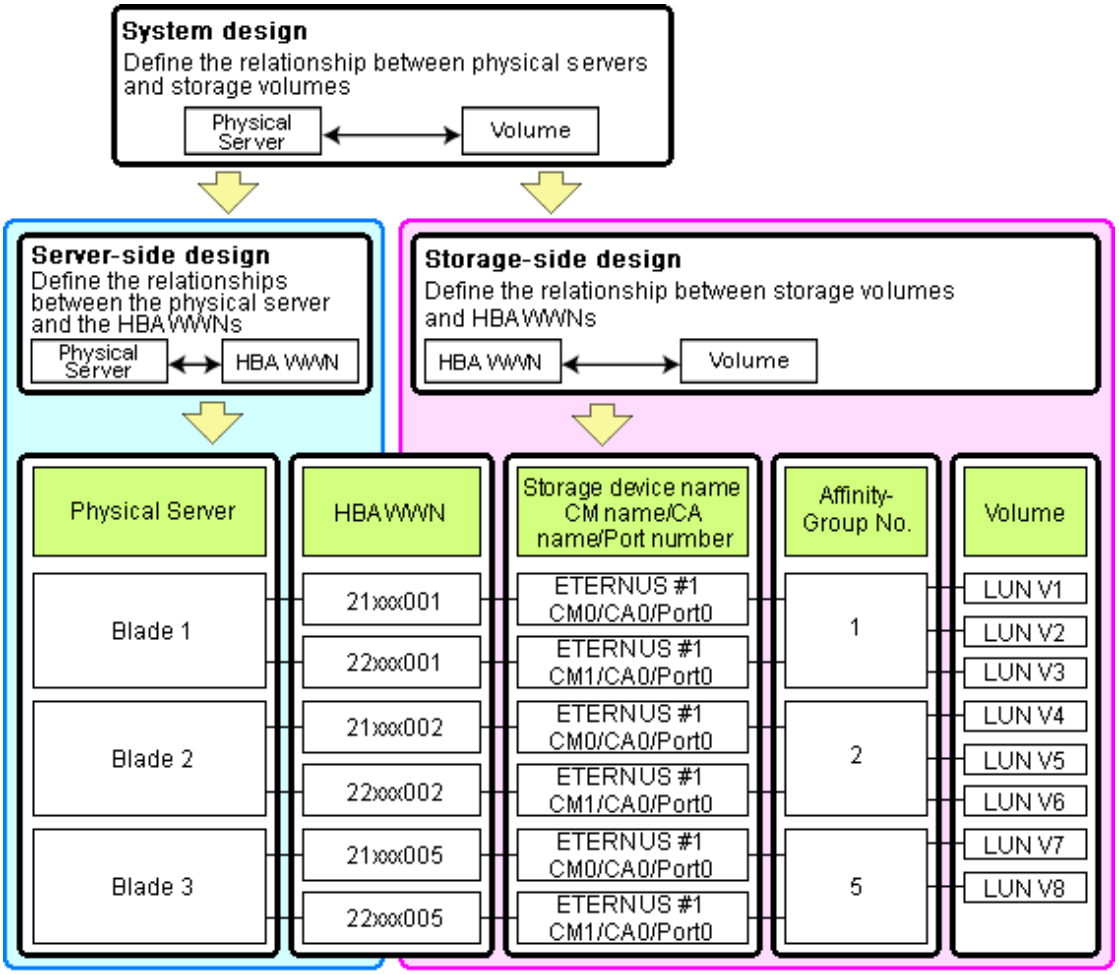
10.1.3 HBA and Storage Device Settings

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 10.1 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".

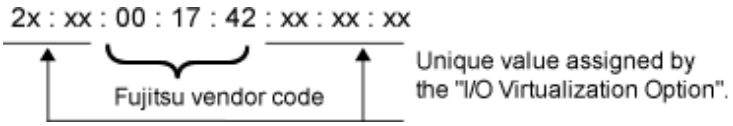
Information

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 WWPN. Define and use each of them as follows.

- 20: Use as a WWNN
- 2x: Use as a WWPN

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.

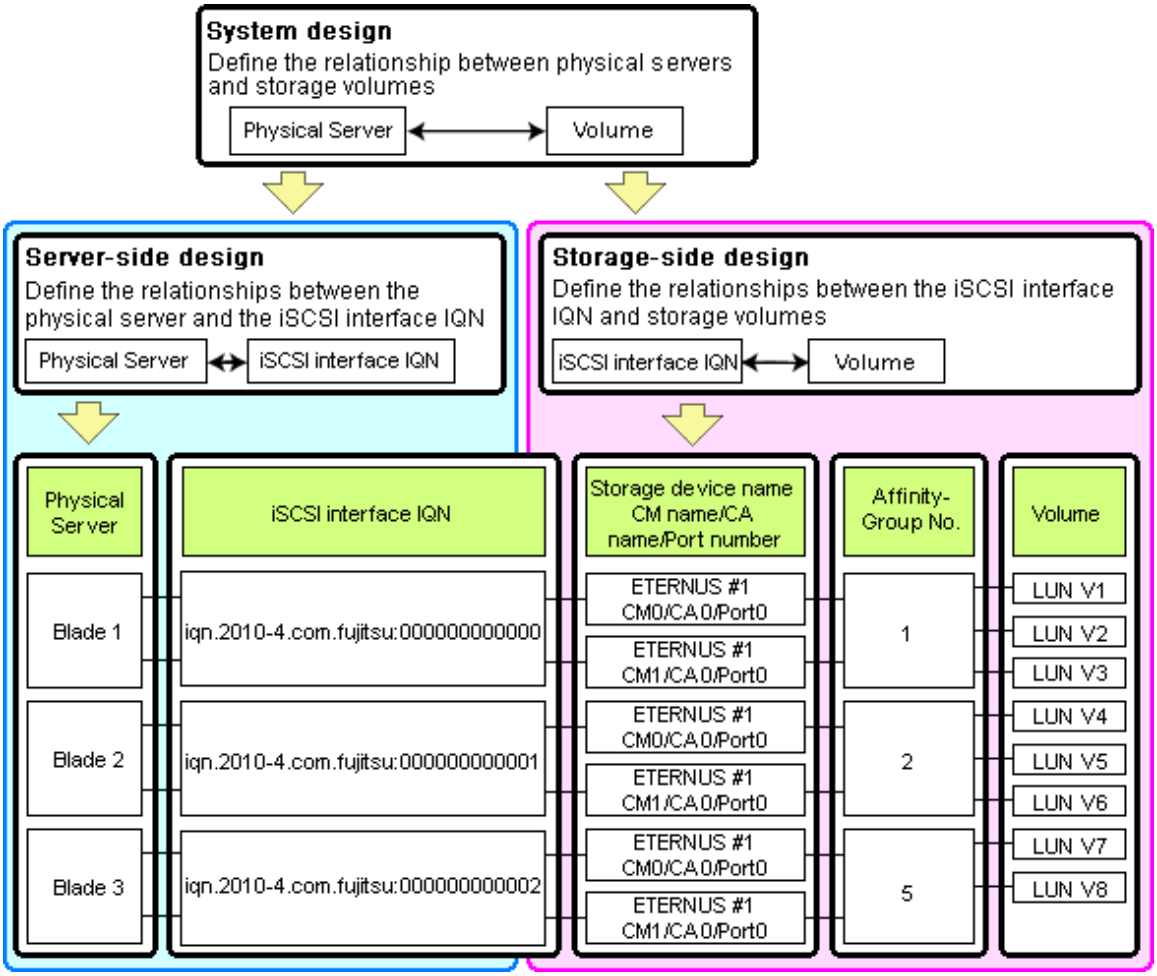
Defining WWN settings for VIOM

VIOM should be configured first. Then, storage devices should also be configured in accordance with the WWN settings that were defined within VIOM.

10.1.4 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 10.2 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.

10.2 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.3.3 When Using ETERNUS Storage".
    - When using NetApp FAS storage

      Refer to "D.3.4 When Using NetApp FAS Storage".
    - When using EMC CLARiiON storage

      Refer to "D.3.5 When Using EMC CLARiiON Storage".
    - When using EMC Symmetrix DMX storage or EMC Symmetrix VMAX storage

      Refer to "D.3.6 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.3.3 When Using ETERNUS Storage".
    - When using NetApp FAS storage

      Refer to "D.3.4 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 "Preparations for Storage Environments" in "E.1.3 Storage Preparations".

- When Using Hyper-V

  Refer to "Preparations for Storage Environments" in "E.2.3 Storage Preparations".

- When Using RHEL5-Xen

  Refer to "Preparations for Storage Environments" in "E.3.3 Storage Preparations".

- When Using Oracle VM

  Refer to "Preparations for Storage Environments" in "E.4.3 Storage Preparations".

- When Using RHEL-KVM

  Refer to "Preparations for Storage Environments" in "E.5.3 Storage Preparations".

- When Using Solaris Containers

  Refer to "Preparations for Storage Environments" in "E.6.3 Storage Preparations".

Chapter 11 Deciding and Configuring Server Virtualization Software

This section explains how to decide and configure server virtualization software.

11.1 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
  - RHEL-KVM
  - Oracle VM
  - Solaris Containers

Settings differ according to the server virtualization software being used.

When using server virtualization software, refer to "Appendix E Preparations for Creating a Virtual L-Server".

Note

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 11.1 List of Resource Orchestrator Functions Enabled by Using Each Server Virtualization Function

Resource Orchestrator Function	VMware Function	Hyper-V Function	RHEL5-Xen Function	RHEL-KVM Function	Oracle VM Function	Solaris Containers Function	Reference
L-Server power operations	VM guest power operations						Refer to "17.1 Power Operations" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".
L-Server cloning image	Template		Yes	Yes	Template	BladeLogic Virtual Guest Package	Refer to the setup section for the server virtualization software to use in "Appendix E Preparations for Creating a Virtual L-Server".

Resource Orchestrator Function	VMware Function	Hyper-V Function	RHEL5-Xen Function	RHEL-KVM Function	Oracle VM Function	Solaris Containers Function	Reference
L-Server snapshots	Snapshot	Checkpoints	-	-	-	-	Refer to "17.6 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	-	Refer to "15.2 VM Maintenance Mode of VM Hosts" in the "User's Guide VE".
Moving an L-Server between VM hosts (migration)	Migration	Migration using clusters	Migration			Yes	Refer to "17.7 Migration of VM Hosts between Servers" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".
Overcommit (CPU)	Reservation / Limit / Shares	Reservation / Limit / Virtual Quantity of VMs	-	Yes	-	Yes	[VMware] Refer to "C.2.11 Overcommit" in the "Setup Guide CE". [Hyper-V] Refer to "C.3.12 Overcommit" in the "Setup Guide CE". [RHEL-KVM] Refer to "C.6.10 Overcommit" in the "Setup Guide CE". [Solaris Containers] Refer to "C.7.9 Overcommit" in the "Setup Guide CE".
Overcommit (memory)	Reservation / Limit / Shares	Dynamic Memory	-	Yes	-	Yes	[VMware] Refer to "C.2.11 Overcommit" in the "Setup Guide CE". [Hyper-V] Refer to "C.3.12 Overcommit" in the "Setup Guide CE". [RHEL-KVM] Refer to "C.6.10

Resource Orchestrator Function	VMware Function	Hyper-V Function	RHEL5-Xen Function	RHEL-KVM Function	Oracle VM Function	Solaris Containers Function	Reference
							Overcommit" in the "Setup Guide CE". [Solaris Containers] Refer to "C.7.9 Overcommit" in the "Setup Guide CE".
Server Recovery	Located on a cluster for which VMware HA is enabled	Located on the MSFC	-	-	Located on a server pool for which HA is enabled	Yes	Refer to "16.3.2 [Server] Tab" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".
Alive Monitoring	VMware HA Cluster VM and Application Monitoring	MSFC Heartbeat	-	-	-	-	Refer to "16.3.2 [Server] Tab" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".
Thin Provisioning	Thin Provisioning	-	-	-	-	-	Refer to "10.1.1 Allocating Storage".
L-Server Console	Virtual Machine Console in the vSphere Web Client	Virtual Machine Console in the SCVMM Administrator Console	-	-	-	-	For details, refer to "17.3 Using the L-Server Console" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Function name: Function name used in Resource Orchestrator
Yes: Function provided without using server virtualization software function
-: Function not provided in Resource Orchestrator

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 11.2 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 4.0 VMware vSphere 4.1 VMware vSphere 5.0	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

[Hyper-V]
VMware 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.

11.2 Settings for 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.1 VMware".

  [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.2 Hyper-V".

  [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.3 RHEL5-Xen".

  [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.4 Oracle VM".

[KVM]

For details, refer to "E.5 KVM".

[Solaris Containers]

For details, refer to "E.6 Solaris Containers".

Chapter 12 Installing and Defining Single Sign-On

The Single Sign-On environment using the function of ServerView Operations Manager is required for Resource Orchestrator Cloud Edition. Before installing Resource Orchestrator, certificate preparation and user registration with the directory service are required. This section explains the necessary preparations.

When upgrading Resource Orchestrator from earlier versions, configure the Single Sign-On environment, referring to "12.5 Updating from Earlier Versions".

12.1 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 only directory server which can be used by Resource Orchestrator is the one that was specified during installation.

After deployment of Resource Orchestrator, only the password of the directory server's administrator can be changed.

12.2 Setting up ServerView Operations Manager and the Directory Service Environment

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

Note

Do not modify the LDAP port number of OpenDS.

12.2.1 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 "8.6.1 Settings for Tenant Management and Account Management" in the "Operation Guide CE". By default, the content of operations 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

  ou=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 definition file includes the setting which reflects the content of operations, when a user is deleted from Resource Orchestrator, the corresponding user account will be deleted from the directory service as well. Exercise caution when using an existing directory service for user management on another system.

12.2.2 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/
```

12.2.3 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. Register a user from the ROR console.
  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. Register a user from the ROR console.
  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\opends\bat\ldapmodify.bat" -p 1473 -f user.ldif -D
   "cn=Directory Manager" -w admin -c <RETURN>
   ```

   [Linux]

   ```
   # /opt/fujitsu/ServerViewSuite/opends/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"

12.2.4 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 restoration of OpenDS, refer to the ServerView Operations Manager manual.

12.3 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 12.1 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 ldif_file -D OpenDS_administrator_user_DN -w Password <RETURN>
```

   [Linux]

```
# "OpenDS_installation_folder/bin/ldapmodify" -p Port_number -f ldif_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\opends\bat\ldapmodify.bat" -p 1473 -f manager.ldif -D "cn=Directory Manager" -w admin <RETURN>
```

12.4 When Reconfiguring Single Sign-On

This section explains how to reconfigure Single Sign-On.

12.4.1 Reconfiguration Procedure

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

12.4.1.1 Confirming Certificates

Execute the keytool command and Resource Orchestrator command, and check if the CA certificate has been imported correctly.

1. Check the content of the CA certificate (keystore) of ServerView Operations Manager.

   Specify the password of a keystore of ServerView Operations Manager as the password of a keystore. Refer to the following manual for the password of a keystore of ServerView Operations Manager.

   The CA certificate (keystore) of ServerView Operations Manager is stored in the following location:

   [Windows]
   ServerView Suite_Installation_folder\jboss\server\serverview\conf\pki\cacerts

   [Linux]
   /opt/fujitsu/ServerViewSuite/jboss/server/serverview/conf/pki/cacerts

   Example

   [Windows Manager]

   ```
   >C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -list -keystore "C:\Program Files\Fujitsu
   \ServerView Suite\jboss\server\serverview\conf\pki\cacerts" <RETURN>
   Enter keystore password:

   Keystore type: JKS
   Keystore provider: SUN

   Your keystore contains 1 entry

   svs_cms, 2011/10/01, trustedCertEntry,
   Certificate fingerprints (MD5): 02:68:56:4C:33:AF:55:34:87:CA:51:FD:BF:66:47:06
   ```

   [Linux Manager]

   ```
   # /opt/FJSVrcvmr/runtime/jre6/bin/keytool -list -keystore /opt/fujitsu/ServerViewSuite/jboss/server/
   serverview/conf/pki/cacerts <RETURN>
   Enter keystore password:

   Keystore type: JKS
   Keystore provider: SUN

   Your keystore contains 1 entry

   svs_cms, 2011/10/01, trustedCertEntry,
   Certificate fingerprints (MD5): 02:68:56:4C:33:AF:55:34:87:CA:51:FD:BF:66:47:06
   ```

2. Check whether the CA certificate of ServerView Operations Manager is imported correctly into the keystore of this product.

   a. Execute the following Resource Orchestrator command.

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

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

   b. Check the displayed difference information.

      The information is displayed as follows:

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

      When difference is displayed, registration of a CA certificate (keystore) may have failed. In this case, register the CA certificate referring to "12.4.1.2 Registering Certificates".

c. Execute the keytool command.

   For the -alias option, specify the "alias" displayed in 1.
   When multiple aliases are displayed as a result of 1., check each of the displayed aliases.

   The password for the keystore of Resource Orchestrator is set to "changeit" by default.

   Check whether the fingerprints of the certificates displayed by 1. and the fingerprints of the certificates displayed in Resource orchestrator match.

   Example

   [Windows Manager]

```
>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, 2012/04/10, trustedCertEntry,
Certificate fingerprints (MD5): 02:68:56:4C:33:AF:55:34:87:CA:51:FD:BF:66:47:06

>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -list -alias Another_name -keystore "C:\Fujitsu
\ROR\IAPS\JDK6\jre\lib\security\cacerts" <RETURN>
Enter keystore password: changeit
svs_cms, 2012/04/10, trustedCertEntry,
Certificate fingerprints (MD5): 02:68:56:4C:33:AF:55:34:87:CA:51:FD:BF:66:47:06

>C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -list -alias Another_name -keystore "C:\Fujitsu
\ROR\SWRBAM\etc\config\ssl\IJINibpmsv\cacerts.jks" <RETURN>
Enter keystore password: changeit
svs_cms, 2012/04/10, trustedCertEntry,
Certificate fingerprints (MD5): 02:68:56:4C:33:AF:55:34:87:CA:51:FD:BF:66:47:06
```

   [Linux Manager]

```
# /opt/FJSVrcvmr/runtime/jre6/bin/keytool -list -alias Another_name -keystore /opt/FJSVawjbk/jdk5/jre/lib/
security/cacerts <RETURN>
Enter keystore password: changeit
svs_cms, 2012/04/10, trustedCertEntry,
Certificate fingerprints (MD5): 02:68:56:4C:33:AF:55:34:87:CA:51:FD:BF:66:47:06

# /opt/FJSVrcvmr/runtime/jre6/bin/keytool -list -alias Another_name -keystore /opt/FJSVawjbk/jdk6/jre/lib/
security/cacerts <RETURN>
Enter keystore password: changeit
svs_cms, 2012/04/10, trustedCertEntry,
Certificate fingerprints (MD5): 02:68:56:4C:33:AF:55:34:87:CA:51:FD:BF:66:47:06

# /opt/FJSVrcvmr/runtime/jre6/bin/keytool -list -alias Another_name -keystore /etc/opt/FJSVswrbam/config/ssl/
IJINibpmsv/cacerts.jks <RETURN>
Enter keystore password: changeit
svs_cms, 2012/04/10, trustedCertEntry,
Certificate fingerprints (MD5): 02:68:56:4C:33:AF:55:34:87:CA:51:FD:BF:66:47:06
```

   When the information on the CA certificate is not displayed, or when the fingerprints of credentials are not in agreement, that means that registration of the CA certificate has failed. In this case, register the CA certificate referring to "12.4.1.2 Registering Certificates".

12.4.1.2 Registering Certificates

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

1. Execute the following command:

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

   Specify the alias of the certificate displayed by performing "12.4.1.1 Confirming Certificates" as *alias*.

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

   Point

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

2. Check the difference of the CA certificate.

   Perform "12.4.1.1 Confirming Certificates", and check that the updated certificate is not displayed.

3. Copy the keystore of Resource Orchestrator.

   [Windows Manager]

   - Files to Copy

     *Installation_folder**IAPS**JDK5**jre**lib**security**cacerts*

   - Copy Destination

     Installation_folder\IAPS\JDK5\jre\lib\security\cacerts.org

   - Files to Copy

     Installation_folder\IAPS\JDK6\jre\lib\security\cacerts

   - Copy Destination

     Installation_folder\IAPS\JDK6\jre\lib\security\cacerts.org

   - Files to Copy

     Installation_folder\SWRBAM\etc\config\ssl\IJINibpmsv\cacerts.jks

   - Copy Destination

     Installation_folder\SWRBAM\etc\config\ssl\IJINibpmsv\cacerts.org

   [Linux Manager]

   - Files to Copy

     /opt/FJSVawjbk/jdk5/jre/lib/security/cacerts

   - Copy Destination

     /opt/FJSVawjbk/jdk5/jre/lib/security/cacerts.org

   - Files to Copy

     /opt/FJSVawjbk/jdk6/jre/lib/security/cacerts

   - Copy Destination

     /opt/FJSVawjbk/jdk6/jre/lib/security/cacerts.org

- Files to Copy

  /etc/opt/FJSVswrbam/config/ssl/IJINibpmsv/cacerts.jks

- Copy Destination

  /etc/opt/FJSVswrbam/config/ssl/IJINibpmsv/cacerts.org

Note

Ensure that the keystore of Resource Orchestrator is copied, as it will be necessary when changing the directory service.

4. Copy 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\cacerts

   [Linux]
   /opt/fujitsu/ServerViewSuite/jboss/server/serverview/conf/pki/cacerts

   Example

   [Windows Manager]

   ```
   >C:\Fujitsu\ROR\SVROR\Manager\runtime\jre6\bin\keytool.exe -importkeystore -srckeystore " C:\Program Files\Fujitsu
   \ServerView Suite\jboss\server\serverview\conf\pki\cacerts" -destkeystore "C:\Fujitsu\ROR\IAPS\JDK5\jre\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\cacerts" -destkeystore "C:\Fujitsu\ROR\IAPS\JDK6\jre\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\cacerts" -destkeystore "C:\Fujitsu\ROR\SWRBAM\etc\config\ssl
   \IJINibpmsv\cacerts.jks"<RETURN>
   ```

   [Linux Manager]

   ```
   # /opt/FJSVrcvmr/runtime/jre6/bin/keytool -importkeystore -srckeystore /opt/fujitsu/ServerViewSuite/jboss/server/serverview/
   conf/pki/cacerts -destkeystore /opt/FJSVawjbk/jdk5/jre/lib/security/cacerts<RETURN>

   # /opt/FJSVrcvmr/runtime/jre6/bin/keytool -importkeystore -srckeystore /opt/fujitsu/ServerViewSuite/jboss/server/serverview/
   conf/pki/cacerts -destkeystore /opt/FJSVawjbk/jdk6/jre/lib/security/cacerts<RETURN>

   # /opt/FJSVrcvmr/runtime/jre6/bin/keytool -importkeystore -srckeystore /opt/fujitsu/ServerViewSuite/jboss/server/serverview/
   conf/pki/cacerts -destkeystore /etc/opt/FJSVswrbam/config/ssl/IJINibpmsv/cacerts.jks<RETURN>
   ```

   After executing the command, enter the password.
   The password for the keystore of Resource Orchestrator is set to "changeit" by default.

5. 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 successfully imported.
   Import command completed: 1 entries successfully imported. 0 entries failed or cancelled.
   ```

6. Execute the keytool command, and check if the CA certificate has been correctly imported.

   Perform the Procedure of "12.4.1.1 Confirming Certificates" and check whether the CA certificates have been imported correctly.

7. Import the server certificate to ServerView Operations Manager. For details, refer to "3.3 Importing a Certificate to ServerView SSO Authentication Server" in the "Setup Guide CE".

12.4.1.3 Checking Directory Service Connection Information

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

1. Execute the following Resource Orchestrator command.

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

   The connection information registered in Resource Orchestrator is displayed.

2. Check the displayed connection information.

   The information is displayed as follows:

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

      - When using Active Directory or ServerView Operations Manager V5.5 or later

        Execute the rcxadm authctl sync command and change the directory service connection information.

      - When using OpenDS provided with ServerView Operations Manager V5.3

        Execute the rcxadm authctl modify command and change the directory service connection information.

        Example

        ```
        >rcxadm 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".

c. Start the manager.

For details on the rcxadm authctl command, refer to "5.4 rcxadm authctl" in the "Reference Guide (Command/XML) CE".

12.4.2 Modifying Directory Service Connection Information

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

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

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

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

2. Refer to "12.4.1.1 Confirming Certificates" and check whether the CA certificate of ServerView Operations Manager has been imported correctly to the Resource Orchestrator keystore .

3. When the certificate has not been imported to the keystore, refer to "12.4.1.2 Registering Certificates" and register a certificate.

4. Change the directory service connection information.

   - When using Active Directory or ServerView Operations Manager V5.5 or later

     Execute the rcxadm authctl sync command and change the directory service connection information.

   - When using OpenDS provided with ServerView Operations Manager V5.3

     Execute the rcxadm authctl modify command and change the directory service connection information.

     Example

     ```
     >rcxadm 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 rcxadm authctl command, refer to "5.4 rcxadm authctl" in the "Reference Guide (Command/XML) CE".

If the directory service is OpenDS and the password of the user with administrator rights has been changed,perform the following procedure. It is not necessary if the directory service is Active Directory.

1. Stop the manager.

   Refer to "2.1 Starting and Stopping the Manager" in the "Operation Guide CE" 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 "2.1 Starting and Stopping the Manager" in the "Operation Guide CE" for information on how to start the manager.

12.4.3 When Certificates Have Expired

When the CA certificate of ServerView Operations Manager or the directory server has expired, re-register the CA certificates after obtaining new certificates. For details on how to register the CA certificates, refer to "12.4.1.2 Registering Certificates".

12.5 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 12.2 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 Administrators (Privileged Users)	Yes	-	Yes	-	-	Yes	-
3	Registering Directory Service Connection Information in Resource Orchestrator	Yes	-	Yes	-	-	Yes	-
4	Changing Already Registered Directory Service Connection Information	-	Yes	-	Yes	Yes	-	Yes
5	Registering CA Certificates of ServerView Operations Manager	Yes	-	Yes	Yes (*)	-	Yes	-
6	Setup	Yes	Yes	Yes	Yes	Yes	Yes	Yes
7	Login on the ROR Console	Yes	Yes	Yes	Yes	Yes	Yes	Yes
8	License Setup	Yes	Yes	Yes	Yes	Yes	Yes	Yes
9	Moving Information in the Directory Service Used in Earlier Versions	-	Yes	-	Yes	Yes	-	-
10	Registering Users in the Directory Service	Yes	-	Yes	-	-	Yes	-
11	Transferring Tenant and Tenant Administrators	-	-	Yes	Yes	Yes	Yes	-
12	Configuration after Installation	Yes	Yes	Yes	Yes	Yes	Yes	Yes
13	Importing a Certificate to a Browser	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Yes: Required, - : Not Required

* Note: This procedure is necessary when using OpenDS or an Active Directory that was configured individually.

1. Installing Resource Orchestrator

   Refer to "Appendix F Upgrading from Earlier Versions" in the "Setup Guide CE".

2. Registering Administrators (Privileged Users)

   For details, refer to "12.3 Registering Administrators".

3. Registering Directory Service Connection Information in Resource Orchestrator

   Refer to "12.5.1 Registering Directory Service Connection Information in Resource Orchestrator".

4. Changing Already Registered Directory Service Connection Information

   Refer to "12.5.2 Changing Already Registered Directory Service Connection Information".

5. Registering CA Certificates of ServerView Operations Manager

   Refer to "12.5.3 Registering CA Certificates of ServerView Operations Manager".

6. Setup

   Set up the manager. Refer to "2.1.4 Setup" in the "Setup Guide CE".

7. Login on the ROR Console

   Refer to "Chapter 4 Login to the ROR Console" in the "Setup Guide CE".

8. License Setup

   Refer to "Chapter 5 License Setup and Confirmation" in the "Setup Guide CE".

9. Moving Information in the Directory Service Used in Earlier Versions

   Refer to "12.5.4 Moving Information in the Directory Service Used in Earlier Versions".

10. Registering Users in the Directory Service

    Refer to "12.5.5 Registering Users in the Directory Service".

11. Transferring Tenant and Tenant Administrators

    For details, refer to "12.5.6 Transferring Tenant and Tenant Administrators".

12. Configuration after Installation

    Set up the SSL communication environment of the ROR console. Set up e-mail and the application process.

    Refer to "Chapter 3 SSL Communication Environment Settings for the ROR Console" and "Chapter 19 To Customize Environment" in the "Setup Guide CE".

13. Importing a Certificate to a Browser

    Refer to "Chapter 6 Importing a Certificate to a Browser" in the "Setup Guide CE".

12.5.1 Registering Directory Service Connection Information in Resource Orchestrator

Register the directory service connection information for performing Single Sign-On in Resource Orchestrator.

Use the following procedure to register the directory service connection information in Resource Orchestrator.

1. Stop the manager.

   Execute the rcxadm mgrctl stop command and stop the manager.

   For details on the rcxadm mgrctl stop command, refer to "5.14 rcxadm mgrctl" in the "Reference Guide (Command/XML) CE".

2. Register the directory service connection information for performing Single Sign-On.

   Execute the rcxadm authctl sync command and register the directory service connection information.

   For details on the rcxadm authctl sync command, refer to "5.4 rcxadm authctl" in the "Reference Guide (Command/XML) CE".

3. Start the manager.

   Execute the rcxadm mgrctl start command and start the manager.

   For details on the rcxadm mgrctl start command, refer to "5.14 rcxadm mgrctl" in the "Reference Guide (Command/XML) CE".

12.5.2 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.
Change the directory service connection information used in earlier versions.

1. Stop the manager.

   Execute the rcxadm mgrctl stop command and stop the manager.

   For details on the rcxadm mgrctl stop command, refer to "5.14 rcxadm mgrctl" in the "Reference Guide (Command/XML) CE".

2. Change the directory service connection information.

   Execute the rcxadm authctl sync command and change the directory service connection information.

   For details on the rcxadm authctl sync command, refer to "5.4 rcxadm authctl" in the "Reference Guide (Command/XML) CE".

   ```
   >rcxadm authctl sync
   ```

3. Start the manager.

   Execute the rcxadm mgrctl start command and start the manager.

   For details on the rcxadm mgrctl start command, refer to "5.14 rcxadm mgrctl" in the "Reference Guide (Command/XML) CE".

12.5.3 Registering CA Certificates of ServerView Operations Manager

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

1. Stop the manager.

   Execute the rcxadm mgrctl stop command and stop the manager.

   For details on the rcxadm mgrctl stop command, refer to "5.14 rcxadm mgrctl" in the "Reference Guide (Command/XML) CE".

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

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

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

   Example

   [Windows Manager]

   ```
   >C:\Fujitsu\ROR\SVROR\Manager\bin\rcxadm authctl diffcert
   svs_cms
   ldaphost.fujitsu.com
   ```

   [Linux Manager]

   ```
   # /opt/FJSVrcvmr/bin/rcxadm authctl diffcert
   svs_cms
   ldaphost.fujitsu.com
   ```

3. Update the CA certificate.

   Execute the following command.

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

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

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

 Example

[Windows Manager]

```
>C:\Fujitsu\ROR\SVROR\Manager\bin\rcxadm authctl refreshcert -alias svs_cms <RETURN>
```

[Linux Manager]

```
# /opt/FJSVrcvmr/bin/rcxadm authctl refreshcert -alias svs_cms <RETURN>
```

4. Check the difference of the CA certificate.

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

5. Start the manager.

   Execute the rcxadm mgrctl start command and start the manager.

   For details on the rcxadm mgrctl start command, refer to "5.14 rcxadm mgrctl" in the "Reference Guide (Command/XML) CE".

12.5.4 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 in 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 "5.4 rcxadm authctl" in the "Reference Guide (Command/XML) CE".

12.5.5 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" in 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
```

3. 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>

   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>
```

4. 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 users, refer to "Chapter 3 Configuring Users for Infrastructure Administrators" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

5. 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" in the "ServerView Suite User Management in ServerView"

   For OpenDS, perform settings for Single Sign-On referring to the setting procedure of Active Directory.

12.5.6 Transferring Tenant and Tenant Administrators

Upgrading from V3.0

Tenants, tenant administrators, and tenant users of the previous version are transferred as it is. The transfer operation here is unnecessary.

Upgrading from V2.3

The tenant management role cannot operate tenants and L-Servers in tenants operating on V2.3.
To make the tenant management role operate the tenant that is operating it with V2.3, you need to transfer the tenant to the newly made tenant.

Transferred Data of Tenants

- Users (users who operates the tenant as tenant administrators, tenant operators, and tenant monitors)
- Resources in local pools of tenants
- L-Servers

Use the multiple roles and operate tenants when the transfer is unnecessary. When one user operates two or more tenants, it is necessary to use the multiple role.

Use the following procedure to transfer tenants and tenant administrators.

1. Create a new tenant.

   In [Tenant] tab of ROR console, create a Tenant.

2. Modify tenant users.

   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.

   a. Output the user information in files in XML format.

      ```
      >rcxadm user list -format xml > myusers.xml
      ```

      For details on the rcxadm user command, refer to "7.1 rcxadm user" in the "Reference Guide (Command/XML) CE".

   b. Edit the XML files.

      Delete the information of other users from the XML file, so that only the users operating as tenant administrators, tenant operators, and tenant monitors remain.

      Define the tenant administrator roles to allocate.

      Add the following information:

      - Email address

- First name
- Family name

For details on the XML definition of tenant administrators, refer to "14.8.1 Tenant Management Roles and Tenant User Role" in the "Reference Guide (Command/XML) CE".

Example

Example of the XML definition in which the tenant administrator role of "NewTenant" is allocated to the user "john"

```
<?xml version="1.0" encoding="utf-8"?>
<Users>
  <User name="john">
    <Roles>
      <Role name="tenant_admin">
        <Scopes>
          <Scope>NewTenant</Scope>
         </Scopes>
      </Role>
    </Roles>
    <MailAddress>john@mail.example.com</MailAddress>
    <ActualName>
      <FirstName>john</FirstName>
      <LastName>fujitsu</LastName>
    </ActualName>
 </User>
</Users>
```

c. 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
```

3. Move resources.

   In [Resource] tab of ROR console, move following resources in the old tenant to the new tenant. Move resources after stopping it when L-Server starts.

   - Resources in the local pool

     Moves to a local pool or a global pool of the tenant that newly made it.

   - L-Servers

     Move to the tenant that newly made it.

4. Import L-Servers to the L-Platform

   Import L-Servers to the L-Platform by using the cfmg_importlserver command.

```
> cfmg_importlserver -user john -org NewTenant -lserver /NewTenant/lserverA
```

5. Delete the old tenant.

   Delete the old tenant by using the rcxadm tenant delete command.

```
> rcxadm tenant delete -name /OldTenant
```

Chapter 13 Deciding and Configuring the Power Monitoring Environment

This section explains how to decide and configure the power monitoring environment.

13.1 Deciding the Power Monitoring Environment

This section explains how to define the power monitoring environment settings required for a Resource Orchestrator setup.

For VMware ESXi, this function is not supported.

13.1.1 Settings for the Power Monitoring Environment

To monitor power consumption, choose values for the following settings.

Polling interval

This determines the time interval for collecting the power consumption data.
The possible values that can be set are any value (at one-minute intervals) between 1 and 6 minutes, or 10 minutes. The default is 5 minutes.

Data storage period

This defines the storage period for the collected environmental data.

Table 13.1 Storage Period Values for Power Monitoring Data

Data Sampling Rate	Lifespan (Unit: month)	
	Default Value	Maximum Value
Finest sampling (The most detailed data secured at the polling interval)	1	12
Hourly sampling	1	60
Daily sampling	12	120
Monthly sampling	60	300
Yearly sampling	60	600

13.1.2 Power Monitoring Device Settings

Choose values for the following power monitoring device (PDU or UPS) settings. If any of those settings have been already determined by other software, use those values.

Device name

This is the name that identifies the power monitoring device. Each device name should be unique within the system. The first character must be alphabetic, and the name can contain up to 15 alphanumeric characters and hyphens ("-").

Admin IP address

This IP address must be in the same subnet as the admin server.

SNMP community name

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

Voltage

This is the voltage (V) supplied to the power monitoring device.

Comments

These comments can be any description desired for the power monitoring device. The comments can contain up to 128 characters.

13.2 Configuring the Power Monitoring Environment

This section describes how to configure power monitor devices for Resource Orchestrator.

Apply the following settings to power monitoring targets. Refer to the manual of each power monitoring target for configuration instructions.

Admin IP address

This IP address is used by the admin server to communicate with a power monitoring target.

SNMP community name

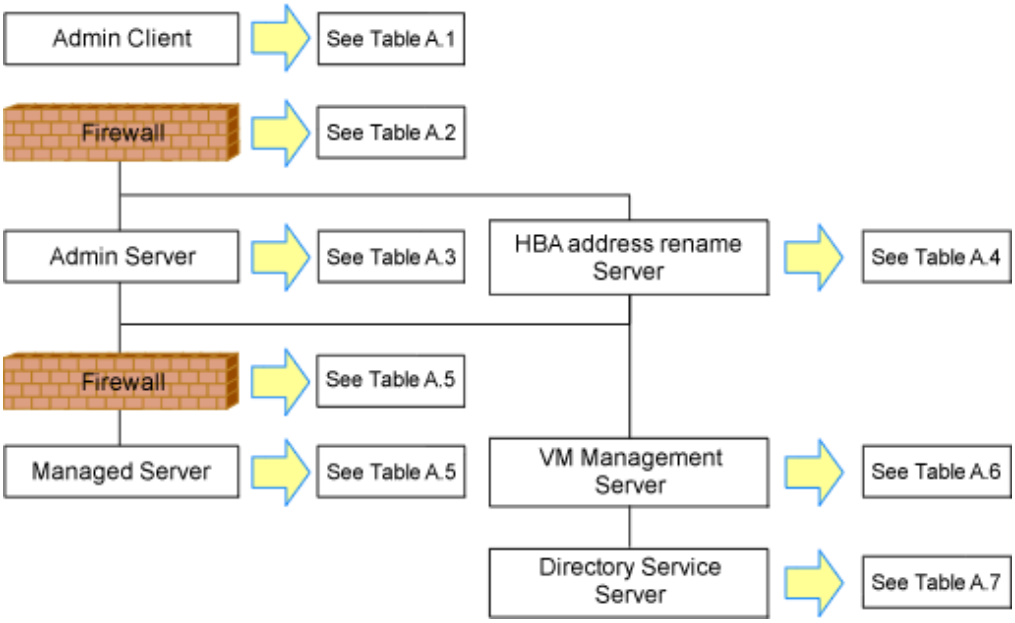
This SNMP community name is used by the admin server to collect power consumption data from a power monitoring target (via the SNMP protocol).

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 setup, refer to the following:

- Changing Admin Server Port Numbers
  - "6.2 Changing Port Numbers" in the "User's Guide for Infrastructure Administrators (Resource Management) CE"
  - "8.3 Changing Admin Server Port Numbers" in the "Operation Guide CE"
- Changing Managed Server Port Numbers
  - "7.1.6 Changing Port Numbers" in 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	
ROR console	Admin client	-	Variable value	Not possible	Admin server	rcxweb	23461	Not possible	tcp
ServerView Operations Manager (*)	Admin client	-	Variable value	Not possible	Admin server	http	3169	Not possible	tcp
						https	3170		
Interstage Business Process						http	80	Not possible	tcp

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
Manager Analytics operation management console									
ROR console - L-Platform - Template - Tenant Management - Request - Usage Condition - Dashboard	Admin client	-	Variable value	Not possible	Admin server	rcxctext	3500	Possible	tcp
						rcxctext2	3501	Possible	tcp
Systemwalker Runbook Automation Web console	Admin client	-	Variable value	Not possible	Admin server	http	80	Possible	tcp

* Note: 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	tcp
					3501	tcp
Systemwalker Runbook	One-way	Admin client	Variable value	Admin server	80	tcp

Function Overview	Direction	Source		Destination		Protocol
		Server	Port	Server	Port	
Automation Web console						
ROR CE e-mail delivery (*2)	One-way	Admin server	Variable value	Mail server	25	smtp
Systemwalker Runbook Automation e-mail delivery (*2)	One-way	Admin server	Variable value	Mail server	25	smtp
ROR CE API	One-way	Admin client	Variable value	Admin server	8014 8015	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	Not 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
		-	Variable value	-		nfdomain	[Windows Manager] 23457 [Linux Manager] 23455	Possible	tcp
		-	Variable value	-		rcxmgr	23460	Possible	tcp
		-	Variable value	-		rcxtask	23462	Possible	tcp
		-	Variable value	-		rcxmongrel1	23463	Possible	tcp

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
						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
		-	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
		-	Variable value	-	Server management unit (Remote Management Controller (XSCF))	snmp	161	Not possible	udp
		-	Variable value	-		snmptrap	162	Not possible	udp
		-	Variable value	-		ssh	22	Not possible	tcp
		-	Variable value	-	L2 Switch	telnet	23	Not possible	tcp
		-	Variable value	-		ping	-	-	ICMP
		-	Variable value	-		snmp	161	Not possible	tcp,udp

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
		-	Variable value	-	Firewall	telnet	23	Not possible	tcp
		-	Variable value	-		ping	-	-	ICMP
		-	Variable value	-		snmp	161	Not possible	tcp,udp
		-	Variable value	-	Server load balancer	telnet	23	Not possible	tcp
		-	Variable value	-		ping	-	-	ICMP
		-	Variable value	-		snmp	161	Not possible	tcp,udp
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 (*5) 4974 -	-	Admin server	-	14974 - 14989 (*5) 4974 -	-	udp

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
			4989 (*6)				4989 (*6)		
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/ Solaris container/ physical OS)	-	-	-	Admin server	-	2344	Not possible	tcp
Collection of performance information	Admin server	-	-	-	Managed server (Xen)	ssh	22	Possible	tcp

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
Storage of performance data configuration definitions	Admin server	-	-	-	Admin server	-	2344	Not possible	tcp
Acquisition of performance information from PDB	Admin server	-	-	-	Admin server	-	2345	Not possible	tcp
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	rcxctext	3500	Not possible	tcp
						rcxctext2	3501	Possible (*9)	tcp
Systemwalker Runbook Automation Web console	Admin client	-	Variable value	Not possible	Admin server	http	80	Possible (*9)	tcp
ROR CE management function	Admin server	-	Variable value	Not possible	Admin server	rcxcfvsys	8013	Possible (*9)	tcp
ROR CE API	Admin client	-	Variable value	Not possible	Admin server	rcxcfapi rcxctacnt	8014 8015	Possible (*9)	tcp
ROR CE for internal control	Admin server	-	Variable value	-	Admin server	rcxctrestchg	3550	Not possible	tcp

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
	Admin server	-	Variable value	-	Admin server	rcxctint	3551	Not possible	tcp
	Admin server	-	Variable value	-	Admin server	rcxctdbchg	5441	Possible (*9)	tcp
	Admin server	-	Variable value	-	Admin server	rcxctdbdsb	5442	Not possible	tcp
	Admin server	-	Variable value	-	Admin server	CORBA	8002	Possible (*9)	tcp
	Admin server	-	Variable value	-	Admin server	Servlet	9 available port numbers are used from Port 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
Interstage Java EE Admin console	Admin server	-	Variable value	-	Admin server	-	12001	Possible (*10)	tcp
Systemwalker Runbook Automation file transfer platform	Admin server	-	Variable value	-	Admin server	-	9664	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	Not possible	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
	Admin server	-	Variable value	-	Admin server	-	28080	Possible (*11)	tcp
	Admin server	-	Variable value	-	Admin server	-	23600	Possible (*12)	tcp
	Admin server	-	Variable value	-	Admin server	-	23601	Possible (*13)	tcp
	Admin server	-	Variable value	-	Admin server	-	23602	Possible (*14)	tcp
	Admin server	-	Variable value	-	Admin server	-	8686	Possible (*15)	tcp
	Admin server	-	Variable value	-	Admin server	-	9690	Possible (*16)	tcp
	Admin server	-	Variable value	-	Admin server	-	9691	Possible (*16)	tcp
	Admin server	-	Variable value	-	Admin server	-	7676	Not possible	tcp
	Admin server	-	Variable value	-	Admin server	-	23700	Not possible	tcp
Network Device Automatic Configuration	Admin server	-	Variable value	-	L2 Switch	ftp	21	Not possible	tcp
						ssh	22	Not possible	tcp

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
						telnet	23	Not possible	tcp
		-	Variable value	-	Firewall	ssh	22	Not possible	tcp
						telnet	23	Not possible	tcp
		-	Variable value	-	Server load balancer	ssh	22	Not possible	tcp
						telnet	23	Not possible	tcp
Network Device Operation	Admin server	-	Variable value	-	Server load balancer	ssh	22	Not possible	tcp
						telnet	23	Not possible	tcp
Open the web management window	Admin server	-	Variable value	-	L2 Switch	http	80	Possible	tcp
		-	Variable value	-		https	443	Possible	tcp
		-	Variable value	-	Firewall	http	80	Possible	tcp
		-	Variable value	-		https	443	Possible	tcp
		-	Variable value	-	Server load balancer	http	80	Possible	tcp
		-	Variable value	-		https	443	Possible	tcp
LAN switch control	Admin server	-	Variable value	-	LAN switch	-	22,23	Not possible	ssh, telnet

*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 via Interstage Java EE Admin Console's **Configurations** >> **server-config** >> **HTTP Service** >> **HTTP listeners** >> **admin-listener** >> **Listener Port**
*11: Can be changed via Interstage Java EE Admin Console's **Configurations** >> **server-config** >> **HTTP Service** >> **HTTP listeners** >> **default** >> **Listener Port.**
*12: Can be changed via Interstage Java EE Admin Console's **Configurations** >> **server-config** >> **ORB** >> **IIOP Listeners** >> **orb-listener-1** >> **Listener Port.**
*13: Can be changed via Interstage Java EE Admin Console's **Configurations** >> **server-config** >> **ORB** >> **IIOP Listeners** >> **SSL** >> **Listener Port**.
*14: Can be changed via Interstage Java EE Admin Console's **Configurations** >> **server-config** >> **ORB** >> **IIOP Listeners** >> **SSL_MUTUALAUTH** >> **Listener Port**.
*15: Can be changed via Interstage Java EE Admin Console's **Configurations** >> **server-config** >> **Admin Service** >> **system** >> **Port**.
*16: Can be changed using the procedure below.

1. Stop the manager.
   Refer to "2.1 Starting and Stopping the Manager" in the "Operation Guide CE" for information on how to stop the manager.

2. Change the port numbers in the services file.

   [Windows]
   Change the following port numbers listed in <Windows system installation directory>\SYSTEM32\DRIVERS\ETC\SERVICES:

   ```
   jobsch_win9      9690/tcp                        #SWRBA Jobsch subsystem
   mjsnet9          9691/tcp                        #SWRBA MpMjes subsystem
   ```

   [Linux]
   Change the following port numbers listed in /etc/services:

   ```
   jobsch_win9      9690/tcp                        #SWRBA Jobsch subsystem
   mjsnet9          9691/tcp                        #SWRBA MpMjes subsystem
   ```

3. Start the manager.
   Refer to ""2.1 Starting and Stopping the Manager" in the "Operation Guide CE" for information on how to start the manager.

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					

Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
		tftp	69	Not possible		-	Variable value	-	udp

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
						NETBIOS Session Service	139	Not possible	tcp
						SMB	445	Not possible	tcp udp
					L2 Switch	telnet	23	Not possible	tcp
						ping	-	-	ICMP
						snmp	161	Not possible	tcp,udp
					Firewall	telnet	23	Not possible	tcp
						ping	-	-	ICMP

Functional Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
						snmp	161	Not possible	tcp,udp
					Server load balancer	telnet	23	Not possible	tcp
						ping	-	-	ICMP
						snmp	161	Not possible	tcp,udp
	System Center Virtual Machine Manager	-	Variable value	-	Managed server (Hyper-V)	RPC	135 Unused port greater than 1024	Not possible	tcp
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
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	-	-	-	Admin server	-	2344	Not possible	tcp

Functional Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
	(Hyper-V/ Solaris container/ physical OS)								
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
Network Device Automatic Configuration	Admin server	-	Variable value	-	L2 Switch	ftp	21	Not possible	tcp
						ssh	22	Not possible	tcp
						telnet	23	Not possible	tcp
					Firewall	ssh	22	Not possible	tcp
						telnet	23	Not possible	tcp
					Server load balancer	ssh	22	Not possible	tcp
						telnet	23	Not possible	tcp
Network Device Operation	Admin server	-	Variable value	-	Server load balancer	ssh	22	Not possible	tcp
						telnet	23	Not possible	tcp
Open the web management window	Admin server	-	Variable value	-	L2 Switch	http	80	Possible	tcp
						https	443	Possible	tcp
					Firewall	http	80	Possible	tcp

Functional Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
						https	443	Possible	tcp
					Server load balancer	http	80	Possible	tcp
						https	443	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
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

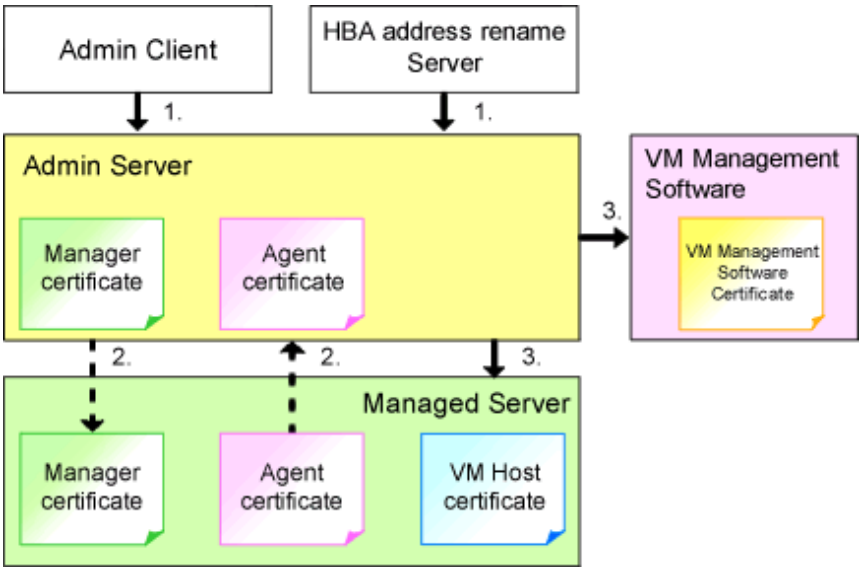
Function Overview	Source				Destination				Protocol
	Server	Service	Port	Modification	Server	Service	Port	Modification	
Hyper-V	Admin server	-	Variable value	-	Managed server	-	2179	Possible	tcp

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 re-installing the manager, back up the certificates referring to "20.1 Uninstall the Manager" in the "Setup Guide CE". When restoring the certificates, refer to "2.1 Installing the Manager" in the "Setup 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 Manager]

      ```
      >cd "Installation_folder\SVROR\Manager\sys\apache\conf" <RETURN>
      ```

      [Linux Manager]

      ```
      # 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 Manager]

```
>cd "C:\Fujitsu\ROR\SVROR\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 (*) <RETURN>
Email Address []: <RETURN>

>..\..\..\bin\rcxmgrctl start <RETURN>
```

   [Linux Manager]

```
# 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 (*) <RETURN>
Email Address []: <RETURN>

# /opt/FJSVrcvmr/bin/rcxmgrctl start <RETURN>
```

* Note: 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 "Chapter 4 Login to the ROR Console" in the "Setup Guide CE". 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 the [Advanced] menu is not displayed, push the [Alt] key.
5. From the list of [Connections] in the [Adapters and Bindings] tab, click the target network adapter, and the "Up" or "Down" buttons to change the order of priority of connections.
6. Click <OK>.

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 "3*N*-2"
Index 2	Onboard LAN2	NET2 port "3*N*-2"
Index 3	Onboard LAN3	NET1 port "3*N*-1"
Index 4	Onboard LAN4	NET2 port "3*N*-1"
Index 5	Onboard LAN5	NET1 port "3*N*"
Index 6	Onboard LAN6	NET2 port "3*N*"
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

Note

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

  ### Example

  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:

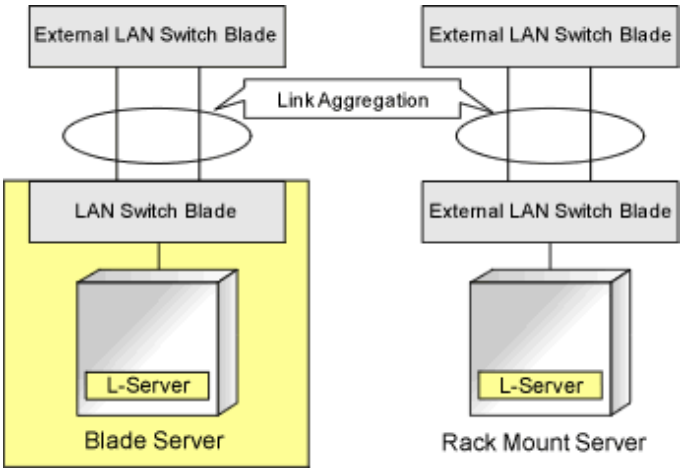
```
slot 2 (port 2) -> slot 2 (port 1)

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

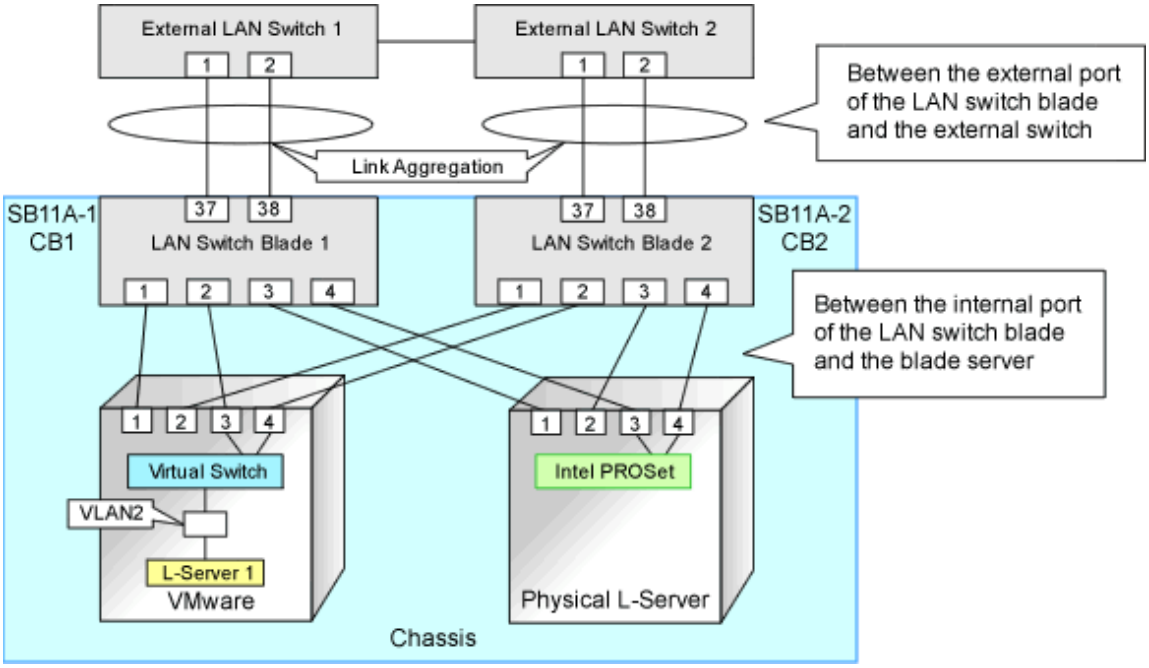
This section explains about link aggregation configuration.

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.
   Do not set VLAN if VLAN auto-configuration is to be used.
   Refer to the manual for the network device 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.

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 "14.3 Network Resources" in 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 Preparations for 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 on HBA address rename, refer to "5.5.3 HBA address rename Settings" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

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.

In other cases, link L-Servers with configured physical servers. For details, refer to "Chapter 18 Linking L-Servers with Configured Physical Servers or Virtual Machines" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

Note

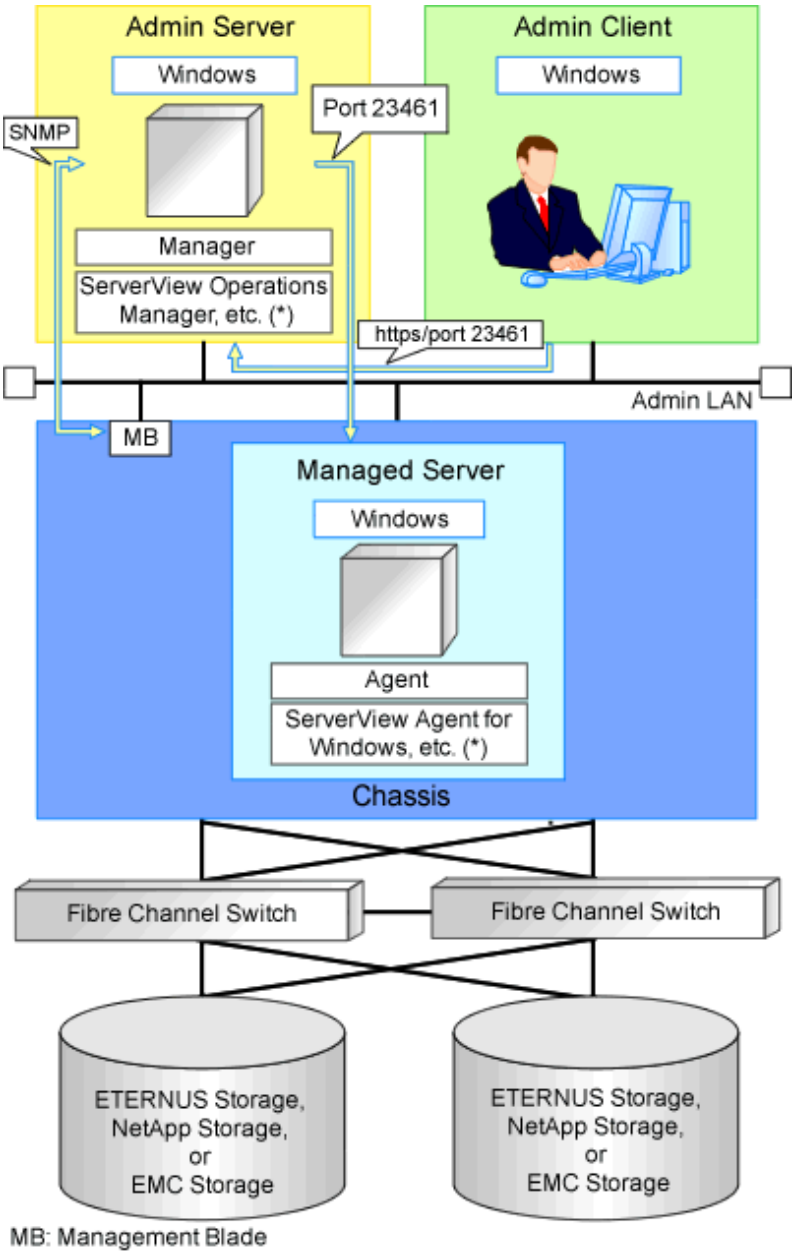
When using iSCSI boot, VIOM is required in the server environment.

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.

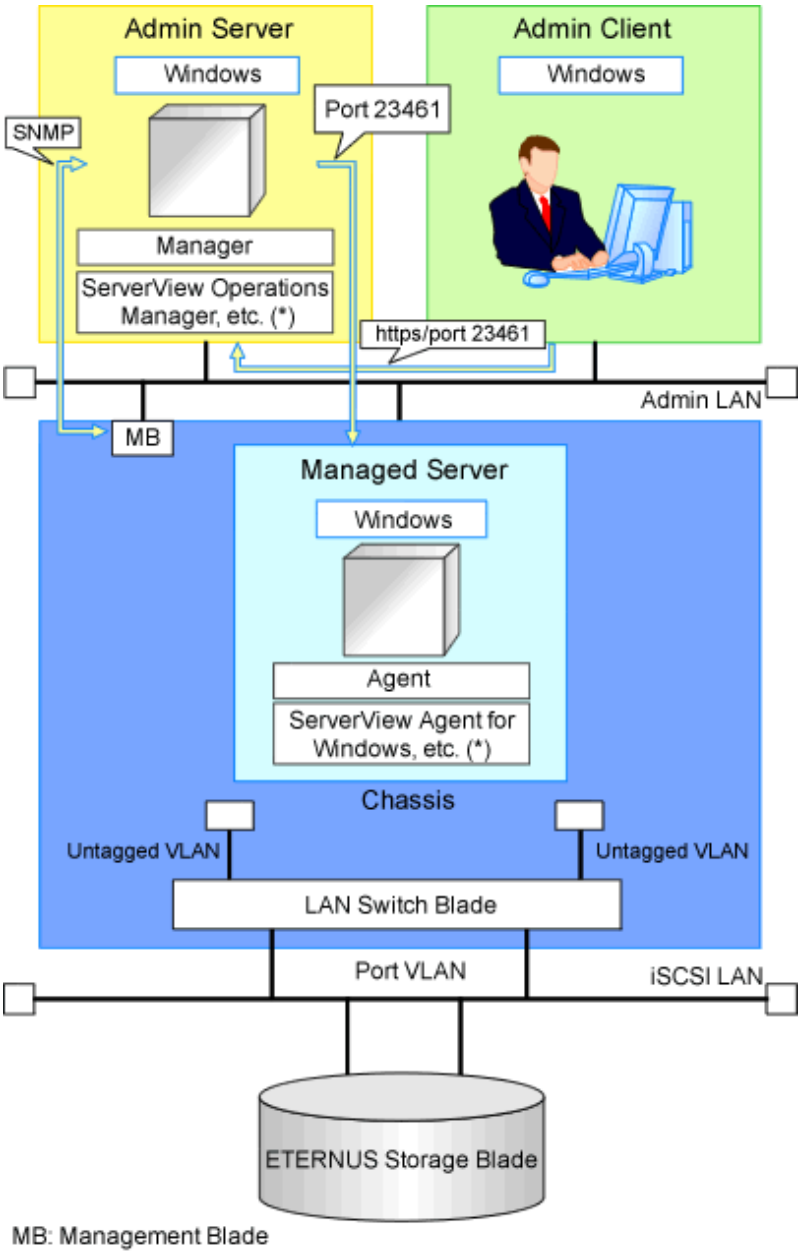
Install ServerView Virtual-IO Manager on the admin server.

Figure D.1 Example of System Configuration for L-Server Creation in a SAN Storage Environment using Virtual I/O by VIOM



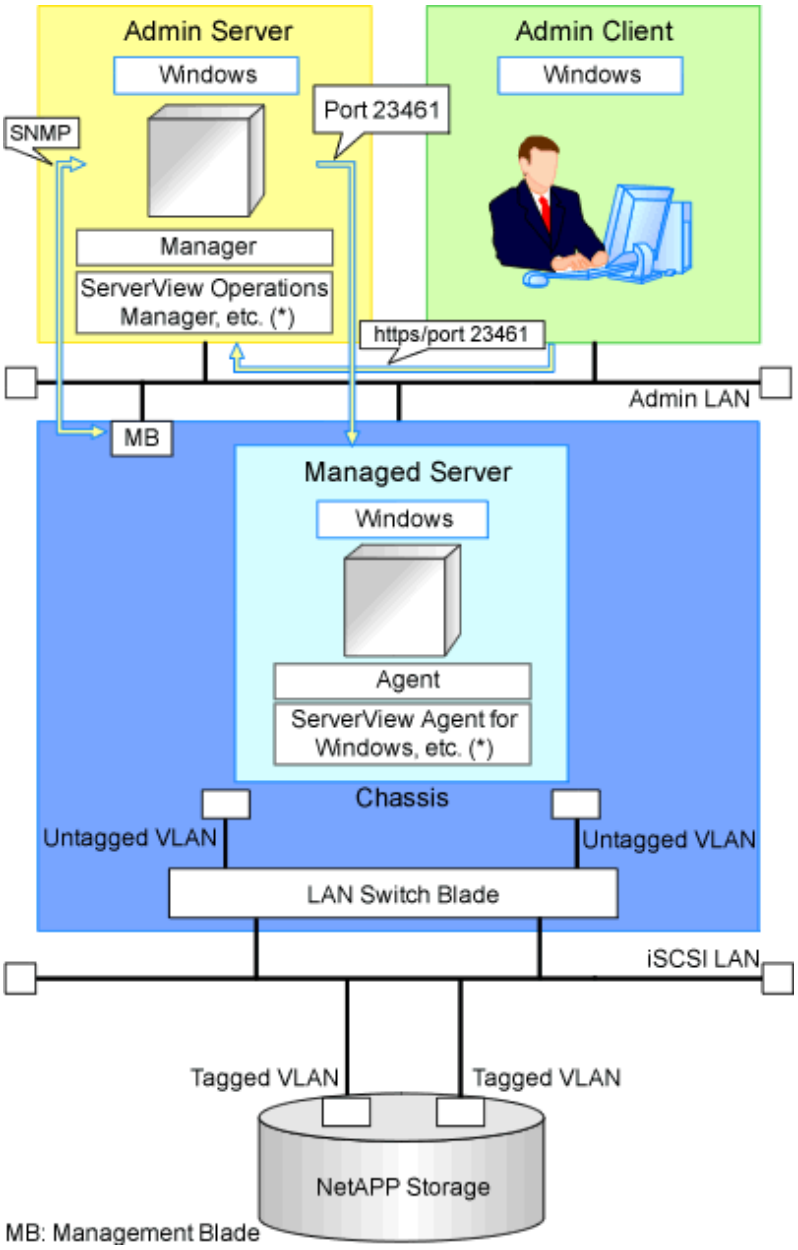
* Note: For details on required software, refer to "2.4.2.2 Required Software".

Figure D.2 Example of System Configuration for L-Server Creation in an ETERNUS-iSCSI Storage Environment using Virtual I/O by VIOM



* Note: For details on required software, refer to "2.4.2.2 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



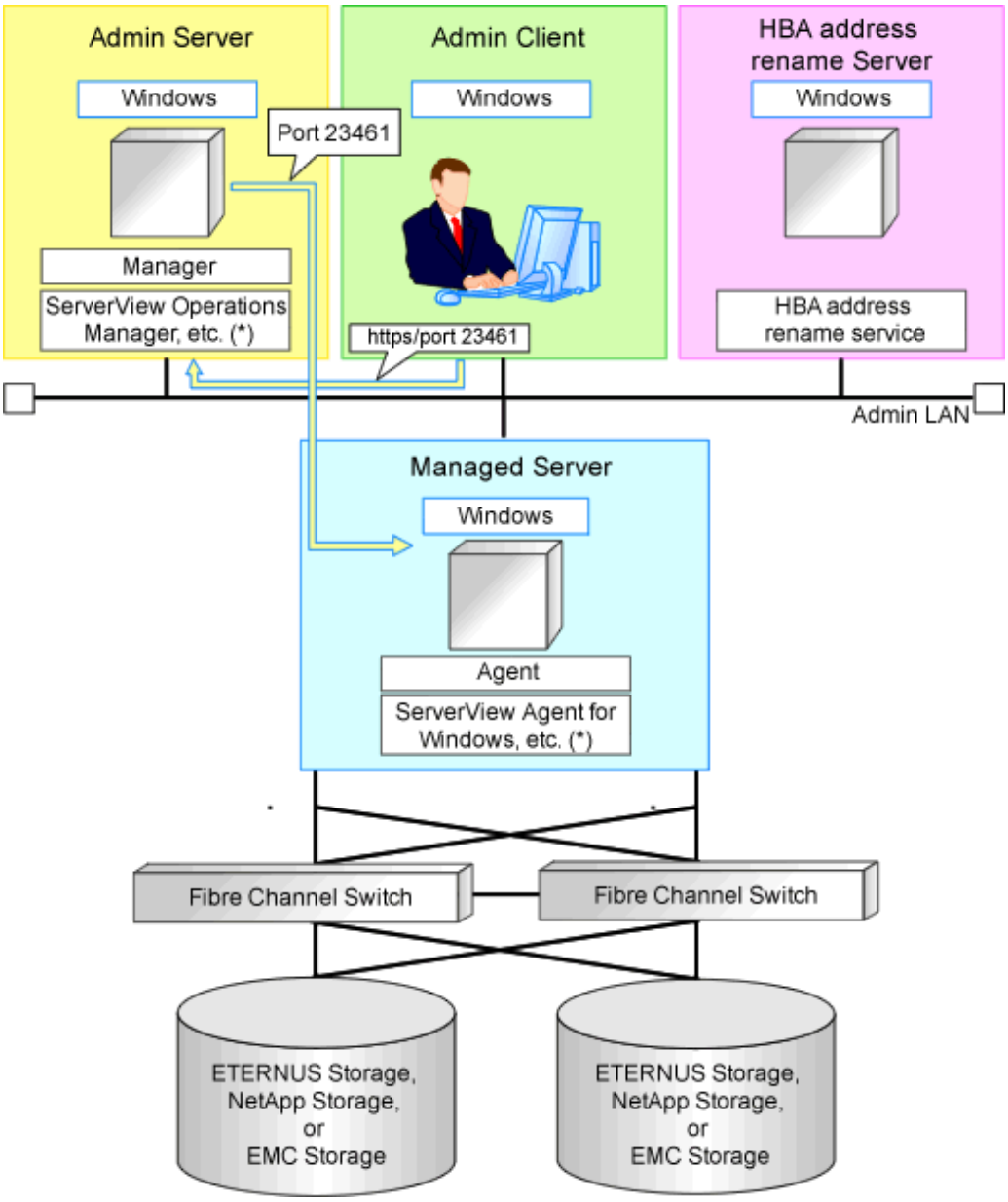
* Note: For details on required software, refer to "2.4.2.2 Required Software".

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

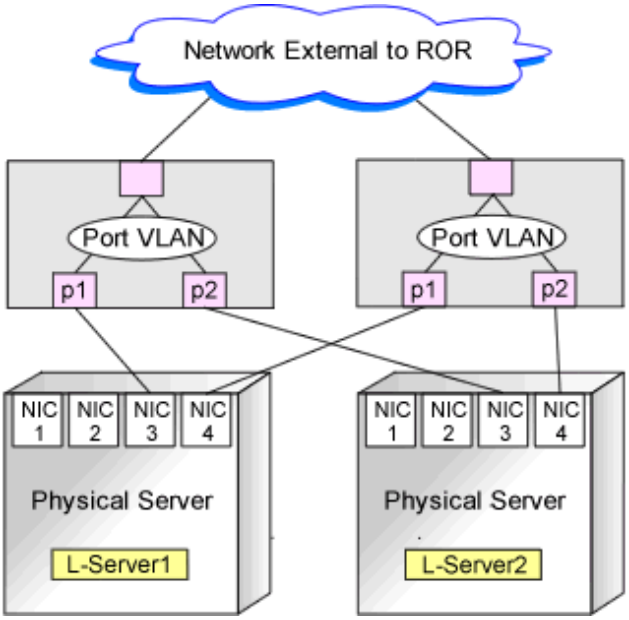


* Note: For details on required software, refer to "2.4.2.2 Required Software".

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 Preparations for 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 "Chapter 8 Defining and Configuring the Server Environment".

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 "8.2 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 "8.2 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 Storage Preparations

This section explains how to decide and configure a storage environment when using a physical L-Server.

D.3.1 Deciding the Storage Environment

Prerequisites for Storage 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 "10.1 Deciding the Storage Environment" and "10.2 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

Regarding Storage Configuration

Decide the storage configuration necessary for the system.

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.

Note

Local disks are not supported. Do not connect local disks.

For details on required VM management software and storage management software, refer to "2.4.2.2 Required Software".
For details on supported storage units and Fibre Channel switches, refer to "2.5 Hardware Environment".

The disk configurations supported by Resource Orchestrator are as follow:

Table D.1 Supported Disk Configurations

L-Server System Disk	L-Server Data Disk
SAN storage	SAN storage
iSCSI storage (*1, *2)	iSCSI storage (*1, *3)

*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 (Excluding ETERNUS VX700 series)

  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.

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.3.3 When Using ETERNUS Storage" and "D.3.4 When Using NetApp FAS Storage".

Dynamic LUN Mirroring Settings

For storage units that support dynamic LUN mirroring, refer to "Table 2.67 Storage Units that can be Connected with L-Servers on Physical Servers".

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".

D.3.2 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.3.3 When Using ETERNUS Storage".

   - When using NetApp FAS series/V series

     Refer to "NetApp FAS Storage Configuration" of "D.3.4 When Using NetApp FAS Storage".

   - When using EMC CLARiiON storage

     Refer to "EMC CLARiiON Storage Configuration" of "D.3.5 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.3.6 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.3.3 When Using ETERNUS Storage".

   - When connecting NetApp storage to fibre channel switches

     Refer to "When Connecting NetApp Storage to Fibre Channel Switches" of "D.3.4 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" in "EMC CLARiiON Storage Configuration".

   - 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.3.6 When Using EMC Symmetrix DMX Storage or EMC Symmetrix VMAX Storage".

D.3.3 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

Note

- 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 ETERNUS Storage for iSCSI Boot

Define the following using storage management software. Regarding the defined information, register a disk on a resource, using the operation command (rcxadm iscsictl) for iSCSI boot.

- Creation of the LUN used by iSCSI boot. Settings to permit access to the LUN from the server.

Note

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 "14.4.2 iSCSI Boot Information" in the "Reference Guide (Command/XML) 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 through coordination 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.3.4 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_(*)
     ```

     * Note: 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 iscsictl)

    The main definition information is as follows:

    For details, refer to "14.4.2 iSCSI Boot Information" in the "Reference Guide (Command/XML) 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.3.5 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 Manager]
Installation_folder\SVROR\Manager\etc\storage\emc\xxx.xxx.xxx.xxx (*)

[Linux Manager]
/etc/opt/FJSVrcvmr/storage/emc/xxx.xxx.xxx.xxx (*)

* Note: IP address of SP for EMC CLARiiON storage.
When there are multiple EMC CLARiiON units, 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 naviseccli 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 naviseccli -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 naviseccli command executed using the SCHTASKS command.
  2. Execute the task created in 1. using the SCHTASKS command.
  3. Delete the task created in 1. using the SCHTASKS command.

Example

```
C:\Program Files (x86)\EMC\Navisphere CLI>SCHTASKS /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>SCHTASKS /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>SCHTASKS /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 there are two or more SPs in EMC CLARiiON storage, access from the L-Server to LUN can be performed using multiple paths.

  Even when an SP fails, access from the L-Server to the LUN can be continued using the remaining SPs.
- To use resources of EMC CLARiiON storage, it is necessary to register the storage management product with this product using the "rcxadm storagemgr register" command. Even when there are multiple SPs in one EMC CLARiiON storage device, it is necessary to specify the IP address of one SP of the EMC CLARiiON storage device for the IP address used to control the storage management product.

  If the selected SP fails, it becomes impossible to create, delete, and attach or detach disks of the physical L-Server that uses the LUN of the EMC CLARiiON storage device. Please request restoration of the SP by the storage manager.

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:

In the following examples, 64 patterns of zoning are performed using combination of 16 WWN and 4 SP ports.

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"
- Content of the definition file "storage_portset.rcxprop"

  192.168.1.24,"SPAPort0:SPBPort0","SPAPort1:SPBPort1"
- WWPN value of SP port "SPAPort0"

  "50:0a:09:81:88:bc:43:dc"
- WWPN value of SP port "SPBPort0"

  "50:0a:09:82:88:bc:43:dc"

- WWPN value of SP port "SPAPort1"

  "50:0a:09:83:88:bc:43:dc"

- WWPN value of SP port "SPBPort1"

  "50:0a:09:84:88: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>
zoneCreate "emc_c_0","50:0a:09:83:88:bc:43:dc;21:00:00:17:42:51:00:00" <RETURN>
zoneCreate "emc_d_0","50:0a:09:84:88:bc:43:dc;22:00:00:17:42:51:00:00" <RETURN>
...
zoneCreate "emc_c_f","50:0a:09:83:88:bc:43:dc;21:01:00:17:42:50:00:0f" <RETURN>
zoneCreate "emc_d_f","50:0a:09:84:88: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;emc_c_0;emc_d_0; ... ;emc_c_f;emc_d_f" <RETURN>
cfgEnable "ror_cfg" <RETURN>
cfgSave <RETURN>
```

D.3.6 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.
- Thin devices are not recognized.

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:

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 Network Preparations

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 "9.1.1 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 "9.1.3 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.

On the physical L-Servers used by L-Platforms, only the default NIC can be used. The physical network adapter number for Network Interface Cards that can be used as an admin LAN on the L-Platform is as below:

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

Information

The first NIC that is available for the admin LAN can be changed.

For details, refer to "5.4.2 Registering Blade Servers" in 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 Manager]
  Installation_folder\SVROR\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:

  ```
  Key = Value
  ```

  Table D.2 List of Items Specified in the Definition File

Item	Key	Value	Remarks
Presence or absence of IBP environment	support_ibp_mode	- true - false	Specify one of the following:

Item	Key	Value	Remarks
			- If LAN switch blades are being operated using IBP firmware Specify "true". - If other than the above Specify "false". 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 "14.4.2 iSCSI Boot Information" in the "Reference Guide (Command/XML) CE" beforehand.

Storage Location of the Definition File

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

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

Definition File Name

- 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.

Variable = *Value*

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

Definition File Items

Table D.3 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	Specify the items in the following format. NIC[*index*] *index* is an integer starting from "1".

Variable	Meaning	Value
	- BX922 - BX924 - BX960 When setting the default, specify an asterisk ("*").	

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
```

Appendix E Preparations for Creating a Virtual L-Server

This section explains how to perform design and configuration when creating a virtual L-Server.

E.1 VMware

This section explains how to use VMware as server virtualization software.

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.

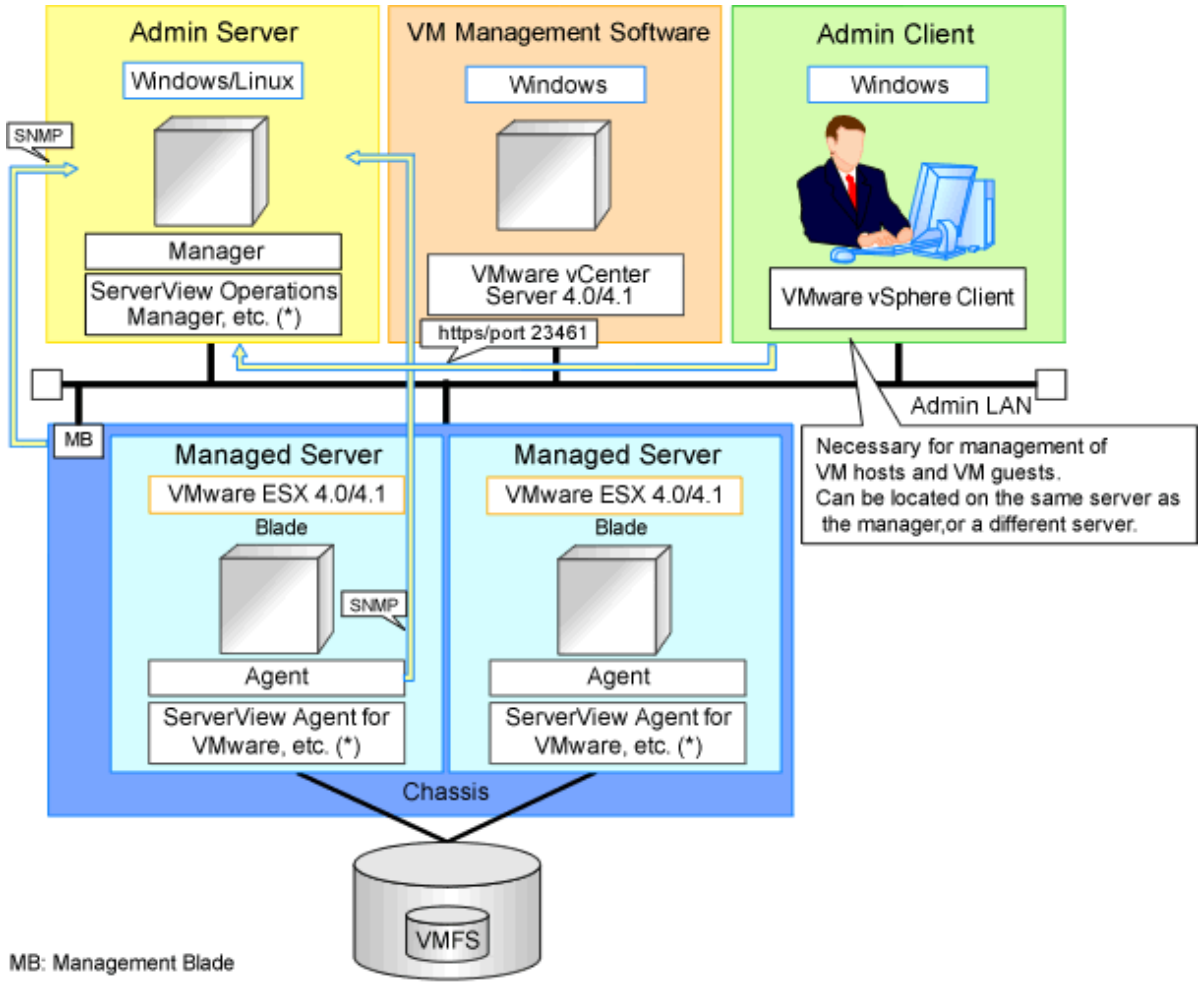
E.1.1 System Configuration

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.

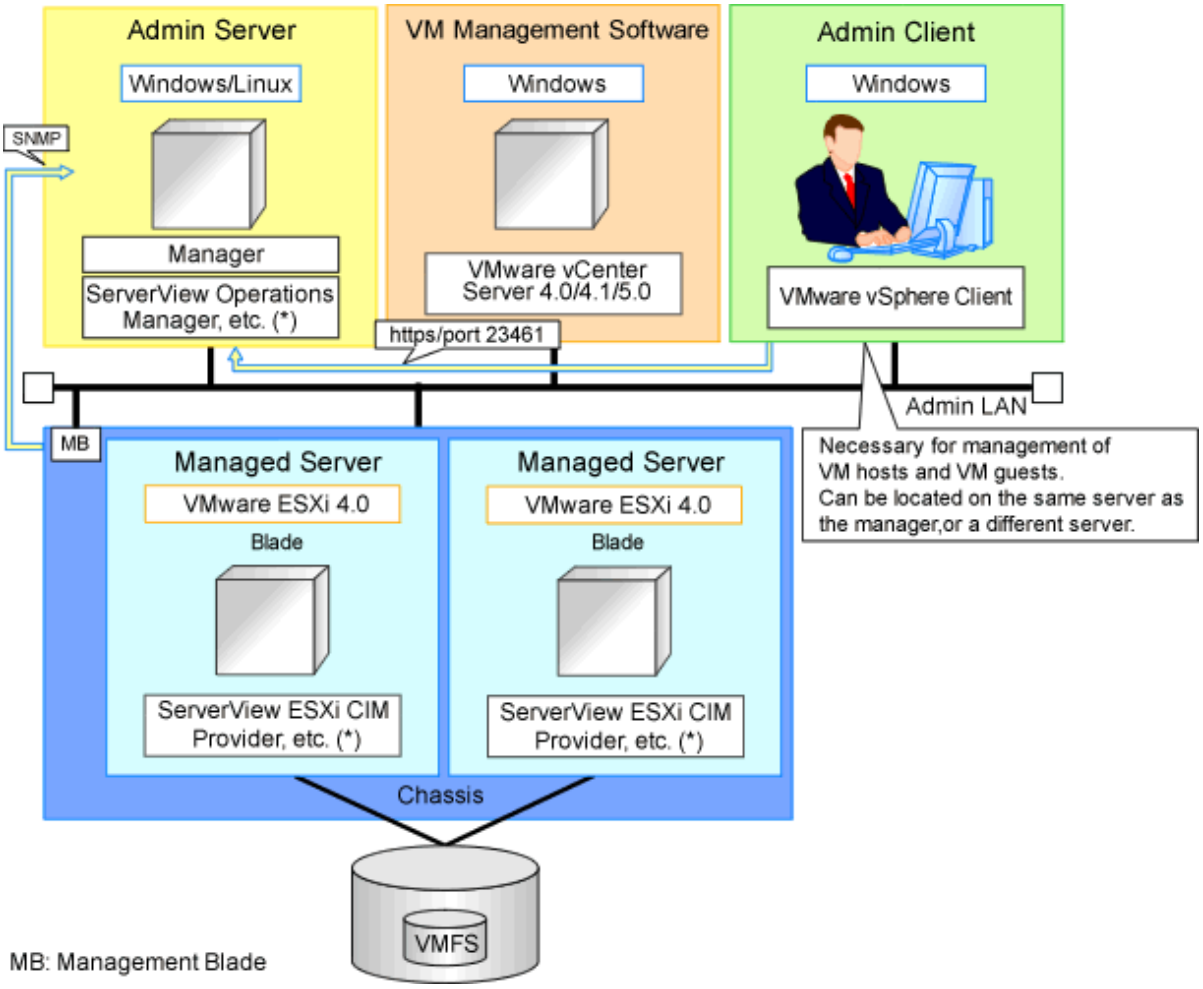
Figure E.1 System Configuration Example Using VMware ESX



* Note: For details on required software, refer to "2.4.2.2 Required Software".

An example system configuration using VMware ESXi is given below.

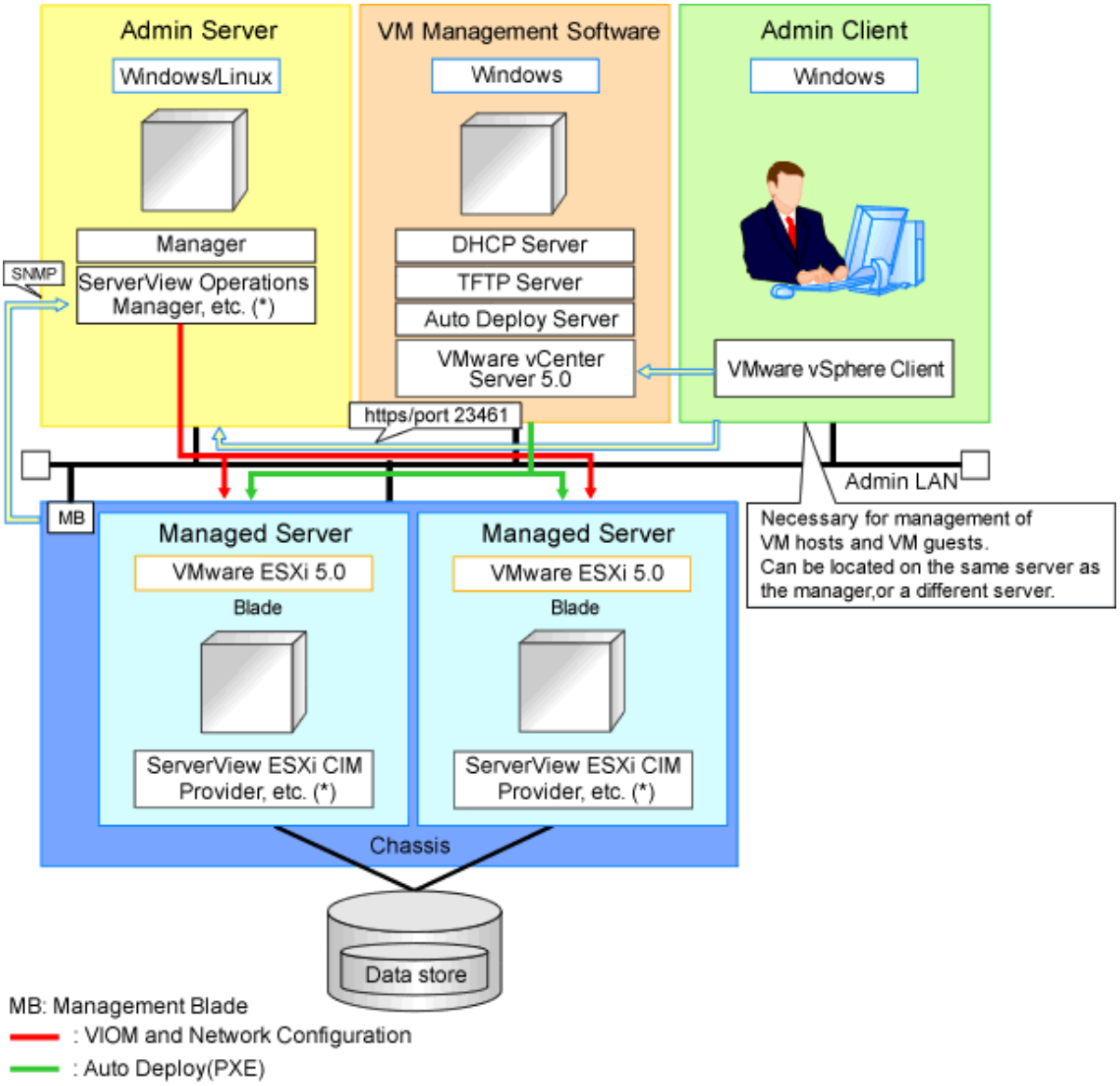
Figure E.2 System Configuration Example Using VMware ESXi



* Note: For details on required software, refer to "2.4.2.2 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



* Note: For details on required software, refer to "2.4.2.2 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.

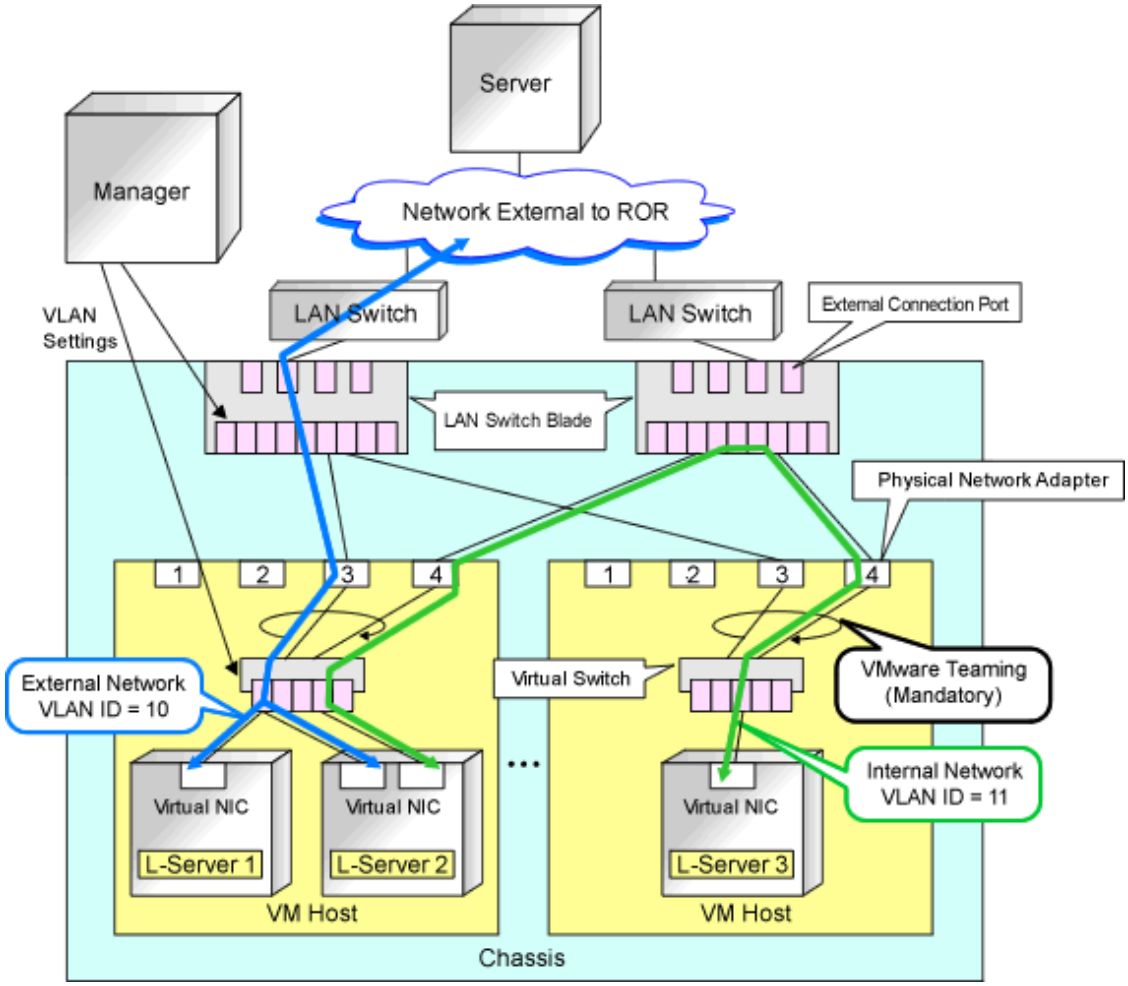
Depending on the conditions, such as hardware (blade servers or rack mount servers) and the presence or absence of network redundancy for L-Servers, the setting ranges of networks differ.

For details, refer to "2.2.7 Simplifying Networks" and "9.4 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]



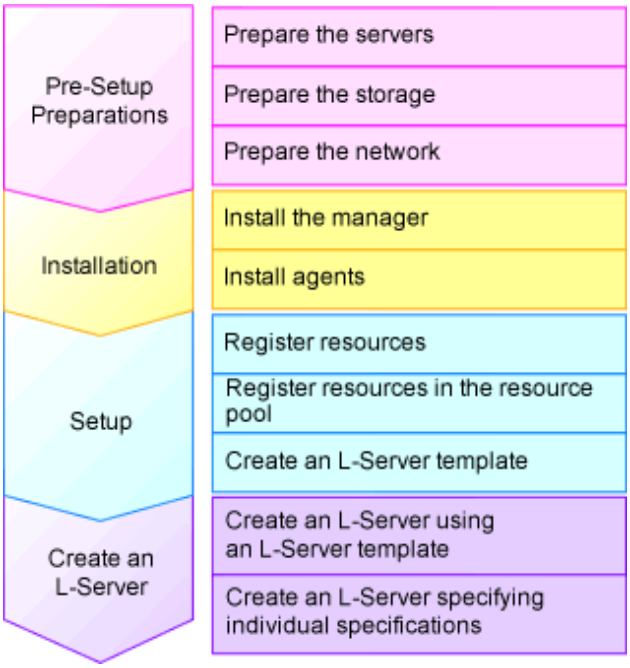
Note

- 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 "Chapter 9 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.1 VMware".
For details on how to install Resource Orchestrator, refer to "Chapter 2 Installation" in the "Setup Guide CE".
For details on how to set up Resource Orchestrator, refer to "C.2 VMware" in the "Setup Guide CE".
For details on how to create an L-Server, refer to "C.2.7 Creating an L-Server" in the "Setup 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.

E.1.2 Preparations for Servers

In addition to the operations in "Chapter 8 Defining and Configuring the Server Environment", 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 D Installing VM Hosts on Physical L-Servers" in the "Setup Guide CE".

- 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

- 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.

  When using VMware HA admission control, set "Role" or "Spare Server" for the admission control policy.

  When multiple VM hosts are set for a "Spare Server", or a policy other than the above is set, the L-Server may fail to start.

- 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" in "C.2.1 Creating Definition Files" in the "Setup Guide CE".

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

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 TFT 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 D Installing VM Hosts on Physical L-Servers" in the "Setup Guide CE", 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.

E.1.3 Storage Preparations

This section explains the preparations for setting up storage.

Supported Storage Configurations

The supported storage configurations are as follow:

- Storage supported by VMware

  For details on the storage supported by VMware, refer to the VMware manual.

- Storage configured for datastores of VMware ESX/ESXi (VMFS Version 3 or later, or NFS mount), including L-Server system disks and data disks

Preparations for Storage Environments

Check the following:

- Volumes to allocate to VMware ESX/VMware ESXi have been already created
- Zoning and affinity have been set
- VMware ESX/VMware ESXi has been configured to recognize a VMFS datastore

E.1.4 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

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 Manager]
   Installation_folder\SVROR\Manager\etc\customize_data

   [Linux Manager]
   /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 Manager]
   Installation_folder\SVROR\Manager\etc\vm

   [Linux Manager]
   /etc/opt/FJSVrcvmr/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 Manager]
   Installation_folder\SVROR\Manager\etc\customize_data

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

   ```
   Port_group_name_to_be_excluded
   ```

Example

```
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:

   - "7.5 Modifying Network Resource Specifications" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".
   - "14.3.1 Creating New Network Resources" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

E.2 Hyper-V

This section explains how to configure Hyper-V as server virtualization software.

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 environments, refer to the Hyper-V manual.

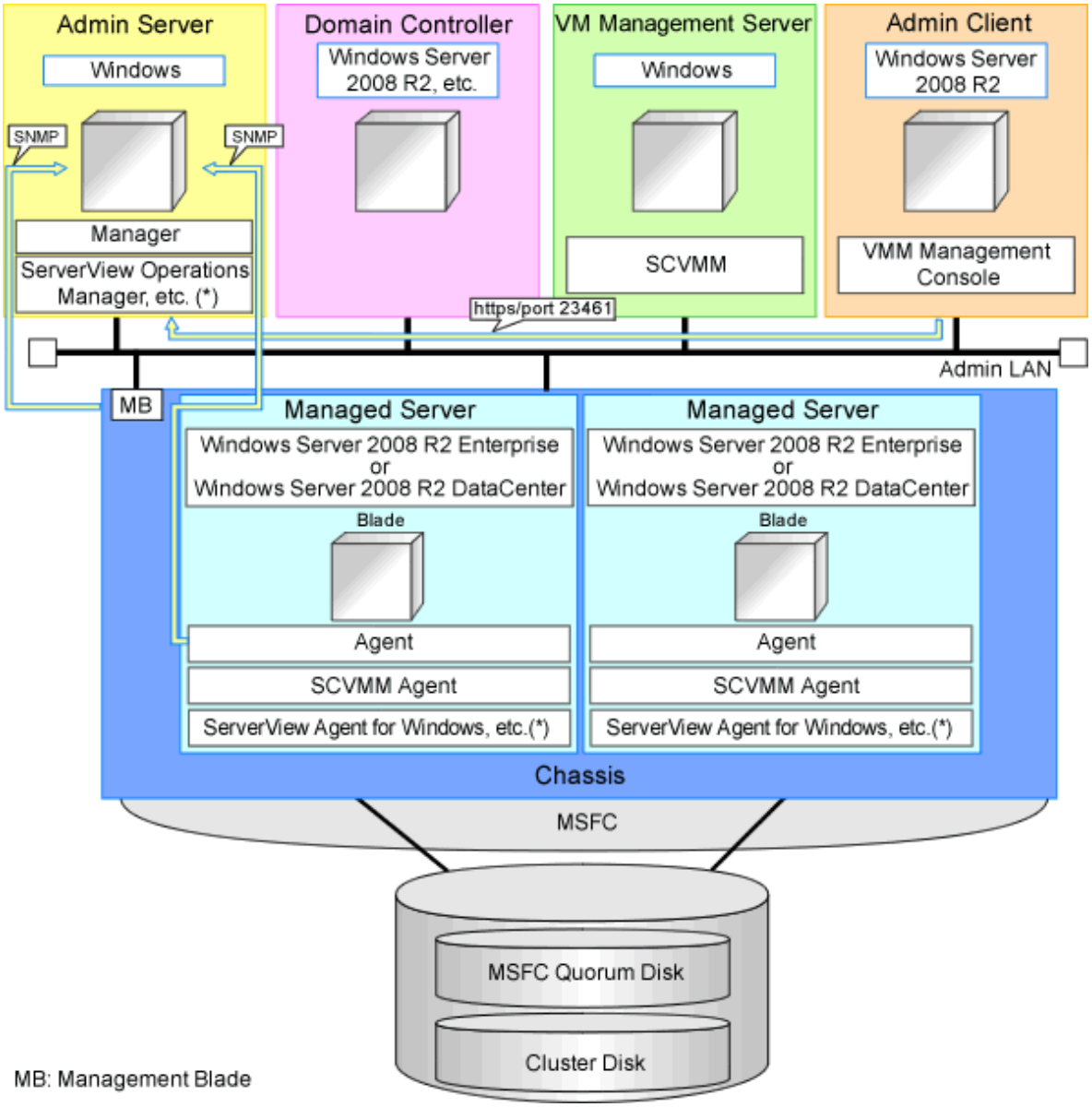
E.2.1 System Configuration

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.6 Example of System Configuration



* Note: For details on required software, refer to "2.4.2.2 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 OSs, 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 "2.2.7 Simplifying Networks" and "9.4 Preparations for Resource Orchestrator Network Environments".

Network Configuration Example

An example network configuration using Hyper-V is given below:

Figure E.7 Configuration when Performing Network Redundancy for L-Servers on Blade Servers (Using Intel PROSet or PRIMECLUSTER GLS)

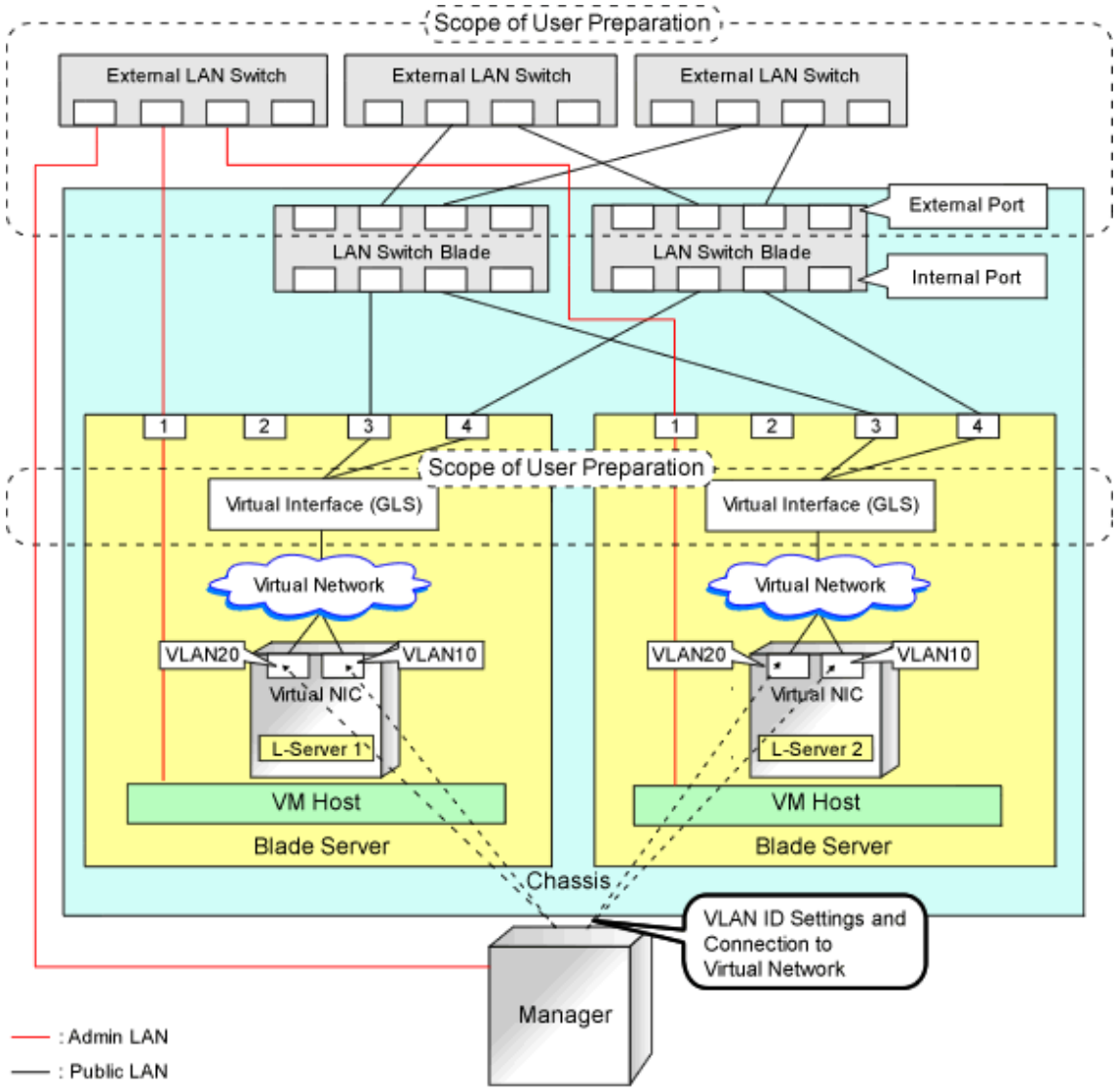
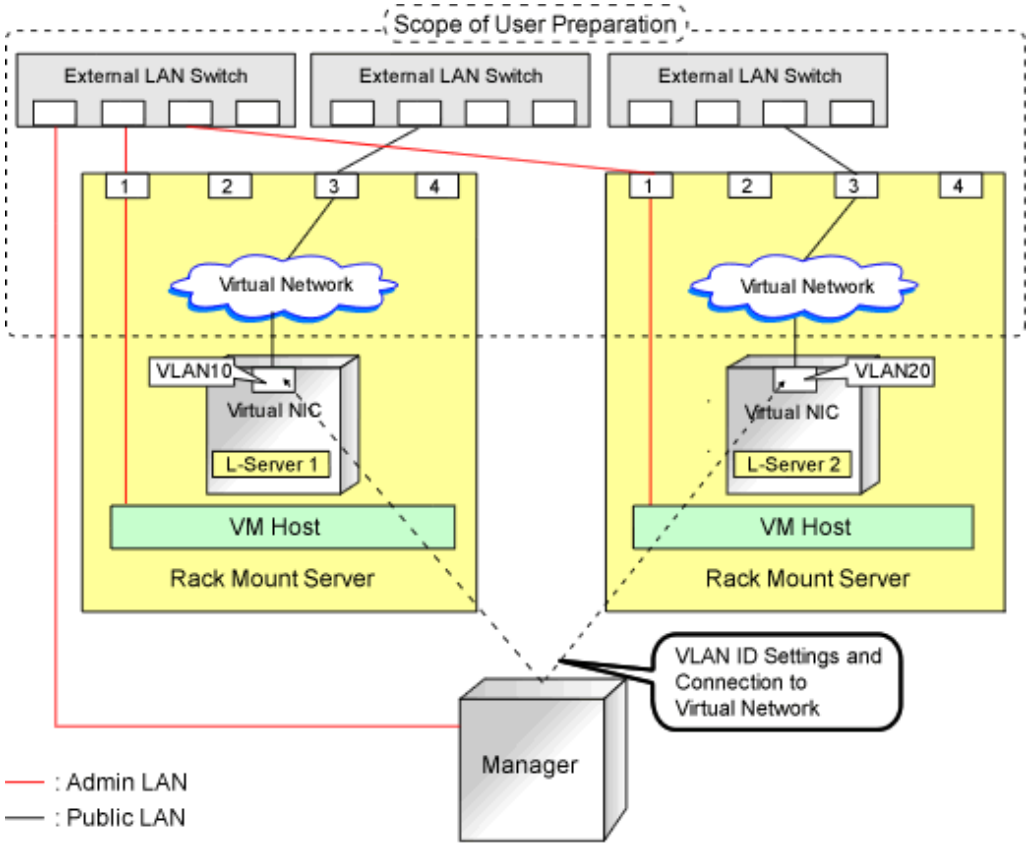


Figure E.8 Network Configurations of L-Servers for Rack Mount Servers



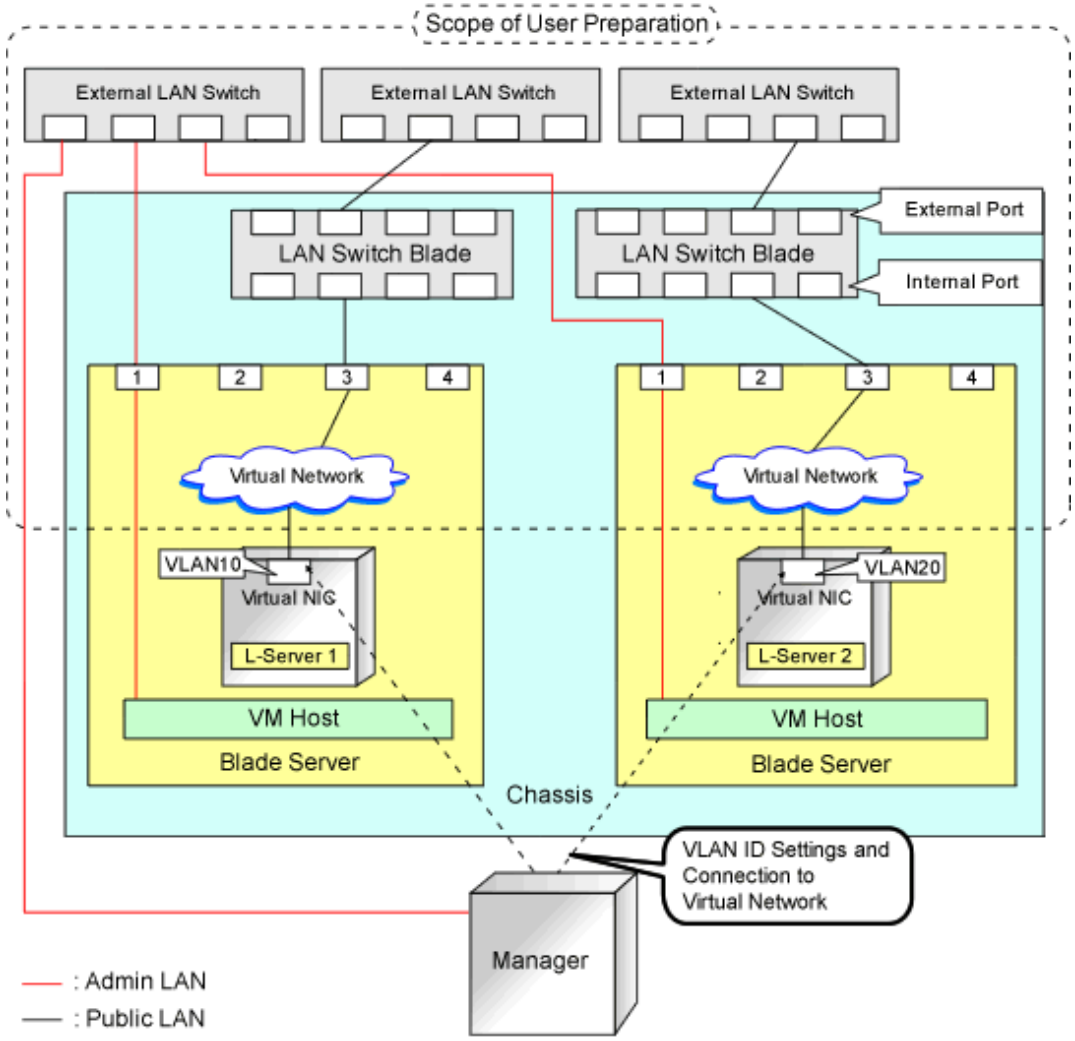
Note

- 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 "C.3.5 Manual Network Configuration" in the "Setup Guide CE".

- For Resource Orchestrator, configure the LAN switch blades when using switch mode or end-host mode.

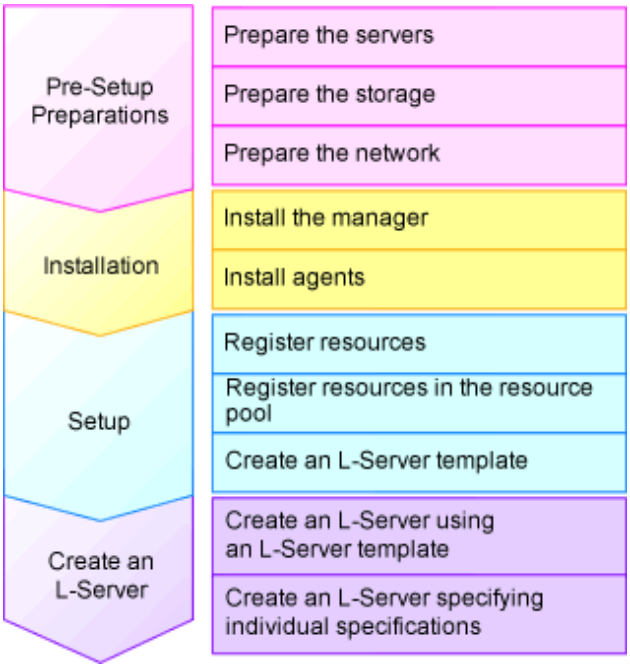
Figure E.9 Configuration When not Performing Network Redundancy for L-Servers with Blade Servers



L-Server Creation Procedure

The procedure for creating L-Servers is shown below.

Figure E.10 Resource Orchestrator Setup Procedure



For details on pre-setup preparations, refer to "E.2 Hyper-V".
For details on how to install Resource Orchestrator, refer to "Chapter 2 Installation" in the "Setup Guide CE".
For details on setup, refer to "C.3 Hyper-V" in the "Setup Guide CE".
For details on how to create an L-Server, refer to "C.3.7 Creating an L-Server" in the "Setup Guide CE".

E.2.2 Preparations for Servers

In addition to the operations in "Chapter 8 Defining and Configuring the Server Environment", 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.

E.2.3 Storage Preparations

This section explains the preparations for setting up storage.

Supported Storage Configurations

The supported storage configurations are as follow:

- Storage supported by Hyper-V
- Storage configured for Cluster Shared Volumes (CSV) of MSFC, including L-Server system disks and data disks

Preparations for Storage Environments

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

E.2.4 Network Preparations

In addition to the operations in "Chapter 9 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 "14.11 Server NIC Definitions" in the "Reference Guide (Command/XML) CE".
- For details on the rcxadm nicdefctl command, refer to "5.15 rcxadm nicdefctl" in the "Reference Guide (Command/XML) 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.

E.2.5 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 D Installing VM Hosts on Physical L-Servers" in the "Setup Guide CE".
   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 software 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 RHEL5-Xen

This section explains how to configure RHEL5-Xen as server virtualization software.

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

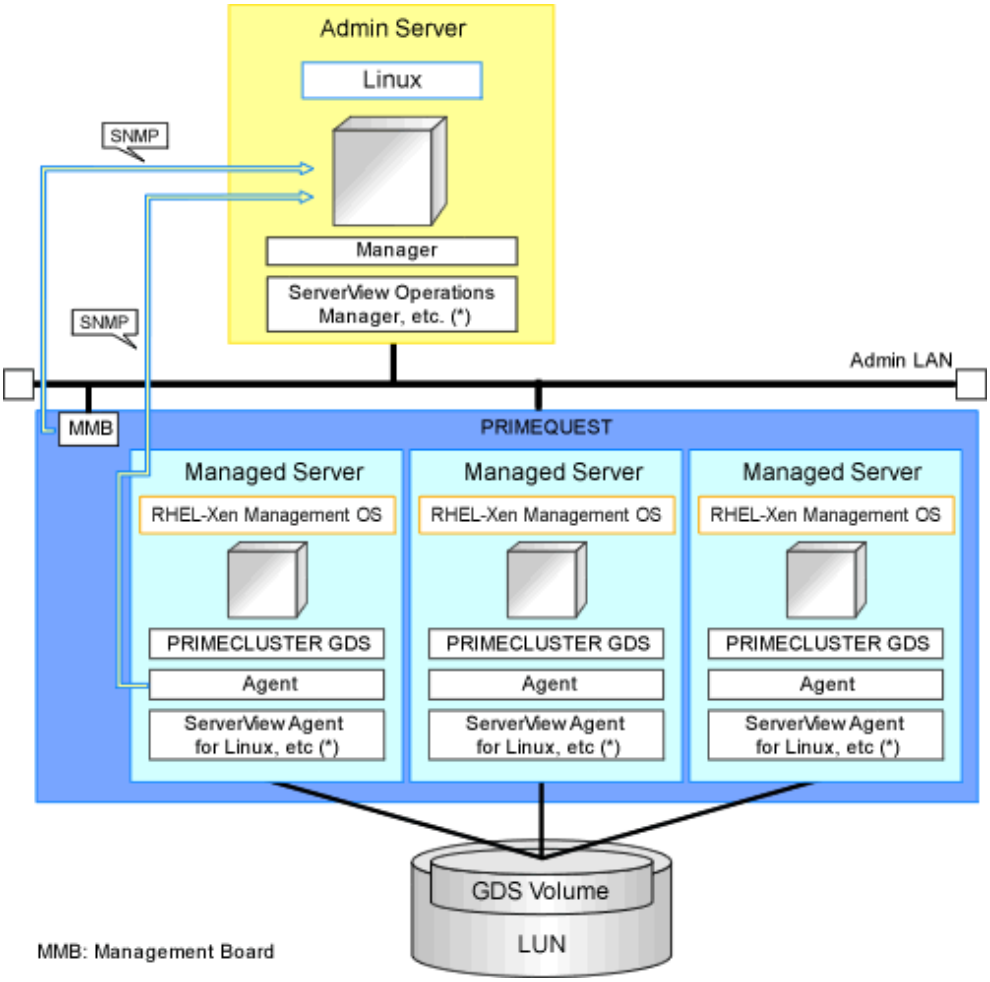
E.3.1 System Configuration

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.11 System Configuration Example Using RHEL5-Xen

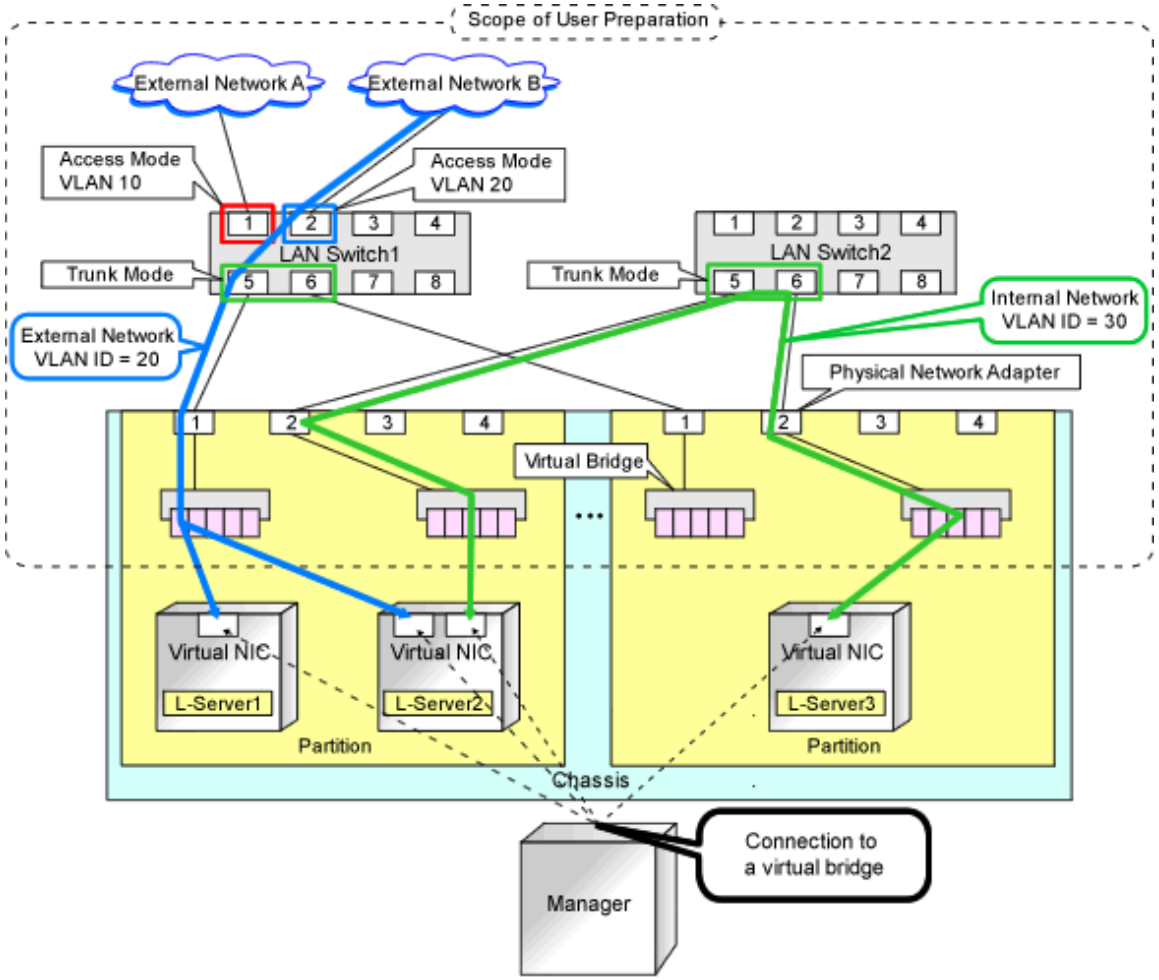


* Note: For details on required software, refer to "2.4.2.2 Required Software".

Network Configuration Example

An example network configuration using RHEL5-Xen is given below:

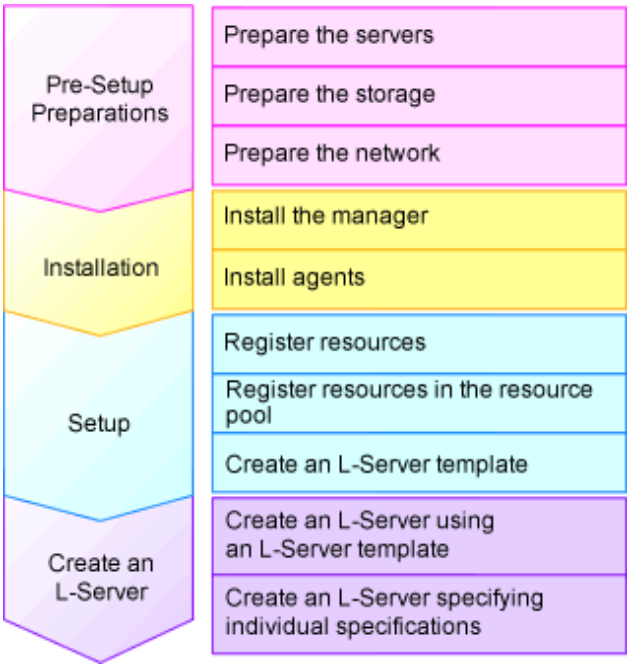
Figure E.12 Virtual Bridge Settings Using Network Resources



L-Server Creation Procedure

Use the following procedure to create L-Servers:

Figure E.13 Resource Orchestrator Setup Procedure



For details on pre-setup preparations, refer to "E.3 RHEL5-Xen".
For details on how to install Resource Orchestrator, refer to "Chapter 2 Installation" in the "Setup Guide CE".
For details on setup, refer to "C.4 RHEL5-Xen" in the "Setup Guide CE".
For details on how to create an L-Server, refer to "C.4.6 Creating an L-Server" in the "Setup Guide CE".

E.3.2 Preparations for Servers

In addition to the operations in "Chapter 8 Defining and Configuring the Server Environment", 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.

E.3.3 Storage Preparations

This section explains the preparations for setting up storage.

Supported Storage Configurations

The supported storage configurations are as follow:

- Storage supported by RHEL5-Xen

  For details on the storage supported by RHEL5-Xen, refer to the RHEL5-Xen manual.

Preparations for Storage Environments

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.

E.3.4 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 "C.4.4 Manual Network Configuration" in the "Setup Guide CE".

E.4 Oracle VM

This section explains how to configure Oracle VM as server virtualization software.

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

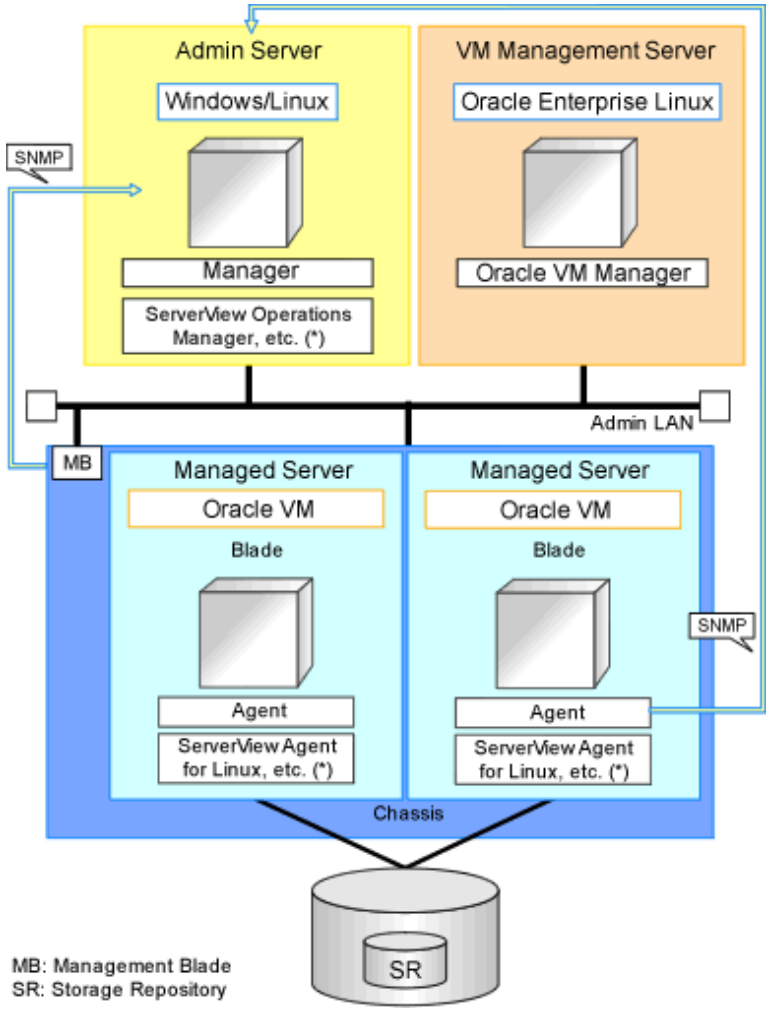
E.4.1 System Configuration

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.14 System Configuration Example Using Oracle VM



* Note: For details on required software, refer to "2.4.2.2 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 "2.2.7 Simplifying Networks".

E.4.2 Preparations for Servers

In addition to the operations in "Chapter 8 Defining and Configuring the Server Environment", 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 D Installing VM Hosts on Physical L-Servers" in the "Setup Guide CE".

- 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.

E.4.3 Storage Preparations

Supported Storage Configurations

The supported storage configurations are as follow:

- Storage supported by Oracle VM

  For details on the storage supported by Oracle VM, refer to the Oracle VM manual.

Preparations for Storage Environments

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

E.4.4 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 "C.5.4 Manual Network Configuration" in the "Setup Guide CE".

E.5 KVM

This section explains how to configure RHEL-KVM as server virtualization software.

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

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

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

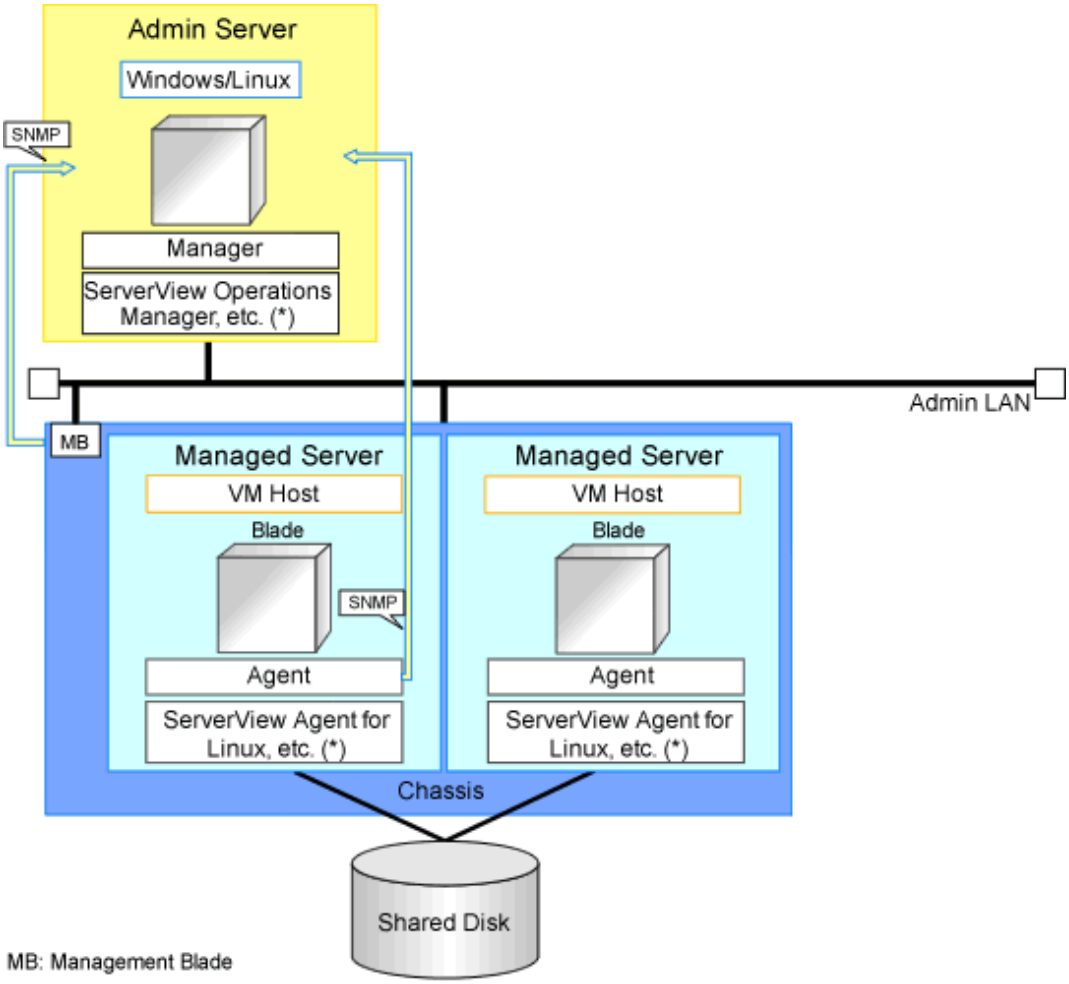
E.5.1 System Configuration

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.15 System Configuration Example Using RHEL-KVM

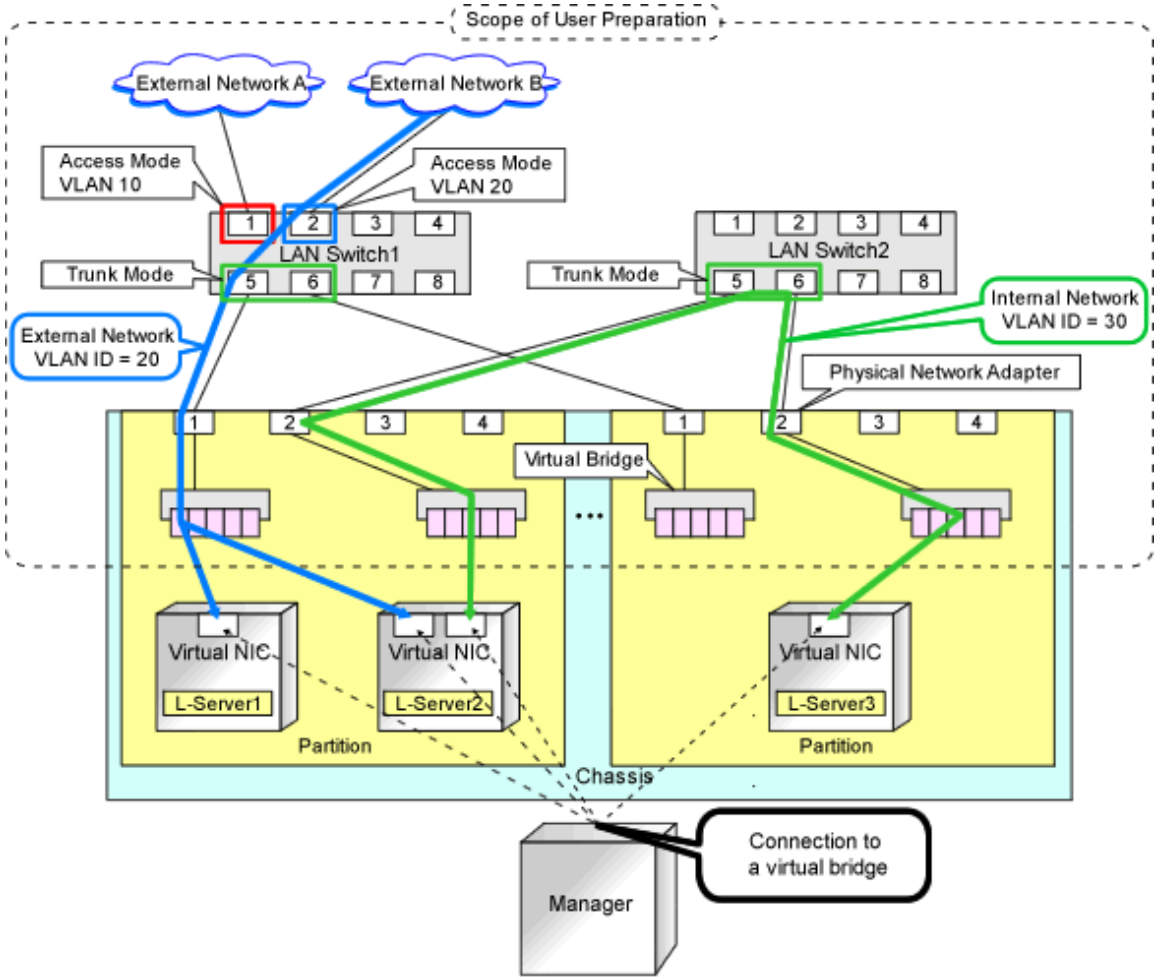


* Note: For details on required software, refer to "2.4.2.2 Required Software".

Network Configuration Example

An example network configuration using RHEL-KVM is given below:

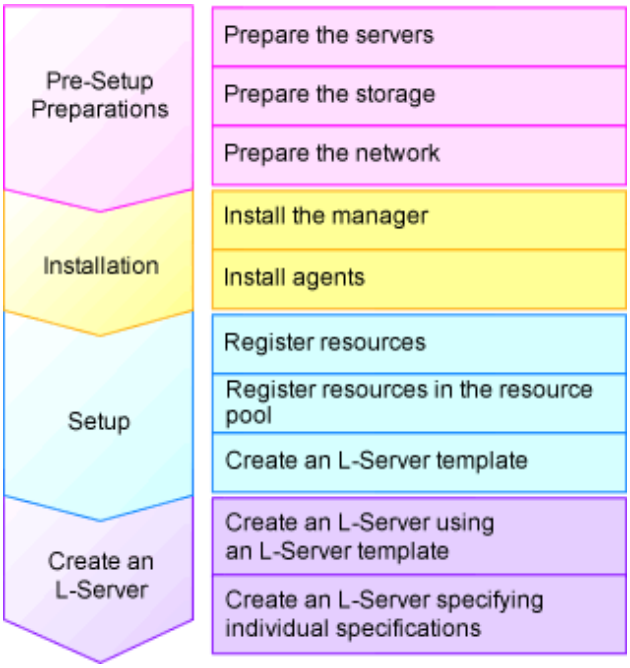
Figure E.16 Virtual Bridge Settings Using Network Resources



L-Server Creation Procedure

The procedure for creating L-Servers is shown below.

Figure E.17 Resource Orchestrator Setup Procedure



For details on pre-setup preparations, refer to "E.5 KVM".
For details on how to install Resource Orchestrator, refer to "Chapter 2 Installation" in the "Setup Guide CE".
For details on setup, refer to "C.6 KVM" in the "Setup Guide CE".
For details on how to create an L-Server, refer to "C.6.6 Creating an L-Server" in the "Setup Guide CE".

E.5.2 Preparations for Servers

In addition to the operations in "Chapter 8 Defining and Configuring the Server Environment", the following operations are necessary.

- Installation and configuration of the host OS
- Settings for /etc/sysconfig/libvirt-guests of the host OS

  /etc/sysconfig/libvirt-guests is a definition file, which is used to automatically stop guest OSs when their hypervisor is stopped.

  If a hypervisor is stopped or restarted while its guest OSs are being operated, all virtual machines on the hypervisor will be suspended. The suspension of the virtual machines is canceled when the hypervisor is started or restarted, and then suspended tasks are resumed.

  Resuming tasks from the point of suspension may cause problems such a contradictions in database transactions. In order to avoid this type of problem, the settings explained in this section are required.

  Edit the /etc/sysconfig/libvirt-guests of the VM host as follows:

  1. Cancel the commenting out of the #ON_BOOT=start line, and then change it to ON_BOOT=ignore.
  2. Cancel the commenting out of the #ON_SHUTDOWN=suspend line, and then change it to ON_SHUTDOWN=shutdown.
  3. Cancel the commenting out of the #SHUTDOWN_TIMEOUT=0 line, and then change it to SHUTDOWN_TIMEOUT=300.

     For the VM guest, set the time between when the shutdown command is sent from the VM host and the when the VM guest is actually powered off. The unit is seconds.

Note

Check if the version of the libvirt package of the Host OS is 0.9.4-23.el6_2.4 or later.
The libvirt package contains some security incompatibilities. If the version is earlier than 0.9.4-23.el6_2.4, please upgrade it.
For details, refer to the following web site.

URL: https://access.redhat.com/knowledge/solutions/71283

E.5.3 Storage Preparations

Supported Storage Configurations

- Storage supported by KVM

  For details on the storage supported by KVM, refer to the KVM manual

Preparations for Storage Environments

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.

E.5.4 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, disable 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 Resource Orchestrator 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 Resource Orchestrator 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 "C.6.4 Manual Network Configuration" in the "Setup Guide CE".

E.6 Solaris Containers

How to virtualize a server using Solaris containers will be explained here.

However, some preliminary preparations are required in order to manage a virtual machine as an L-Server of this product.

Refer to the Solaris Containers manual for the Solaris Containers preliminary preparations.

URL: http://docs.oracle.com/cd/E23823_01/index.html

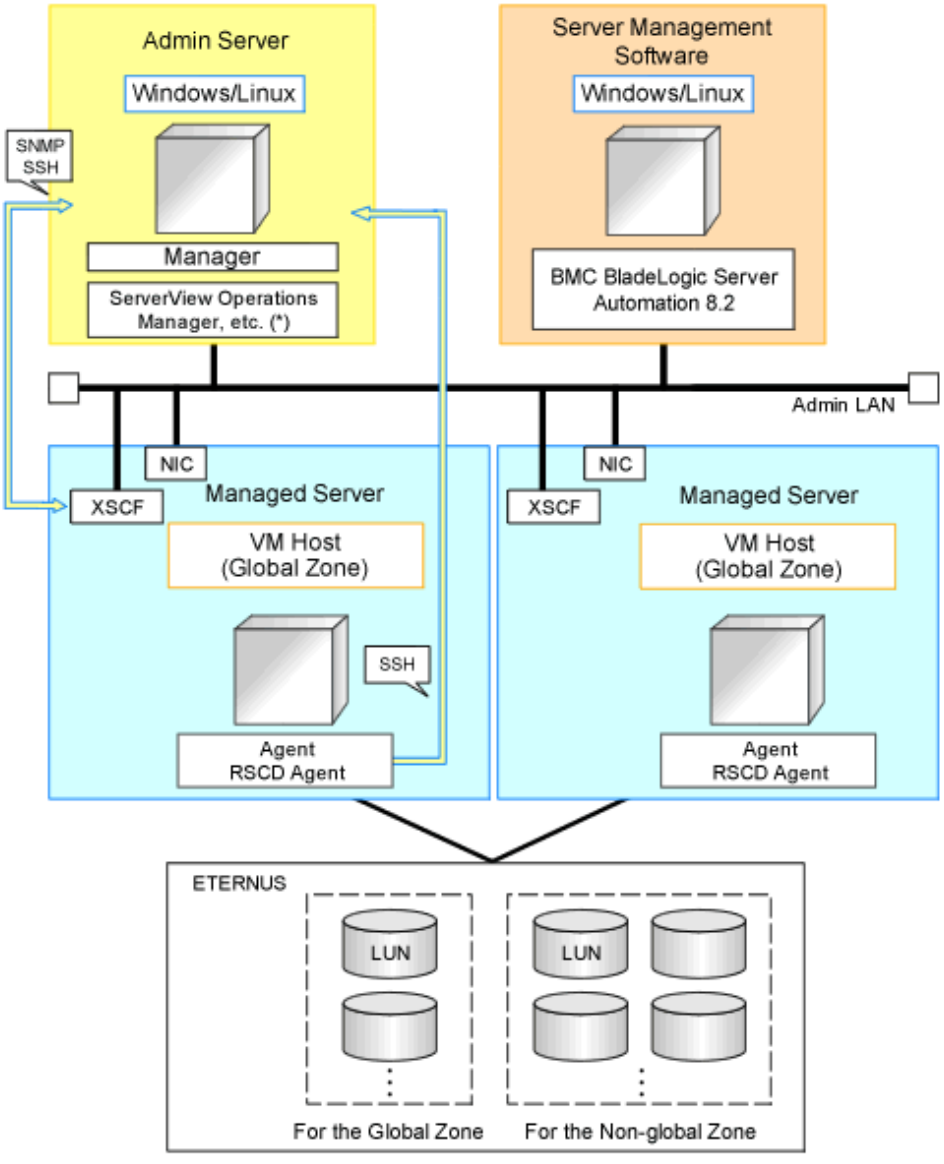
E.6.1 System Configuration

System configuration of the virtualized server using Solaris containers is explained here.

Example of System Configuration

Below is a sample of system configuration when using Solaris containers.

Figure E.18 System Configuration Example Using Solaris Containers



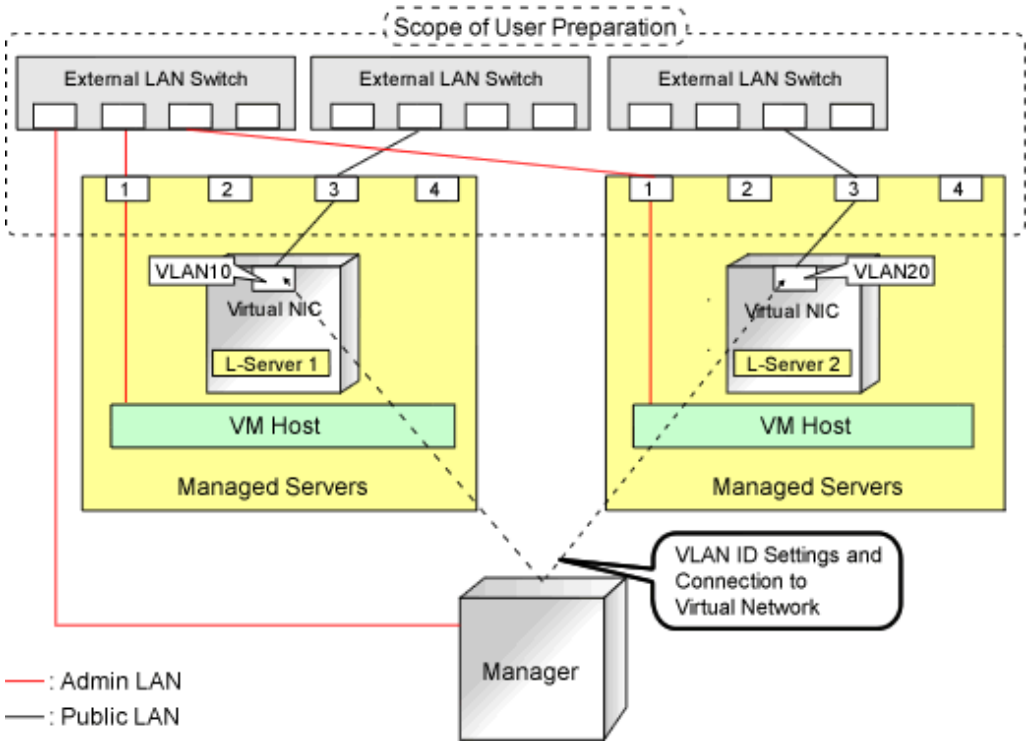
XSCF: eXtended System Control Facility

* Note: For details on required software, refer to "2.4.2.2 Required Software".

Network Configuration Example

An example network configuration using Solaris containers is given below:

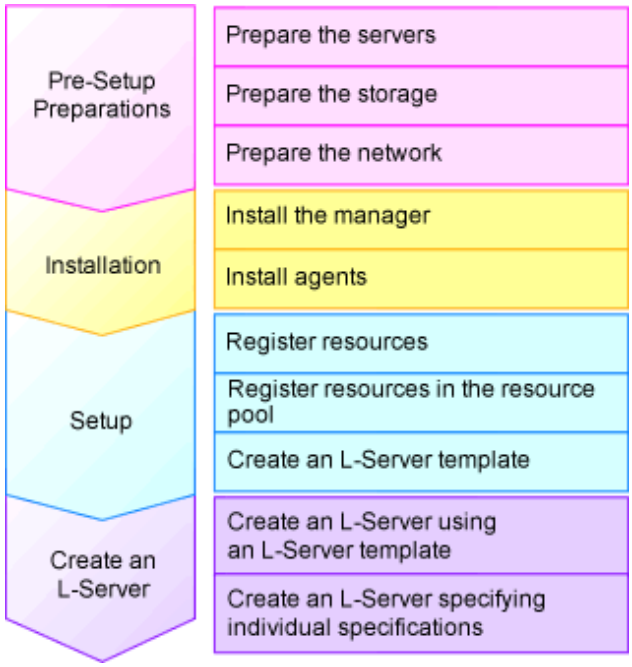
Figure E.19 Network Configuration of L-Servers for Solaris Containers



L-Server Creation Procedure

The procedure for creating L-Servers is shown below.

Figure E.20 Resource Orchestrator Setup Procedure



For details on pre-setup preparations, refer to "E.6 Solaris Containers".
For details on how to install Resource Orchestrator, refer to "Chapter 2 Installation" in the "Setup Guide CE".

For details on setup, refer to "C.7 Solaris Containers" in the "Setup Guide CE".
For details on how to create an L-Server, refer to "C.7.6 Creating an L-Server" in the "Setup Guide CE".

E.6.2 Preparations for Servers

The following procedures are required.

- Installation and configuration of the admin OS

  Installation and configuration the global zone.

  Use UFS as the file system.

  Set SSH access permission, and enable password authentication for accounts with administrator privileges.

  When mounting a pool on a system, resources are classified using their settings.

  Create pools with configurations that give consideration to operation with reduced hardware.

  This configuration is necessary to obtain information of Virtual L-Servers and VM guests and perform power operation of them.

- Create the Solaris Container resource pool

  Create the Solaris Containers resource pool for global and non-global zone.

  The resource pools of Solaris Containers are referred to as Solaris Container resource pools.

  If this product is used for managing resources, create a resource pool for non-global only, and name the resource pool "pool_resource".

  The resource pool name can be changed.

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

- Set the capping of CPU and capping of the memory for the non-global zone

  Already created non-global zones will be the target of resource management when the capping value is set.

  The capping supported with this product is as follows.

  - CPU capping

    zone.cpu-cap

  - Memory capping

    rcapd

  This product does not show the capping value applied to the running non-global zone (using the prctl command) but configuration information of the non-global zone.

  Therefore set the zone.cpu-cap using the zonecfg command.

  Design capping values based on the estimated resource usage of a non-global zone.

  When the non-global zone uses resources beyond capping, it will have impact on system performance.

  Please refer to the relevant version of the document, referring to the following URL:

  Oracle corporation

URL: http://www.oracle.com/index.html

- When the non-global zone is the target of resource management, the amount of resources of this product is calculated as follows:

  - CPU capping

    Number of CPUs = capping of CPUs / 100 (if there is a decimal value, round it up)

    CPU performance = (capping of CPUs / (number of CPUs * 100)) * performance of physical CPUs(GHz)

Example

- When capping of CPUs is 720 and performance of physical CPUs is 3.0GHz

  Number of CPUs = 720 / 100 (rounded up) = 8

  CPU performance = (720 / (8 * 100)) * 3.0 = 2.7(GHz)

- Memory capping

  Capping of memory resources

- Install the RSCD agent

  When creating an L-Server, do so using the following procedure.

  1. Install the RSCD agent.
  2. Enable control of the global zone of the RSCD agent.
  3. Add the managed server to BladeLogic.

     At this time, specify the IP address of the managed server when adding it.

  For details, contact Fujitsu technical staff.

E.6.3 Storage Preparations

This section explains the preparations for setting up storage.

Supported Storage Configurations

The supported storage configurations are as follow:

- LUNs managed by ETERNUS

Preparations for Storage Environments

- When use disks in non-global zones, prepare a LUN for each non-global zone.
- Mount a LUN for each zone path of a non-global zone.

  Configure a non-global zone in the mounted LUN.
- Configure /etc/vfstab so that LUNs corresponding to the zone paths used by virtual L-Servers will be mounted.
- For the zone path used by the virtual L-Server, provide only the owner of the directory with read, write, and execution permissions (700).
- The storage affinity switchover method can be used as a server switchover function.

  For details on how to configure the server switchover, refer to "8.1.6 Settings when Switching Over SPARC Enterprise Servers".

  For details on the function, refer to "Chapter 4 Server Switchover" in the "Operation Guide VE".
- Only the server switchover function or the migration function can be used.

  Perform design of the configuration based on the function that you will be using.

  - When using the server switchover function, the following configurations are necessary:

    - Design the area used for the non-global zone so that it can be referred to in the same way both before and after switchover.

      Use the switchover SAN area for server switchover.

    - When using the server switchover function, non-global zones are not automatically started.

      Perform configuration so that non-global zones are automatically started when global zones are started after server switchover.

- When using the migration function, or [Relocate at startup] has been configured for the L-Server boot location, the following configurations are necessary.

  - Perform configuration so that LUNs corresponding to the zone paths used by virtual L-Servers will not be automatically mounted.

  - Connect a disk on which a non-global zone is to be created that can be mounted on both the migration source and destination.

    However, do not mount it in a location other than the global zone where the non-global zone operates.

Note

- Do not execute the mounting of LUNs in other global zones when the LUN is shared from two or more global zones and the LUN corresponds to the zone path that a virtual L-Server uses. There is a possibility that the data of the LUN will be damaged due to an access conflict when a virtual L-Server that uses this LUN is created.

E.6.4 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
- A global zone is already connected to the admin LAN
- NICs to be used in the non-global zones are already designed
- The IDs for distinguishing the NICs used in the non-global zone have been designed.

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.

Designing NICs to be Used in Non-Global Zones

- When creating L-Servers using Resource Orchestrator, create a non-global zone using exclusive IP settings.

  For the NICs to be used by L-Servers, design them so those NICs will not be used in the global zone or non-global zones which have already been created.
  When migrating VM guests (non-global zone) between VM hosts (global zones), perform design so a NIC with the same name is used on the source and destination.
  Also, design the IDs for distinguishing the NICs used by the L-Server. This value corresponds to the VLAN ID of the network resource, so please use a value between 1 and 4094.

- When associating already created non-global zones with L-Servers, there are no restrictions on the network configurations.
- When NICs for L-Servers are DHCP, place the DHCP servers, and configure the settings to allocate IP addresses to L-Servers.
- Design IP addresses to allocate to L-Servers that do not overlap with IP addresses that are not managed in Resource Orchestrator.
- The NIC hardware configurations must be the same on servers in the same pool.

Appendix F Preparing for Automatic Configuration and Operation of Network Devices

This section explains how to prepare automatic configuration and operation of network devices

F.1 Creating Model Definitions for Network Devices

Rulesets used for the function that automatically configures network devices are registered by the 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 Manager]
Installation_folder\SVROR\Manager\etc\customize_data\network_device_model.xml

[Linux Manager]
/etc/opt/FJSVrcvmr/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 auto-configuration of network devices are automatically acquired, therefore it is not necessary to enter them in the model definition file.

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.

- 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.
- If product name or model name is specified in network configuration information used at network device registration, specified product name or model name is regarded as a model.

See

For details on model definitions for network devices, refer to "14.13 Network Device Model Definitions" in the "Reference Guide (Command/XML) CE".

F.2 Configuring Execution Environment

This section explains how to configure execution environment for automatic configuration and operation of network devices.

F.2.1 When Connecting to Network Device with SSH

When connecting to network device with SSH in automatic configuration and operation of network devices, infrastructure administrator prepares SSH environment using the following procedure.

1. Download "Ganymed SSH-2 for Java (build 250)" form internet and so on.
2. Decompress downloaded "Ganymed SSH-2 for Java (build 250)" and store it in the following directory.

   [Windows Manager]
   Installation_folder\SVROR\Manager\etc\scripts*vendor_name**unit_name or model_name*\common\

   [Linux Manager]
   /etc/opt/FJSVrcvmr/scripts/*vendor_name*/*unit_name or model_name*/common/

F.2.2 When using script language excluding ruby

When using script language excluding ruby in automatic configuration and operation of network devices, infrastructure administrator prepares script language environment using the following procedure.

1. Store script language library in any folder recognizable by ROR manager.
2. Define the script language in definition file of automatic configuration and operation of network devices.

For the information of how to defining the script language, refer to "Script language" in "F.7.3 Definition File Format".

F.2.3 When large amount of data is output as a result of executing a ruleset for operations on network devices

When amount of output data as a result of executing a ruleset for operation on network devices exceeds 500 Kbyte, infrastructure administrator defines upper output limit of operation ruleset in network device automatic configuration and operation definition file.

For the information about how to defining upper output limit of operation ruleset, refer to "Upper output limit of operation ruleset" in "F. 7.3 Definition File Format".

F.3 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 with a unique name in the system 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.

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 "14.13 Network Device Model Definitions" in the "Reference Guide (Command/XML) CE".

  About "Vender name" and "unit name" when using sample script, refer to "Vender name" and "unit name" in "Table G.2 Units for which Sample Scripts are Provided" and "Table G.9 List of Unit Name that offer sample Script for Operations".

- 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 Manager]
  Installation_folder\SVROR\Manager\etc\scripts\

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

About folder where sample scripts are registered at installation, refer to "G.3 Sample Scripts(For automatic configuration)" and "G.4 Sample Scripts(For Operation)".

F.3.1 Folders for L-Platform Templates (Automatic Configuration)

Create folders for registering rulesets for automatic configuration of firewall or server load balancer.
Create the folders for registering rulesets for L-Platform templates with the following name:

[Windows Manager]
Installation_folder\SVROR\Manager\etc\scripts*vendor_name**unit_name or model_name*\rulesets*ruleset_name*\

[Linux Manager]
/etc/opt/FJSVrcvmr/scripts/*vendor_name*/*unit_name or model_name*/rulesets/*ruleset_name*/

Information

The following folders for registering ruleset used at sample scripts are created automatically at the installation of this product.

[Windows Manager]
Installation_folder\SVROR\Manager\etc\scripts*vendor_name**unit_name or model_name*\rulesets\

[Linux Manager]
/etc/opt/FJSVrcvmr/scripts/*vendor_name*/*unit_name or model_name*/rulesets/

F.3.2 Folders for Network Resources

Create folders for registering rulesets for automatic configuration of L2 switch.

Particular network device folders include rulesets per network device unit name or model name.

Create the following two types of folders.

- The folder common to network devices

  Regiseter ruleset selected at creating network resources.

  Create the folder with the following name.

  [Windows Manager]
  Installation_folder\SVROR\Manager\etc\scripts\network_resource*ruleset_name*\

  [Linux Manager]
  /etc/opt/FJSVrcvmr/scripts/network_resource/*ruleset_name*/

- The folder for the particular network device

  Register ruleset per network device unit name or model name. This ruleset includes scripts used by ruleset common to network device.

  Create the folder with the following name.

  [Windows Manager]
  Installation_folder\SVROR\Manager\etc\scripts\vendor_name*unit_name or model_name*\rulesets*ruleset_name*\

  [Linux Manager]
  /etc/opt/FJSVrcvmr/scripts/*vendor_name*/*unit_name or model_name*/rulesets/*ruleset_name*/

Information

- The following folders for registering ruleset to use sample scripts are created automatically at the installation of this product.
  - The folder common to network devices

    [Windows Manager]
    Installation_folder\SVROR\Manager\etc\scripts\network_resource\

    [Linux Manager]
    /etc/opt/FJSVrcvmr/scripts/network_resource/

  - The folder for the particular network device

    [Windows Manager]
    Installation_folder\SVROR\Manager\etc\scripts*vendor_name**unit_name or model_name*\rulesets\

    [Linux Manager]
    /etc/opt/FJSVrcvmr/scripts/*vendor_name*/*unit_name or model_name*/rulesets/

- When configuring tag vlan in SR-X300 using sample script, register the following rulesets in the folder for registering ruleset for network resources.
  - Rulesets registered in the folder for the particular network device
    - tag_vlan_port--SR-X300tag_vlan_port--SR-X300_n or
    - tag_vlan_port--SR-X300tag_vlan_port--SR-X300_n
  - Rulesets registered in the folder common to network devices
    - tag_vlan_net--SR-X300tag_vlan_net--SR-X300_n or
    - tag_vlan_net--SR-X300tag_vlan_net--SR-X300_n

  About combination of ruleset of sample script, refer to "G.3.9 For deploying L2 Switches".

F.3.3 Common Information of Ruleset

It is possible to share the information used for ensuring consistency of configurations between multiple rulesets for automatic configuration of the same device type. For example, there is an information file to share information for identifying definition.

The infrastructure administrator should create the following system directory and place the files in it:

[Windows Manager]
Installation_folder\SVROR\Manager\etc\scripts*vendor_name**unit_name or model_name*\common\

[Linux Manager]
/etc/opt/FJSVrcvmr/scripts/*vendor_name*/*unit_name or model_name*/common/

Information

The folders for registering ruleset used at sample scripts are created automatically at the installation of this product.

F.3.4 Folders for L-Platform Templates (Operations)

Create folders for registering rulesets for operation of server load balancer.
Create the folders for registering rulesets for L-Platform templates with the following name:

[Windows Manager]
Installation_folder\SVROR\Manager\etc\scripts*vendor_name**unit_name or model_name*\operations*ruleset_name*\

[Linux Manager]
/etc/opt/FJSVrcvmr/scripts/*vendor_name*/*unit_name or model_name*/operations/*ruleset_name*/

Information

The following folders for registering ruleset used at sample scripts are created automatically at the installation of this product.

[Windows Manager]
Installation_folder\SVROR\Manager\etc\scripts*vendor_name**unit_name or model_name* \operations\

[Linux Manager]
/etc/opt/FJSVrcvmr/scripts/*vendor_name*/*unit_name or model_name* /operations/

F.4 Basic Structure of a Script

This section explains the basic operation and structure of a script used for automatic configuration and operation of network devices.

The basic flow of configuration and operation of network devices using scripts is as follows:

1. Confirm the syntax of script list file.
2. The following process is done orderly form the head in script list file.
    a. Specify the target network device.
    b. Complete script file to convert variable information in script file corresponding to "Script Name" with the information of parameter file and so on.
    c. When "cmd operand" is specified in script list, complete specified command file. In this process, variable information in the command file is converted using the information of parameter file and so on.
    d. Script file is executed sequentially from top to bottom.
    At this time, read commands in command file if necessary.

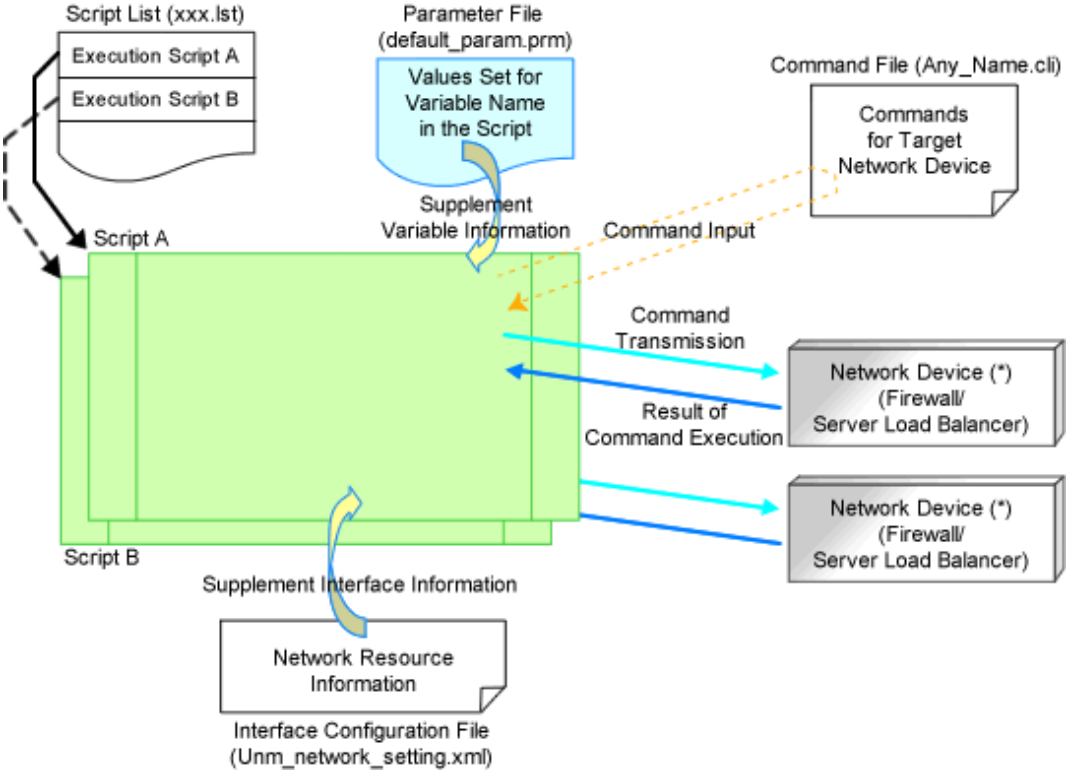
About the function of each files, refer to "F.4.1 Function and Attributes of Each File".

As the example of basic script structure, the following basic structure is shown.

- Basic Structure Example when Using Scripts for L-Platform Templates (Automatic Configuration)
- Basic structure for network resource
- Basic structure of L-Platform template (operation)

Basic Structure Example when Using Scripts for L-Platform Templates (Automatic Configuration)

Figure F.1 Basic Structure Example when Using Scripts for L-Platform Templates (Automatic Configuration)



Note that selected network device (firewall or server load balancer) is registered at network pool which tenant administrators or tenant users can use.

Script A

Infrastructure administrator prepares this.
The example of basic process in script is the following.

1. Define variable
2. Establish telnet/ssh connection with variable (IP address in admin LAN)
3. Send variable (login account 1)
4. Send variable (login password 1)
5. Process command file
   - If command files exist.

     Read command file and send the content of command file by a line. [command transmission]
   - If command files don't exist.

     Execute process of sending and receiving commands. [Command transmission]
6. Command process ends.
   - If command process ends normally

     Set return value normal.
   - If command process ends abnormally

     Set return value abnormal.
7. Send variable (logout character string). [Command transmission]
8. Disconnect telnet/ssh connection.

Script B

Infrastructure administrator prepares this.
The example of basic process in script is the same as script A.

Sclipt List(*xxx*.lst)

Infrastructure administrator prepares this.
Script list of ruleset selected at creating L-Platform.
Scripts specified in script list are executed sequentially.

Parameter ile(default_param.prm)

Infrastructure administrator prepares this.
Information for setting or changing specified parameter value when tenant administrators or users create or modify L-Platform.

Command File(*Any_Name*.cli)

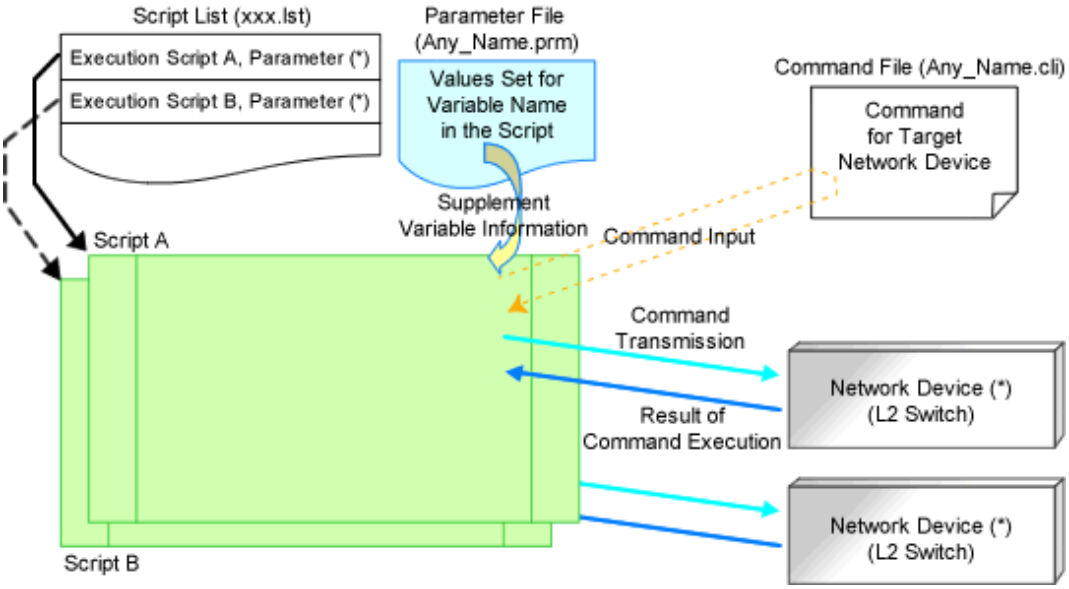
Infrastructure administrator prepares this.
Write process after log in to devices with log in accounts excluding command process included in script.

Interface Configuration File(Unm_network_setting.xml)

Infrastructure administrator prepares this.
There is one file per system.

Basic structure for network resource

Figure F.2 Basic Structure Example when Using Scripts for Network Resources



Note that it is possible to specify parameters in script without parameter file.

Script A

This script is prepared by Infrastructure administrator and registered under particular network device ruleset folder.
The example of basic process in script is as follows:

1. Define variable
2. Establish telnet/ssh connection with variable (IP address in admin LAN)
3. Send variable (login account 1)
4. Send variable (login password 1)

5. Process command file

   - If command files exist.

     Read command file and send the content of command file by one line. [command transmission]

   - If command files don't exist.

     Execute process of sending and receiving commands. [Command transmission]

6. Command process ends.

   - If command process ends normally

     Set return value normal.

   - If command process ends abnormally

     Set return value abnormal.

7. Send variable (logout character string). [Command transmission]

8. Disconnect telnet/ssh connection.

Script B

This script is prepared by Infrastructure administrator and registered under particular network device ruleset.
The example of basic process in script is the same as script A.

Script List(*xxx*.lst)

This script is prepared by Infrastructure administrator and registered under particular network device ruleset folder.
For network device related to operated L-Platform.
Scripts specified in script list are executed orderly.

Parameter File(*Any_Name*.prm)

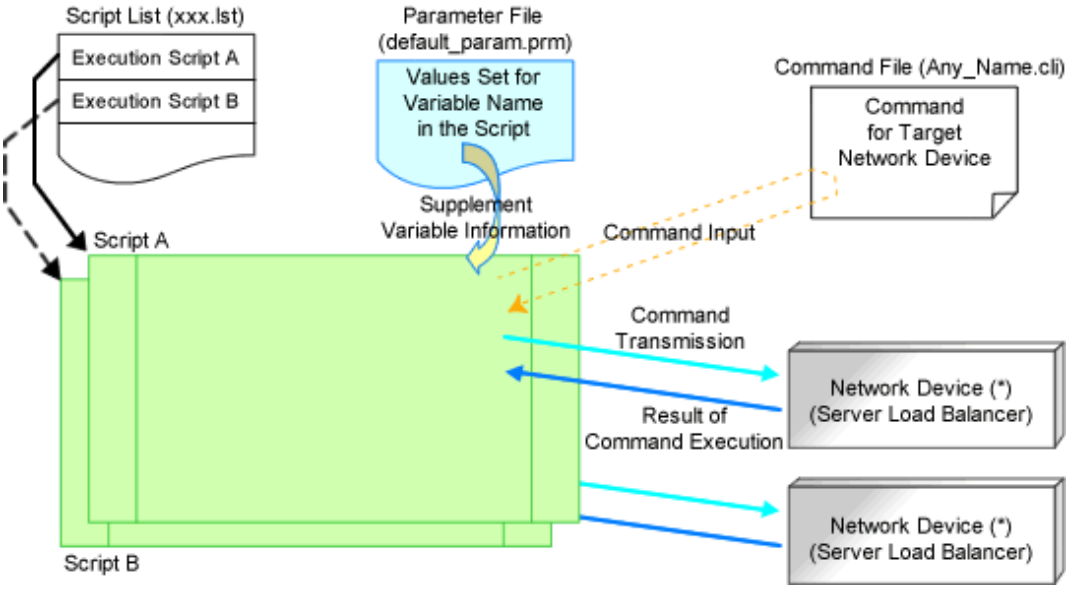
Infrastructure administrator prepares this if necessary.

Command File(*Any_Name*.cli)

Infrastructure administrator prepares this.
Write process after log in to devices with log in accounts excluding command process included in script.

Basic structure of L-Platform template (operation)

Figure F.3 Basic Structure Example when Using Scripts for L-Platform Templates (Operations)



Note that network device (server load balancer) registered at network pool which tenant administrators or tenant users creating L-Platform can use is selected.

Script A

Infrastructure administrator prepares this.
The basic flow of configuring or operating network devices used by scripts is as follows.

1. Define variable
2. Establish telnet/ssh connection with variable (IP address in admin LAN)
3. Send variable (login account 1)
4. Send variable (login password 1)
5. Process command file
   - If command files exist.

     Read command file and send the content of command file by one line. [command transmission]
     Get command execution results and write it to the standard output.
   - If command files don't exist.

     Execute process of sending and receiving commands. [Command transmission]
     Get command execution results and write it to the standard output.
6. Command process ends.
   - If command process ends normally

     Set return value normal.
   - If command process ends abnormally

     Set return value abnormal.
7. Send variable (logout character string). [Command transmission]
8. Disconnect telnet/ssh connection.

Script B

Infrastructure administrator prepares this.
The example of basic process in script is the same as script A.

Script List(*xxx*.lst)

Infrastructure administrator prepares this.
Script list of ruleset selected at creating L-Platform.
Scripts specified in script list are executed orderly.

Parameter File(default_param.prm)

Infrastructure administrator prepares this.
Information for setting specified parameter value when tenant administrators or users operate L-Platform.

Command File(*Any_Name*.cli)

Infrastructure administrator prepares this.
Write process after log in to devices with log in accounts excluding command process included in script.

Note that each file is created according to used script.
The example of basic structure is the explanation of the structure corresponding to sample script offered by this product.

F.4.1 Function and Attributes of Each File

This section explains the functions and attributes of each file which compose a script.

Table F.1 Function and Attributes of Each File

File Type	Function	File Name Rule	Extension

F.6.1 Script List File	In this file, scripts are arranged in the order of execution for auto-configuration of network devices. Write all script list for operating network devices at one operation (creation, modification, deletion etc.).	- "create.lst" Script list for creation - "create_recovery.lst" Script list for recovery at creation error - "modify.lst" Script list for modification - "modify_recovery.lst" Script list for recovery at modification error - "delete.lst" Script list for deletion - "connect.lst" Script list for creation of interface adjoining server - "connect_recovery.lst" Script list for recovery at creation error of interface adjoining server - "disconnect.lst" Script list for deletion of interface adjoining server - "operate.lst" Script lists for operations	lst
F.6.2 Script File	In this file, the procedure for auto-configuration of network devices is written.	An arbitrary character string composed of alphanumeric characters, hyphens ("-"), and underscores ("_"). The valid characters and string lengths depend on the OS or the rules of the script language.	Language dependent
F.6.3 Command File	In this file, the list of commands which will be sent to network devices are written.	A string of alphanumeric characters, hyphens ("-"), and underscores ("_"), within 32 characters in length.	cli
F.6.4 Parameter File	In this file, the parameters which can be customized in the scripts are written.	- "default_param.prm" In case of ruleset for L-Platform template, this name is fixed. - *Any name* In case of ruleset used at network resource, specify this with alphanumeric character, hyphen ("-"), and underscore ("_") within 32 characters	prm
F.6.5 Interface Configuration File	In this file, the parameters for network device interface configuration which can be customized in the scripts are written.	"Unm_network_setting"	xml

F.4.2 Location of Each File

This section explains the location of each file which composes a script.

The placement of script list file and parameter file

- Ruleset used by L-Platform template
  - Ruleset for automatic configuration

    [Windows Manager]
    Installation_folder\SVROR\Manager\etc\scripts*vendor_name**unit_name or model_name*\rulesets*ruleset_name*\

    [Linux Manager]
    /etc/opt/FJSVrcvmr/scripts/*vendor_name*/*unit_name or model_name*/rulesets/*ruleset_name*/

  - Ruleset for opeartion

    [Windows Manager]
    Installation_folder\SVROR\Manager\etc\scripts*vendor_name**unit_name or model_name*\operations*ruleset_name*\

    [Linux Manager]
    /etc/opt/FJSVrcvmr/scripts/*vendor_name*/*unit_name or model_name*/operations/*ruleset_name*/

- Ruleset used by network resource

  [Windows Manager]
  Installation_folder\SVROR\Manager\etc\scripts\network_resource*ruleset_name*\

  [Linux Manager]
  /etc/opt/FJSVrcvmr/scripts/network_resource/*ruleset_name*/

The placement of script file and command file

- Ruleset for automatic configuration

  [Windows Manager]
  Installation_folder\SVROR\Manager\etc\scripts*vendor_name**unit_name or model_name*\rulesets*ruleset_name*\

  [Linux Manager]
  /etc/opt/FJSVrcvmr/scripts/*vendor_name*/*unit_name or model_name*/rulesets/*ruleset_name*/

- Ruleset for operation

  [Windows Manager]
  Installation_folder\SVROR\Manager\etc\scripts\vendor_name*unit_name or model_name*\operations*ruleset_name*\

  [Linux Manager]
  /etc/opt/FJSVrcvmr/scripts/*vendor_name*/*unit_name or model_name*/operations/*ruleset_name*/

Placement of interface configuration file

[Windows Manager]
Installation_folder\SVROR\Manager\etc\scripts\network_resource\

[Linux Manager]
/etc/opt/FJSVrcvmr/scripts/network_resource/

F.5 The time when ruleset is executed

The time when ruleset in folder for ruleset registration is executed is listed below.

Table F.2 List of the time when ruleset is executed

Operation	Registration Folder	Target Device	Note
L-Platform creation L-Platform modification L-Platform deletion	For L-Platform template (automatic configuration)	Firewall	Set initial firewall rule.
		Server Load Balancer	
	For network resource	L2 Switch	When deploying physical L-Server using rack mount

			server, configure L2 switch.
In "L-Platform Details", do "setting"	For L-Platform template (automatic configuration)	Firewall	Modify firewall rule and so on.
In "L-Platform Details", do "SLB settings"		Server Load Balancer	Set server load balancer rule and so on.
In "L-Platform Details", do "Operation"	For L-Platform template (operation)	Server Load Balancer	Execute operation.
In "L-Platform Details", do "Operation log"			Display operation log.
Network resource creation Network resource modification Network resource deletion	For network resource	L2 Switch	Set vlan responding to network resource and so on.

F.6 File Components of Ruleset

This section describes each file contents for configuration and operation according to structure of a script described in "F.4 Basic Structure of a Script".

F.6.1 Script List File

This section explains format of script list file and how to write parameters in script list file.

Script Lists for L-Platform Templates

This section explains script lists (for setup and for operations) of rulesets used in L-Platform templates.

Format

[*Script Path*]*Script Name*[,cmd=*Script Command file Name*][,node=none][,group=*Group Number*][,param=(*Parameter Name1*=*Parameter Value1*,*Parameter Name2*=*Parameter Value2*,...)]

Script lists for setup and script lists for operations use the same format.

Description

This section explains each item.

Script Path

Specify the folder path for the script to execute using an absolute path or relative path from the scripts folder.
If you do not specify this path, the path of the script to execute is regarded as being the folder path including the script list.

Script Name

Specify the name of the script you want to execute.
Do not specify a script list name in this field.
If you specify it, it is regarded as designating execution script name.

cmd=*Script Command File Name*

Specify the name of the script command file you want to execute.
The value specified for this operand will be configured for the reserved variable "command file name".
If you invoke some command files, use the command file name with a serial number (in ascending order from 1) in the script.
If you do not specify the command file name in the script, the command file is not invoked from the script.

node=none

If you want to unconditionally execute the script regardless of the existence or status of network devices (firewalls or server load balancers), specify "none" for this operand.

group=*Group Number*

If you execute a script for redundant network devices, set a group number between 1 and 99. This number is used to distinguish network devices in the same redundant configuration.
If there are 2 lines in a script with the same group number, then an available pair of network devices will be selected from the network pool.
(If there are no redundant network devices (at least one device in a pair is alive) available in a network pool, a script list execution error occurs due to the lack of available network devices).

param=(*Parameter Name1=Parameter Value1*,*Parameter Name2=Parameter Value2*,...)

If you want to change the configuration values of variable parameters in a parameter file per script list line, specify this operand.
Specify all parameter names and changed parameter values that you want to change.
If infrastructure administrators want to decide parameter values per script, writing parameters and their values at this operand means those variable parameters do not have fixed values in scripts.
If tenant users or administrators specify these parameters when creating an L-Platform, the parameter values are used in the script.

- Specified parameters are separated by "," and blank spaces between parameters and "," are ignored.
- The number of lines specified in a script list is limited to 100, excluding comment lines.
- Comments begin with "#" in the first column. Any characters can be used in the comment line.
  Write comments such as description of executed scripts when necessary.
  Comments are ignored when script lists are processed.
- Blank lines are regarded as comments and ignored when a script list is processed.
- Scripts in a script list are executed in the defined order.

Execution Image

Script list is executed in the order of the list.

```
[Script Path]Script Name1,group=1[,cmd=Command File Name1]
[Script Path]Script Name2,group=2[,cmd=Command File Name2]
```

Script list for network resources

This section explains the ruleset script list used by network resources.

Format

```
Script Path Script Name[,cmd=Script Command File Name],node=Network Device Name[,paramfile=Parameter File Name]
[,param=(Parameter Name1=Parameter Value1,Parameter Name2=Parameter Value2,...)]
```

Description

This section explains each item.

Script Path

Specify the folder path for the script to execute using an absolute path or relative path from the scripts folder.
The folder path, including the execution script, is necessary.

Script Name

Specify the name of the script you want to execute.
Do not specify a script list name in this field. If you specify it, it is regarded as designating the name of the script to execute.

cmd=*Script Command File Name*

Specify the name of the script command file you want to execute.
The value specified for this operand will be configured for the reserved variable "command file name".

If you invoke multiple command files, it is necessary to use command file names including a serial number (in ascending order from 1).
If you do not specify the command file name in the script, the command file is not invoked from the script.

node=*Network Device Name*

Specify the name of the network device to execute the script.
If you specify the wrong network device name in this field, an automatic configuration error or incorrect configuration occurs when the script is executed. Specify the network device name carefully.

paramfile=*Parameter File Name*

Specify the parameter file name of the variable information passed to the script.
If you use variable information from a parameter file, specify the name of the parameter file.

param=(*Parameter Name1=Parameter Value1*,*Parameter Name2=Parameter Value2*,...)

If you want to change the settings of variable parameters in the parameter file specified for the "paramfile" field per line of script list, use this operand.
Specify all parameter names and changed parameter values that you want to change.

Information

- Specified parameters are separated by "," and blank spaces between parameters and "," are ignored.
- The number of lines specified in a script list is limited to 100, excluding comment lines.
- Comments begin with "#" in the first column. Any characters can be used in the comment line.
  Write comments such as description of executed scripts when necessary.
  Comments are ignored when script lists are processed.
- Blank lines are regarded as comments and ignored when a script list is processed.
- When a script list processes the same network device, the script list is not executed at the same time but executed in order. On the other hand, when a script list does not process the same network device, the script list is executed at the same time.

Execution Image

Script list is executed in the order of the list.

[*Script Path*]*Script Name1*,node=*Network Device Name1*,param=(*Parameter Name1*=*Value*,...)
[*Script Path*]*Script Name2*,node=*Network Device Name2*,param=(*Parameter Name2*=*Value*,...)
[*Script Path*]*Script Name3*,node=*Network Device Name3*,param=(*Parameter Name3*=*Value*,...)

The difference between script list of L-Platform template and that of network resource

This section explains the difference between script list of L-Platform template and that of network resource.

Table F.3 The difference of script list

Item	Folders for L-Platform Templates	Folders for Network Resources
node operand: network device name configured by scripts	Cannot be specified. The network device configured by scripts is automatically selected. "none" can be specified when the script is not related to the specified network device.	Can be specified
group operand: The number to distinguish a network device in a redundant configuration	Can be specified	Cannot be specified

paramfile operand: parameter file name	Cannot be specified	Can be specified

F.6.2 Script File

This section explains how to create script files.

Script Structure

This section explains the structure of scripts.
The process from establishing to releasing a telnet/ssh connection with the target network device is written in scripts.
The basic structure is shown in the following figure.

Variable Definition Section

Variable information is converted using information from the parameter file and DB and defined as a variable.

Connection(login)

Establishes a telnet connection to the admin LAN IP address defined in the variable.
Sends the login account defined in the variable.
Sends the login password defined in the variable.

Command Sending Section

- If command files exist

  Send the content of the command file line by line.

- If command files do not exist

  Executes the process of sending and receiving commands in a script.

Verification of execution results

If the command ends normally, the return value "normal" is set.
If the command process ends abnormally, the return value "error" is set.

Disconnection (logout)

Send the variable (logout string).
Disconnect the telnet connection.

Write process from connection to disconnection in script.

Variable Information Usable at Script

Variables used in scripts are defined in the variable definition section.
Variables including variable information are defined between the reserved variables "%Unm_DefineStart%" and "%Unm_DefineEnd%" as follows.

```
# %Unm_DefineStart%

Define variables including variable information.

# %Unm_DefineEnd%
```

Reserved variable names consist of character strings with "Unm" as a prefix and alphanumeric characters and an ampersand ("&"), underscores ("_"), and hyphens ("-"). "&" in a character string is a symbol utilized to split a character string into a meaningful string such

as an L-Server name and a network resource name.
Reserved variable names which can be used in scripts are shown in the following table.

Table F.4 Reserved Variables that can be Used in Scripts

Information Type	Variable Name	Usage After Conversion
Variable information (beginning)	%Unm_DefineStart% (*1)	Specify the beginning of the range for variable conversion in a script. Include this as a comment line once in script.
Variable information (end)	%Unm_DefineEnd% (*1)	Specify the end of the range for variable conversion in a script. Include this as a comment line once in script.
Command file name	%Unm_CommandFileName% (*2)	Command file name
VLAN-ID	%Unm_VlanId% (*3)	VLAN-ID value
VLAN-ID	%Unm_VlanId&Network Resource Name% (*3)	VLAN-ID value
Admin IP address	%Unm_MyLoginIp%	IP address used for logging into the target device via SSH/ TELNET/FTP
Login account 1	%Unm_MyLoginAccount1%	Account name used for logging into the target device via SSH/ TELNET/FTP
Login account 2	%Unm_MyLoginAccount2%	Account name used for logging into the target device via FTP
Login password 1	%Unm_MyLoginPass1%	SSH/TELNET password for logging into the target device
Login password 2	%Unm_MyLoginPass2%	FTP password for logging into the target device
Admin password 1	%Unm_MyAdminPass1%	Password to change to admin privileges of the target device
Admin account	%Unm_MyAdminAccount%	Admin account of the target device
Admin password 2	%Unm_MyAdminPass2%	Admin password of the target device
Login port	%Unm_LoginPort%	SSH/TELNET port for logging into the target device
FTP admin IP address	%Unm_FtpLoginIp%	IP address for logging in from the target device via FTP
FTP login port	%Unm_FtpLoginPort%	Port used for logging in from the target device via FTP
FTP login account	%Unm_FtpLoginAccount%	Account name for logging in from the target device via FTP
FTP login password	%Unm_FtpLoginPass%	Password for logging in from the target device via FTP
Adjoining L2 switch 1	%Unm_SwNode1% (*4)	Network device name of the adjoining L2 switch connected to the physical rack server NIC (If a physical server has redundant NICs, specify the first

		L2 switch connected to the first NIC)
Adjoining L2 switch 2	%Unm_SwNode2% (*4)	Network device name of second adjoining L2 switch connected to physical rack server redundant NIC
Adjoining L2 switch port 1	%Unm_SwPort1% (*4)	Port name of the second adjoining L2 switch connected to the physical rack server redundant NIC Port name of the adjoining L2 switch connected to the physical rack server redundant NIC
Adjoining L2 switch port 2	%Unm_SwPort2% (*4)	Port name of second adjoining L2 switch connected to physical rack server redundant NIC
Network device IPv$ address	%Unm_Ipv4&Sequential Number&Network Resource Name%(*5)	IPv4 address configured on the interface of the automatic configuration target device
Network device IPv4 subnet	%Unm_Ipv4Subnet&Network Resource Name%	IPv4 subnet configured on the interface of the automatic configuration target device
Network device IPv4 subnet mask	%Unm_Ipv4SubnetMask&Network Resource Name%	IPv4 subnet mask configured on the interface of the automatic configuration target device
Network device IPv4 subnet mask length	%Unm_Ipv4SubnetMaskLength&Network Resource Name%	IPv4 subnet mask length configured on the interface of the automatic configuration device
Network device IPv6 address	%Unm_Ipv6&Sequential Number& Network Resource Name%	IPv6 address configured on the interface of the automatic configuration target device
Network device IPv6 prefix	%Unm_Ipv6Prefix&Network Resource Name%	IPv6 prefix configured on the interface of the automatic configuration target device
Network device IPv6 prefix length	%Unm_Ipv6PrefixLength&Network Resource Name%	IPv6 prefix length configured on the interface of the automatic configuration target device
VRID	%Unm_Vrid&Network Resource Name%	VRID configured on the interface of the automatic configuration target device
L-Platform name	%Unm_LplatformName%	Name of the L-Platform performing processing
L-PlatformID	%Unm_LplatformId%	Number of the L-Platform (1 - 99) performing processing
Firewall name	%Unm_FirewallName%	Name of the firewall processing the L-Platform
Firewall resource ID	%Unm_FirewallId%	Resource ID of the firewall processing the L-Platform
Server load balancer name	%Unm_SlbName%	The name of the processed SLB on the L-Platform

The server load balancer resource ID	%Unm_SlbId%	The resource ID of the processed SLB on the L-Platform
List of admin IP addresses of redundant network devices	%Unm_Group&Group Number%	List of admin IP addresses of the redundant network device corresponding to the group number of the script The group number specified in the script list
Backup directory	%Unm_BackupDir% (*6)	Absolute path name of the backup directory
Current setting information	%Unm_Present&Variable name% (*7)	The content of the variable name used in the most recent configuration
Variable parameter specified by an infrastructure administrator	%Unm_Set_Variable_Character&Network_Resource_Name%	The value when a variable parameter excluding variable parameter limited by the system is specified in the interface configuration file

*1: The scope of the script lines converted by the script which converts variable information

- When %Unm_DefineStart% is defined, but %Unm_DefineEnd% is not defined

  Lines from %Unm_DefineStart% to the last line of script files are considered as variable parameters to be converted.

- When %Unm_DefineStart% is not defined, but %Unm_DefineEnd% is defined

  Variable parameter conversion is not executed in the script file.

- When that %Unm_DefineStart% and %Unm_DefineEnd% are multiply defined

  Variable parameters between first %Unm_DefineStart% and %Unm_DefineEnd% from first line of file are the targets of variable parameter conversion.

*2: Command file name

In variable information of the command file name, configure the name added to "exec_discrimination number (8 - 10 digits)" before the command file name prescribed by the system.
When you use multiple command files in a script, it is necessary that variable parameters of the script are written as variable information of the command file name + *n* (*n* is a sequential number).

Example

"%Unm_CommandFileName%1.cli"
"%Unm_CommandFileName%2.cli"
"%Unm_CommandFileName%3.cli"
...

*3: VLAN-ID value of multiple network resources

When you use the VLAN-ID values of multiple network resources as variable information, specify it in the following format in the script and each value will be processed by the system.

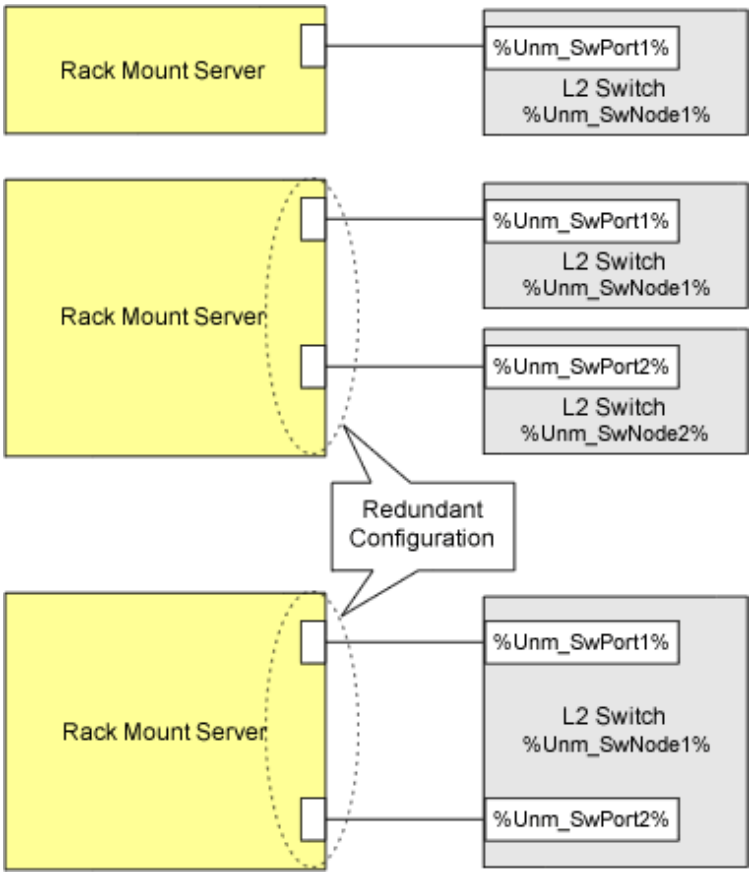
- VLAN-ID value : %Unm_VlanId%

  %Unm_VlanId & Network resource name (up to 32 characters)%
  The VLAN-ID configured in the network resource corresponding to the specified network resource name is configured as variable information.

*4: Reserved variable names when physical rack servers have redundant NICs

For a physical rack server with redundant NICs, the reserved variable names are as follow:

Figure F.4 Reserved Variable Names for Physical Rack Mount Servers with Redundant NICs



*5: Sequential numbers

Ensure that specified sequential numbers are the values corresponding to the IPv4/IPv6 addresses for the desired purpose.
Assign sequential numbers for each purpose to the IPv4/IPv6 addresses required by network devices, such as physical IPv4/IPv6 addresses for active units and virtual IPv4/IPv6 addresses for standby units.
Specify the mapping of the IPv4/IPv6 addresses for each purpose and assign sequential numbers in the following elements in the interface configuration file:

- The IPv4Address element
- The IPv4Address element

*6: Backup directory

Parameters in the following definition files are configured as a backup directory name.

- Storage Location of the Definition File

  [Windows Manager]
  Installation_folder\SVROR\Manager\etc\customize_data\manager_backup.rcxprop

  [Linux Manager]
  /etc/opt/FJSVrcvmr/customize_data/manager_backup.rcxprop

- Parameter Format of Definition Files

  ruleset_backup_dir=backup directory

  backup directory: specify the backup directory name using an absolute path.

  If this parameter is not specified, the following backup directory is specified by default.

[Windows Manager]
Installation_folder\SVROR\Manager\var\lserver_repair\ruleset_backup

[Linux Manager]
/var/opt/FJSVrcvmr/lserver_repair/ruleset_backup

*7: Current setting information

It is possible to obtain information from when creating resources for firewalls and server load balancers until those resources are deleted. The variable name used when the script was last executed during creation or modification of firewalls or server load balancers can be used as the current setting information.
When using the current setting information, it is not possible to configure different values for individual scripts or to use different variable information names for individual scripts in the script list. The variable information name and value must be the same throughout the script list.
The variable names which can be specified for "variable name" of this reserved variable are the following reserved variable names, and user-defined variable names stated in the parameter file.

Table F.5 Reserved Variable Names that can be Used for "Variable Name"

Information Type	Reserved Variable Name
Command file name	%Unm_CommandFileName%
VLAN-ID	%Unm_VlanId&Network Resource Name%
L-Platform name	%Unm_LplatformName%
L-Platform resource ID	%Unm_LplatformId%
Firewall name	%Unm_FirewallName%
Firewall resource ID	%Unm_FirewallId%
Server load balancer name	%Unm_SlbName%
The server load balancer resource ID	%Unm_SlbId%
List of admin IP addresses of redundant network devices	%Unm_Group&Group Number%

Current setting information varies depending on how many times automatic configuration was performed.
"None" indicates that the variable name will not be converted because there is no value.

Table F.6 Example of Information Changed each time Auto-configuration is Executed

Number of Times Executed	Variable Name	Information of %Unm_Present & Variable name%	Variable Name Information
First time	A	None	1
	B	None	2
	C	None	3
Second time	A	1	11
	B	2	2
	C	3	None
Third time	A	11	11
	B	2	2
	C	None	1

Information

- Reserved variable names are written in the following locations.
  - Any place in a command file
  - In the "node" operand and "param" operand in script lists
  - Between the "%Unm_DefineStart%" line and "%Unm_DefineEnd%" line in a script
- When you do not use a sample script (as in cases where an infrastructure administrator creates their own new script), specify variable information which is usable in command files and scripts using character strings enclosed by % like "%...%". The maximum length of a variable information string is 128 characters.
- In the character string enclosed by %, alphanumeric characters, underscores ("_"), and hyphens ("-") can be used. "Unm_" is a reserved variable name, so it cannot be included in variable names specified by users.
- Variable information can be written in the following locations.
  - Any place in a command file
  - Between the "%Unm_DefineStart%" line and "%Unm_DefineEnd%" line in a script

Operation when Variable Information Conversion in a Script Fails

If conversion of variable information fails, variable information parameters are not converted and the script is executed.
If variable information in the command file is a character string before conversion, the script will not send that command or any associated commands to the network device.
A script execution error is not returned just because the conversion of variable information fails.
If conversion of the following variable information related with the adjoining L2 switch fails, the script is not executed and an error is returned because there is a problem when constructing information of the network device.

- %Unm_SwNode1%
- %Unm_SwNode2%
- %Unm_SwPort1%
- %Unm_SwPort2%

Return Codes Used by Scripts

The results of script execution are determined to be normal or abnormal based on their return code.
Based the code returned by a script, the process ends normally or recovery action is executed.
Return codes used for scripts are as follows.

Table F.7 Return Codes Used by Scripts

Return Code	Return Code Meaning
0	Processing of the script ended normally.
4	An error occurred in script execution, but the script can be executed again. (Connection closed or connection time out)
8	An error occurred in script execution, and the script cannot be executed again. (Errors other than the above) Network devices which fail to execute scripts are removed from the candidates for auto-configuration. To be candidates of the automatic configuration by scripts, the following command is used for network devices - "rcxadm netdevice set" with the option "-attr auto_conf=true" For information about the rcxadm netdevice command, refer to "3.8 rcxadm netdevice" in the "Reference Guide (Command/XML) CE"

Confirming Results of Script Execution

In order to check the progress of script execution and any errors in a script, create the script so that process content is logged to an arbitrary file.
Refer to the contents of the output log file to confirm results of script execution.
Sample scripts generate logs in the folder where rulesets are placed to provide reference information for infrastructure administrators.
When checking the content, copy the log file to an arbitrary user directory and then open the copied log file.

About log file name sample scripts output, refer to "G.5.4 Log Files of Sample Script".

Note

- The above log file is used when infrastructure administrators check script action. Use of this log file by tenant users and administrators has not been considered. Accordingly, there is no protection between tenants.
- Do not perform standard output or standard error output of script execution results, except for script files used by the rulesets for operations. If scripts which perform standard output or standard error output are used, automatic network device configuration may be aborted.
- To perform standard output and standard error output of script execution results using the script files used by a ruleset for operations, it is necessary to specify the same processing method as the one used in the sample script. If you create and use an original processing method for standard output and standard error output, the execution result of the scripts for operations cannot be obtained and L-Platform operations may fail.

F.6.3 Command File

This section explains the format of command files.

Format

```
Command for Network Device
.....
Command for Network Device
```

Only include commands for the target network device in the command file.

Information

- Command format depends on the type of network device.
- When creating scripts referring to sample scripts, initial commands executed after logging in to a network device depend on the type of network device. So, it is necessary to change the initial commands and their responses in the script.
- If the structure of a script is same as that of a sample script, commands in the command file are executed after the execution of initial commands.

Creation example

```
class-map match-all %classmapname%
match source-address ip %ip%
match source-port %port%
match destination-address ip %Unm_IPv4& LServer_name&network_resource_name %
match destination-port %serverport%
...
interface %ifname%
rule access %num% in %classmapname% accept audit-session-norma audit-match-none
...
```

```
commit
save startup-config
```

Point

- All variable information in a command file is within the conversion range and converted before script execution.
  About variable information which can be used, refer to "Variable Information Usable at Script".
- When not using any sample scripts (such as when the infrastructure administrator creates their own new script), create command files in the appropriate format for the created script.
- When scripts do not invoke command files, such as when not using sample scripts, it is no necessary to create a command file.

F.6.4 Parameter File

This section explains the format of the parameter file.

Format

The parameter file is in XML format.
Refer to "14.14 Parameter Files (for Scripts)" in the "Reference Guide (Command/XML) CE" for details.

F.6.5 Interface Configuration File

This section explains the format of the interface configuration file.

Format

The interface configuration file is in XML format.
Refer to "14.15 Network Device Interface Configuration File" in the "Reference Guide (Command/XML) CE" for details.

F.7 Network Device Automatic Configuration and Operation Definition File

The definition used for network device automatic configuration or operation can be changed by setting the value in the following definition file beforehand.

F.7.1 Storage Location of the Definition File

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

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

F.7.2 Definition File Name

unm_provisioning.rcxprop

F.7.3 Definition File Format

Script language

Specify the script language when you want to use a language other than ruby.

Information

Ruby is used as the script language in sample scripts.

Parameter Format of Definition Files

```
extension_EXTENSION=execution file path
```

Specify the extension of the script language such as "rb" or "pl" for *EXTENSION*.

When there is no specification for the *EXTENSION* jruby is used.

Execution file path specifies the absolute path.

Example

```
extension_rb=/usr/bin/jruby
```

Monitoring Time of Script

Specify the monitoring time when you want to change it to a value besides 300(s).

Information

In the network device automatic configuration function, script execution time is monitored.
When the monitoring time has passed since the beginning of the script execution, the processing of the script is terminated.

Parameter Format of Definition Files

```
EXECUTE_TIMEOUT=monitoring time
```

Specify the *monitoring time* within the range of 1 to 7200(s).

When the specified value is non-numeric or is outside of the above mentioned range, 300(s) is used.

Example

```
EXECUTE_TIMEOUT=600
```

Upper output limit of operation ruleset

Specify the upper output limit of operation ruleset when you want to change it to a value besides 500(Kbyte).

Information

When a large amount of data is output as a result of executing a ruleset for operations on network devices, a large amount of memory resources is consumed. By customizing the upper output limit, the memory consumption can be limited.

Parameter Format of Definition Files

```
SCRIPT_OUTPUT_SIZE_LIMIT= upper output limit
```

Specify the *upper output limit* within the range of 1-1000(Kbyte).

When the specified value is non-numeric or is outside the range mentioned above, 500 (KB) is used.

Example

```
SCRIPT_OUTPUT_SIZE_LIMIT=300
```

Appendix G Sample Script for Automatic Configuration and Operation of Network Devices

This section explains about sample scripts provided by Resource Orchestrator for automatic configuration and operation of network devices.

G.1 Sample List

Sample scripts are provided as rulesets. The following table shows the list of rulesets.

Table G.1 Rulesets list which is provided as sample scripts

Ruleset Name	Use	
3Tier_system_firewall--IPCOMSC1	For deploying firewalls (IPCOM EX series)	For IPCOM EX SC
3Tier_system_firewall--IPCOMSC2		
3Tier_system_firewall--IPCOMSC3		
3Tier_system_firewall--IPCOMIN2		For IPCOM EX IN
3Tier_system_firewall--IPCOMIN3		
FW_of_3Tier_sys--NSAppliance1	For deploying firewalls (NSAppliance)	For NSAppliance
FW_of_3Tier_sys--NSAppliance2		
3Tier_system_firewall--ASA1	For deploying firewalls (ASA5500 series)	For ASA5500
3Tier_system_firewall--ASA2		
3Tier_system_firewall--ASA3		
SLB_with_SSL-ACC--IPCOM1	For deploying firewall and server load balancer (IPCOM EX IN series)	For deploying IPCOM EX IN series as server load balancer
SLB_without_SSL-ACC--IPCOM1		
FW_of_3Tier_sys_inc_SLB--IPCOM1		For deploying IPCOM EX IN series as firewall
FW_of_3Tier_sys_inc_SLB--IPCOM2		
FW_of_3Tier_sys_inc_SLB--IPCOM3		
SLB_with_SSL-ACC--BIGIP1	For deploying firewall or server load balancer (combination of ASA5500 series and BIG-IP LTM series)	For deploying BIG-IP LTM series as server load balancer
SLB_without_SSL-ACC--BIGIP1		
FW_of_3Tier_sys_inc_SLB--ASA1		For deploying ASA5500 series as firewall(for ASA5500)
FW_of_3Tier_sys_inc_SLB--ASA2		
FW_of_3Tier_sys_inc_SLB--ASA3		
SLB_with_SSL-ACC--BIGIP2	For deploying server load balancers (BIG-IP LTM series)	For BIG-IP LTM series
SLB_without_SSL-ACC--BIGIP2		
tag_vlan_net--SR-X300tag_vlan_net--SR-X300_n or tag_vlan_net--SR-X300tag_vlan_net--SR-X300_n	For deploying L2 switches (the folder common to network devices)	For SR-X300
tag_vlan_port--SR-X300tag_vlan_port--SR-X300_n or tag_vlan_port--SR-X300tag_vlan_port--SR-X300_n	For deploying L2 switches (the folder for the particular network device)	
untag_vlan_net--SR-X300untag_vlan_net--SR-X300_n or	For deploying L2 switches (the folder common to network devices)	

untag_vlan_port--SR-X300untag_vlan_port--SR-X300_n		
untag_vlan_port--SR-X300untag_vlan_port--SR-X300_n or untag_vlan_port--SR-X300untag_vlan_port--SR-X300_n	For deploying L2 switches (the folder for the particular network device)	
tag_vlan_net--SR-X500tag_vlan_net--SR-X500_n or tag_vlan_net--SR-X500tag_vlan_net--SR-X500_n	For deploying L2 switches (the folder common to network devices)	For SR-X500
tag_vlan_port--SR-X500tag_vlan_port--SR-X500_n or tag_vlan_port--SR-X500tag_vlan_port--SR-X500_n	For deploying L2 switches (the folder for the particular network device)	
untag_vlan_net--SR-X500untag_vlan_net--SR-X500_n or untag_vlan_net--SR-X500untag_vlan_net--SR-X500_n	For deploying L2 switches (the folder common to network devices)	
untag_vlan_port--SR-X500untag_vlan_port--SR-X500_n or untag_vlan_port--SR-X500untag_vlan_port--SR-X500_n	For deploying L2 switches (the folder for the particular network device)	
tag_vlan_net--Catalysttag_vlan_net--Catalystn or tag_vlan_net--Catalysttag_vlan_net--Catalystn	For deploying L2 switches (the folder common to network devices)	For Catalyst
tag_vlan_port--Catalysttag_vlan_port--Catalystn or tag_vlan_port--Catalysttag_vlan_port--Catalystn	For deploying L2 switches (the folder for the particular network device)	
untag_vlan_net--Catalystuntag_vlan_net--Catalystn or untag_vlan_net--Catalystuntag_vlan_net--Catalystn	For deploying L2 switches (the folder common to network devices)	
untag_vlan_port--Catalystuntag_vlan_port--Catalystn or untag_vlan_port--Catalystuntag_vlan_port--Catalystn	For deploying L2 switches (the folder for the particular network device)	
SLB_server_disable--IPCOM SLB_server_enable--IPCOM SLB_vserver_status--IPCOM SLB_vserver_statistics--IPCOM	For operating server load balancers	For operating IPCOM EX IN series
SLB_server_disable--BIGIP SLB_server_enable--BIGIP SLB_vserver_status--BIGIP		For operating BIG-IP LTM series

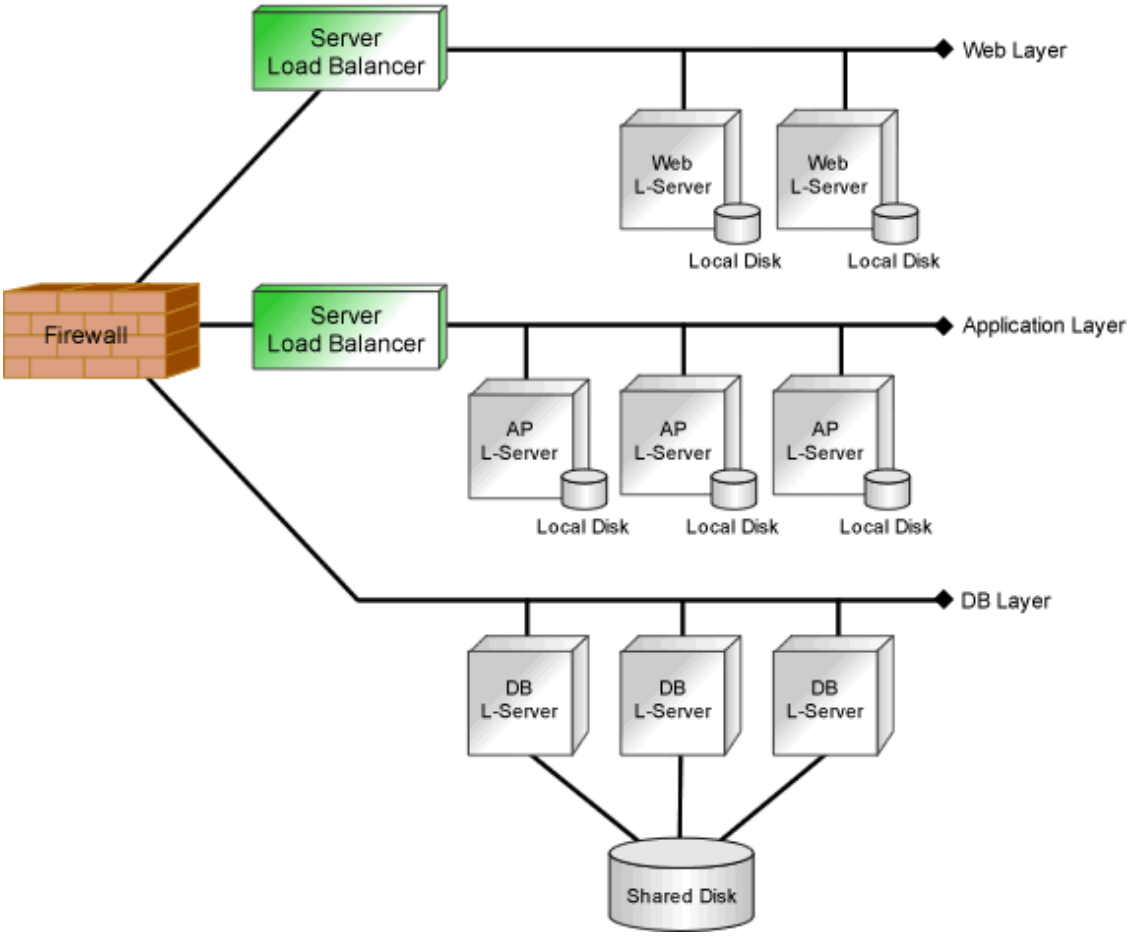
n: Number of "2" or larger

G.2 Relationship between Logical Network Configuration and Sample Script

This section explains about relationship between logical network configuration and sample script.

The following figure shows an example logical network configuration.

Figure G.1 An example logical network configuration



Information

The example logical network configuration explained above includes both firewall and server load balancer.
Other possible logical network configurations are as follows:

- Configuration includes firewalls, but does not include server load balancers.
- Configuration includes server load balancers, but does not include firewalls.

G.2.1 Rulesets that can be used for Automatic Configuration of Logical Network Configurations including both Firewall and Server Load Balancer

This section explains about rulesets used for automatic configuration of logical network configurations including both firewall and server load balancer.

When using the IPCOM EX IN series

- For Firewall

Ruleset name	Target model	Remarks
FW_of_3Tier_sys_inc_SLB--IPCOM1	IPCOMEX2000A_IN IPCOMEX2300_IN	Non-Redundant LAN Channels
FW_of_3Tier_sys_inc_SLB--IPCOM2	IPCOMEX2000A_IN IPCOMEX2300_IN	Redundant LAN Channels
FW_of_3Tier_sys_inc_SLB--IPCOM3	IPCOMEX2500_IN	

- For Server Load Balancer

Ruleset name	Remarks
SLB_with_SSL-ACC--IPCOM1	With SSL accelerator
SLB_without_SSL-ACC--IPCOM1	Without SSL accelerator

When using ASA5500 series and BIG-IP LTM series

- For Firewall

Ruleset name	Target model
FW_of_3Tier_sys_inc_SLB--ASA1	ASA5510
FW_of_3Tier_sys_inc_SLB--ASA2	ASA5520 ASA5540 ASA5550
FW_of_3Tier_sys_inc_SLB--ASA3	ASA5580

- For Server Load Balancer

Ruleset name	Remarks
SLB_with_SSL-ACC--BIGIP1	With SSL accelerator
SLB_without_SSL-ACC--BIGIP1	Without SSL accelerator

G.2.2 Rulesets that can be used for automatic configuration of logical network configurations including only Firewall

This section explains about rulesets used for automatic configuration of logical network configurations including only firewall.

When using IPCOM EX SC series

Ruleset name	Target model
3Tier_system_firewall--IPCOMSC1	IPCOMEX1100_SC IPCOMEX1300_SC IPCOMEX2000A_SC
3Tier_system_firewall--IPCOMSC2	IPCOMEX2000A_SC IPCOMEX2300_SC
3Tier_system_firewall--IPCOMSC3	IPCOMEX2500_SC

When using IPCOM EX IN series

Ruleset name	Target model
3Tier_system_firewall--IPCOMIN2	IPCOMEX2000A_IN IPCOMEX2300_IN
3Tier_system_firewall--IPCOMIN3	IPCOMEX2500_IN

When using NSAppliance

Ruleset name	Remarks
FW_of_3Tier_sys--NSAppliance1	For network configuration including customer firewalls
FW_of_3Tier_sys--NSAppliance2	For network configuration not including customer firewalls

When using ASA5500 series

Ruleset name	Target model
3Tier_system_firewall--ASA1	ASA5510
3Tier_system_firewall--ASA2	ASA5520 ASA5540 ASA5550
3Tier_system_firewall--ASA3	ASA5580

G.2.3 Rulesets that can be used for automatic configuration of logical network configurations including only Server Load Balancer

This section explains about ruleset used for automatic configuration of logical network configurations including only server load balancer.

When using BIG-IP LTM series

Ruleset name	Remarks
SLB_with_SSL-ACC--BIGIP2	With SSL accelerator
SLB_without_SSL-ACC--BIGIP2	Without SSL accelerator

G.2.4 Rulesets that can be used for Automatic Configuration of all Logical Network Configurations

This section explains about rulesets used for automatic configuration of L2 switches. Though L2 switches do not appear on logical network configuration, the configuration of the L2 switches are required to connect firewall, server load balancer and L-Server.

For SR-X300

Ruleset name	Remarks
tag_vlan_net--SR-X300tag_vlan_net--SR-X300_n and tag_vlan_port--SR-X300tag_vlan_port--SR-X300_n	For tagged VLAN network
tag_vlan_net--SR-X300tag_vlan_net--SR-X300_n and tag_vlan_port--SR-X300tag_vlan_port--SR-X300_n	
untag_vlan_net--SR-X300untag_vlan_net--SR-X300_n and untag_vlan_port--SR-X300untag_vlan_port--SR-X300_n	For untagged VLAN network
untag_vlan_net--SR-X300untag_vlan_net--SR-X300_n and untag_vlan_port--SR-X300untag_vlan_port--SR-X300_n	

n: Number of "2" or larger

For SR-X500

Ruleset name	Remarks
tag_vlan_net--SR-X500tag_vlan_net--SR-X500_n and tag_vlan_port--SR-X500tag_vlan_port--SR-X500_n	For tagged VLAN network
tag_vlan_net--SR-X500tag_vlan_net--SR-X500_n and tag_vlan_port--SR-X500tag_vlan_port--SR-X500_n	
untag_vlan_net--SR-X500untag_vlan_net--SR-X500_n and untag_vlan_port--SR-X500untag_vlan_port--SR-X500_n	For untagged VLAN network
untag_vlan_net--SR-X500untag_vlan_net--SR-X500_n and untag_vlan_port--SR-X500untag_vlan_port--SR-X500_n	

n: Number of "2" or larger

For Catalyst

Ruleset name	Remarks
tag_vlan_net--Catalysttag_vlan_net--Catalystn and tag_vlan_port--Catalysttag_vlan_port--Catalystn	For tagged VLAN network
tag_vlan_net--Catalysttag_vlan_net--Catalystn and tag_vlan_port--Catalysttag_vlan_port--Catalystn	
untag_vlan_net--Catalystuntag_vlan_net--Catalystn and untag_vlan_port--Catalystuntag_vlan_port--Catalystn	For untagged VLAN network
untag_vlan_net--Catalystuntag_vlan_net--Catalystn and untag_vlan_port--Catalystuntag_vlan_port--Catalystn	

n: Number of "2" or larger

G.2.5 Rulesets for Operating Server Load Balancers

This section explains about rulesets used for operation of server load balancers deployed on logical network configuration.

When server load balancers are deployed, the rulesets are available for the server load balancers without depending on logical network configuration.

When using IPCOM EX IN series

Ruleset name	Remarks
SLB_server_disable--IPCOM	Remove a server from load balancing group
SLB_server_enable--IPCOM	Add a server to load balancing group
SLB_vserver_status--IPCOM	Show load balance status of the server load balancer rule
SLB_vserver_statistics--IPCOM	Collect load balance statistics information about a server load balancing rule

When using BIG-IP LTM series

Ruleset name	Remarks
SLB_server_disable--BIGIP	Disable pool member
SLB_server_enable--BIGIP	Enable pool member
SLB_vserver_status--BIGIP	Collect status and statistics information about virtual server and pool member

G.3 Sample Scripts(For automatic configuration)

Sample scripts to be used for automatic configuration of network devices are registered in the following folder when Resource Orchestrator is installed.

[Windows Manager]
Installation_folder\SVROR\Manager\etc\scripts\original*vendor_name**unit_name*\rulesets*ruleset_name*\
Installation_folder\SVROR\Manager\etc\scripts\original\network_resource*ruleset_name*\

[Linux Manager]
/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 G.2 Units for which Sample Scripts are Provided

Vendor	Unit Name	Type	Setting Details
Fujitsu	SR-X500	L2 switch	[When creating network resource by Resource Orchestrator] - Add VLAN to interface (tagged VLAN, port VLAN) or - Add VLAN to LAG interface (tagged VLAN, port VLAN) [When deleting network resource] - Delete VLAN of interface (tagged VLAN, port VLAN) or - Delete VLAN of LAG interface (tagged VLAN, port VLAN)
	SR-X300		

	IPCOMEXSC	Firewall
		(*1)
			[When creating L-Platform]
			- External interface (center switch side)
			  - Add Firewall rules
			- Internal interface (L2 switches)
			  - Add VLAN interface
			  - Add Firewall rules
			[When modifying firewall configurations of L-Platform]
			- External interface (center switch side)
			  - Change Firewall rules

	IPCOMEXIN		
	NSAppliance		

Vendor	Unit Name	Type	Setting Details
			- Add dstNAT rules - Add srcNAT rules - Internal interface (L2 switches) - Change Firewall rules [When deleting L-Platform] - External interface (center switch side) - Delete Firewall rules - Delete dstNAT rules - Delete srcNAT rules - Internal interface (L2 switches) - Delete VLAN interface - Delete Firewall rules
	IPCOMEXIN	Server load balancer (*3)	[When creating L-Platform] - No operation [When modifying server load balancer configurations of L-Platform] - Add Server load balancer rules - Add SSL accelerator configurations [When deleting L-Platform] - Delete Server load balancer rules - Delete SSL accelerator configurations
Cisco	Catalyst	L2 switch	[When creating network resource] - Add VLAN to interface (tagged VLAN, port VLAN) or - Add VLAN to LAG interface (tagged VLAN, port VLAN) [When deleting network resource] - Delete VLAN of interface (tagged VLAN, port VLAN) or - Delete VLAN of LAG interface (tagged VLAN, port VLAN)
	ASA5500	Firewall (*1)	[When creating L-Platform] - External interface (center switch side) - Add Firewall rules - Add dstNAT rules - Add srcNAT rules - Internal interface (L2 switches) - Add VLAN interface - Add Firewall rules [When modifying firewall configurations of L-Platform]

Vendor	Unit Name	Type	Setting Details

			- External interface (center switch side)
			  - Change Firewall rules
			  - Change dstNAT rules
			  - Chande srcNAT rules
			- Internal interface (L2 switches)
			  - Change Firewall rules
			[When deleting L-Platform]
			- External interface (center switch side)
			  - Delete Firewall rules
			  - Delete dstNAT rules
			  - Delete srcNAT rules
			- Internal interface (L2 switches)
			  - Delete VLAN interface
			  - Delete Firewall rules

F5 Networks	BIG-IP (*2)	Server load balancer (*3)	[When creating L-Platform] - Add VLAN interface [When modifying server load balancer configurations of L-Platform] - Add VLAN interface - Add Server load balancer rules - Add SSL accelerator configurations [When deleting L-Platform] - Delete VLAN interface - Delete Server load balancer rules - Delete SSL accelerator configurations

*1: Firewall rules are configured for public LAN connection.
*2: Network device name of BIG-IP LTM series are regarded as "BIG-IP".
*3: Server load balancer rules are configured for public LAN connection.

Information

When using sample scripts provided by Resource Orchestrator, protocols used for automatic configuration and network device names are as follows:

Sample script uses those protocols when connecting to network device.

- With TELNET protocol
  - SR-X300/SR-X500
  - IPCOMEXSC/IPCOMEXIN
  - NSAppliance
  - Catalyst

  - ASA5500
- With SSH protocol
  - BIG-IP

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.

G.3.1 Preparations for using sample scripts

This section explains about preparations for using sample scripts for automatic configurations of network devices.

- For ruleset, It is necessary to register a folder created using the "Vendor" and "Unit Name" described in "Table G.2 Units for which Sample Scripts are Provided". If the necessary sample scripts are not registered in the folder, the sample scripts registered when this product was installed will be copied.
- It is required to change the following files based on your system configuration.
  - Parameter Files (for Scripts)

    For information about parameter files, refer to "14.14 Parameter Files (for Scripts)" in the "Reference Guide (Command/XML) CE".
  - Network Device Interface Configuration File

    For information about interface configuration of network devices, refer to "14.15 Network Device Interface Configuration File" in the "Reference Guide (Command/XML) CE".
- It is necessary to customize parameter of sample scripts for deploying L2 switch according to model configuration.
  For information about customization refer to explanation of each ruleset
- When using BIG-IP LTM series, it is necessary to prepare SSH environment.
  Refer to "F.2.1 When Connecting to Network Device with SSH" for more information.

G.3.2 A Class of Sample Scripts

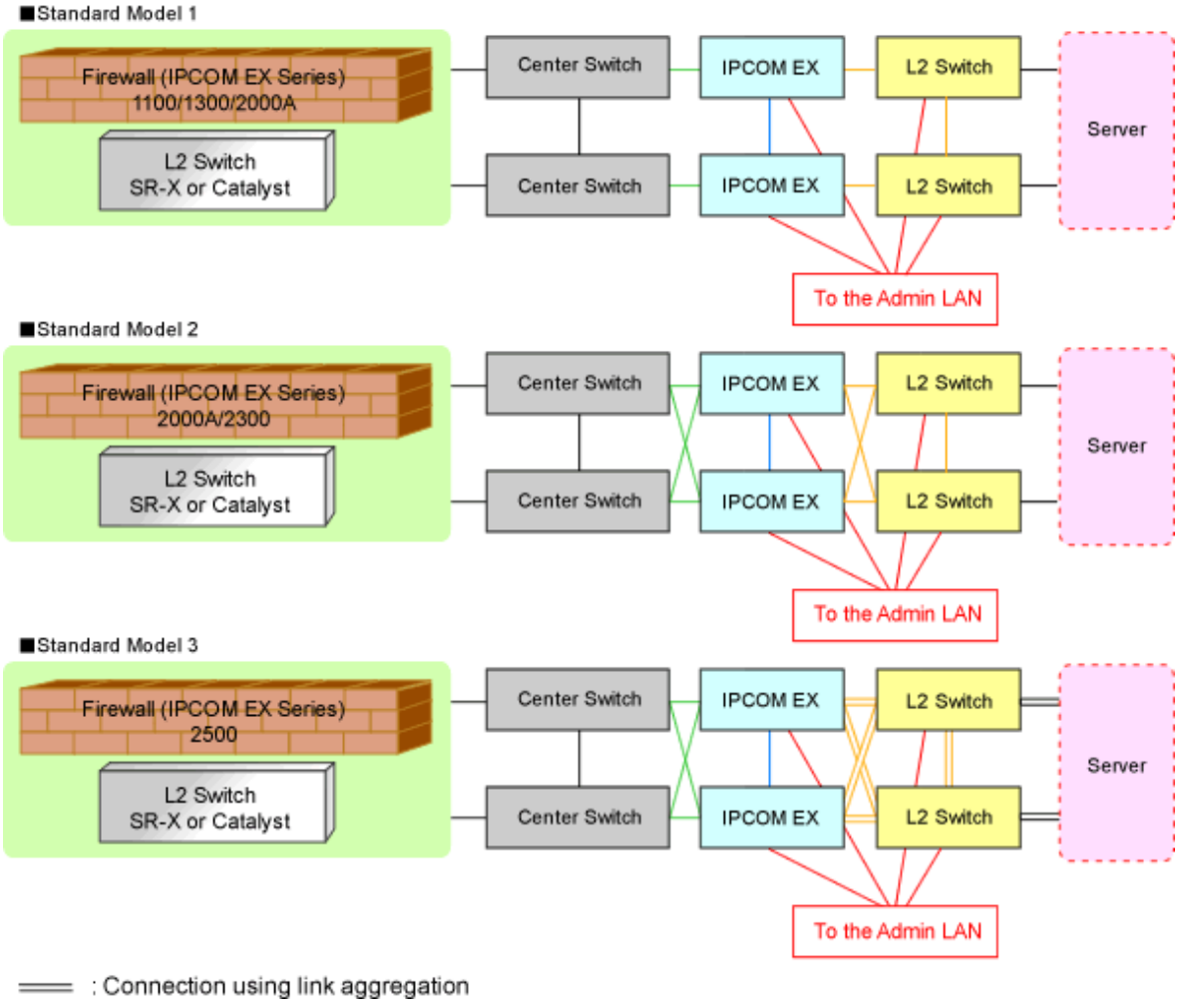
This section explains about sample scripts according to the following list.

- G.3.3 For deploying firewalls(for IPCOM EX series)
- G.3.4 For deploying firewalls(for NSAppliance)
- G.3.5 For deploying firewalls(for ASA5500 series)
- G.3.6 For deploying firewall and server load balancer(for IPCOM EX IN series)
- G.3.7 For deploying firewall and server load balancer(for combination of ASA5500 series and BIG-IP LTM series)
- G.3.8 For deploying server load balancers(BIG-IP LTM series)
- G.3.9 For deploying L2 Switches

G.3.3 For deploying firewalls(for IPCOM EX series)

Standard model configurations of sample script are as follows:

Figure G.2 Standard model configurations of sample script(firewalls: IPCOM EX series)



Listed below are sample ruleset names provided by Resource Orchestrator:

For IPCOM EX SC

3Tier_system_firewall--IPCOMSC1

It is used IPCOM EX SC series as a firewall for 3 tier models.
For the systems that use IPCOMEX1100_SC/1300_SC/200A_SC

Adaptive model configuration: Standard Model 1

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

It is used IPCOM EX SC series as a firewall for 3 tier models.
For the systems that use IPCOMEX2000A_SC/2300_SC

Adaptive model configuration: Standard Model 2

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

It is used IPCOM EX SC series as a firewall for 3 tier models.
For the systems that use IPCOMEX2500_SC

Adaptive model configuration: Standard Model 3

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

It is used IPCOM EX IN series as a firewall for 3 tier models.
For the systems that use IPCOMEX2000A_IN/2300_IN

Adaptive model configuration: Standard Model 2

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

It is used IPCOM EX IN series as a firewall for 3 tier models.
For the systems that use IPCOMEX2500_IN

Adaptive model configuration: Standard Model 3

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

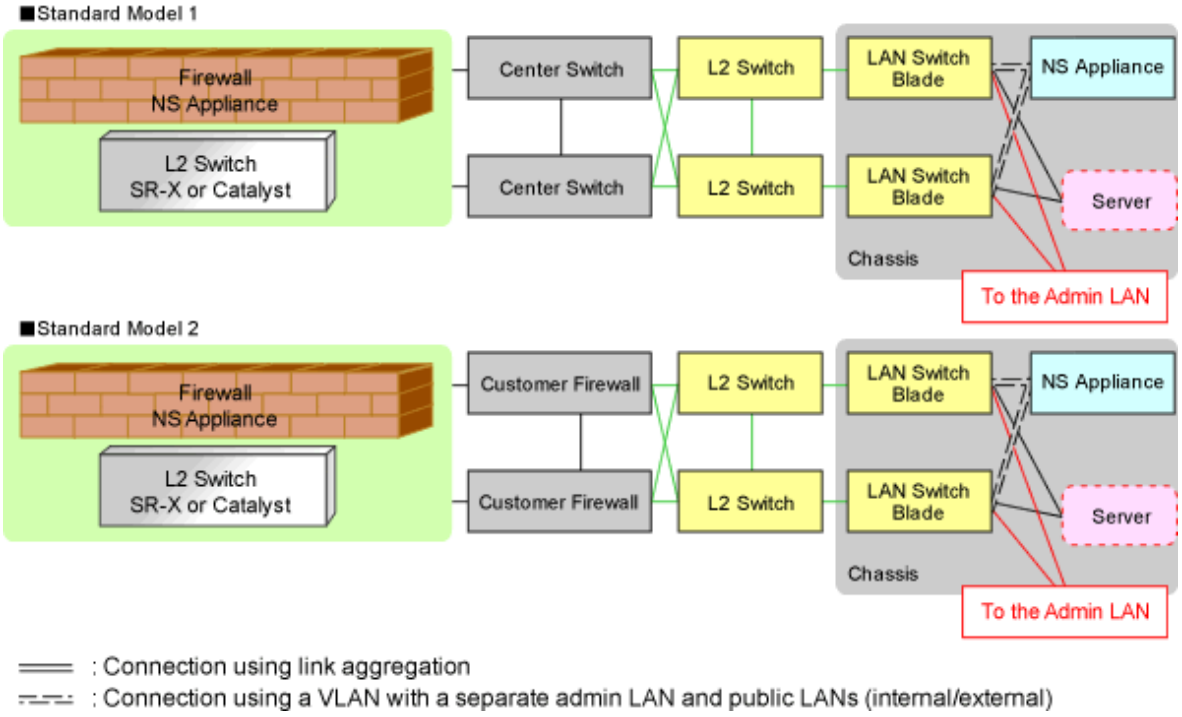
- For Unit Synchronization

  LAN1.3

G.3.4 For deploying firewalls(for NSAppliance)

The default model configuration assumed by a sample script is given below:

Figure G.3 Standard model configurations of sample script(NSAppliance)



Listed below are sample ruleset names provided by Resource Orchestrator:

For NS Appliance

FW_of_3Tier_sys--NSAppliance1

For a system that uses NS Appliance with a 3Tier model

Adaptive model configuration: Standard Model 2

LAN Ports to be Used

- For Public LANs (Customer Firewall Side)

  LAN0.0

- For Public LANs (L2 Switch Side)

  LAN0.1

- For the Admin LAN

  LAN0.3

FW_of_3Tier_sys--NSAppliance2

For a system that uses NS Appliance with a 3Tier model

Adaptive model configuration: Standard Model 1

LAN Ports to be Used

- For Public LANs (Center Switch Side)

  LAN0.0

- For Public LANs (L2 Switch Side)

  LAN0.1

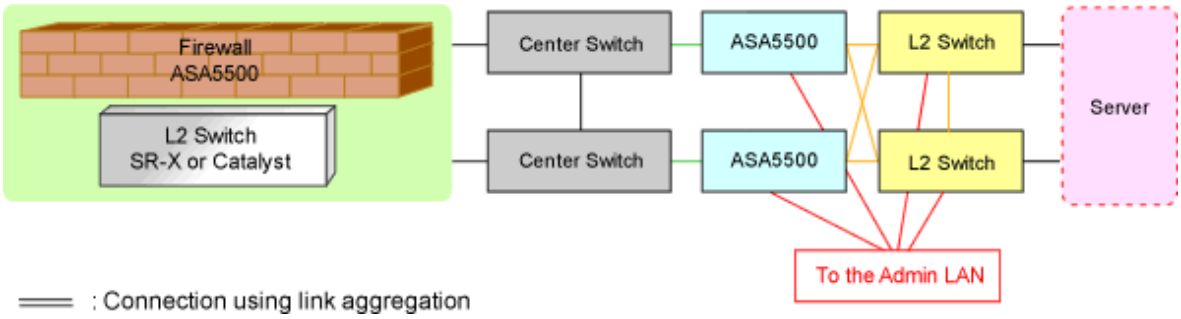
- For the Admin LAN

  LAN0.3

G.3.5 For deploying firewalls(for ASA5500 series)

The default model configuration assumed by a sample script is given below:

Figure G.4 Standard model configurations of sample script(ASA5500 series)



Listed below are sample ruleset names provided by Resource Orchestrator:

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)

  ethernet0/0

- For Public LANs (L2 Switch Side)

  redundant1: Redundant LAN Channels

  - ethernet0/1
  - ethernet0/2

- For the Admin LAN

  management0/0

- For Unit Synchronization

  ethernet0/3

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)

  gigabitethernet0/0

- For Public LANs (L2 Switch Side)

  redundant1: Redundant LAN Channels

  - gigabitethernet0/1
  - gigabitethernet0/2

- For the Admin LAN

  management0/0

- For Unit Synchronization

  gigabitethernet0/3

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)

  gigabitethernet3/0

- For Public LANs (L2 Switch Side)

  redundant1: Redundant LAN Channels

  - gigabitethernet3/1
  - gigabitethernet3/2

- For the Admin LAN

  management0/0

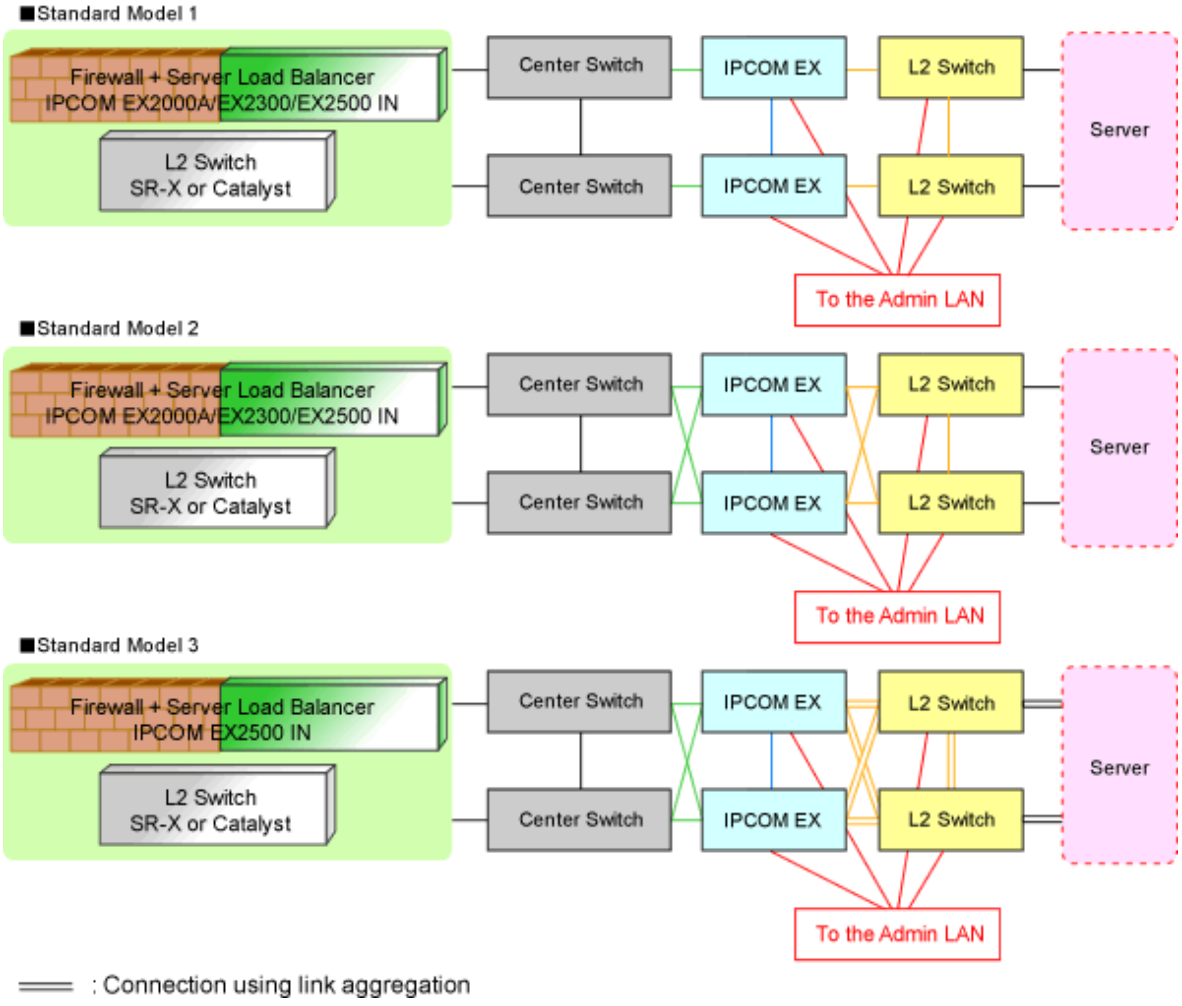
- For Unit Synchronization

  gigabitethernet3/3

G.3.6 For deploying firewall and server load balancer(for IPCOM EX IN series)

The default model configuration assumed by a sample script is given below:

Figure G.5 Standard model configurations of sample script(firewall and server load balancer: IPCOM EX IN series)



When single IPCOM EX IN series is used as both firewall and server load balancer for tier models in the system, firewall rulesets are used together with server load balancer rulesets.

Listed below are sample ruleset names provided by Resource Orchestrator:

For deploying IPCOM EX IN series as server load balancers

SLB_with_SSL-ACC--IPCOM1

For the systems that use IPCOM EX IN series for server load balancers(with SSL accelerator).

Adaptive model configuration: all standard models

LAN Ports to be Used

Port is determined by sample script(FW_of_3Tier_sys_inc_SLB--IPCOM*n*).

SLB_without_SSL-ACC--IPCOM1

For the systems that use IPCOM EX IN series for server load balancers(without SSL accelerator).

Adaptive model configuration: all standard models

LAN Ports to be Used

Port is determined by sample script(FW_of_3Tier_sys_inc_SLB--IPCOM*n*).

n: Number within 1 - 3

For deploying IPCOM EX IN series as firewalls

FW_of_3Tier_sys_inc_SLB--IPCOM1

For the systems that use IPCOMEX2000A_IN/2300_IN(Non-Redundant LAN Channels).

Adaptive model configuration: Standard Model 1

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

FW_of_3Tier_sys_inc_SLB--IPCOM2

For the systems that use IPCOMEX2000A_IN/2300_IN(Redundant LAN Channels).

Adaptive model configuration: Standard Model 2

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

FW_of_3Tier_sys_inc_SLB--IPCOM3

For the systems that use IPCOMEX2500_IN.

Adaptive model configuration: Standard Model 3

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

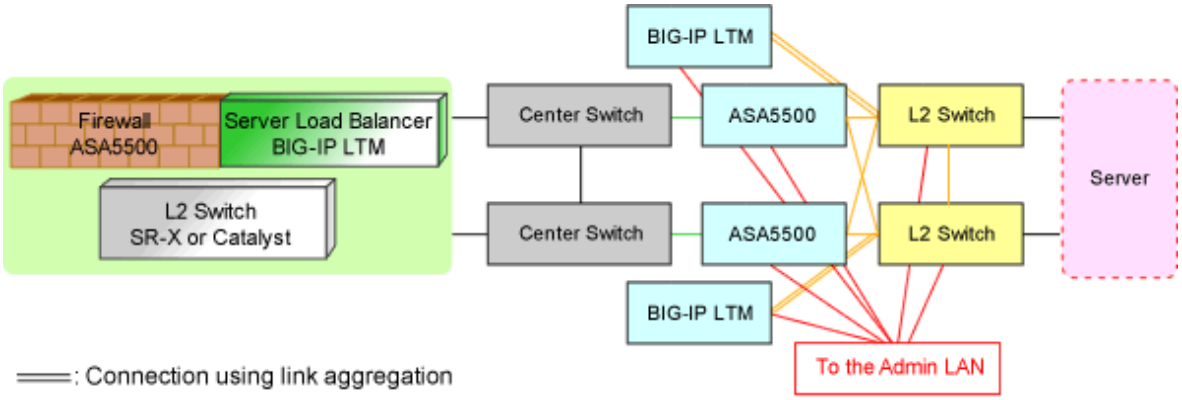
- For Unit Synchronization

  LAN1.3

G.3.7 For deploying firewall and server load balancer(for combination of ASA5500 series and BIG-IP LTM series)

The default model configuration assumed by a sample script is given below:

Figure G.6 Default Model Configuration for a Sample Script(firewall and server load balancer: ASA5500 series and BIG-IP LTM series)



When the combination of ASA5500 series and BIG-IP LTM series are used as firewall and server load balancer for tier models in the system, firewall rulesets are used together with server load balancer rulesets.

Listed below are sample ruleset names provided by Resource Orchestrator:

For deploying BIG-IP LTM series as server load balancers

SLB_with_SSL-ACC--BIGIP1

For the systems that use BIG-IP LTM series for server load balancers(using SSL accelerator).

LAN Ports to be Used

- For Public LANs and Unit Synchronization

  mytrunk: Connection using Link aggregation

  - 1.1
  - 1.2

- For the Admin LAN

  mgmt

SLB_without_SSL-ACC--BIGIP1

For the systems that use BIG-IP LTM series for server load balancers(without SSL accelerator).

LAN Ports to be Used

- For Public LANs and Unit Synchronization

  mytrunk: Connection using Link aggregation

  - 1.1
  - 1.2

- For the Admin LAN

  mgmt

For deploying ASA5500 series(for ASA5500) as firewalls

FW_of_3Tier_sys_inc_SLB--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)

  ethernet0/0

- For Public LANs (L2 Switch Side)

  redundant1: Redundant LAN Channels

  - ethernet0/1
  - ethernet0/2

- For the Admin LAN

  management0/0

- For Unit Synchronization

  ethernet0/3

FW_of_3Tier_sys_inc_SLB--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)

  gigabitethernet0/0

- For Public LANs (L2 Switch Side)

  redundant1: Redundant LAN Channels

  - gigabitethernet0/1
  - gigabitethernet0/2

- For the Admin LAN

  management0/0

- For Unit Synchronization

  gigabitethernet0/3

FW_of_3Tier_sys_inc_SLB--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)

  gigabitethernet3/0

- For Public LANs (L2 Switch Side)

  redundant1: Redundant LAN Channels

  - gigabitethernet3/1
  - gigabitethernet3/2

- For the Admin LAN

  management0/0

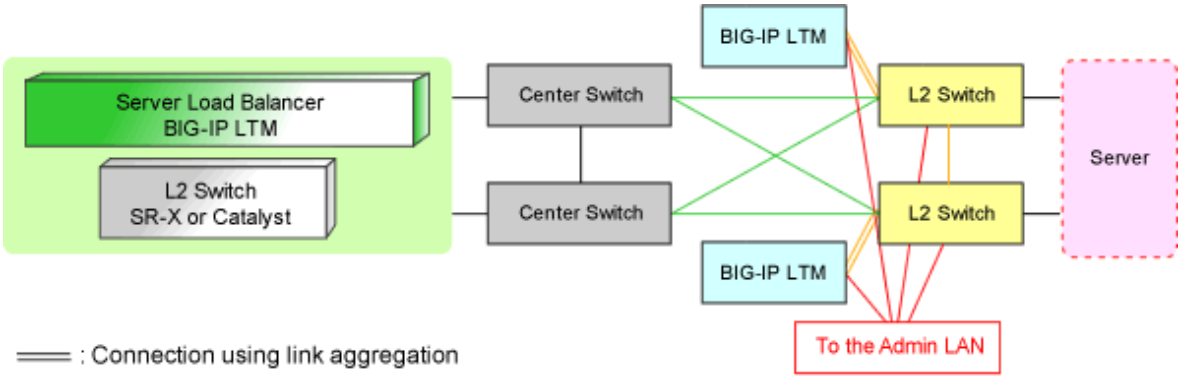
- For Unit Synchronization

  gigabitethernet3/3

G.3.8 For deploying server load balancers(BIG-IP LTM series)

The default model configuration assumed by a sample script is given below:

Figure G.7 Standard model configurations of sample script(server load balancers:BIG-IP LTM series)



Listed below are sample ruleset names provided by Resource Orchestrator:

For the BIG-IP LTM Series

SLB_with_SSL-ACC--BIGIP2

For the systems that use BIG-IP LTM series as server load balancers(with SSL accelerator)

LAN Ports to be Used

- For Public LANs and Unit Synchronization

  mytrunk: Connection using Link aggregation

  - 1.1
  - 1.2

- For the Admin LAN

  mgmt

SLB_without_SSL-ACC--BIGIP2

For the systems that use BIG-IP LTM series as server load balancers(without SSL accelerator)

LAN Ports to be Used

- For Public LANs and Unit Synchronization

  mytrunk: Connection using Link aggregation

- 1.1
- 1.2

- For the Admin LAN

  mgmt

G.3.9 For deploying L2 Switches

Resource Orchestrator provides sample rulesets for the L2 switch used in the standard model in which firewall and server load balancer are used. The sample ruleset names are shown below.

For SR-X300

tag_vlan_net--SR-X300
tag_vlan_net--SR-X300_*n*

For system that sets tagged VLAN network
Tagged VLAN is set to port by using tag_vlan_port--SR-X300 or tag_vlan_port--SR-X300_*n*.
Register this ruleset in the ruleset registration folder common to network devices.

Parameters need to be customized

The target of customizing is a parameter in all the related script list.
The list of parameters needs to be customized is shown.

Table G.3 The list of parameters needs to be customized (For SR-X300 tagged VLAN setting)

Parameter	Details of Modification	Ruleset name
node operand:	Change this to the network device name of the L2 switch registered in Resource Orchestrator.	tag_vlan_net--SR-X300 tag_vlan_net--SR-X300_*n*
%UP_PORT1%	Change this to the physical port number connected to the firewall or the server load balancer. When there are some physical ports connected to servers or server load balancers, change sample script.	tag_vlan_net--SR-X300
	Change this to the physical port number connected to the "Active" side of the firewall or the server load balancer of the redundant configuration. When there are some physical ports connected to servers or server load balancers, change sample script.	tag_vlan_net--SR-X300_2
	Change this to the physical port number of LAG connected to the "Active" side of the firewall or the server load balancer of the redundant configuration. When there are some physical ports connected to servers or server load balancers, change sample script.	tag_vlan_net--SR-X300_3
%UP_PORT2%	Change this to the physical port number connected to the "Standby" side of the firewall or the server load balancer of the redundant configuration. When there are some physical ports connected to servers or server load balancers, change sample script.	tag_vlan_net--SR-X300_2
	Change this to the physical port number of LAG connected to the "Active" side of the firewall or the server load balancer of the redundant configuration. Note that this port number must not be equal to that of %UP_PORT1%. When there are some physical ports connected to servers or server load balancers, change sample script.	tag_vlan_net--SR-X300_3

%UP_PORT3%	Change this to the physical port number of LAG connected to the "Standby" side of the firewall or the server load balancer of the redundant configuration. When there are some physical ports connected to servers or server load balancers, change sample script.	tag_vlan_net--SR-X300_3
%UP_PORT4%	Change this to the physical port number of LAG connected to the "Standby" side of the firewall or the server load balancer of the redundant configuration. Note that this port number must not be equal to that of %UP_PORT3%. When there are some physical ports connected to servers or server load balancers, change sample script.	tag_vlan_net--SR-X300_3
%DOWN_PORT1%	Change this to the physical port number connected to the server. When there are some physical ports connected to servers, change sample script.	tag_vlan_net--SR-X300 tag_vlan_net--SR-X300_2
	Change this to the physical port number of LAG connected to the server.	tag_vlan_net--SR-X300_3
%DOWN_PORT2%	Change this to physical port number of LAG connected to the server. Note that this port number must not be equal to that of %DOWN_PORT1%. When there are several LAGs connected to the server, change sample script.	tag_vlan_net--SR-X300_3

tag_vlan_port--SR-X300
tag_vlan_port--SR-X300_*n*

For SR-X300 that sets tagged VLAN to the port connected to the firewall, the server load balancer, or the server
Register this ruleset in the specfic ruleset registration folder of the network device.

untag_vlan_net--SR-X300
untag_vlan_net--SR-X300_*n*

For system that sets untagged VLAN network
Port VLAN is set to port by using untag_vlan_port--SR-X300 or untag_vlan_port--SR-X300_*n*.
Register this ruleset in the ruleset registration folder common to network devices.

Parameters need to be customized

The target of customizing is a parameter in all the related script list.
The list of parameters needs to be customized is shown.

Table G.4 The list of parameters needs to be customized (For SR-X300 port VLAN setting)

Parameter	Details of Modification	Ruleset name
node operand:	Change this to the network device name of the L2 switch registered in Resource Orchestrator.	untag_vlan_net--SR-X300 untag_vlan_net--SR-X300_*n*
%UP_PORT1%	Change this to the physical port number connected to the firewall or the server load balancer. When there are some physical ports connected to servers or server load balancers, change sample script.	untag_vlan_net--SR-X300
	Change this to the physical port number connected to the "Active" side of the firewall or the server load balancer of the redundant configuration. When there are some physical ports connected to servers or server load balancers, change sample script.	untag_vlan_net--SR-X300_2

	Change this to the physical port number of LAG connected to the "Active" side of the firewall or the server load balancer of the redundant configuration. When there are some physical ports connected to servers or server load balancers, change sample script.	untag_vlan_net--SR-X300_3
%UP_PORT2%	Change this to the physical port number connected to the "Standby" side of the firewall or the server load balancer of the redundant configuration. When there are some physical ports connected to servers or server load balancers, change sample script.	untag_vlan_net--SR-X300_2
	Change this to the physical port number of LAG connected to the "Active" side of the firewall or the server load balancer of the redundant configuration. Note that this port number must not be equal to that of %UP_PORT1%. When there are some physical ports connected to servers or server load balancers, change sample script.	untag_vlan_net--SR-X300_3
%UP_PORT3%	Change this to the physical port number of LAG connected to the "Standby" side of the firewall or the server load balancer of the redundant configuration. When there are some physical ports connected to servers or server load balancers, change sample script.	untag_vlan_net--SR-X300_3
%UP_PORT4%	Change this to the physical port number of LAG connected to the "Standby" side of the firewall or the server load balancer of the redundant configuration. Note that this port number must not be equal to that of %UP_PORT3%. When there are some physical ports connected to servers or server load balancers, change sample script.	untag_vlan_net--SR-X300_3
%DOWN_PORT1%	Change this to the physical port number connected to the server. When there are some physical ports connected to servers, change sample script.	untag_vlan_net--SR-X300 untag_vlan_net--SR-X300_2
	Change this to the physical port number of LAG connected to the server.	untag_vlan_net--SR-X300_3
%DOWN_PORT2%	Change this to physical port number of LAG connected to the server. Note that this port number must not be equal to that of %DOWN_PORT1%. When there are several LAGs connected to the server, change sample script.	untag_vlan_net--SR-X300_3

untag_vlan_port--SR-X300
untag_vlan_port--SR-X300_*n*

For SR-X300 that sets port VLAN to the port connected to the firewall, the server load balancer, or the server
Register this ruleset in the specfic ruleset registration folder of the network device.

n: Number of "2" or larger

For SR-X500

tag_vlan_net--SR-X500
tag_vlan_net--SR-X500_*n*

For system that sets tagged VLAN network
Tagged VLAN is set to port by using tag_vlan_port--SR-X500 or tag_vlan_port--SR-X500_*n*.
Register this ruleset in the ruleset registration folder common to network devices.

Parameters need to be customized

The target of customizing is a parameter in all the related script list.
The list of parameters needs to be customized is shown.

Table G.5 The list of parameters needs to be customized (For SR-X500 tagged VLAN setting)

Parameter	Details of Modification	Ruleset name
node operand:	Change this to the network device name of the L2 switch registered in Resource Orchestrator.	tag_vlan_net--SR-X500 tag_vlan_net--SR-X500_*n*
%UP_PORT1%	Change this to the physical port number connected to the firewall or the server load balancer. When there are some physical ports connected to servers or server load balancers, change sample script.	tag_vlan_net--SR-X500
	Change this to the physical port number connected to the "Active" side of the firewall or the server load balancer of the redundant configuration. When there are some physical ports connected to servers or server load balancers, change sample script.	tag_vlan_net--SR-X500_2
	Change this to the physical port number of LAG connected to the "Active" side of the firewall or the server load balancer of the redundant configuration. When there are some physical ports connected to servers or server load balancers, change sample script.	tag_vlan_net--SR-X500_3
%UP_PORT2%	Change this to the physical port number connected to the "Standby" side of the firewall or the server load balancer of the redundant configuration. When there are some physical ports connected to servers or server load balancers, change sample script.	tag_vlan_net--SR-X500_2
	Change this to the physical port number of LAG connected to the "Active" side of the firewall or the server load balancer of the redundant configuration. Note that this port number must not be equal to that of %UP_PORT1%. When there are some physical ports connected to servers or server load balancers, change sample script.	tag_vlan_net--SR-X500_3
%UP_PORT3%	Change this to the physical port number of LAG connected to the "Standby" side of the firewall or the server load balancer of the redundant configuration. When there are some physical ports connected to servers or server load balancers, change sample script.	tag_vlan_net--SR-X500_3
%UP_PORT4%	Change this to the physical port number of LAG connected to the "Standby" side of the firewall or the server load balancer of the redundant configuration. Note that this port number must not be equal to that of %UP_PORT3%.	tag_vlan_net--SR-X500_3

	When there are some physical ports connected to servers or server load balancers, change sample script.	
%DOWN_PORT1%	Change this to the physical port number connected to the server. When there are some physical ports connected to servers, change sample script.	tag_vlan_net--SR-X500 tag_vlan_net--SR-X500_2
	Change this to the physical port number of LAG connected to the server.	tag_vlan_net--SR-X500_3
%DOWN_PORT2%	Change this to physical port number of LAG connected to the server. Note that this port number must not be equal to that of %DOWN_PORT1%. When there are several LAGs connected to the server, change sample script.	tag_vlan_net--SR-X500_3

tag_vlan_port--SR-X500
tag_vlan_port--SR-X500_*n*

For SR-X500 that sets tagged VLAN to the port connected to the firewall, the server load balancer, or the server
Register this ruleset in the specfic ruleset registration folder of the network device.

untag_vlan_net--SR-X500
untag_vlan_net--SR-X500_*n*

For system that sets untagged VLAN network
Port VLAN is set to port by using untag_vlan_port--SR-X500 or untag_vlan_port--SR-X500_*n*.
Register this ruleset in the ruleset registration folder common to network devices.

Parameters need to be customized

The target of customizing is a parameter in all the related script list.
The list of parameters needs to be customized is shown.

Table G.6 The list of parameters needs to be customized (For SR-X500 port VLAN setting)

Parameter	Details of Modification	Ruleset name
node operand:	Change this to the network device name of the L2 switch registered in Resource Orchestrator.	untag_vlan_net--SR-X500 untag_vlan_net--SR-X500_*n*
%UP_PORT1%	Change this to the physical port number connected to the firewall or the server load balancer. When there are some physical ports connected to servers or server load balancers, change sample script.	untag_vlan_net--SR-X500
	Change this to the physical port number connected to the "Active" side of the firewall or the server load balancer of the redundant configuration. When there are some physical ports connected to servers or server load balancers, change sample script.	untag_vlan_net--SR-X500_2
	Change this to the physical port number of LAG connected to the "Active" side of the firewall or the server load balancer of the redundant configuration. When there are some physical ports connected to servers or server load balancers, change sample script.	untag_vlan_net--SR-X500_3
%UP_PORT2%	Change this to the physical port number connected to the "Standby" side of the firewall or the server load balancer of the redundant configuration. When there are some physical ports connected to servers or server load balancers, change sample script.	untag_vlan_net--SR-X500_2

	Change this to the physical port number of LAG connected to the "Active" side of the firewall or the server load balancer of the redundant configuration. Note that this port number must not be equal to that of %UP_PORT1%. When there are some physical ports connected to servers or server load balancers, change sample script.	untag_vlan_net--SR-X500_3
%UP_PORT3%	Change this to the physical port number of LAG connected to the "Standby" side of the firewall or the server load balancer of the redundant configuration. When there are some physical ports connected to servers or server load balancers, change sample script.	untag_vlan_net--SR-X500_3
%UP_PORT4%	Change this to the physical port number of LAG connected to the "Standby" side of the firewall or the server load balancer of the redundant configuration. Note that this port number must not be equal to that of %UP_PORT3%. When there are some physical ports connected to servers or server load balancers, change sample script.	untag_vlan_net--SR-X500_3
%DOWN_PORT1%	Change this to the physical port number connected to the server. When there are some physical ports connected to servers, change sample script.	untag_vlan_net--SR-X500 untag_vlan_net--SR-X500_2
	Change this to the physical port number of LAG connected to the server.	untag_vlan_net--SR-X500_3
%DOWN_PORT2%	Change this to physical port number of LAG connected to the server. Note that this port number must not be equal to that of %DOWN_PORT1%. When there are several LAGs connected to the server, change sample script.	untag_vlan_net--SR-X500_3

untag_vlan_port--SR-X500
untag_vlan_port--SR-X500_*n*

For SR-X500 that sets port VLAN to the port connected to the firewall, the server load balancer, or the server
Register this ruleset in the specfic ruleset registration folder of the network device.

n: Number of "2" or larger

For Catalyst

tag_vlan_net--Catalyst
tag_vlan_net--Catalyst*n*

For system that sets tagged VLAN network
Tagged VLAN is set to port by using tag_vlan_port--Catalyst or tag_vlan_port--Catalyst*n*.
Register this ruleset in the ruleset registration folder common to network devices.

Parameters need to be customized

The target of customizing is a parameter in all the related script list.
The list of parameters needs to be customized is shown.

Table G.7 The list of parameters needs to be customized (Catalyst tagged VLAN setting)

Parameter	Details of Modification	Ruleset name

node operand:	Change this to the network device name of the L2 switch registered in Resource Orchestrator.	tag_vlan_net--Catalyst tag_vlan_net--Catalyst*n*
%UP_PORT1%	Change this to the physical interface name connected to the firewall or the server load balancer. When there are some physical interfaces connected to servers or server load balancers, change sample script.	tag_vlan_net--Catalyst
	Change this to the physical interface name connected to the "Active" side of the firewall or the server load balancer of the redundant configuration. When there are some physical interfaces connected to servers or server load balancers, change sample script.	tag_vlan_net--Catalyst2
	Change this to the physical interface name of LAG connected to the "Active" side of the firewall or the server load balancer of the redundant configuration. When there are some physical interfaces connected to servers or server load balancers, change sample script.	tag_vlan_net--Catalyst3
%UP_PORT2%	Change this to the physical interface name connected to the "Standby" side of the firewall or the server load balancer of the redundant configuration. When there are some physical interfaces connected to servers or server load balancers, change sample script.	tag_vlan_net--Catalyst2
	Change this to the physical interface name of LAG connected to the "Active" side of the firewall or the server load balancer of the redundant configuration. Note that this port number must not be equal to that of %UP_PORT1%. When there are some physical interfaces connected to servers or server load balancers, change sample script.	tag_vlan_net--Catalyst3
%UP_PORT3%	Change this to the physical interface name of LAG connected to the "Standby" side of the firewall or the server load balancer of the redundant configuration. When there are some physical interfaces connected to servers or server load balancers, change sample script.	tag_vlan_net--Catalyst3
%UP_PORT4%	Change this to the physical interface name of LAG connected to the "Standby" side of the firewall or the server load balancer of the redundant configuration. Note that this interface name must not be equal to that of %UP_PORT3%. When there are some physical interfaces connected to servers or server load balancers, change sample script.	tag_vlan_net--Catalyst3
%DOWN_PORT1%	Change this to the physical interface name connected to the server. When there are some physical interfaces connected to servers, change sample script.	tag_vlan_net--Catalyst tag_vlan_net--Catalyst2
	Change this to the physical interface name of LAG connected to the server.	tag_vlan_net--Catalyst3
%DOWN_PORT2%	Change this to physical interface name of LAG connected to the server. Note that this interface must not be equal to that of %DOWN_PORT1%. When there are plural physical LAG interface connected to the server, change sample script.	tag_vlan_net--Catalyst3

tag_vlan_port--Catalyst
tag_vlan_port--Catalyst*n*

For Catalyst that sets tagged VLAN to the port connected to the firewall, the server load balancer, or the server
Register this ruleset in the specfic ruleset registration folder of the network device.

untag_vlan_net--Catalyst
untag_vlan_net--Catalyst*n*

For system that sets untagged VLAN network
Port VLAN is set to port by using untag_vlan_port--Catalyst or untag_vlan_port--Catalyst*n*.
Register this ruleset in the ruleset registration folder common to network devices.

Parameters need to be customized

The target of customizing is a parameter in all the related script list.
The list of parameters needs to be customized is shown.

Table G.8 The list of parameters needs to be customized (Catalyst port VLAN setting)

Parameter	Details of Modification	Ruleset name
node operand:	Change this to the network device name of the L2 switch registered in Resource Orchestrator.	untag_vlan_net--Catalyst untag_vlan_net--Catalyst*n*
%UP_PORT1%	Change this to the physical interface name connected to the firewall or the server load balancer. When there are some physical interfaces connected to servers or server load balancers, change sample script.	untag_vlan_net--Catalyst
	Change this to the physical interface name connected to the "Active" side of the firewall or the server load balancer of the redundant configuration. When there are some physical interfaces connected to servers or server load balancers, change sample script.	untag_vlan_net--Catalyst2
	Change this to the physical interface name of LAG connected to the "Active" side of the firewall or the server load balancer of the redundant configuration. When there are some physical interfaces connected to servers or server load balancers, change sample script.	untag_vlan_net--Catalyst3
%UP_PORT2%	Change this to the physical interface name connected to the "Standby" side of the firewall or the server load balancer of the redundant configuration. When there are some physical interfaces connected to servers or server load balancers, change sample script.	untag_vlan_net--Catalyst2
	Change this to the physical interface name of LAG connected to the "Active" side of the firewall or the server load balancer of the redundant configuration. Note that this interface name must not be equal to that of %UP_PORT1%. When there are some physical interfaces connected to servers or server load balancers, change sample script.	untag_vlan_net--Catalyst3
%UP_PORT3%	Change this to the physical interface name of LAG connected to the "Standby" side of the firewall or the server load balancer of the redundant configuration. When there are some physical interfaces connected to servers or server load balancers, change sample script.	untag_vlan_net--Catalyst3
%UP_PORT4%	Change this to the physical interface name of LAG connected to the "Standby" side of the firewall or the server load balancer of the redundant configuration.	untag_vlan_net--Catalyst3

	Note that this interface name must not be equal to that of %UP_PORT3%. When there are some physical interfaces connected to servers or server load balancers, change sample script.	
%DOWN_PORT1%	Change this to the physical interface name connected to the server. When there are some physical interfaces connected to servers, change sample script.	untag_vlan_net--Catalyst untag_vlan_net--Catalyst2
	Change this to the physical interface name of LAG connected to the server.	untag_vlan_net--Catalyst3
%DOWN_PORT2%	Change this to physical interface name of LAG connected to the server. Note that this interface name must not be equal to that of %DOWN_PORT1%. When there are plural physical LAG interface connected to the server, change sample script.	untag_vlan_net--Catalyst3

untag_vlan_port--Catalyst
untag_vlan_port--Catalyst*n*

For Catalyst that sets port VLAN to the port connected to the firewall, the server load balancer, or the server
Register this ruleset in the specfic ruleset registration folder of the network device.

n: Number of "2" or larger

G.3.10 Condition of using sample scripts

When using sample scripts, configure the target devices in advance according to "9.2.3.3 Settings for Automatically Configured Devices" The conditions on using sample scripts of each type is as follows:

- For deployment of Firewall (for IPCOM EX series)
  - Creating an L-Platform is up to 99.
- For deployment of Firewall (for NSappliance)
  - Creating an L-Platform is up to 99.
- For deployment of firewall (for ASA5500 series)
  - Creating an L-Platform is up to 99.
- For deployment of Firewall and Server Load Balancer(for IPCOM EX series)
  - Creating an L-Platform is up to 99.
  - Single IPCOM EX IN series can cope with up to 999 Server load balancer of L-Platform.
  - It won't be able to target the same server between more than one L-Platform to load balancing. (If configuration is fails is up to design of device that are targeted.)
- For deployment of Firewall and Server Load Balancer (for Combination of ASA5520 Series and BIG-IP LTM Series)
  - Creating an L-Platform is up to 99.
  - Single BIG-IP LTM series can cope with up to 999 Server load balancer of L-Platform.
  - It won't be able to target the same server between more than one L-Platform to load balancing. (If configuration is fails is up to design of device that are targeted.)
- For deployment of Server Load Balancer (for BIG-IP LTM Series)
  - Single BIG-IP LTM series can cope with up to 999 Server load balancer of L-Platform.

    - It won't be able to target the same server between more than one L-Platform to load balancing. (If configuration is fails is up to design of device that are targeted.)

- For deployment of L2 switches
    - There is no limit

G.4 Sample Scripts(For Operation)

Sample script to operate such as status display, operations of management resources to network device is registered to under the following folder.

[Windows Manager]
Installation_folder\SVROR\Manager\etc\scripts\original*vendor_name**unit_name*\operations*ruleset_name*\

[Linux Manager]
/etc/opt/FJSVrcvmr/scripts/original/*vendor_name*/*unit_name*/operations/*ruleset_name*/

The following table lists the unit names supported by the sample scripts provided by Resource Orchestrator:

Table G.9 List of Unit Name that offer sample Script for Operations

Vendor	Unit Name	Type	Operation Contents
Fujitsu	IPCOMEXIN	Server load balancer	- Instruction in order to activate to load balancer server. - Instruction in order to deactivate from load balanced server. - Instruction in order to display of load balancing status in server load balancer rule. - Instruction in order to collect statistics information of load balancing status in server load balancer rule.
F5 Networks	BIG-IP (*)		- Enable instruction to pool member. - Disable instruction to pool member. - Virtual server and status of pool member and instruction to collect statistics information.

*: We deal with BIG-IP LTM series as "BIG-IP" in device name.

Information

If you use sample scripts that are provided by this product, protocols that are used when manager connect to network device in order to do auto-configuration are as follows:

- Network Devices that are connected by TELNET Protocol.
    - IPCOMEXIN
- Network Devices that are connected by SSH Protocol.
    - BIG-IP

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.

G.4.1 Tasks that are required if you use sample Script

Describe about tasks that are required if you use sample script for auto-configuration of network device.

- Make sure that "Folder for Registering rule set" created.
  These folders name are "Vendor" and "Unit name" and "ruleset name" of sample scripts described in"Table G.9 List of Unit Name that offer sample Script for Operations".
  When needed sample scripts are not registered, copy the sample scripts registered in installing this product.

G.4.2 Prerequisite for when you execute sample Script for Operations

If you execute sample script for operations, it is necessary to meet following conditions.

- Server Load Balancer is deployed using sample Script provided In sample Script for deploy Server Load Balancer.
- Rule of Server Load Balancer was configured to Server Load Balancer after deploying L-Platform.
- For IPCOM EX IN series and BIG-IP LTM series of redundant configuration, the device in active status is not set at maintenance mode.

G.4.3 For operation of Server Load Balancer

Sample ruleset name for operations that are provided in this product is shown in the following text.

For Operation of IPCOM EX IN Series

SLB_server_disable--IPCOM

For system uses IPCOM EX IN series to server load balancer.

Operation contents

Modify server to maintenance mode and instruct to be excluded from load balanced servers.

SLB_server_enable--IPCOM

For system uses IPCOM EX IN series to server load balancer.

Operation contents

Release maintenance mode of server and instruct to be included from load balanced servers.

SLB_vserver_status--IPCOM

For system uses IPCOM EX IN series to server load balancer.

Operation contents

Instruct display of load balance status in rule of server load balancer.

SLB_vserver_statistics--IPCOM

For system uses IPCOM EX IN series to server load balancer.

Operation contents

Instruct display of load balance statistics information in rule of server load balancer.

For Operation of BIG-IP LTM Series

SLB_server_disable--BIGIP

For system uses BIG-IP LTM series to server load balancer.

Operation contents

Modify pool member (server targeted variance) to disable status to be excluded from load balanced servers.

SLB_server_enable--BIGIP

For system uses BIG-IP LTM series to server load balancer.

Operation contents

Modify pool member (server targeted variance) to enable status and instruct to be included from load balanced servers.

SLB_vserver_status--BIGIP

For system uses BIG-IP LTM series to server load balancer.

Operation contents

Instruct to collect virtual server and status of pool member and statistics information.

G.5 Sample Script Files

This section describes files related to sample script.

G.5.1 Script List File

This section describes script list file that are provided in rule set unit.

Table G.10 List of Script List File that is provided in RuleSet Unit

Script List Type	File Name
Script lists for setup	create.lst
Script lists for setup error recovery	create_recovery.lst
Script list for modification	modify.lst
Script lists for modification error recovery	modify_recovery.lst
Script list for deletion	delete.lst
Script lists for setup (physical server added)	connect.lst (*1)
Script lists for setup error recovery (physical server added)	connect_recovery.lst (*1)
Script lists for deletion (physical server deleted)	disconnect.lst (*1)
Script lists for operations	operate.lst (*2)

*1: These files only exist for ruleset for deployment of L2 Switches.
*2: This file only exists for ruleset for operations of server load balancer.

G.5.2 Script File

This section describes script file that are provided in ruleset unit.

Table G.11 List of Script File that is provided in RuleSet Unit

Script Type	File Name
Script for creation	*xxx*_create.rb
Script for setup error recovery	*xxx*_create_recovery.rb
Script for modification	*xxx*_modify.rb
Script for modification error recovery	*xxx*_modify_recovery.rb
Script for deletion	*xxx*_delete.rb
Script for creation of interface for adjoining server	*xxx*_connect.rb (*1)
Script for setup (physical server added)	*xxx*_connect_recovery.rb (*1)
Script for setup error recovery (physical server added)	*xxx*_disconnect.rb (*1)
Script definition	*xxx*_params.rb
Common method used by scripts	*xxx*_common.rb

Post-processing script after deletion script	*xxx*_clean.rb
Scripts for operations	*xxx*_operate.rb (*2)
Script for pretreatment before execution of script for operations	*xxx*_pre_operate.rb (*2)
Script for outputting result after execution of script for operations	*xxx*_output.rb (*2)
Script for SSH connection	unm_script_ssh2_comm.rb (*3)

xxx: Character String that identifies L2 Switches, firewalls and server load balancers.
*1: These files only exist for ruleset for deployment of L2 Switches.
*2: These files only exist for ruleset for operations of server load balancer.
*3: This file only exists for ruleset of BIG-IP LTM.

G.5.3 Command File

This section describes command files that are provided in rule set unit.

For deploying L2 Switches

Command files that are provided for deployment of L2 Switches are shown in the following.

Table G.12 List of Command Files that are provided in Rule Set Unit (For Deployment of L2 Switches)

Command File Type		File Name
For setup	Configuration definition command file Definition reflection command file	*xxx*_create_cmd*n*.cli
For recovery when setup error	Configuration definition command file Definition reflection command file	*xxx*_create_recovery_cmd*n*.cli
For modification	Configuration definition command file Definition reflection command file	*xxx*_modify_cmd*n*.cli
For recovery when modification error	Configuration definition command file Definition reflection command file	*xxx*_modify_recovery_cmd*n*.cli
For interfaces configuration of adjoining server	Configuration definition command file Definition reflection command file	*xxx*_connect_cmd*n*.cli
For recovery when interface configuration error of adjoining server	Configuration definition command file Definition reflection command file	*xxx*_connect_recovery_cmd*n*.cli
For interfaces deletion of adjoining server	Configuration definition command file Definition reflection command file	*xxx*_disconnect_cmd*n*.cli
For deletion	Configuration definition command file Definition reflection command file	*xxx*_delete_cmd*n*.cli

xxx: Character String that identifies L2 Switches.
n: Serial numbers begin from 1. File given the biggest number is the command file for reflecting definition.

For deploying Firewalls

Command files that are provided for deploy firewalls are shown in the following list.

Table G.13 List of Command Files that are provided in RuleSet Unit (For Deployment of Firewalls)

Command File Type		File Name
For setup	Configuration definition command file Definition reflection command file	*yyy*_create_cmd*n*.cli
For recovery when setup error	Configuration definition command file Definition reflection command file	*yyy*_create_recovery_cmd*n*.cli

For modification	Configuration definition command file Definition reflection command file	*yyy*_modify_cmd*n*.cli
For recovery when modification error	Configuration definition command file Definition reflection command file	*yyy*_modify_recovery_cmd*n*.cli
For deletion	Configuration definition command file Definition reflection command file	*yyy*_delete_cmd*n*.cli

yyy: Character String that identifies firewall.
n: Serial numbers begin from 1. File given the biggest number is the command file for reflecting definition.

For deploying Server Load Balancers

Command files that are provided for deployment of server load balancers are shown in the following list.

Table G.14 List of Command Files provided in RuleSet Unit (For Deployment of Server Load Balancer "IPCOM EX IN")

Command File Type		File Name
For modification	Configuration definition command file Definition reflection command file	ipcom_modify_cmd*n*.cli
For recovery when modification error	Configuration definition command file Definition reflection command file	ipcom_modify_recovery_cmd*n*.cli
For deletion	Configuration definition command file Definition reflection command file	ipcom_delete_cmd*n*.cli
For operation	Command file	ipcom_operate_cmd*m*.cli

zzz: Character string that identifies server load balancer.
n: Serial numbers begin from 1. File given the biggest number is the command file for reflecting definition.
m: Serial numbers begin from 1.

Table G.15 List of Command Files provided in RuleSet Unit (For Deployment of Server Load Balancer "BIG-IP")

Command File Type		File Name
For setup	Configuration definition command file Definition reflection command file	bigip_create_cmd*n*.cli
For recovery when setup error	Configuration definition command file Definition reflection command file	bigip_create_recovery_cmd*n*.cli
For modification	Configuration definition command file Definition reflection command file	bigip_modify_cmd*n*.cli
For recovery when modification error	Configuration definition command file Definition reflection command file	bigip_modify_recovery_cmd*n*.cli
For deletion	Configuration definition command file Definition reflection command file	bigip_delete_cmd*n*.cli
For operation	Command file	bigip_operate_cmd*m*.cli

zzz: Character string that identifies server load balancer.
n: Serial numbers begin from 1. File given the biggest number is the command file for reflecting definition.
m: Serial numbers begin from 1.

Information

In sample script, following operations are surely executed after logging in to network device and before executing command.
Therefore, commands described in command files are shown only after executing following operations.

- Transition to authority requires Modification of Configuration.
- Disabling inquiry to terminal Control and Executing Command.
- Transition to Edit Mode of Configuration Definition.
- Reading Configuration Definition in Action.

G.5.4 Log Files of Sample Script

In sample script, outputs processing contents in files as log to recognize progress of execution in sample script and error occurs in script.

In sample script, output log file to under the folder ruleset is stored in following file name.

When checking the content, copy the log file to an arbitrary user directory and then open the copied log file.

- Catalyst
  - "catalyst_script_*admin IP address*.log"
  - "catalyst_telnet_*admin IP address*.log"
- SR-X
  - "srx_script_*admin IP address*.log"
  - "srx_telnet_*admin IP address*.log"
- IPCOM EX and NSAppliance
  - "ipcom_script_*admin IP address*.log"
  - "ipcom_telnet_*admin IP address*.log"
- ASA5500
  - "asa_script_*admin IP address*.log"
  - "asa_telnet_*admin IP address*.log"
- BIG-IP LTM
  - "bigip_script_*admin IP address*.log"
  - "bigip_ssh_*admin IP address*.log"

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 ESXi 5.0 to servers using the PXE boot mechanism.

Automatic Storage Layering

A function that optimizes performance 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.

Basic Mode

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

BASP (Broadcom Advanced Server Program)

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

blade server

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

blade type

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

BladeViewer

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

BMC (Baseboard Management Controller)

A Remote Management Controller used for remote operation of servers.

boot agent

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

CA (Channel Adapter)

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

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.

external FTP server

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

FC switch (Fibre Channel Switch)

A switch that connects Fibre Channel interfaces and storage devices.

Fibre Channel

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 CLARiiON, 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.

global zone

The actual OS that is used for a Solaris container.

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

GLS (Global Link Services)

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

GSPB (Giga-LAN SAS and PCI_Box Interface Board)

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

GUI (Graphical User Interface)

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

HA (High Availability)

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

hardware initiator

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

hardware maintenance mode

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

HBA (Host Bus Adapter)

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

HBA address rename setup service

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

HBAAR (HBA address rename)

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

host affinity

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

Hyper-V

Virtualization software from Microsoft Corporation.

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

I/O virtualization option

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

IBP (Intelligent Blade Panel)

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

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.

integrated network device

A network device with integrated firewall or server load balancing functions.
The IPCOM EX IN series fits into this category.

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 configuration file

This is the original network device configuration file that is backed up from each network device immediately after Resource Orchestrator is set up.
It is used for the following purposes:

- When initializing the settings of network devices
- When checking the differences between the current and original configurations
- For providing the initial settings when creating a new system with the same configuration

In regards to the network device file management function, these files are excluded from the scope of version management (They are not automatically deleted).

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, firewalls, and server load balancers fit into this category.

network device configuration file

These files contain definitions of settings regarding communication, such as VLAN information for network devices and interfaces, rules for firewalls and server load balancers, etc.
As the content of these files changes each time settings are configured from the CLI, they are the target of automatic backup by Resource Orchestrator, and a constant number of versions (32 by default) are backed up inside Resource Orchestrator.
Many network devices have two types of network device configuration files: "running config", which holds the current configuration details, and "startup config", which holds the configuration that is valid directly after startup.
In Resource Orchestrator these two types of files are the target of backup and restore operations.

network device environment file

A collective term that refers to the files necessary for operating devices, such as CA certificates, user authentication databases, customized user information, etc. (but excluding the network device configuration file).
As these files are not usually changed after they have been configured, Resource Orchestrator does not back them up each time automatic configuration is performed.

network device file

Regarding the network device file management function, this is a collective term that refers to the files held by network devices that are the target of backup and restore operations.
The two types of network device files are network device configuration files and network device environment files.

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.

non-global zone

A virtual machine environment that has been prepared in a global zone. Its OS kernel is shared with the global zone. Non-global zones are completely separate from each other.

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 are 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 resource pool

The Solaris Containers resource pool used in the global zone and the non-global zone.

Solaris Containers

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 failback nor continuation have been performed.

system administrator

The administrator who manages the entire system. They perform pre-configuration and installation of Resource Orchestrator.

Administrator privileges for the operating system are required. Normally the roles of the infrastructure administrator and system administrator are performed concurrently.

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 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.