FUJITSU

ServerView Resource Coordinator VE

Setup Guide

Windows/Linux

J2X1-7459-01ENZ0(00)
September 2009

Preface

Purpose

This manual contains an outline of ServerView Resource Coordinator VE (hereinafter Resource Coordinator VE) and the operations and settings required for setup.

Target Readers

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

Organization

This manual consists of ten chapters, seven appendices, and a glossary. The contents of these chapters, the appendices, and the glossary are listed below.

Title	Description
Chapter 1 Overview	Provides an overview of Resource Coordinator VE.
Chapter 2 User Interface	Provides an overview of the RC console.
Chapter 3 System Design and Initial Setup	Explains how to design and prepare a Resource Coordinator VE installation.
Chapter 4 Installation	Explains how to install Resource Coordinator VE.
Chapter 5 Starting and Stopping	Explains how to start and stop Resource Coordinator VE services, and how to open and close the RC console.
Chapter 6 Setup	Explains how to register, change, and delete the resources used by Resource Coordinator VE.
Chapter 7 Pre-configuration	Provides an overview of the pre-configuration function and explains how to use system configuration files.
Chapter 8 Cloning [Windows/Linux]	Explains how to use the server cloning function.
Chapter 9 Server Switchover Settings	Explains how to use server switchover settings and automatically recover from server failures.
Chapter 10 Saving Environment Settings	Explains how to save environment settings.
Appendix A Server virtualization Products	Details the functions available for each server virtualization product managed in Resource Coordinator VE.
Appendix B Connections between Server Network Interfaces and LAN Switch Ports	Describes the connections between server network interfaces and LAN switches ports.
Appendix C Port List	Describes the ports used by Resource Coordinator VE.
Appendix D Format of CSV System Configuration Files	Describes the format of the CSV system configuration files used by Resource Coordinator's pre-configuration function.
Appendix E HTTPS Communications	Explains the security features of the HTTPS communication protocol used by Resource Coordinator VE.
Appendix F Maintenance Mode	Explains the maintenance mode available in Resource Coordinator VE and how to use it.
Appendix G Notes on Installation	Gives important information regarding the installation of Resource Coordinator VE.

Title	Description
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 Coordinator VE and the functions necessary differ due to the necessary basic software (OS), it is indicated as follows:

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

- Unless specified otherwise, the blade servers mentioned in this manual refer to PRIMERGY BX servers.
- References and character strings or values requiring emphasis are indicated using double quotes (").
- Window names, dialog names, menu names, and tab names are shown enclosed by square brackets ([ ]).
- Button names are shown enclosed by angle 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.

Menus in the RC console

Operations on the RC 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.

Related Manuals

The following manuals are provided with Resource Coordinator VE. Please refer to them when necessary.

- ServerView Resource Coordinator VE Installation Guide

  Explains the methods for installing and configuring the software components of Resource Coordinator VE.

- ServerView Resource Coordinator VE Setup Guide (This manual)

  Explains Resource Coordinator VE and its functions, as well as the settings and operations necessary for setup.

- ServerView Resource Coordinator VE Operation Guide

  Explains the functions provided by Resource Coordinator VE as well as the settings and operations necessary when using it.

- ServerView Resource Coordinator VE Command Reference

  Explains the types, formats, and functions of the commands used with Resource Coordinator VE.

- ServerView Resource Coordinator VE Messages

  Explains the meanings of messages output by Resource Coordinator VE, and the corrective action to be taken.

Related Documentation

Please refer to these manuals when necessary.

- Systemwalker Resource Coordinator Virtual server Edition Setup Guide

Abbreviations

The following abbreviations are used in this manual:

Abbreviation	Products
Windows	Microsoft(R) Windows Server(R) 2008 Standard (x86, x64) Microsoft(R) Windows Server(R) 2008 Enterprise (x86, x64) Microsoft(R) Windows Server(R) 2003 R2, Standard Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition Microsoft(R) Windows Vista(R) Business Microsoft(R) Windows Vista(R) Enterprise Microsoft(R) Windows Vista(R) Ultimate Microsoft(R) Windows(R) XP Professional operating system
Windows Server 2008	Microsoft(R) Windows Server(R) 2008 Standard (x86, x64) Microsoft(R) Windows Server(R) 2008 Enterprise (x86, x64)
Windows 2008 x64 Edition	Microsoft(R) Windows Server(R) 2008 Standard (x64) Microsoft(R) Windows Server(R) 2008 Enterprise (x64)
Windows Server 2003	Microsoft(R) Windows Server(R) 2003 R2, Standard Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
Windows 2003 x64 Edition	Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
Windows Vista	Microsoft(R) Windows Vista(R) Business Microsoft(R) Windows Vista(R) Enterprise Microsoft(R) Windows Vista(R) Ultimate
Windows XP	Microsoft(R) Windows(R) XP Professional operating system
Linux	Red Hat(R) Enterprise Linux(R) AS (v.4 for x86) Red Hat(R) Enterprise Linux(R) ES (v.4 for x86) Red Hat(R) Enterprise Linux(R) AS (v.4 for EM64T) Red Hat(R) Enterprise Linux(R) ES (v.4 for EM64T) Red Hat(R) Enterprise Linux(R) AS (4.5 for x86) Red Hat(R) Enterprise Linux(R) ES (4.5 for x86) Red Hat(R) Enterprise Linux(R) AS (4.5 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.5 for EM64T)

Abbreviation	Products
	Red Hat(R) Enterprise Linux(R) AS (4.6 for x86) Red Hat(R) Enterprise Linux(R) ES (4.6 for x86) Red Hat(R) Enterprise Linux(R) AS (4.6 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.6 for EM64T) Red Hat(R) Enterprise Linux(R) AS (4.7 for x86) Red Hat(R) Enterprise Linux(R) ES (4.7 for x86) Red Hat(R) Enterprise Linux(R) AS (4.7 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.7 for EM64T) Red Hat(R) Enterprise Linux(R) AS (4.8 for x86) Red Hat(R) Enterprise Linux(R) ES (4.8 for x86) Red Hat(R) Enterprise Linux(R) AS (4.8 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.8 for EM64T) Red Hat(R) Enterprise Linux(R) 5 (for x86) Red Hat(R) Enterprise Linux(R) 5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.1 (for x86) Red Hat(R) Enterprise Linux(R) 5.1 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.2 (for x86) Red Hat(R) Enterprise Linux(R) 5.2 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.3 (for x86) Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64) SUSE Linux Enterprise Server 10 SP2 for x86, AMD64, Intel64
Red Hat Enterprise Linux	Red Hat(R) Enterprise Linux(R) AS (v.4 for x86) Red Hat(R) Enterprise Linux(R) ES (v.4 for x86) Red Hat(R) Enterprise Linux(R) AS (v.4 for EM64T) Red Hat(R) Enterprise Linux(R) ES (v.4 for EM64T) Red Hat(R) Enterprise Linux(R) AS (4.5 for x86) Red Hat(R) Enterprise Linux(R) ES (4.5 for x86) Red Hat(R) Enterprise Linux(R) AS (4.5 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.5 for EM64T) Red Hat(R) Enterprise Linux(R) AS (4.6 for x86) Red Hat(R) Enterprise Linux(R) ES (4.6 for x86) Red Hat(R) Enterprise Linux(R) AS (4.6 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.6 for EM64T) Red Hat(R) Enterprise Linux(R) AS (4.7 for x86) Red Hat(R) Enterprise Linux(R) ES (4.7 for x86) Red Hat(R) Enterprise Linux(R) AS (4.7 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.7 for EM64T) Red Hat(R) Enterprise Linux(R) AS (4.8 for x86) Red Hat(R) Enterprise Linux(R) ES (4.8 for x86) Red Hat(R) Enterprise Linux(R) AS (4.8 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.8 for EM64T) Red Hat(R) Enterprise Linux(R) 5 (for x86) Red Hat(R) Enterprise Linux(R) 5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.1 (for x86) Red Hat(R) Enterprise Linux(R) 5.1 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.2 (for x86) Red Hat(R) Enterprise Linux(R) 5.2 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.3 (for x86) Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64)
Red Hat Enterprise Linux 5	Red Hat(R) Enterprise Linux(R) 5 (for x86) Red Hat(R) Enterprise Linux(R) 5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.1 (for x86) Red Hat(R) Enterprise Linux(R) 5.1 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.2 (for x86) Red Hat(R) Enterprise Linux(R) 5.2 (for Intel64)

Abbreviation	Products
	Red Hat(R) Enterprise Linux(R) 5.3 (for x86) Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64)
SUSE Linux Enterprise Server	SUSE Linux Enterprise Server 10 SP2 for x86, AMD64, Intel64
VMware	VMware(R) Infrastructure 3 VMware vSphere(TM) 4
Xen	Citrix XenServer(TM) 5.5 Citrix Essentials(TM) for XenServer 5.5, Enterprise Edition
Excel	Microsoft(R) Office Excel(R) 2007 Microsoft(R) Office Excel(R) 2003 Microsoft(R) Office Excel(R) 2002
Excel 2007	Microsoft(R) Office Excel(R) 2007
Excel 2003	Microsoft(R) Office Excel(R) 2003
Excel 2002	Microsoft(R) Office Excel(R) 2002
Resource Coordinator	Systemwalker Resource Coordinator
Resource Coordinator VE	ServerView Resource Coordinator VE
ServerView Agent	ServerView SNMP Agents for MS Windows (32bit-64bit) ServerView Agents Linux for SUSE Linux Enterprise Server (SLES) and Red Hat Enterprise Linux (RHEL) ServerView Agents VMware for VMware ESX Server

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

- Citrix(R), Citrix XenServer(TM), Citrix Essentials(TM), and Citrix StorageLink(TM) are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.
- Dell is a registered trademark of Dell Computer Corp.
- HP is a registered trademark of Hewlett-Packard Company.
- IBM is a registered trademark of International Business Machines Corporation.
- Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.
- Linux is a trademark or registered trademark of Linus Torvalds in the United States and other countries.
- Microsoft, Windows, Windows XP, Windows Server, Windows Vista, Excel, and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.
- Red Hat, RPM and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries.
- SUSE is a registered trademark of SUSE LINUX AG, a Novell business.
- VMware, the VMware "boxes" logo and design, Virtual SMP, and VMotion are trademarks or registered 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.

September 2009, First Edition

Contents

Chapter 1 Overview

This chapter provides an overview of Resource Coordinator VE.

1.1 Features

Resource Coordinator VE is a server management product which improves the usability and availability of server systems. It uniformly manages physical servers as well as virtual servers created using server virtualization software (VMware and others).

The level of functionality provided by Resource Coordinator VE may differ depending on the managed hardware environment. Refer to the corresponding "Note" in "1.2 Hardware Environment" of the "ServerView Resource Coordinator VE Installation Guide" for details.

This section explains some of the features provided by Resource Coordinator VE.

- **Integrated management of physical and virtual servers**

  Resource Coordinator VE provides an integrated management console for environments made of virtual and physical servers. It helps administrators manage server configurations, monitor hardware failures and determine the cause and impact of system errors by automatically detecting and displaying the following information.

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

  Resource Coordinator VE 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.

- **Auto-Recovery of failed servers**

  When used with PRIMERGY BX servers, pre-allocating spare servers to primary servers allows the Auto-Recovery function to automatically recover failed applications onto an available spare server. Depending on the server's boot method, either one of the following two switchover methods can be used to recover applications on a spare server:

  - Backup and restore

    This method is used in local boot environments where servers boot from an internal disk. Backing up the system disk of a primary server in advance allows an automatic restoration and startup of the spare server when the primary server fails.

  - 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 (*1) capabilities of the HBA address rename function, which is able to dynamically re-configure the WWN of an I/O adapter (HBA).

    *1: Refer to "I/O Virtualization".

  If VLANs have been set on the LAN switches connected to the primary and spare servers, these VLAN settings are automatically exchanged during server switchover.

  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 the 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 or remote management controllers). It cannot detect system slowdowns or hang-ups.

- **Automated server installation and setup**

  The following three features simplify server installation and setup:

  - Deploying multiple servers via server cloning

    Server cloning is a feature that distributes a cloning image (collected from the system disk of a reference server) to other physical servers. When a cloning image is created, network-specific configuration 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.

  - Simplified server installation with I/O virtualization

    I/O virtualization via HBA address rename (*1) allows storage devices to be set up 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.

    *1: Refer to "I/O Virtualization".

  - Multiple server installations using the pre-configuration feature

    The pre-configuration feature can be used to configure various Resource Coordinator VE settings (registration of managed resources and others settings) in one operation. All settings required for a Resource Coordinator VE setup can be defined in a system configuration file, which can then be easily imported from the RC console.
    The system configuration file is in CSV format and can be edited easily in environments where Resource Coordinator VE is not installed.

- **Streamlined server maintenance**

  The following features help to identify which servers need to be replaced, and assist administrators with maintenance required after a server replacement:

  - Automatic maintenance LED activation on failed servers. (*1)

    *1: Depending on the hardware being used, this feature may or may not be available. Refer to the corresponding "Note" in "1.2 Hardware Environment" of the "ServerView Resource Coordinator VE Installation Guide" for details.

  - In SAN boot environments, I/O virtualization (*1) provided by HBA address rename makes it possible to restore a failed server's original WWN definition to the replacement server. Resource Coordinator VE is able to quickly reconnect a replaced server to its original volume(s) and start it up from the same operating system without accessing any storage device.

    *1: Refer to "I/O Virtualization".

  - In local boot environments, a system image backed up beforehand can be easily restored to the replaced server to simplify server replacements.

- **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.

  - Provides an intuitive way to monitor and control multiple servers' power state.

  - Makes it easier to visualize which applications are running on each blade. This helps identifying quickly any affected applications when a hardware fault occurs on a server blade.

- **Easy Network Monitoring**

  For PRIMERGY BX servers, Resource Coordinator VE 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:

  - Automatically detects and displays 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 as a communication basis for server and network administrators, thus smoothing out coordination between the two parties.

- **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.

- **Relocation of VM guests**

  By integrating with VM management software (such as VMware vCenter Server or others) and VM hosts (such as Citrix XenServer or others), Resource Coordinator VE provides the ability to migrate VM guests between physical servers directly from the RC console.
  When used with other Resource Coordinator VE functions, this enables the following:

  - Regroup all VM guests to a subset of servers and shut down any unused server 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.

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 Coordinator VE 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 Coordinator VE provides I/O virtualization via its HBA address rename function.

The "I/O Virtualization Option" is required when using HBA address rename.

1.2 Function Overview

This section details the functions provided by Resource Coordinator VE.

1.2.1 Available Functions

Resource Coordinator VE provides the following functions.

Table 1.1 Functions Available for Managed Servers

Function	Description	Benefits	Target resource		
			Physical OS	VM host (*1)	VM guest (*1)
Monitoring	Monitors resources, such as servers, and displays their status (normal, error, etc.) on the RC console.	Helps identifying the cause of a failure and determine its impact on servers, thereby streamlining hardware maintenance.	Yes (*2)	Yes (*2)	Yes
Power Control	Powers on and off managed servers.	Enables remote control of a server's power state without having direct access to it. This simplifies periodic maintenance tasks that involve power control operations.	Yes	Yes	Yes
Backup and Restore	Creates system image backups of servers that can be easily restored when needed.	Creating backups before any configuration change, software installation or patch application can	Yes	Yes (*3)	No

Function	Description	Benefits	Target resource		
			Physical OS	VM host (*1)	VM guest (*1)
	System images are centrally stored on a disk on the Admin Server.	drastically reduces the time to restore a server to its original state when hardware or software problems occur.			
Hardware Maintenance	Simplifies the re-configuration tasks required after replacement of a hardware part. In SAN environments, re-configuration of attached storage devices (access paths and other security settings) is no longer required when using I/O virtualization.	Lightens the work load associated with hardware replacement and reduces operational errors.	Yes	Yes	-
Server Switchover	Recover applications upon hardware failure by switching over primary servers with pre-assigned spare servers.	Shortens and simplifies the recovery procedure in the event of a server failure.	Yes	Yes	No
Cloning	Creates a cloning image of a reference server and distribute it to other managed servers. Cloning images are centrally stored on a disk on the Admin Server.	Simplifies OS and software installation when servers are added. Allows servers with identical OS and software configurations to share common backups.	Yes (*4)	No	No

Yes: Supported
No: Not supported
-: Not applicable
*1: The level of functionality may differ depending on the server virtualization software used for VM hosts and VM guests. Refer to "A.1 Supported Functions" for details.
*2: Depending on the hardware being used, this feature may or may not be available. Refer to the corresponding "Note" in "1.2 Hardware Environment" of the "ServerView Resource Coordinator VE Installation Guide" for details.
*3: When backing up a VM host containing VM guests on its own boot disk, behavior differs according to the server virtualization product used. Refer to "A.3 Functional Differences between Products" for details.

*4: This function is not available for servers running a SUSE Linux Enterprise Server operating system.

Table 1.2 Functions Available for Blade Chassis

Function	Description	Benefits
Power Control	Powers on and off blade chassis.	Enables remote control of a chassis's power state without needing to connect to its management blade. This simplifies periodic maintenance tasks that involve power control operations.

Table 1.3 Functions Available for the Admin Server

Function	Description	Benefits
Pre-configuration	Systems made up of multiple servers can be easily configured or modified using the pre-	Prevents setup mistakes by performing numerous setup operations in a single action. System configuration files can be easily edited on

Function	Description	Benefits
	configuration function to import a pre-defined system configuration file.	machines where Resource Coordinator VE is not installed.
Backup and Restore	Backs up or restores a Resource Coordinator VE installation.	Performing backups after configuration changes are made in Resource Coordinator VE enables prompt recovery of the Admin Server in case its internal data is damaged due to administration mistakes or other problems.

Table 1.4 Functions Available for LAN Switches

Function	Description	Benefits
Monitoring	Monitors LAN switches and displays their statuses (normal or error) graphically.	Simplifies identification of the cause and impact of LAN switch failure on servers and speeds up hardware maintenance.
Network Map	Helps visualize and relate physical networks (between servers and LAN switch blades) together with virtualized networks (from VLANs or virtual switches used in server virtualization software).	Automatically detects and displays network connections (topology) and link statuses for different kinds of resources (network equipment or server virtualization software).
VLAN settings	Automates VLAN settings (port VLAN or tagged VLAN) on LAN switches adjacent to servers.	Simplifies the VLAN configuration of LAN switches when adding new servers. During automatic recovery of a failed server, VLANs are automatically reconfigured to preserve connectivity and avoid manual network re-configurations.
Restore	Restores a LAN switch to its latest VLAN configuration.	Restores the VLAN configuration on a replaced LAN switch to the configuration that was active before replacement.

Table 1.5 Functions Available for Power Monitoring Targets

Function	Description	Benefits
Power consumption monitoring	Monitors power consumption trends for resources equipped with power monitoring capabilities, or resources connected to power monitoring devices (PDU or UPS). Collects and outputs power consumption data over a given period of time.	This function can be used to measure the effectiveness of environmental policies and cost-saving initiatives on power consumption.

Table 1.6 Functions Available for Virtual Machines

Function (*1)	Description	Benefits
Migration of VM guests between servers	Migrates a VM guest from one physical server to another.	Facilitates optimization of VM guest deployments according to server load or planned maintenance.
VM maintenance mode control	Sets (or releases) VM hosts to (or from) a specific state that allows safe server maintenance.	VM hosts can be easily set out of and back into operation.

*1: Available functions may vary according to the server virtualization software used. Refer to "A.1 Supported Functions" for details.

1.2.2 Usage

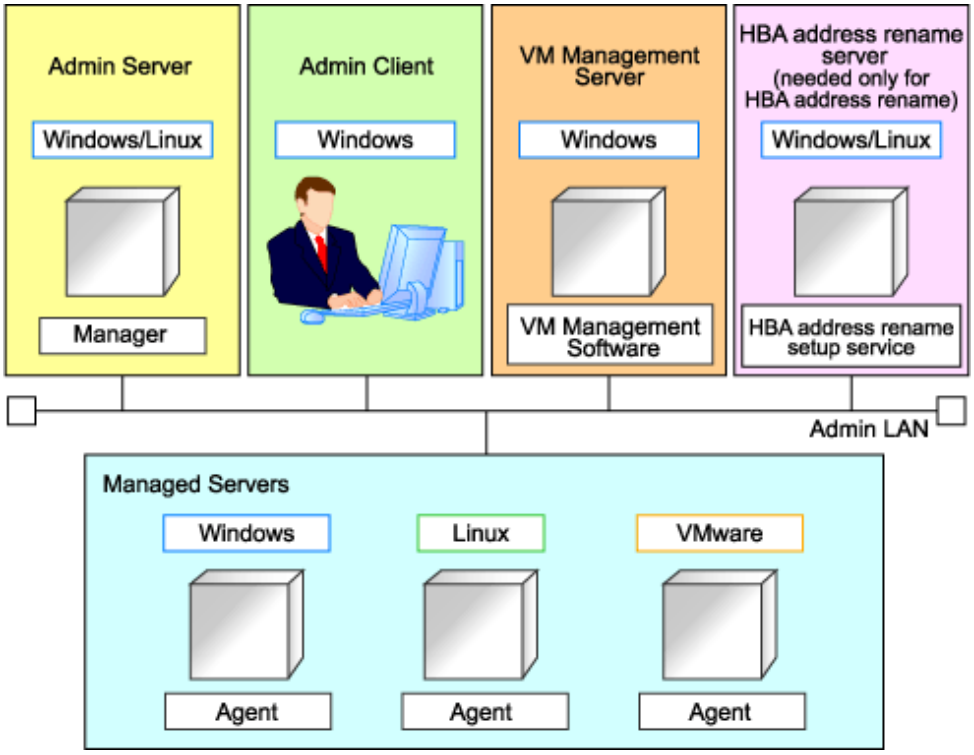
Resource Coordinator VE provides two different graphical views (*1), the RC console and BladeViewer, as well as a command line interface.
For details on the RC console, refer to "Chapter 2 User Interface".
For details on BladeViewer, refer to "Chapter 3 BladeViewer" of the "ServerView Resource Coordinator VE Operation Guide".
For details on the command line, refer to "Chapter 1 Overview" of the "ServerView Resource Coordinator VE Command Reference".

*1: When logging into Resource Coordinator VE for the first time, the RC console is displayed.

1.3 System Configuration

This section provides an example of a Resource Coordinator VE system configuration.

Figure 1.1 System configuration example



Admin Server

The Admin Server is a server used to manage several managed servers.
The Admin Server operates in a Windows or Linux environment.
The Resource Coordinator VE Manager should be installed on the Admin Server.
The Admin Server can be made redundant by using clustering software.
The Admin Client can operate on the same machine as the Admin Server.
The Resource Coordinator VE Agent cannot be installed on the Admin Server to monitor and manage the Admin Server itself.

Managed Servers

Managed servers are the servers used to run applications. They are managed by the Admin Server.
They include primary servers running Windows, Linux and server virtualization environments, and spare servers used to recover applications in case a primary server fails. A Resource Coordinator VE Agent should be installed on each managed server. Note that in server virtualization environments, the Agent should only be installed on the VM host (it does not need to be installed on the VM guests).

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.

A Web browser should be installed on Admin Clients.
If a server virtualization software client is installed on an Admin Client, it can be launched directly from the RC console.

VM Management Server

A server on which VM management software (such as VMware vCenter Server and others) has been installed. Such a server is used to centrally manage virtualization environments.

HBA address rename server

This server is used to run the HBA address rename setup service, and is required when using HBA address rename.
This server takes care of configuring a managed server's WWN settings in place of the Admin Server if the Admin Server is unreachable when the managed server starts up.
The HBA address rename server operates in a Windows or Linux environment.
The HBA address rename setup service should be installed on this server for the HBA address rename function to operate properly.
This server cannot serve as an Admin Server or as a managed server.
This server must be powered on at all times to standby for an Admin Server failure or communication problems between a managed server and the Admin Server.

Admin LAN

The Admin LAN is the LAN used by the Admin Server to control managed servers.
The Admin LAN is set up separately from the Public LAN used by applications on managed servers.
Use of network redundancy software on the Admin LAN enables redundancy for monitoring and power control functions. For the backup and restore function, network redundancy can only be enabled by using the redundant line control function of PRIMERGY GLS.

1.4 Managed Resources

Resource Coordinator VE can be used to manage the following resources:

Chassis

A chassis is an enclosure used to house server blades.
Resource Coordinator VE can monitor chassis statuses, display their properties, and control their power states. It can also automatically detect the server blades contained in a chassis and register them as managed resources.

Server

This is a general term for any physical server. This term is used to distinguish physical servers from virtual servers that are created using server virtualization software such as VMware.
Resource Coordinator VE can monitor server statuses, display their properties, and control their power states.
It can also detect the Physical OS's and VM hosts running on servers and register them as managed resources.

Physical OS

This refers to the operating system that operates directly on a physical server (instead of a virtual server).
Resource Coordinator VE can monitor Physical OS statuses and display their properties. It can also perform operations such as backup, HBA address rename and server switchover.

VM host

This refers to the server virtualization software installed on a server that is used to run virtual machines. For example, in a VMware environment, VMware ESX is the VM host used to provide server virtualization.
Resource Coordinator VE manages VM hosts in the same manner as Physical OS's: it can monitor their statuses, display their properties, and perform 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.

VM guest

This refers to the operating system running on top of a virtual machine.
Resource Coordinator VE can monitor VM guest statuses, display their properties, and control their power states.

VM management software

A software product used to centrally manage an entire virtualization environment (e.g. VMware vCenter Server).
VM management software can be integrated (registered) into Resource Coordinator VE to broaden the range of functions available for VM guests.

LAN switch

This term encompasses both the network switches that are mounted in a blade chassis (LAN switch blades), and the external LAN switches that are directly connected to them.
Resource Coordinator VE can monitor LAN switch blade statuses, display their properties, and manage their VLAN configuration.
LAN switch blades and external LAN switches can be displayed in a comprehensive Network Map.

Storage blade

This is a storage device mounted in a blade server chassis.
It is automatically detected and displayed once its enclosing chassis has been registered. Its power state can be controlled in conjunction with the power state of the server it is connected to.

Chapter 2 User Interface

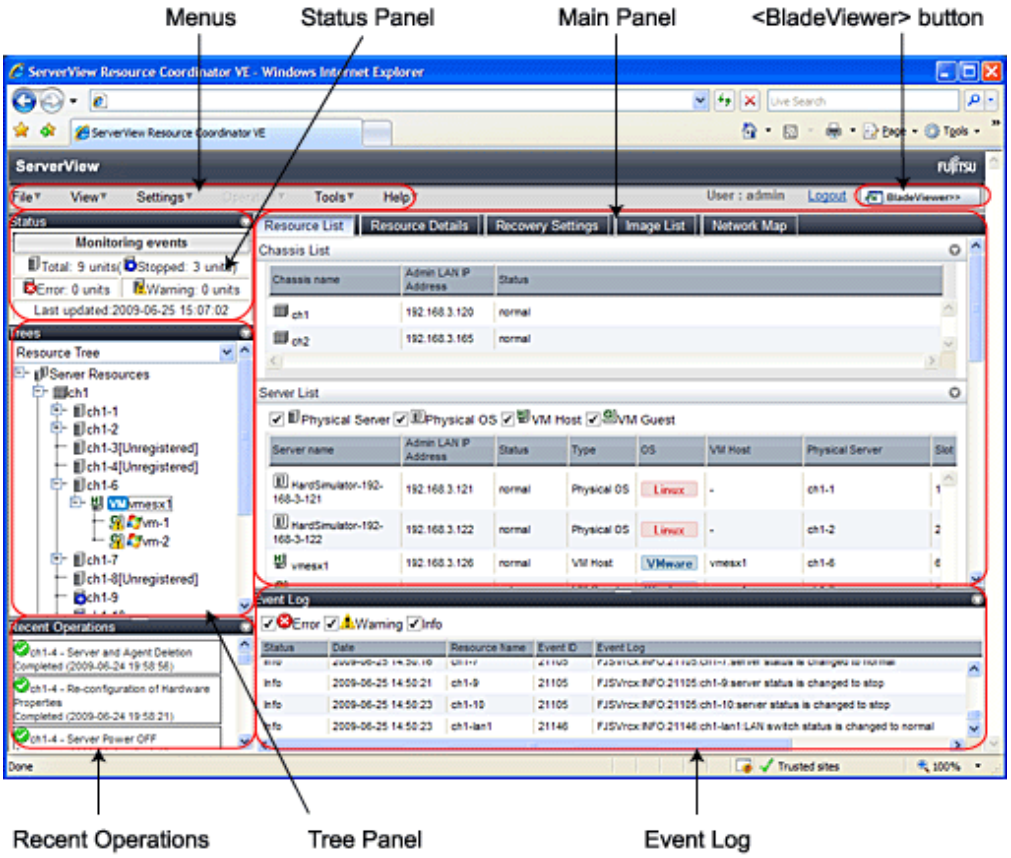
Resource Coordinator VE includes two graphical user interfaces: the RC console and BladeViewer.
This chapter provides an overview of the RC console.

Refer to "5.3 RC Console" for details on how to open and close the RC console.
Refer to "Chapter 3 BladeViewer" of the "ServerView Resource Coordinator VE Operation Guide" for details on BladeViewer.

2.1 RC console Layout

This section explains how the RC console is organized.

Figure 2.1 RC console



Menus

Operations can be performed either from the menu bar or popup menus.

Status Panel

The Status Panel displays the status of managed servers.
If a warning or error event occurs on a managed server, the status monitoring area starts to blink.

Tree Panel

The Tree Panel provides two types of trees: a resource tree and a VLAN tree.
The resource tree is also split between three sub-trees: one for server resources, one for network resources, and one for power monitoring devices.

Resource Tree

Server Resources

The resources below are shown in a tree view. A status icon is displayed over each resource's icon.

- Chassis
- Server
- Physical OS
- VM host
- VM guest
- LAN switch

Network Resources

The resources below are shown in a tree view. A status icon is displayed over each resource's icon.

- LAN switch (excluding LAN switch blades)

Power Monitoring Devices

The following power monitoring devices are shown in a tree view.

- PDU
- UPS

VLAN Tree

Selecting a VLAN ID shows a list of resources on which this ID has been applied to.

- Chassis
- Server
- VM host
- VM guest
- LAN switch
- NIC
- LAN switch port

Main Panel

The Main Panel displays information on resources selected in the tree.

- [Resource List] tab

  Displays information on resources related to the resource selected in the resource tree.

- [Resource Details] tab

  Displays more detailed information on the resource selected in the tree, or on a resource that was double-clicked in the [Resource List] tab.

- [Recovery Settings] tab

  Displays information on the spare servers assigned to the resource selected in the resource tree.

- [Image List] tab

  Displays system and cloning image information.

- [Network Map] tab

  Displays a network diagram of registered resources.

Recent Operations

Displays the progress statuses and results of operations performed in Resource Coordinator VE.

Event Log

The Event Log displays information on events that have occurred.
It displays a log of events that have occurred on managed resources.

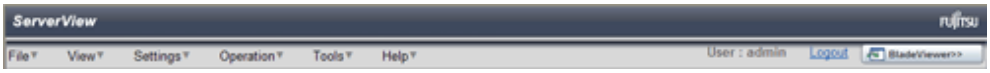
<BladeViewer> button

Opens the BladeViewer interface.
BladeViewer is a management interface specially designed for blade servers. It can only be used in conjunction with PRIMERGY BX servers.

2.2 Menus

This section describes the menus available in the RC console.

Figure 2.2 Menus



2.2.1 List of Menus

The menus provided on the menu bar of the RC console are listed in table below.
Options available vary according to the authority level of the user account.

Table 2.1 Menu Items

Menu bar	Menu	Submenu	Privileged user	General user	Function
File	Import	-	Yes	No	Imports the system configuration file for pre-configuration.
	Export	-	Yes	No	Exports the system configuration file for pre-configuration.
	Download Template	CSV format	Yes	Yes	Downloads a sample of the system configuration file (CSV format) for pre-configuration.
	Export Environmental Data	Chassis	Yes	Yes	Exports environmental data collected from chassis.
		Servers	Yes	Yes	Exports environmental data collected from servers.
		Power Monitoring Devices	Yes	Yes	Exports environmental data collected from power monitoring devices.
	Logout	-	Yes	Yes	Logs out of the RC console. (*1)
View	Reset Layout	-	Yes	Yes	Returns the layout of the RC console to its initial state.
Settings	Register	Chassis	Yes	No	Registers a chassis.
		Server	Yes	No	Registers a server.
		LAN Switch	Yes	No	Registers a LAN switch.
		Agent	Yes	No	Registers an Agent.
		Power Monitoring Device	Yes	No	Registers a power monitoring device.
	Delete	-	Yes	No	Deletes a resource.

Menu bar	Menu	Submenu	Privileged user	General user	Function
	Modify (*2)	Registration Settings	Yes	No	Modifies a resource's registration settings.
		HBA Address Rename Settings	Yes	No	Modifies a server's HBA address rename settings.
		Network Settings (*3)	Yes	No	Modifies the network settings of a LAN switch.
		Spare Server Settings	Yes	No	Modifies the spare server settings of a server.
		VM Host Login Account	Yes	No	Modifies the registered login account used to communicate with the VM host.
	User Accounts	-	Yes	Yes	Adds, changes and deletes user accounts.
	VM Management Software	-	Yes	No	Configures VM management software settings.
Operation	Update	-	Yes	Yes	Updates a resource.
	Power	ON	Yes	No	Powers on a server.
		OFF	Yes	No	Powers off a server after shutting down its operating system.
		OFF (Forced)	Yes	No	Powers off a server without shutting down its operating system.
		Reboot	Yes	No	Reboots a server after shutting down its operating system.
		Reboot (Forced)	Yes	No	Reboots a server without shutting down its operating system.
	LED (*3)	ON	Yes	No	Turns the maintenance LED on.
		OFF	Yes	No	Turns the maintenance LED off.
	Spare Server (*2)	Switchover	Yes	No	Switches over a server with one of its spare servers.
		Failback	Yes	No	Switches back a server to its pre-switchover state.
		Takeover	Yes	No	Accepts a switched over configuration as final (without switching back to the original configuration).
	Hardware Maintenance	Re-configure	Yes	No	Detects and re-configures the properties of a replaced server.
		Restore LAN Switch	Yes	No	Restores a LAN switch configuration.
	Maintenance Mode (*2)	Set	Yes	No	Sets a server to maintenance mode.
		Release	Yes	No	Sets a server to active mode.
	Backup/Restore (*2)	Backup	Yes	No	Backs up a system image from a server.
		Restore	Yes	No	Restores a system image to a server.
	Cloning (*2, *4)	Collect	Yes	No	Collects a cloning image from a server.
		Deploy	Yes	No	Deploys a cloning image to a server.

Menu bar	Menu	Submenu	Privileged user	General user	Function
Tools	Options	-	Yes	Yes (*5)	Modifies console and environmental data settings.
	Topology	Discover LAN switches	Yes	No	Discovers LAN switches within the Admin LAN.
		Detect physical links	Yes	No	Acquires physical link data from registered LAN switches.
Help	Manual	-	Yes	Yes	Displays product manuals.
	About	-	Yes	Yes	Displays product version.

*1: If multiple RC console or BladeViewer sessions exist, the login sessions may be terminated.
*2: Cannot be selected for a VM guest.
*3: Available only for PRIMERGY BX servers.
*4: Cannot be selected for a VM host.
*5: General users cannot change environmental data settings.

2.2.2 Popup Menus

Right-clicking an object displayed in the resource tree or in the [Image List] tab displays a popup menu with a list of options available for that object.
The tables below detail the popup menus provided for each object.
Available menus vary according to user account privileges.

Table 2.2 Popup Menus Available for the "Server Resources" Tree Node

Popup menu		Privileged user	General user	Function
Menu	Submenu			
Register	Chassis	Yes	No	Registers a chassis.
	Server	Yes	No	Registers a server.
Export	Environmental Data (Chassis)	Yes	Yes	Exports environmental data collected from chassis.
	Environmental Data (Servers)	Yes	Yes	Exports environmental data collected from servers.

Table 2.3 Popup Menus Available for Chassis

Popup menu		Privileged user	General user	Function
Menu	Submenu			
Delete	-	Yes	No	Deletes a chassis.
Update	-	Yes	Yes	Updates a chassis.
Modify	Registration Settings	Yes	No	Modifies a chassis' registration settings.
External Management Software	-	Yes	Yes	Opens a Management Blade's Web interface.
Export (*1)	Environmental Data	Yes	Yes	Exports environmental data collected from chassis.

*1: This option is only available for chassis equipped with power monitoring capabilities.

Table 2.4 Popup Menus Available for Servers

Popup menu		Privileged user	General user	Function
Menu	Submenu			
Register	Server (*1)	Yes	No	Registers a server.
	Agent	Yes	No	Registers an Agent.
Delete	-	Yes	No	Deletes a server.
Update	-	Yes	Yes	Updates a server.
Modify	Registration Settings	Yes	No	Modifies a server's registration settings.
	HBA Address Rename Settings	Yes	No	Modifies a server's HBA address rename settings.
	Network Settings (*1)	Yes	No	Modifies a server's network settings.
	Spare Server Settings	Yes	No	Modifies a server's recovery settings.
Maintenance Mode	Set	Yes	No	Sets a server to maintenance mode.
	Release	Yes	No	Sets a server to active mode.
Power	ON	Yes	No	Powers on a server.
	OFF	Yes	No	Powers off a server after shutting down its operating system.
	OFF (Forced)	Yes	No	Powers off a server without shutting down its operating system.
	Reboot	Yes	No	Reboots a server after shutting down its operating system.
	Reboot (Forced)	Yes	No	Reboots a server without shutting down its operating system.
LED (*1)	ON	Yes	No	Turns the maintenance LED on.
	OFF	Yes	No	Turns the maintenance LED off.
Hardware Maintenance	Re-configure	Yes	No	Detects and re-configures the properties of a replaced server.
Backup/Restore	Restore	Yes	No	Restores a system image to a server.
Cloning	Deploy	Yes	No	Deploys a cloning image to a server.
External Management Software (*2)	-	Yes	Yes	Opens external server management software.
Export (*8)	Environmental Data	Yes	Yes	Exports environmental data collected from servers.

Table 2.5 Popup Menus Available for Physical OS's, VM Hosts and VM Guests

Popup menu		Privileged user	General user	Function
Menu	Submenu			
Delete (*3)	-	Yes	No	Deletes a physical OS or VM host.
Update	-	Yes	Yes	Updates a physical OS, VM host or VM guest.
Modify (*3)	HBA Address Rename Settings	Yes	No	Modifies the HBA address rename settings of a server.
	Network Settings (*1)	Yes	No	Modifies the network settings of a server.
	Spare Server Settings	Yes	No	Modifies the recovery settings of a server.

Popup menu		Privileged user	General user	Function
Menu	Submenu			
	VM Host Login Account (*4)	Yes	No	Modifies the registered login account used to communicate with the VM host.
Power	ON	Yes	No	Powers on a server.
	OFF	Yes	No	Powers off a server after shutting down its operating system.
	OFF (Forced)	Yes	No	Powers off a server without shutting down its operating system.
	Reboot	Yes	No	Reboots a server after shutting down its operating system.
	Reboot (Forced)	Yes	No	Reboots a server without shutting down its operating system.
Spare Server (*3)	Switchover	Yes	No	Switchover a server with one of its spare servers.
	Failback	Yes	No	Switches back a server to its pre-switchover state.
	Takeover	Yes	No	Sets a spare server in switchover state as the new primary server (the spare server will take over the original primary server's role).
Maintenance Mode (*3)	Set	Yes	No	Sets a server to maintenance mode.
	Release	Yes	No	Sets a server to active mode.
Backup/Restore (*3)	Backup	Yes	No	Backs up a system image from a server.
	Restore	Yes	No	Restores a system image to a server.
Cloning (*3, *5)	Collect	Yes	No	Collects a cloning image from a server.
	Deploy	Yes	No	Deploys a cloning image to a server.
External Management Software (*2, *3)	-	Yes	Yes	Opens external management software.
VM Management Console (*4, *6, *7)	-	Yes	Yes	Opens the VM management console installed on the client machine.

*1: Available only for PRIMERGY BX servers.
*2: Available only for PRIMERGY servers.
*3: Cannot be selected for a VM guest.
*4: This menu is not available for a physical OS.
*5: Cannot be selected for a VM host.
*6: To use this feature, a VM management console must be installed and the Admin Client must be configured properly. After installing the VM management console, select this menu item and follow the instructions shown in the displayed dialog.
*7: This option may or may not be available according to the server virtualization server used. Refer to "A.1 Supported Functions" for details.
*8: This option is only available for servers equipped with power monitoring capabilities.

Table 2.6 Popup Menus Available for LAN Switches

Popup menu		Privileged user	General user	Function
Menu	Submenu			
Register	LAN Switch	Yes	No	Registers a LAN switch.
Delete	-	Yes	No	Deletes a LAN switch.
Update	-	Yes	Yes	Updates a LAN switch.

Popup menu		Privileged user	General user	Function
Menu	Submenu			
Modify	Registration Settings	Yes	No	Modifies a LAN switch's registration settings.
	Network Settings	Yes	No	Modifies VLAN settings of a LAN switch's external ports.
Restore	-	Yes	No	Restores a LAN switch configuration.
External Management Software	-	Yes	Yes	Opens a LAN switch's Web interface.

Table 2.7 Popup Menus Available for System Images

Popup menu		Privileged user	General user	Function
Menu	Submenu			
Restore	-	Yes	No	Restores a system image to a server.
Delete	-	Yes	No	Deletes a system image.

Table 2.8 Popup Menus Available for Cloning Images

Popup menu		Privileged user	General user	Function
Menu	Submenu			
Deploy	-	Yes	No	Deploys a cloning image to a server.
Delete	-	Yes	No	Deletes a cloning image.

Table 2.9 Popup Menus Available for the "Network Resources" Tree Node

Popup menu		Privileged user	General user	Function
Menu	Submenu			
Topology	Discover LAN switches	Yes	No	Discovers LAN switches within the Admin LAN.
	Detect physical links	Yes	No	Acquires physical link data from registered LAN switches.

Table 2.10 Popup Menus Available for the "Power Monitoring Devices" Tree Node

Popup menu		Privileged user	General user	Function
Menu	Submenu			
Register	Power Monitoring Device	Yes	No	Registers a power monitoring device.
Export	Environmental Data	Yes	Yes	Outputs environmental data.

Table 2.11 Popup Menus Available for Power Monitoring Devices

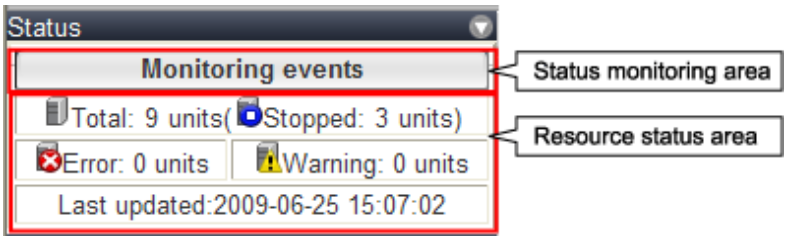
Popup menu		Privileged user	General user	Function
Menu	Submenu			
Delete	-	Yes	No	Deletes a power monitoring device.
Update (*1)	-	Yes	Yes	Updates a power monitoring device.
Modify	Registration Settings	Yes	No	Modifies a power monitoring device's registration settings.
Hardware Maintenance	Re-configure	Yes	No	Detects and re-configures the properties of a replaced power monitoring device.
Export	Environmental Data	Yes	Yes	Outputs environmental data.

*1: Unlike other resources, the properties of a power monitoring devices are not automatically updated. Use this option to update them manually when necessary.

2.3 Status Panel

This section explains the different statuses that are displayed in the RC console.

Figure 2.3 Status Panel



Status monitoring area

This area is used to monitor events that occur on managed resources. The status monitoring area changes color and blinks according to the event detected.
Clicking on the blinking area will stop the blinking.
The following table details the different statuses and their associated corrective actions.

Table 2.12 Monitor Status

Monitoring status	Background color	Details	Corrective Action
Monitoring events	Grey	This indicates a normal state. No warning or error-level events have occurred on the displayed resources.	No action is necessary.
Warning event detected	Yellow	This indicates a warning state. A warning-level event has occurred on one or more of the displayed resources.	Click the status monitoring area to stop the blinking and fix the cause of the problem.
Error event detected	Red	This indicates an error state. An error-level event has occurred on one or more of the displayed resources.	Click the status monitoring area to stop the blinking and fix the cause of the problem.

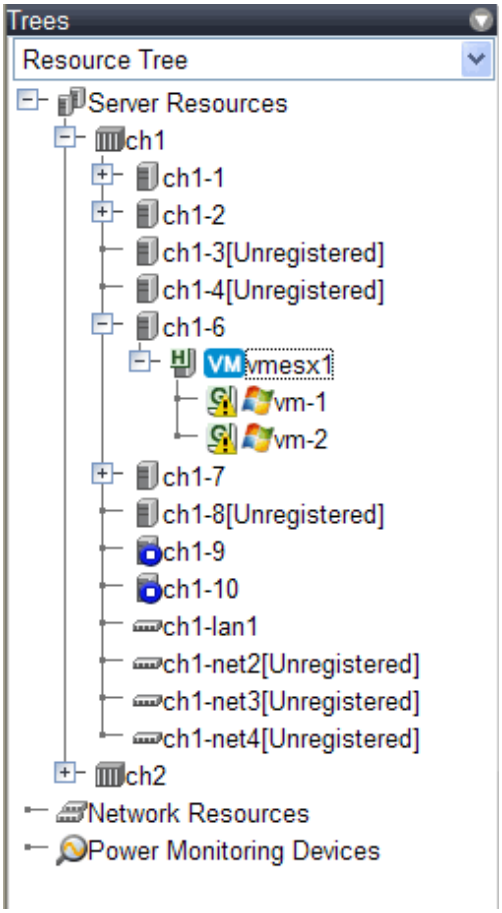
Resource status area

This area displays the number of registered servers experiencing each status.
The status monitoring area lights up when there is at least one server in either "Error" or "Warning" status.
Clicking a lit up status area will display a list of resources with that status in the [Resource List] tab. Double-click a displayed resource to switch to its [Resource Details] tab and open either its external management software or the Management Blade's Web interface to investigate the problem.

2.4 Tree Panel

This section describes the trees used in the RC console.

Figure 2.4 Tree Panel



Two trees are available under the Tree Panel: a resource tree and a VLAN tree. A drop-down menu located at the top of the Tree Panel enables selection of the displayed tree.

The resource tree is also split between three sub-trees: one for server resources, one for network resources, and one for power monitoring devices.

Resource Tree

Server Resources

Chassis, servers, physical OS's, VM hosts, VM guests, and LAN switches managed in Resource Coordinator VE are displayed in a tree view. Resources are primarily displayed in registration order. However, for server blades within a common chassis, the order by which Resource Coordinator VE detects blades takes precedence.
Resources displayed in the resource tree are represented by an icon and their resource name. Refer to "5.2 Resource Status" of the "ServerView Resource Coordinator VE Operation Guide" for details about the icons used to represent different resources.
For a non-registered resource, one of the following registration states is displayed at the end of the resource's name.

Table 2.13 Resource Registration States

[Unregistered]	The resource was automatically detected, but has not been registered yet.
[Registering]	The resource is being registered.
[Admin Server]	This server is the Admin Server itself.

If a label was set for a resource (in BladeViewer), this label is displayed after the resource name.

Display format

resource_name(label)

Clicking a resource in the resource tree displays information related to that resource in the Main Panel. Right-clicking a resource displays a list of available operations in a popup menu.
Refer to "2.2.2 Popup Menus" for details on popup menus.

When a problem occurs on a resource, it is represented by an icon shown on top of the resource icon.
Refer to "5.2 Resource Status" of the "ServerView Resource Coordinator VE Operation Guide" for details on status icons.
Clicking a resource icon will show information related to that resource in the Main Panel. Use this information to investigate the problem.
Refer to "2.5 Main Panel" for details on the information displayed in the Main Panel.

Network Resources

External LAN switches (those other than LAN switch blades) managed in Resource Coordinator VE are shown in a tree view. Resources are sorted and displayed by name in alphabetical order.

Resources displayed in the resource tree are represented by an icon and their resource name. Refer to "5.2 Resource Status" of the "ServerView Resource Coordinator VE Operation Guide" for details about the icons used to represent different resources.

For a non-registered resource, one of the following registration states is displayed at the end of the resource's name.

Table 2.14 Resource Registration States

[Unregistered]	The resource was automatically detected, but has not been registered yet.
[Registering]	The resource is being registered.

When a problem occurs on a resource, it is represented by an icon shown on top of the resource icon.

Refer to "5.2 Resource Status" of the "ServerView Resource Coordinator VE Operation Guide" for details on status icons.

Clicking a resource icon will show information related to that resource in the Main Panel. Use this information to investigate the problem.

Power Monitoring Devices

The power monitoring devices (PDU or UPS) used by Resource Coordinator VE to monitor power consumption are displayed in a tree view.
Refer to "5.2 Resource Status" of the "ServerView Resource Coordinator VE Operation Guide" for details on icons used to represent power monitoring devices.
Clicking a power monitoring device displayed in the resource tree will display its attributes in the Main Panel. Right-clicking a power monitoring device will display a list of available operations in a popup menu. Refer to "2.2.2 Popup Menus" for details on popup menus, and "2.5 Main Panel" for details on the information displayed in the Main Panel.

VLAN Tree

Resources for which VLAN IDs have been applied are displayed in a tree view. The following resource types are displayed.

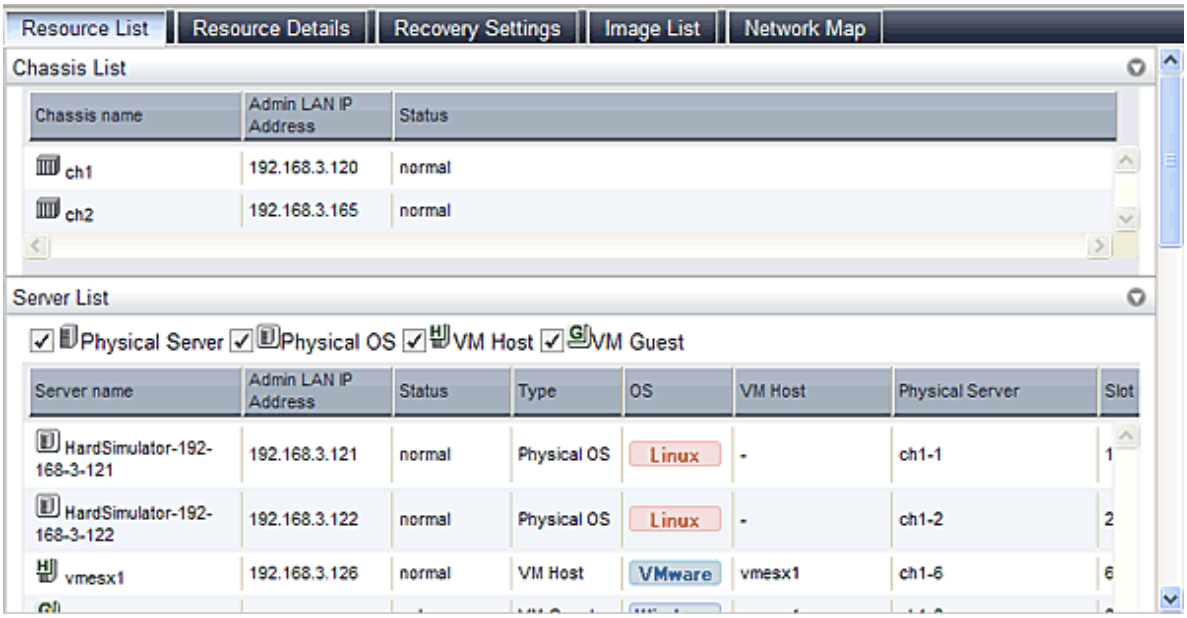
- Servers
- LAN Switches

Refer to "5.2 Resource Status" of the "ServerView Resource Coordinator VE Operation Guide" for details about the icons used to represent each resource.

2.5 Main Panel

This section describes the Main Panel of the RC console.

Figure 2.5 Main Panel



2.5.1 [Resource List] tab

The [Resource List] tab in the Main Panel displays a list of resources related to the resource that was selected in the resource tree.
Refer to "5.2 Resource Status" of the "ServerView Resource Coordinator VE Operation Guide" for details on the icons used to indicate different resources.
The table below shows the information displayed in the Resource List for each selectable resource.

Table 2.15 Resource List

Selected resource	Content displayed
Server Resources	Information on all registered chassis, servers, and LAN switches.
Chassis	Information on registered servers and LAN switches mounted in the selected chassis.
Server	Information on the physical OS's, VM hosts and VM guests running on the selected server.
Physical OS	Information on the selected physical OS.
VM host	Information on the VM guests running on the selected VM host.
VM guest	Information on the selected VM guest.
Unregistered server	Information on the selected unregistered server.
Network Resources	Information on all registered LAN switches (except LAN switch blades).
LAN switch	Information on the selected LAN switch.
Power Monitoring Device	Information on all registered power monitoring devices.
PDU or UPS	Information on the selected PDU or UPS.

Double-clicking a resource in the "Resource List" displays its "Resource Details" tab in the Main Panel. This tab shows detailed information on the selected resource.
In the "Resource List" tab, resources experiencing problems are shown by a status icons displayed on top of their resource icon. Switch to the "Resource Details" tab to check the faulty component or open external management software to investigate the problem. Refer to "Chapter 5 Monitoring" of the "ServerView Resource Coordinator VE Operation Guide" for details.

Clicking a column heading in the "Resource List" will sort the displayed resources in ascending or descending order.

Physical servers, Physical OS's, VM hosts and VM guests are displayed under the "Server List". Resources displayed in the "Server List" can be filtered by selecting or deselecting their corresponding checkboxes.

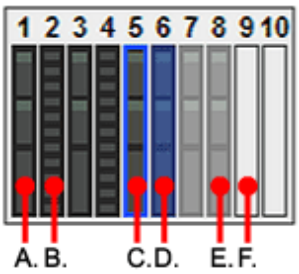
2.5.2 [Resource Details] tab

The [Resource Details] tab displays detailed information on registered resources.
This information is displayed by double-clicking any of the following resources in the resource tree:

- Chassis
- Server
- Physical OS
- VM host
- VM guest
- LAN switch
- PDU or UPS

Selecting a blade server displays the following chassis image in the [Resource Details] tab. This image shows the slot positions of all server blades installed in the chassis.

Figure 2.6 Chassis



The resource images shown in the above chassis image are explained in the table below.

Table 2.16 Meaning of the resources shown in the chassis image

Image	Meaning
A.	Registered server blade.
B.	Detected storage blade.
C.	Currently displayed server blade.
D.	Server blade selected within the chassis image.
E.	Server blade that has not been registered yet.
F.	Empty slot.

Attributes of Displayed Resources

The [Resource Details] tab displays different attributes for each resource, as described below.

- **Chassis Attributes**

Table 2.17 General Area

Item	Content displayed
Chassis name	Name used to identify a chassis.
Model name	Chassis model name.
Admin LAN (IP address)	Chassis management IP address.
Status	Chassis status.
Server blades	Number of server blades mounted in the chassis.

Item	Content displayed
LAN switch blades	Number of LAN switches mounted in the chassis.

See

Refer to "5.2 Resource Status" of the "ServerView Resource Coordinator VE Operation Guide" for details on the different resource statuses.

Table 2.18 Hardware Details Area

Item	Content displayed
Launch Management Blade Web UI	Link to the management blade's Web interface.

- **Server Attributes**

Table 2.19 General Area

Item	Content displayed
Physical server name	Name used to identify a server.
Model name	Server model name. (*1)
Product name	Server product name. (*2)
Status	Server status.
Slot (*3)	A slot number representing the mounted location.
Maintenance Mode	Operational status of a server (active or maintenance).
LED status (*3)	Illumination status of the maintenance LED.
Admin LAN (MAC address)	MAC address of the NIC used for the Admin LAN.
CPU type (*5)	Type of CPU.
CPU clock speed (*5)	CPU clock speed (frequency).
Memory capacity (*5)	Total capacity of server memory.
HBAAR LAN (MAC address) (*4)	MAC address used for the HBA address rename setup service.

*1: The model name displayed for powered-on, registered servers is obtained from ServerView Operations Manager. Otherwise, no model name is displayed.
*2: For PRIMERGY BX servers, the product name obtained from the management blade is displayed. For other servers, the model name is displayed.
*3: Displayed only for PRIMERGY BX servers.
*4: Displayed only for servers other than PRIMERGY BX servers.
*5: This attribute is displayed as "-" for servers other than PRIMERGY BX servers.

See

- Refer to the Management Blade's manual for details on management blades' product names.
- Refer to the ServerView Operation Manager manual for details on the server models displayed and obtained from ServerView Operation Manager.
- Refer to "5.2 Resource Status" of the "ServerView Resource Coordinator VE Operation Guide" for details on the different resource statuses.

Table 2.20 Hardware Details Area

Item	Content displayed
Server Management Software (*1)	Link to external server management software.

Item	Content displayed
Remote Management Controller IP address (*2)	IP address of the remote management controller.

*1: Displayed only for PRIMERGY BX servers.
*2: Displayed only for servers other than PRIMERGY BX servers.

Table 2.21 Network Properties Area

Item	Content displayed
Physical Connections	List of physical connections between the server's network interfaces and LAN switches ports.

Clicking a column heading in this list will change the color of the selected column and sort resources in either ascending or descending order.

Table 2.22 Hardware Maintenance Area

Item	Content displayed
NIC Summary (*1)	Shows the IP addresses associated with each MAC address.

*1: For servers other than PRIMERGY BX servers, only Admin LAN information is displayed.

Information

The IP address displayed is the one set within the server's operating system.
For network interfaces that were made redundant using BACS software, the information set in BACS (within the operating system) is displayed.

- **Attributes of Physical OS, VM Host or VM Guest**

Table 2.23 General Area

Item	Content displayed
Server name	Name used to identify a physical OS, VM host or VM guest.
Admin LAN (IP address) (*1)	IP address used on the Admin LAN.
Status	Status of the physical OS, VM host or VM guest.
Type	Type of the OS running on the server (physical OS, VM host or VM guest).
OS	Name of the operating system running on the server.
Physical server name (*1)	Name of the server on which the physical OS, VM host or VM guest is operating.

*1: Not displayed for VM guests.

See

Refer to "5.2 Resource Status" of the "ServerView Resource Coordinator VE Operation Guide" for an explanation of the resource status.

The following information is displayed only for VM Hosts.

Table 2.24 VM Host Information Area

Item	Content displayed
VM type	Type of VM.

Item	Content displayed
VM software name	Name of the VM software used.
VM software VL	Version level of the VM software used.
Number of VM guests	Number of VM guests.
VM management software	Link to the VM management console.
VM Guests	List of hosted VM guests.

The following information is displayed only for VM Guests.

Table 2.25 VM Guest Information Area

Item	Content displayed
VM type	Type of VM.
VM host name	Name of the VM host on which the VM guest is stored.
VM name	VM name.
VM management software	Link to the VM management console.

The following information is not displayed for VM guests.

Table 2.26 Hardware Details Area

Item	Content displayed
Server Management Software (*1)	Link to external server management software.
Remote Management Controller IP address (*2)	IP address of the remote management controller.

*1: Displayed only for PRIMERGY BX servers.
*2: Displayed only for servers other than PRIMERGY BX servers.

The following information is not displayed for VM guests.

Table 2.27 Latest System Image Area

Item	Content displayed
Version	Latest version of the system image.
Backup date	Date and time of the most recent system image backup.
Comments	Comments describing the system image.

The following information is not displayed for VM guests.

Table 2.28 Spare Server Settings Area

Item	Content displayed
Primary server	Name of the physical server that will be switched over during a server switchover.
Active server	Name of the currently active physical server.
Server switchover method	Method used to perform server switchover.
Boot type	System disk boot type.
Automatic server recovery	Flag indicating whether automatic server recovery is enabled or not.
Network switchover	Flag indicating whether or not to switch over network settings during a server switchover.

Item	Content displayed
Spare server	Assigned spare server(s).

The following information is not displayed for VM guests.

Table 2.29 HBA Address Rename Settings Area

Item	Content displayed
WWNN	The WWNN set on the HBA.
WWPN port1	The WWPN set on port 1 of the HBA.
WWPN port2	The WWPN set on port 2 of the HBA.

The following information is not displayed for VM guests.

Table 2.30 Network Properties Area

Item	Content displayed
VLAN	List of VLAN IDs set on the ports of adjacent LAN switches

When a column heading in the list is clicked, the color of the selected column will change and the resource can be sorted in either ascending or descending order.

- **LAN Switch Attributes**

Table 2.31 General Area

Item	Content displayed
LAN switch name	Name used to identify a LAN switch.
System Name (sysName)	System name set on the LAN switch.
IP address	IP address on the Admin LAN.
Device name (Product name)	Device name of the LAN switch.
Model name	Model name of the LAN switch.
Vendor	LAN switch vendor. This is not displayed for LAN switch blades.
Serial number	Serial number of the LAN switch.
Firmware version	Firmware version of the LAN switch.
Device status	Status of the LAN switch.
Slot	Slot number (mounted position) of the LAN switch. This is only displayed for LAN switch blades.

See

Refer to "5.2 Resource Status" of the "ServerView Resource Coordinator VE Operation Guide" for details on resource statuses.

Table 2.32 Port Properties Area

Item	Content displayed
Port Number	Selected LAN switch port.
Port Name	Name assigned to the selected port.
Link Status	Link status (up or down) of the selected port.
Speed/Duplex Mode	Speed and duplex mode of the selected port. (10M/H, 10M/F, 100M/H, 100M/F, 1G/F, 10G/F).

Table 2.33 VLAN Area

Item	Content displayed
VLAN ID	List of VLAN IDs set in the selected LAN switch.
Untagged Port(s)	List of ports set with a port VLAN ID.
Tagged Port(s)	List of ports sets with tagged VLAN ID(s).

Table 2.34 Link Data Area

Item	Content displayed
Resource Name (left side)	Name of the selected LAN switch.
I/F (left side)	Ports of the selected LAN switch.
I/F (right side)	Network interface (of a server resource) connected to the LAN switch port shown on the left side.
Resource Name (right side)	Name of the server resource connected to the LAN switch.

Table 2.35 Hardware Details Area

Item	Content displayed
Launch Switch Blade Web UI	Link to the LAN switch's Web interface.

Note

If no Web interface is available for the selected LAN switch, the following message is displayed: "There is no information to display". Refer to the LAN switch manual to confirm whether a Web interface is provided or not.

- **Power monitoring devices (PDU or UPS) attributes**

Table 2.36 General Area

Item	Content displayed
Device name	Name used to identify a power monitoring device.
Admin LAN (IP address)	IP address on the Admin LAN.
Device type	Device type (PDU or UPS).
Model name	Model name of the device.
Comments	Comments describing the device.

Table 2.37 Hardware Details Area

Item	Content displayed
Serial number	Serial number of the device.
Voltage	Voltage supplied to the device.
Hardware revision	Hardware version of the PDU device (not displayed for UPS devices).
Firmware revision	Firmware version of the device.
Date of manufacture	Manufacturing date of the device.
Outlets	Number of outlets provided by the PDU device (not displayed for UPS devices).
Intended orientation	Intended orientation (horizontal or vertical) of the PDU device (not displayed for UPS devices).

2.5.3 [Recovery Settings] tab

The [Recovery Settings] tab displays a list of spare servers assigned to the resource selected in the resource tree.
The table below shows the information displayed in the [Recovery Settings] tab.

Table 2.38 Recovery Settings Area

Item	Content displayed
Server Name	Name used to identify a physical OS or VM host.
Admin LAN IP Address	IP address on the Admin LAN.
Primary Server	Name of the currently active server.
Switchover State	Current switchover state.
Spare Server(s)	Name(s) of the server(s) assigned as spare server(s).

The switchover state is indicated by an arrow shown next to the currently active Primary Server. The messages "Switchover in progress", "Failback in progress" or "Takeover in progress" are displayed respectively during a server switchover, failback or takeover process.
If more than one spare server has been set, the first server listed is the one that is currently running.

Clicking a column heading in this list will change the color of the selected column and sort the displayed recovery settings in either ascending or descending order.

2.5.4 [Image List] tab

The [Image List] tab displays information regarding available images.
Those lists can be used to manage both system images and cloning images.

The following two tables list the items that are displayed in System Image List and Cloning Image List.

Table 2.39 System Image List Area

Item	Content displayed
Server Name	Name used to identify a physical OS or VM host.
Version	Version of the system image.
Backup Date	Date and time of the system image backup.
Comments	Comments describing the system image.

Table 2.40 Cloning Image List Area

Item	Content displayed
Cloning Image Name	Name used to identify a cloning image.
Version	Version of the cloning image.
Collection Date	Collection date and time of the cloning image.
OS	Name of the operating system stored in the cloning image.
Comments	Comments describing the cloning image.

Right-clicking a resource in the list displays a list of available operations in a popup menu.
Refer to "2.2.2 Popup Menus" for details on the operations available from popup menus.
Clicking a column heading in this list will change the color of the selected column and sort images in either ascending or descending order.

2.5.5 [Network Map] tab

Resource Coordinator VE displays the following information.

- Network configuration of physical and virtual servers (virtual switches and VM guests)
- Link state of each resource connection

- VLAN settings applied to physical and virtual servers

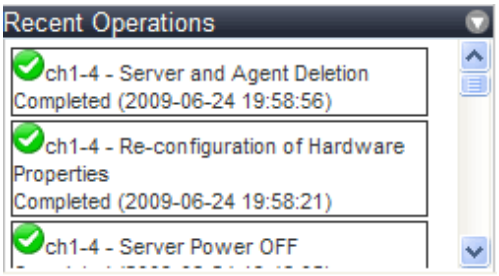
See

For details on the Network Map, refer to "Chapter 12 Network Map" in the "ServerView Resource Coordinator VE Operation Guide".

2.6 Recent Operations

This section describes the Recent Operations area of the RC console.

Figure 2.7 Recent Operations

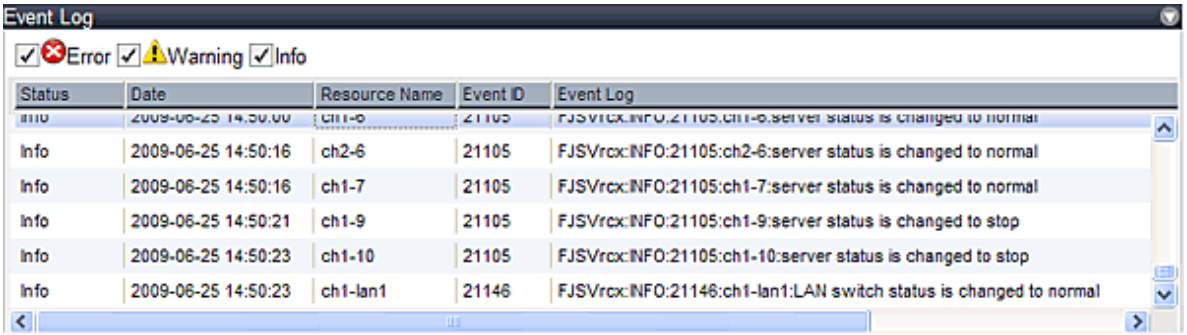


The Recent Operations area shows the status of operations that were recently performed. The result of a completed operation shows the operation's completion time and the related resource name. For operations that are still running, a progress bar is shown to indicate the current progress state.

2.7 Event Log

This section describes the Event Log displayed in the RC console.

Figure 2.8 Event Log



The Event Log displays a history of events that have occurred on managed resources. These events are added to the log automatically. Each event displayed in the Event Log provides the following information.

Table 2.41 Information Displayed in the Event Log

Item	Content displayed
Status	Displays the level of the event. There are three levels; "Error", "Warning" or "Info".
Date	Date and time at which the event occurred.
Resource Name	Name of the resource associated with the event.
Event ID	Identifier related to the event. No event ID is displayed for network resources.
Event Log	Content of the event.

The Event Log can be filtered using the Event Log checkboxes.
Selecting a checkbox will show the events whose status corresponds to that of the selected checkbox. Deselecting a checkbox will hide such events.
Clicking a column heading will change the color of the selected column and sort events in either ascending or descending order.

Note

When a resource's status becomes "fatal", its related event shows an "Error" status in the event log. For this reason, the actual status of a resource should be confirmed from either the resource tree or the [Resource List] tab.

Chapter 3 System Design and Initial Setup

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

3.1 Defining the Server Environment

This section explains how to define the server environment settings required for a Resource Coordinator VE setup.

3.1.1 Chassis Settings (For blade server environments)

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

Chassis name

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

Admin IP address (IP address of the management blade)

This IP address must be in the same subnet as the Admin Server.

SNMP Community

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

SNMP trap destination

The SNMP trap destination must be the Admin Server's IP address.

Note

- To enable server switchover and cloning between servers in different chassis, use the same SNMP community for each chassis.
- For servers other than PRIMERGY BX servers, refer to the settings mentioned in "3.1.2 Settings for Rack-Mount or Tower Servers".

3.1.2 Settings for Rack-Mount or Tower Servers

Resource Coordinator VE 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)

The IP address must be in the same subnet as 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 is already 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 password 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 is already 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 Agent). In that case, choose a value for the following setting.

SNMP community name

Name of the SNMP community used to communicate with the management software (ServerView Agent) on the managed server.
This string can contain up to 32 alphanumeric characters (upper or lower case), underscores ("_") and hyphens ("-").

Note

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

3.2 Defining the Network Environment

This section explains how to define the network environment configuration and settings required for a Resource Coordinator VE setup.

3.2.1 Network Configuration

The following will define the network configuration required by the system.

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

- Network interface assigned to the Admin LAN
- Network interface assigned to the Public LAN

Choose the following settings to fit the system environment.

- Network redundancy settings
- Network configuration of LAN switch blades (when using PRIMERGY BX servers)

Refer to "Example of VLAN network configuration (with PRIMERGY BX600)" and the description below to define a network configuration.

- Admin LAN

  The Admin LAN is the network used by the Manager to communicate with Agents on the managed servers and other managed devices.
  The number of network interfaces required for the Admin Server and managed servers can be determined as follows.
  For a non-redundant configuration: 1 network interface.
  For a redundant configuration: 2 network interfaces.

  If HBA address rename is used, two network interfaces (named NIC1 and NIC2) are required regardless of network redundancy. Refer to "Required Network Configuration when Using HBA Address Rename" for details.

  For PRIMERGY BX managed servers:

  - For a non-redundant configuration

    NIC1 (Index1)

  - For a redundant configuration, or when using HBA address rename

    NIC1 (Index1) and NIC2 (Index2)

Set up routing to enable communications from the Admin Client to the Admin Server. It is also suggested to allow communications from the Admin Client to managed servers, server management units, and switch blades. Such routing configuration is necessary to allow access to ServerView and other management consoles. There is no need to set up routing if the Admin Client is already located within the Admin LAN.

Note

- 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 a LAN switch outside the chassis.
- 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 a 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 when ports with different speeds co-exist in the same network, or multiple image operations are run simultaneously.

- Public LAN

  The Public LAN is the network used by managed servers to provide services over internal or external networks (such as intranets or the internet).

  Use NIC3 or higher (Index3 or higher) on managed servers:

  A network interface can be shared between multiple Public LANs by using a redundant configuration and tagged VLAN.

Information

For blade servers, depending on the model of LAN switch used in the same chassis, the network interfaces whose index number is comprised between 3 and 6 (NIC3 - NIC6) can not be used.
Instead, it is possible to use two more interfaces for the Public LAN by adding expansion cards (NIC7 and NIC8) and a LAN switch blade, or by sharing the NIC1 and NIC2 interfaces with the Admin LAN.
All network interfaces shared between the Admin and Public LANs should be configured with tagged VLAN IDs.

- 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. 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 (blade server side) and external ports of each LAN switch blade.

  - Internal ports

    For the internal ports connected to Admin LAN network interfaces (see "Admin LAN"), only port VLAN is supported. Be sure to configure those ports with port VLAN IDs.
    For the internal ports connected to Public LAN network interfaces (see "Public LAN"), be sure to assign different VLAN IDs (port or tagged VLAN) for each subnet, while avoiding the VLAN ID "1" (default VLAN ID).
    Using tagged VLANs on LAN switch ports also requires configuring the network interfaces of managed servers with tagged VLANs. As Resource Coordinator VE cannot set tagged VLANs to network interfaces on servers, this must be done manually.

  - External 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.

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 port(s) used for the Admin LAN.

     - Change the VLAN ID used by the admin IP of the LAN switch blade.

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

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

- VLANs can not be set from the RC console on ports set with any of the following:

  - Link state group

  - Backup port

  - Deactivated (depends on LAN switch blade model)

Choose VLAN IDs as well as VLAN types (port or tagged VLAN) for the ports on LAN switch blades that are connected to each server blade's network interfaces. For each if a physical server's network interfaces, choose:

- Physical server name

- NIC index

- VLAN ID

- VLAN type (port or tagged VLAN)

Note

On servers, operating systems associate each physical network interface with a connection name (Local area connection *X* in windows and eth*X* in Linux).
If more than one network interface is installed, 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.
Refer to network interface manuals for details.
Also note that Resource Coordinator VE uses the physical index of a network interface (based on physical mount order).

[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 3.1 With port VLANs

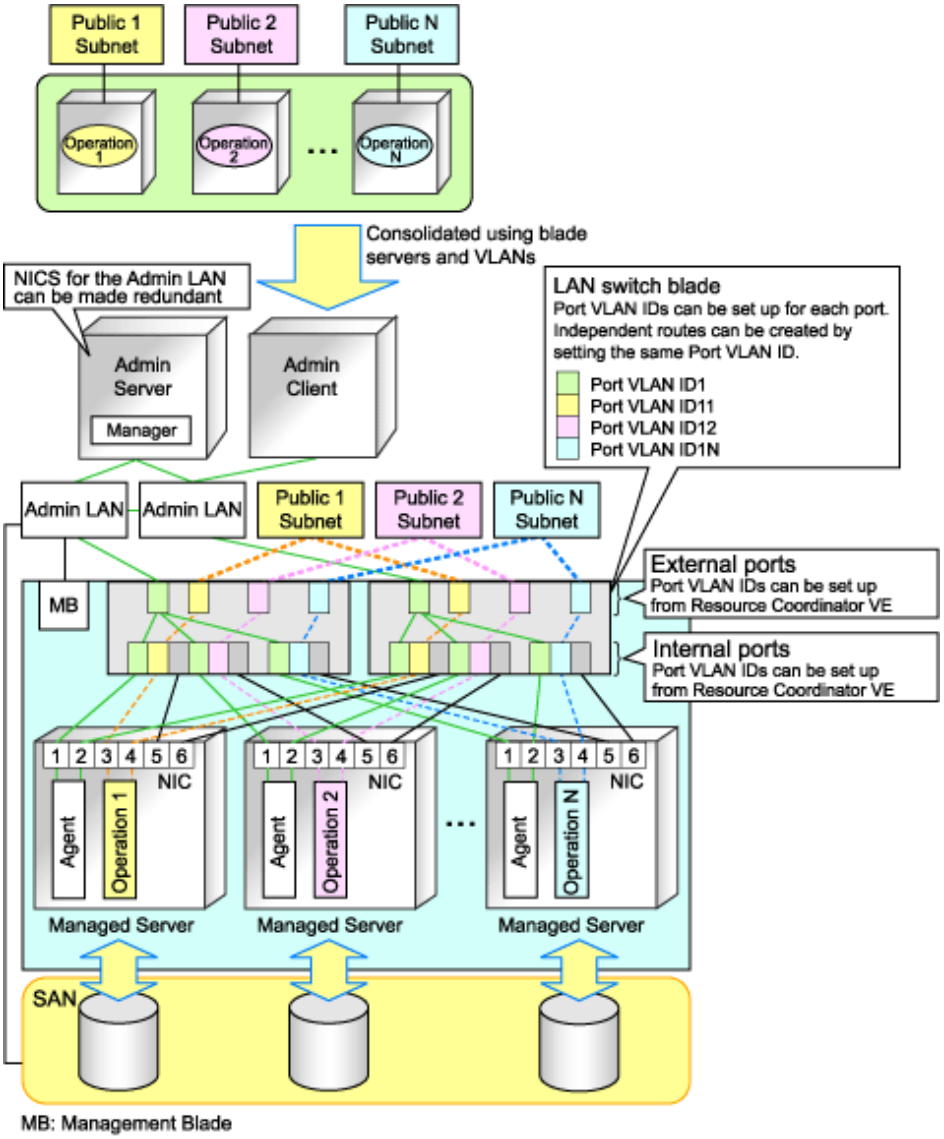
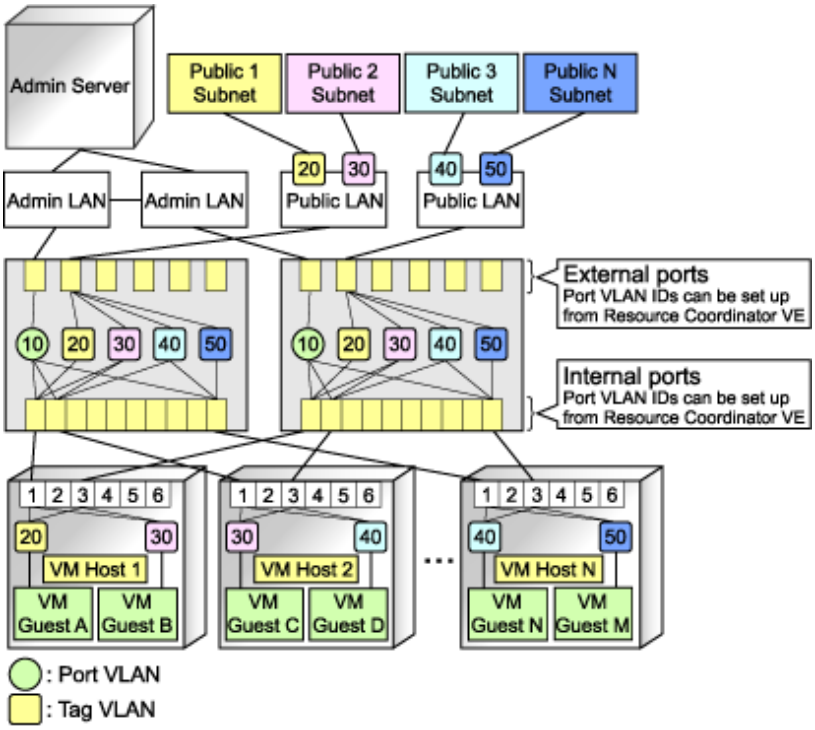


Figure 3.2 With tagged VLANs



Information

It is recommended that a dedicated Admin LAN is 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 Coordinator VE.

- 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 LAN and a Public LAN where a dedicated Admin LAN is required.

Required Network Configuration when Using HBA Address Rename

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

- Manager cluster configuration with Admin LAN redundancy

  For details, refer to "Appendix B Manager Cluster Operation Settings and Deletion" in the "ServerView Resource Coordinator VE Installation Guide".

- Dedicated HBA address rename setup server

This section describes the network configuration that is required for an environment with a dedicated HBA address rename server.
For details about the HBA address rename setup service, refer to "6.2.2.1 Settings for the HBA address rename setup service".

- This service uses NIC2 (Index2). Connect NIC2 to the Admin LAN.

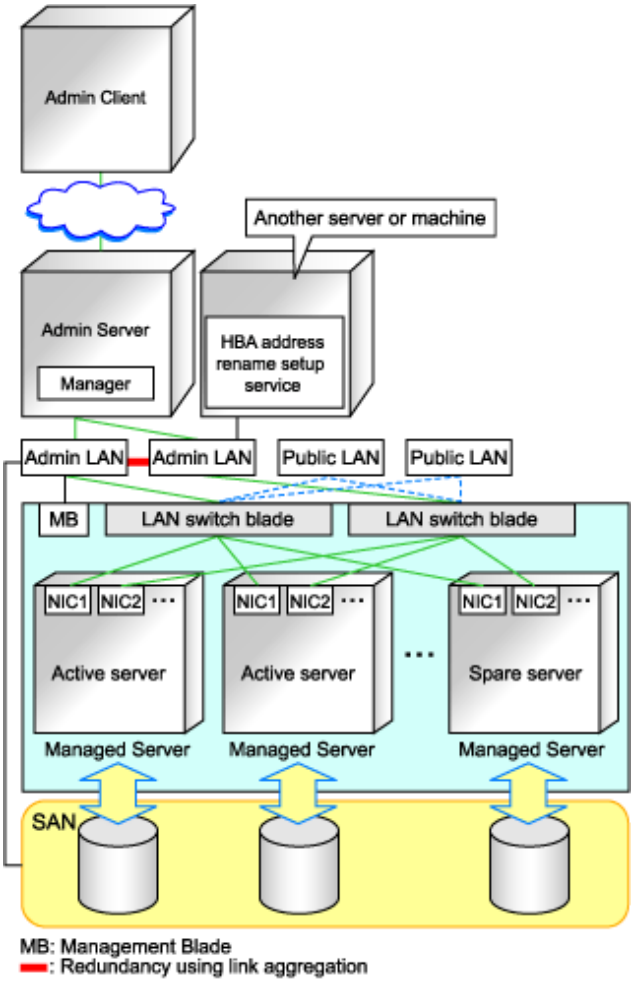
- This service periodically obtains information about managed servers from the Admin Server and operates using this information. For this reason, it should be installed on a server that can be left active all the time.
- There must be two LAN cables between LAN switches (cascade connection) on the Admin 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 3.3 Sample configuration showing the HBA address rename setup service (with PRIMERGY BX600)



- Connections between LAN switches on the Admin LAN can be made redundant using link aggregation.
- Connect the NIC2 (Index2) to the Admin LAN.
- 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.

Functions Provided by Resource Coordinator VE

Resource Coordinator VE provides the following VLAN management functions for PRIMERGY BX LAN switch blades.

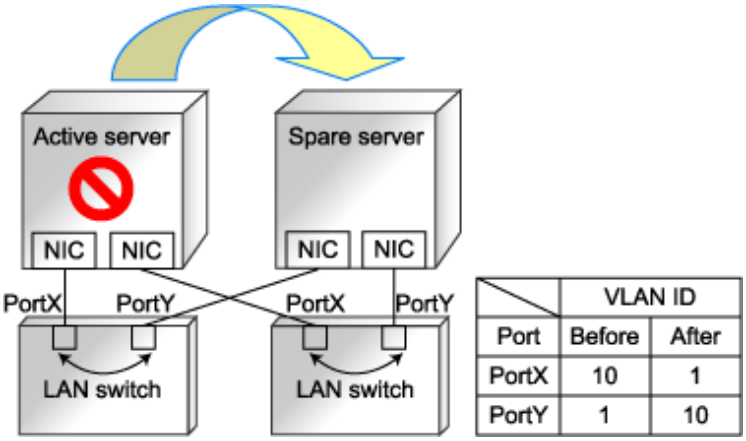
- VLAN configuration

  VLAN IDs of switch blade ports can be configured from the RC console.

- Exchange of VLAN IDs within each LAN switch blade in conjunction with server switchovers

  When a server switchover occurs, the VLAN configuration of related LAN switch blades is automatically adjusted to preserve the network connectivity of applications.
  VLAN IDs that were set on the LAN switch blade ports connected to the original server are exchanged with the VLAN IDs set on the ports connected to the spare server, as shown in "Figure 3.4 VLAN exchange mechanism for Auto-Recovery, server switchover and server failback".

Figure 3.4 VLAN exchange mechanism for Auto-Recovery, server switchover and server failback



	VLAN ID	
Port	Before	After
PortX	10	1
PortY	1	10

Note

The targets of this VLAN ID exchange are the LAN switch blade ports connected to the switched over servers. If the switched over servers are connected to different LAN switch blades, the external ports of those LAN switches should be set with the same VLAN configuration, and the switch blades placed in the same network.

3.2.2 IP Addresses (Admin LAN)

This section describes how to choose IP addresses for devices to be set on the Admin LAN.
Ensure that all of the IP addresses chosen here are on the same subnet.

- IP address used by the Admin Server for management purposes

  Choose an IP address for the network interface used to communicate with managed devices.
  This IP address will be asked during the Manager's installation.
  Note that clients can also access the Manager via IP addresses other than this Admin LAN IP address, as long as those addresses were set within the Admin Server operating system.

- IP addresses used by managed servers for management purposes

  These are IP addresses that are used to communicate with the Admin Server.
  They are specified when a managed server is registered.
  Refer to "6.1.2 Registering Managed Servers" for more information about registering managed servers.
  When registering a server that will be used as a spare server, assign an IP address that does not conflict with IP addresses of other managed servers.

- IP addresses used by other devices for management purposes

  - LAN switches blades
  - Server management units such as management blades or IPMI controllers.
  - Power monitoring devices

A management IP address must also be chosen for each of the following devices if they are to be registered into Resource Coordinator VE. For the following components, IP addresses can be chosen either within or outside of the Admin LAN.

- VM Management Product
  IP address of the server on which a VM management product is to be installed.
- LAN switches other than LAN switch blades
  IP address used by the Admin Server to track network connections (topology) between managed servers (PRIMERGY BX) and their adjacent LAN switches, and display them in the Network Map.

3.2.3 Public LAN Settings for Managed Servers

The Public LAN network settings for a managed server will be configured automatically when a cloning image is deployed.
Refer to "8.6 Network Parameter Auto-Configuration for Cloning Images" for how to set up a managed server in a Public LAN.

3.2.4 LAN Switch Settings

Choose the following settings for LAN switches that will be managed by Resource Coordinator VE.

- Telnet login user name

  This user name can contain up to 64 alphanumeric characters (upper or lower case), underscores ("_") and hyphens ("-").

- Telnet password

  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

  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 community name

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

- SNMP trap destination

  This must be the IP address of the Admin Server.

Note

Depending on the LAN switch used, setting an SNMP trap destination may restrict SNMP access to that switch.
In a clustered Manager configuration, set the physical IP addresses of both the primary and secondary nodes as SNMP trap destinations.
If the LAN switch is set to only grant access from known IP addresses, be sure to give permissions to the physical IP addresses of both the primary and secondary cluster nodes, as is done with trap destination settings.
Refer to the LAN switch manual for details.

Information

Character limitations may vary depending on the LAN switch used.
Refer to the LAN switch manual for details.

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

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

Note

- Adjacent LAN switches should be set to use the same protocol.
  Refer to LAN switch manuals for details.
  If a LAN switch does not support either one of those two protocols (LLDP or CDP), it should be set up to use the supported protocol.
- Resource Coordinator VE can not detect the network connections between a LAN switch set in IBP mode and its adjacent LAN switches.
- 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 blade

  - PY CB Eth Switch/IBP 1Gb 36/12

  The following settings must be set to the same value.

  - 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
- Network connections may not display properly if two or more LAN switches are set with a conflicting system name (sysName).

3.3 Defining the Storage Environment

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

3.3.1 Storage Configuration

Define the storage configuration required for the system.

Resource Coordinator VE supports the following configurations.

Table 3.1 Supported storage device configurations

Configuration	System disk	Data disk(s)
1	SAN storage	SAN storage
2	Local disk	Local disk (*1), NAS
3	Local disk	SAN storage

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

Information

- Configurations 1 and 3 support I/O virtualization.
- A server switchover can be performed only on servers that are connected to a single SAN storage system.
  Resource Coordinator VE does not support a server's switchover when it is connected to multiple SAN storage systems.
- A SAN storage system can be used as a shared cluster disk.
  However, a server which is defined in a cluster cannot be switched over.

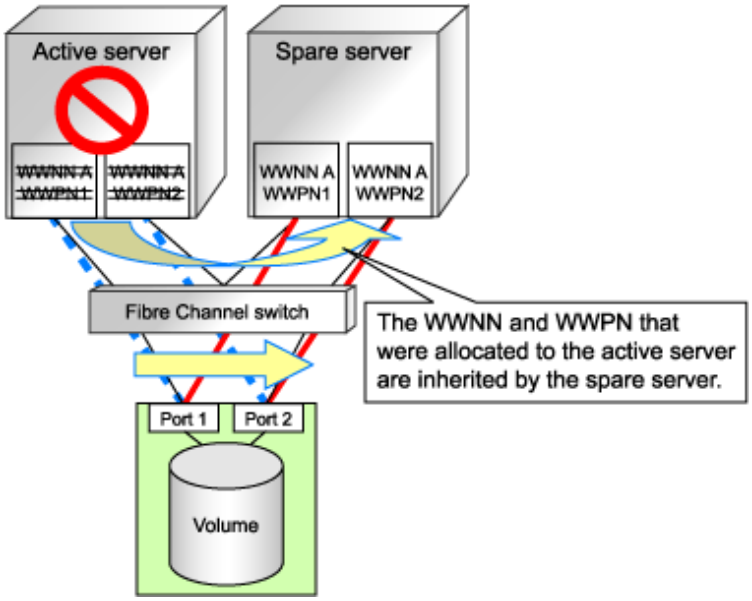
- Resource Coordinator VE supports both single path and multi-path storage connections.

Functions Provided by Resource Coordinator VE

The I/O virtualization features available with Resource Coordinator VE allow spare servers to inherit the WWN of Primary Servers. As a result, there is no more need to reconfigure the storage devices connected to the involved servers.
Note that WWN is a general term for both WWNN and WWPN. WWNN stands for node name and WWPN stands for port name.

The following example shows how server switchovers occur.

Figure 3.5 Example of a server switchover based on I/O virtualization



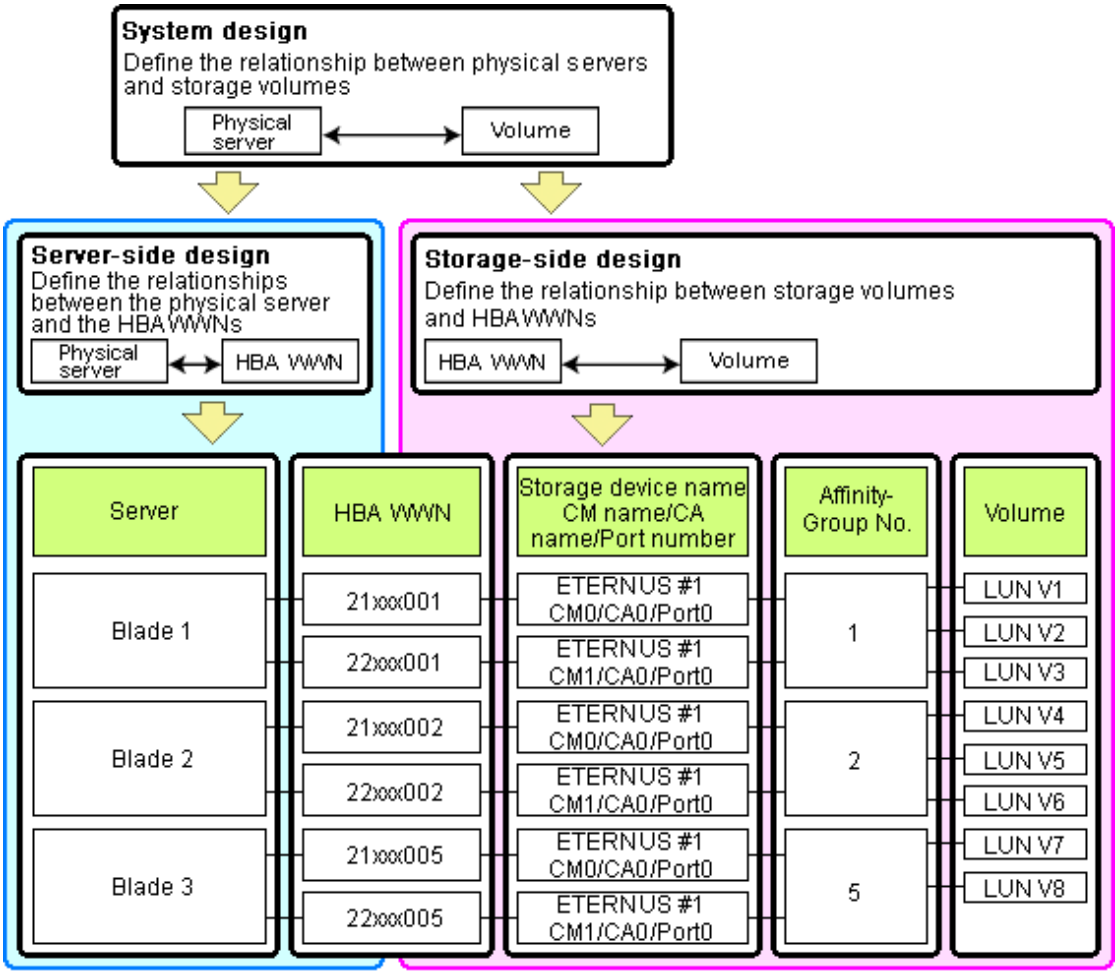
3.3.2 HBA and Storage Device Settings

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 storage device manuals each storage device for details.

Note

Resource Coordinator VE does not support configurations where managed servers are mounted with three or more HBA ports.

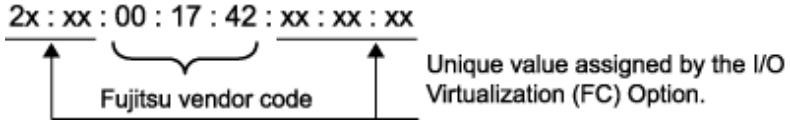
Figure 3.6 WWN system design



Choosing WWNs (when the HBA address rename function is used)

Choose the WWNs to use with the HBA address rename 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, 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.

The value provided by the "I/O Virtualization Option" is used as the WWN.
The WWN format used by the HBA address rename function is 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

The "x" part should be set to the I/O address of each HBA adapter (in descending order).
I/O addresses of HBA adapters can be confirmed using the HBA BIOS or other tools provided by HBA vendors.

Example

For a server with two ports, WWNs could be configured 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               : 21:00:00:17:42:51:00:00
WWPN value for HBA port 2               : 22:00:00:17:42:51:00:00
```

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.

3.4 Defining the Power Monitoring Device Environment

This explains how to define the power monitoring environment settings required for a Resource Coordinator VE setup.

3.4.1 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 one and six minutes, or 10 minutes. The default is 5 minutes.

Data storage period

This defines the storage period for the collected environmental data.

Table 3.2 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

3.4.2 Power Monitoring Device Settings

Choose values for the following power monitoring device (PDU or UPS) settings. If any of those settings is already determined by other software, use that value.

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.

3.5 Configuring the Server Environment

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

Chassis Settings (for Blade Servers)

Refer to the management blade manual to apply the settings chosen in "3.1.1 Chassis Settings (For blade server environments)" to the management blade.
Note that the SNMP Community must be set to Write (read and write) access.

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

  Set the Admin Server IP address.

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".

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

Remote Management Controller Settings (for Rack-Mount or Tower Servers)

Refer to the remote management controller manual to apply the settings chosen in "3.1.2 Settings for Rack-Mount or Tower Servers" to the IPMI controller.

- IP address
- User name
- Password
- SNMP community (for servers other than PRIMERGY BX servers)
- SNMP trap destination

  Set the Admin Server IP address.

BIOS Settings for Managed Servers

The following BIOS configurations must be modified.

System BIOS

This is the system BIOS for a managed server.
Enable or disable the internal SCSI BIOS and FC-HBA BIOS as appropriate, and set up the appropriate boot order.

Note

The BIOS settings of server blades include an option to automatically start up servers when their enclosing chassis is powered on. Refer to the server blade manual for details.

Internal SCSI BIOS

These are the BIOS settings for the internal SCSI disk(s) of a managed server.
Enable or disable booting from internal disks as appropriate.

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 the backup/restore or cloning function**

  System BIOS

  Set the boot order as follows.

  1. Boot from the first Admin LAN network interface (NIC1: Index1)
  2. Boot from the second Admin LAN network interface (NIC2: Index2)
  3. Boot from the CD-ROM (when a CD-ROM is connected)
  4. Boot from the disk

  Note

  - Do not change the boot order once a Primary Server has commenced operation. Even when booting from disk, there is no need to change the boot order.
  - Step 2 is only required for a redundant Admin LAN configuration.

  Internal SCSI BIOS

  The servers to which a cloning image is deployed should have the same internal SCSI BIOS settings as those of the server from which the image was collected. Similarly, when using server switchover, primary servers and their spare servers should have the same internal SCSI BIOS settings.

  FC-HBA BIOS

  No specific setting is required.

  When using HBA address rename and SAN storage only for data storing purposes, disable boot from SAN. Refer to the manual of each FC-HBA for details on FC-HBA BIOS settings.
  This setting is only required if a SAN storage system is used.

- **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 network interface used by the Admin LAN. (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 Primary Server has commenced operation. Even when booting from disk, there is no need to change the boot order.

Internal SCSI BIOS

If the managed server does not have an internal SCSI disk, disable the option to boot from an internal SCSI disk. However, in some cases (depending on a combination of factors such as server model, HBA model, and firmware), this option should either be enabled or disabled. Refer to the FC-HBA manual for instructions on whether or not to enable or disable boot from internal SCSI disk.

FC-HBA BIOS

Enable booting from SAN storage devices.

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

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 page.

  URL: http://www.fujitsu.com/global/services/computing/server/ia/ (As of September 2009)

Settings for Server Virtualization Software

Server Virtualization Software must be configured appropriately for Resource Coordinator VE. Refer to "A.2 Configuration Requirements" for details on the required server virtualization software settings.

3.6 Configuring the Network Environment

This section describes how to configure LAN switches for Resource Coordinator VE.

LAN Switch Settings

- LAN switch blades

  Refer to the LAN switch blade manual to apply the following settings.

  - VLAN IDs for the Admin LAN ports used to communicate with the Admin Server, as chosen in "3.2.1 Network Configuration"
  - Settings chosen in "3.2.4 LAN Switch Settings"

  VLAN settings for other switch blade ports can be set from the RC console.
  Refer to "6.2.1 Configuring VLANs on LAN Switches" for details.

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

  After setting up a LAN switch blade, perform a backup of the LAN switch blade's configuration. Refer to the manual of the LAN switch blade used for details how to backup of a switch blade.

- LAN switches other than LAN switch blades

  Refer to the LAN switch manual to apply the settings chosen in "3.2.4 LAN Switch Settings".

Note

Resource Coordinator VE uses telnet to log into LAN switches and automate settings.
Some models may restrict the number of simultaneous connections. In this case, log out from other telnet connections.

3.7 Configuring the Storage Environment

This section describes how to configure storage devices for Resource Coordinator VE.

Storage Device Settings

Using the HBA address rename function requires adequate preparation of storage environment settings (described below).

Storage settings can be configured using storage management software (such as ETERNUSmgr, ETERNUS SF Storage Cruiser or others). For details, refer to the manual of the relevant product.
The storage settings mentioned here are those that apply to the servers to be managed with I/O virtualization. If storage settings (zoning, LUN masking or any other security setting) were already made for managed servers, those settings should be cancelled and re-defined using the server-side WWPN settings chosen in "3.3.2 HBA and Storage Device Settings".

Note that the storage settings described here use ETERNUS terminology. "Affinity groups" in ETERNUS are usually referred to as "LUN masking" or "LUN mapping" in other storage products.

Setting up Logical Volumes and Affinity Groups

The logical volumes for storage devices and affinity groups allocated for servers must be configured.
These settings can be configured easily using either storage management software (such as ETERNUSmgr or the Storage Volume Configuration Navigator feature of ETERNUS SF Storage Cruiser).

Access Path Settings

Access paths between servers and storage devices must be made by applying the WWPN values chosen in "3.3.2 HBA and Storage Device Settings" to each server HBA. This will allow servers to access storage devices.
To configure storage devices and Fibre Channel switches, use appropriate storage management software.
Note that these configurations are best performed using the ETERNUS SF Storage Cruiser's storageadm zone command.

- Using the ETERNUS SF Storage Cruiser's storageadm zone command

  After registering the storage for management in the ETERNUS SF Storage Cruiser manager, set up access paths using the "add" parameter of the storageadm zone command, based on the storage-side designs that were chosen in "3.3.2 HBA and Storage Device Settings".
  The WWPN of the target storage device CA port must be specified with the storageadm zone command. Check this WWPN using either storage management software (such as ETERNUSmgr) or ETERNUS SF Storage Cruiser after the storage device has been configured.

  Refer to the ETERNUS SF Storage Cruiser manual for details on the storageadm zone command, configurable storage devices, and the graphical interface used to check access path settings.

Note

For access paths, point-to-point WWPN zoning is required.
Zoning (or port zoning) is required for configuring access paths.

3.8 Configuring the Power Monitoring Environment

This section describes how to configure power monitor devices for Resource Coordinator VE.

Apply the following settings to power monitoring targets. Refer to the manual of each 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).

Chapter 4 Installation

Installation of Resource Coordinator VE requires the preparations described in "Chapter 3 System Design and Initial Setup" to be performed first.
Refer to the "ServerView Resource Coordinator VE Installation Guide" for details on how to install Resource Coordinator VE.

Chapter 5 Starting and Stopping

This chapter explains how to start and stop the Resource Coordinator VE Manager and Agent services, how to check their running state, and how to open and close the RC console.

Managers and Agents start automatically when their respective servers are powered on. Normally no special operation is required to start them.

Note

When using the HBA address rename function, ensure that the Manager is started before powering on any managed servers. The power on procedure should be managed as follows: start the Admin Server together with storage devices, then start managed servers 10 minutes later.
Managed servers will not boot up properly if they are started before the Manager. Make sure that the Manager is running before turning on the managed servers.
Additionally, when using the HBA address rename function, the HBA address rename setup service should be started on a server and left running all the time. Refer to "6.2.2.1 Settings for the HBA address rename setup service" for details on starting, stopping and checking the state of the HBA address rename setup service.

5.1 Manager

The Resource Coordinator VE Manager starts automatically on the Admin Server.
This section explains how to manually start or stop the Manager and how to check its running state.

[Windows]
The Manager is made up of the following two groups of Windows services:

- Manager services

  Resource Coordinator Manager
  Resource Coordinator Task Manager
  Resource Coordinator Web Server(Apache)
  Resource Coordinator Sub Web Server(Mongrel)
  Resource Coordinator Sub Web Server(Mongrel2)
  SystemWalker MpWksttr

- Deployment services

  Deployment Service
  TFTP Service
  PXE Services

The state of these services can be checked from the Windows Control Panel. Open "Administrative Tools", and then open the [Services] window.
Services should be started and stopped from the rcxadm mgrctl command (start and stop subcommands), as this command collectively controls both Manager and deployment services.

Refer to "5.6 rcxadm mgrctl" of the "ServerView Resource Coordinator VE Command Reference" for details on these commands.

To start or stop a Manager in a clustered configuration, right-click the Manager application shown under the Failover Cluster Management tree, and select either [Bring this service or application online] or [Take this service or application offline].

[Linux]
The Manager is made up of the following two groups of Linux services.

- Manager services

  rcvmr

  Besides, Manager services include the following daemons.

  rcxmanager
  rcxtaskmgr

rcxmongrel1
rcxmongrel2
rcxhttpd

- Deployment services

  scwdepsvd
  scwpxesvd
  scwtftpd

The status of each of those services can be confirmed from the "service" command, as shown below.

```
# service rcvmr status <RETURN>
# service scwdepsvd status <RETURN>
# service scwpxesvd status <RETURN>
# service scwtftpd status <RETURN>
```

Services should be started and stopped from the rcxadm mgrctl command (start and stop subcommands), as this command collectively controls both Manager and deployment services.
Refer to "5.6 rcxadm mgrctl" of the "ServerView Resource Coordinator VE Command Reference" for details on these commands.

To start or stop a Manager in a clustered configuration, use the cluster administration view (Cluster Admin).

Refer to the PRIMECLUSTER manual for details.

Note

- The "Systemwalker MpWksttr" service is shared between the following products:

  - Systemwalker Centric Manager
  - ETERNUS SF Storage Cruiser

  Since the Systemwalker MpWksttr service is shared, the rcxadm mgrctl command has the following effects:

  - rcxadm mgrctl start

    This command starts the Systemwalker MpWksttr service only if it was not already running.

  - rcxadm mgrctl stop

    This command leaves the Systemwalker MpWksttr service running.

  Use the following procedure to stop the Systemwalker MpWksttr service.

  [Windows]

  1. Stop the other Manager services using the "rcxadm mgrctl stop" command.
  2. If there are other products installed on the Admin Server that share the Systemwalker MpWksttr service, stop the services associated with these products.
  3. From the Control Panel, open "Administrative Tools", open the [Services] window, and stop the Systemwalker MpWksttr service.

  [Linux]

  1. Stop the other Manager services using the "rcxadm mgrctl stop" command.
  2. If there are other products installed on the Admin Server that share the Systemwalker MpWksttr service, stop the services associated with these products.
  3. Use the following command to stop the Systemwalker MpWksttr service.

     ```
     # /opt/FJSVswstt/bin/mpnm-trapd stop <RETURN>
     ```

- Resource Coordinator VE cannot operate if any of the Manager services are stopped. Ensure that all services are running when Resource Coordinator VE is running.

- If the Manager is unable to communicate on the Admin LAN when started up (because of LAN cable disconnections or any other causes), PXE Services may not start automatically. If PXE Services are stopped, investigate the network interface used for the Admin LAN and confirm whether it can communicate with other nodes on the Admin LAN.

  If the Manager can not communicate with Admin LAN nodes, restore the Admin LAN itself and restart the Manager according to the above procedure.

5.2 Agent

The Resource Coordinator VE Agent starts automatically on managed servers.
This section explains how to manually start or stop an Agent and how to check its power state.

[Windows/Hyper-V]
The Agent consists of the following two Windows services.

- Agent service

  Resource Coordinator Agent

- Deployment service

  Deployment Agent

From the Windows Control Panel, open "Administrative Tools". Then, open the [Services] window to check the state of each service.
The following explains how to start and stop each service.

- Agent service

  Agents can be started and stopped using the "start" and "stop" subcommands of the rcxadm agtctl command.
  Refer to "5.1 rcxadm agtctl" of the "ServerView Resource Coordinator VE Command Reference" for details on this command.

- Deployment service

  From the Windows Control Panel, open "Administrative Tools". Then, open the [Services] window to stop or start the Deployment Agent service.

[Linux/VMware]
The Agent consists of the following services.

- Agent service
- Deployment service

Execute the following commands to determine whether the Agent is running or not. If those commands show that the processes for the Agent and deployment services (respectively 'FJSVssagt' and 'scwagent') are running, then the Agent can be asserted to be running.

- Agent service

  # **/bin/ps -ef | grep FJSVssagt** <RETURN>

- Deployment service

  # **/bin/ps -ef | grep scwagent** <RETURN>

The start and stop procedures for the two Agent services are described below.

- Agent service

  Agents can be started and stopped using the "start" and "stop" subcommands of the rcxadm agtctl command.
  Refer to "5.1 rcxadm agtctl" of the "ServerView Resource Coordinator VE Command Reference" for details on the command.

- Deployment service

  Execute the following command to start or stop the collection of image files, deployment of image files, and server startup control.

  Start

  # **/etc/init.d/scwagent start** <RETURN>

Stop

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

5.3 RC Console

This section describes how to open and close the RC console.

Note

- When accessing the RC console from Internet Explorer 8, be sure to enable the Compatibility View in Internet Explorer.
- The RC console uses the Web browser's standard fonts and is best viewed in a window size of 1024 by 768 pixels. If the Web browser is resized a significant amount, the display quality may deteriorate.
- The RC console uses JavaScript, Cookies and IFRAMEs. These must be enabled in the Web browser settings before using the RC console.
- The RC console communicates with the Admin Server using XMLHttpRequest. In Internet Explorer 6, XMLHttpRequest is implemented as an ActiveX object. As a result, the following settings must be enabled if the RC console is used in Internet Explorer 6.
  - Execution of the ActiveX control and plug-in.
  - Execution of the ActiveX control scripts which are marked as safe for execution.

Opening the RC Console

Start a Web browser from an Admin Client and specify the URL of the RC console for connection. If the port number was changed, specify the new port number.
This will open the Resource Coordinator VE login screen.

```
URL: https://Admin Server IP address:23461/
```

On a Windows Admin Server, the RC console can also be opened by selecting [Start]-[All programs]-[Resource Coordinator VE]-[RC console].

This will display the Resource Coordinator VE login screen.

Note

- If the login screen is not displayed, make sure that the following settings are correct.
  - URL entered in address bar of the Web browser.
  - Proxy settings of the Web browser.
  - Firewall settings on the Admin Server.
- When opening the RC console right after launching a Web browser, a warning window concerning the site's security certificate will be displayed. With Internet Explorer 7 or 8, the following message is displayed: "There is a problem with the security certificate of this Web site". This warns the user that Resource Coordinator VE uses a self-signed certificate to encrypt its HTTPS (SSL) communication with the Web browser.
  Resource Coordinator VE generates unique, self-signed certificates for each Admin Server when the Manager is installed.
  Within a firewall-protected intranet, a network where the risk of identity theft is low, or where all correspondents are trusted, there is no risk in using self-signature certificates for communications. Accept the warning to display the Resource Coordinator VE login screen.
  With Internet Explorer 7 or 8, the login screen can be displayed by selecting the following option: "Continue to view this site (not recommended)".

- When connecting to the Manager from Internet Explorer 7 or 8, the background of the address bar will become red and the words "Certificate error" will be displayed on the right side of the address bar of the login screen, the RC console and BladeViewer. Furthermore, the Phishing Filter may show a warning on the status bar. These warnings are referring to the same self-signed certificate issue discussed in the previous bullet. It is safe to continue with the current browser settings.
- To stop displaying the security certificate warning screen and the certificate error icon, create a certificate associated with the IP address or hostname of the Admin Server and add it to the Web browser. Refer to "Appendix E HTTPS Communications" for details.
- If already logged in from another Web browser window, login may be performed automatically (without displaying the login screen).

Login

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

- "User name"
- "Password"

Information

- At installation, enter the name and password of the user account specified in "2.1 Manager Installation" of the "ServerView Resource Coordinator VE Installation Guide".
- When logging in for the first time, the RC console is displayed.
  Otherwise, the view that was used right before logging out (either the RC console or BladeViewer) is displayed.
- In order to switch from the RC console to BladeViewer, use the <BladeViewer>>> button.
- Opening the RC console in multiple Web browsers may not allow multi-user login. To log in as a different user, start up a new Web browser from the Windows start menu.

Logout

To log out, select [File]-[Log out] from the RC console menu, and click the <OK> button in the confirmation dialog.

Note

- If the Web browser is closed without logging out, the user may stay logged in, making it possible to access the RC console without authentication. It is advised that the user be logged out properly after use of the RC console or BladeViewer.
- If the RC console or BladeViewer is opened simultaneously in several Web browser windows, those login sessions may be terminated.

Exit

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

Chapter 6 Setup

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

In addition to the usual way of registering each resource individually, it is also possible to register or change registration settings of multiple resources together using the pre-configuration function.

- Registering or modifying resources individually

  This method is used when the number of servers to be installed is small (from 1 to 4), or when adding a similar number of servers to an existing environment.

- Registering or modifying multiple resources collectively

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

Refer to "Chapter 7 Pre-configuration" for information on registering multiple resources together.

Information

- **User accounts**

  When creating new user accounts, changing passwords or modifying permission levels during setup, refer to "Chapter 4 User Accounts" of the "ServerView Resource Coordinator VE Operation Guide".

- **Backing up the Admin Server**

  The Admin Server should be backed up after the entire system has been completely set up, or after registering, changing or deleting resources.
  Refer to "B.2 Backup" of the "ServerView Resource Coordinator VE Operation Guide" for information about backing up the Admin Server.

6.1 Registering Resources

This section explains how to register resources with the Admin Server.
The following resources can be registered.

- Chassis
- Managed servers
- LAN switches
- VM management software
- Power monitoring devices

When using blade servers, register resources in the order listed below:

1. Chassis
2. Managed servers (within the chassis)
3. LAN switch blades (within the chassis)

In a same chassis, managed servers and LAN switch blades can only be registered or deleted one at a time.
As a result, no operations can be performed on a server while registering or deleting a LAN switch blade.
Simultaneously performing operations on more than one resource at a time will produce the following error message.
In this case, wait until the current operation is completed before executing the desired operation again.

FJSVrcx:ERROR:67210: *LAN switch name* (LAN switch):is busy

or

FJSVrcx:ERROR:67210: *Managed server name* (physical server):is busy

6.1.1 Registering Chassis

This section explains how to register a chassis.
By registering a chassis, every server blade mounted in the chassis will be automatically detected and displayed as an unregistered server in the resource tree.
Refer to "6.1.2 Registering Managed Servers" for details on registering servers.

Use the following procedure to register a chassis:

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

   The [Register Chassis] dialog is displayed.

2. In the [Register Chassis] dialog, set the following items.

   Admin LAN (IP address)

   Enter the IP address that was set on the chassis management blade.
   Use standard dot notation.

   Example

   100.100.100.100

   Chassis name

   Enter a name to assign to this chassis.
   Use no more than 10 characters, including alphanumeric characters or hyphens ("-"). This name should start with an alphabet character.

   SNMP Community

   Enter the SNMP community that was set on the chassis management blade.
   Select "public", or enter an arbitrary string.
   Enter no more than 32 characters, including alphanumeric characters, underscores ("_") or hyphens ("-").

3. Click the <OK> button.

   The registered chassis will be displayed under the resource tree.
   Any server blade mounted within this chassis will be detected automatically and shown as: "*chassis_name*-*Slot_number*[Unregistered]".
   The only operation available for those unregistered servers is server registration, while the RC console can only display their hardware statuses and properties.
   If the Manager is installed on one of those server blades, this blade will be shown as: "*chassis_name*-*Slot_number*[Admin Server]".
   In that case, server registration will not be available for the Admin Server blade, but its hardware status and properties will be displayed in the RC console.

6.1.2 Registering Managed Servers

This section explains how to register managed servers.

The following features are available for managed servers.

- **Without a registered Agent**
  - HBA address rename settings
  - Cloning image deployment
  - Being allocated as a spare server for the Auto-Recovery of other servers
  - Allocation of a spare server for Auto-Recovery

- VLAN settings on LAN switch blades

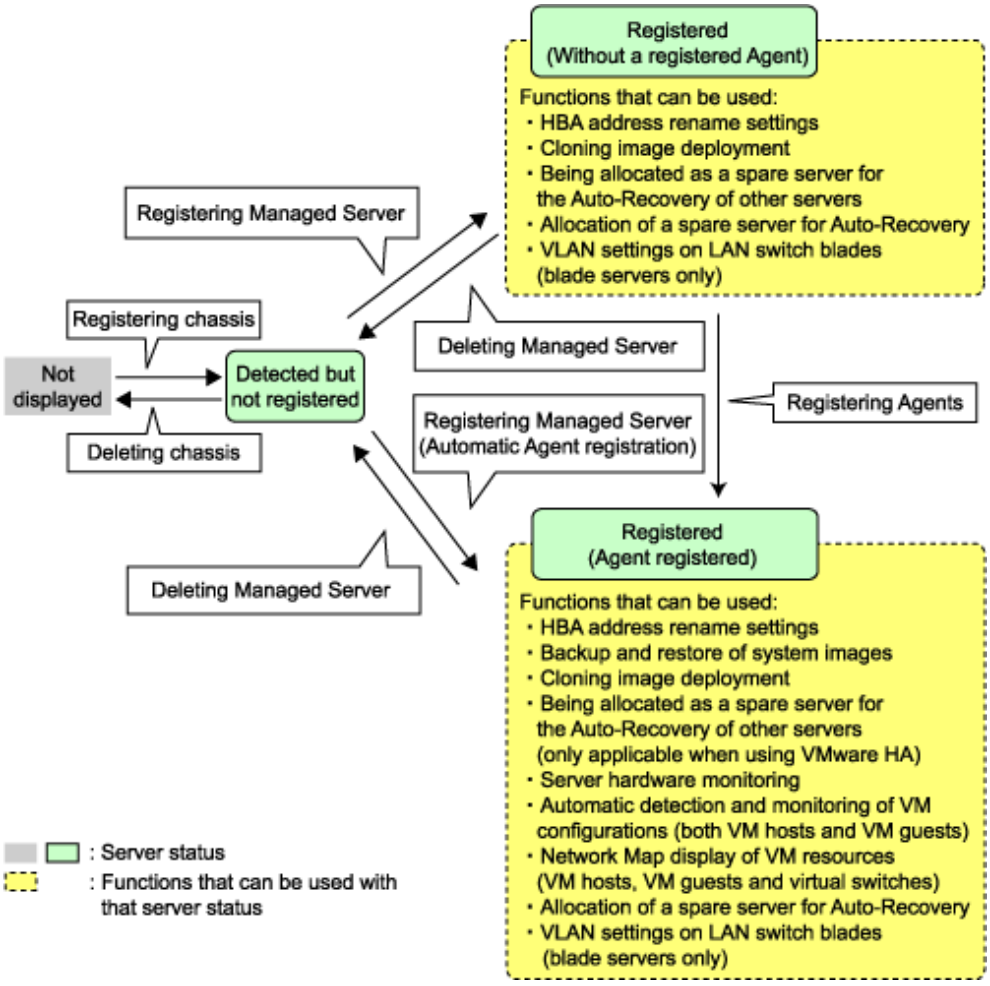
- **With a registered Agent**
  - HBA address rename settings
  - Backup and restore of system images
  - Cloning image deployment
  - Being allocated as a spare server for the Auto-Recovery of other servers (only applicable when using VMware HA)
  - Server hardware monitoring
  - Automatic detection and monitoring of VM configurations (both VM hosts and VM guests)
  - Network Map display of VM resources (blade servers only): VM hosts, VM guests and virtual switches
  - Allocation of a spare server for Auto-Recovery
  - VLAN settings on LAN switch blades

6.1.2.1 Registering Blade Servers

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

To register servers other than PRIMERGY BX servers, refer to "6.1.2.2 Registering Rack-Mount or Tower Servers".

Figure 6.1 State transition diagram for managed servers



Use the following procedure to register blade servers (PRIMERGY BX series).

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

   The [Register Server] dialog is displayed.

2. In the [Register Server] dialog, set up the following items.

   Physical server name

   Enter a name to assign to this physical server.
   Enter no more than 15 characters, including alphanumeric characters or hyphens ("-"). This name should start with an alphabet character.

   Admin LAN

   IP address

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

   For servers running a physical OS or VM host

   Resource Coordinator VE will automatically obtain this IP address, and register the Agent installed on the server.
   If ServerView Agent (mandatory software) is not running, "Message number 67231" will be displayed. In this case, server registration succeeds but the Agent is not registered.

   For other servers

   Enter the Admin LAN IP address of this server.
   The Agent will not be registered automatically, but can be manually registered after server registration if necessary.

   Server OS

   Category

   This option is displayed if the target server runs a physical OS or VM host.
   Select the appropriate server OS category (Physical OS or VM host).

   Selecting "VM Host" activates the user name and password input fields. Those refer to the user name and password entered during installation of this VM host.

   For a Physical OS
   Select "Windows/Linux".

   For a VM host
   Select "VM Host" and enter the VM host login account information.
   This login account information will be used by Resource Coordinator VE to control and communicate with the registered VM host.

   User name

   Enter the name of a user account with administrative authority over this VM host.

   Password

   Enter the password of the above VM host user account.

Note

- For details about the network interface used for the Admin LAN, refer to "3.2.1 Network Configuration".
  If an incorrect network interface is used, Resource Coordinator VE will not be able to detect the correct IP address from the operating system running on the target server.
  An Admin LAN IP address is required even when registering a spare server.
  Enter an IP address that does not conflict with the IP address of any other managed server on the Admin LAN.

- The Admin LAN (IP address) will be detected automatically if an operating system is running on the target server. However, the following cases may occur depending on detection timing.

  - The Admin LAN (IP address) is not obtained automatically even though an operating system is running.

  - The Admin LAN (IP address) is obtained automatically even though an operating system is not running.

In this case, cancel the server registration process, right-click the chassis in the resource tree, and select [Update] from the popup menu. The IP address is updated to the correct value (it takes several seconds to obtain the information and to update).

Register the server again after checking that the IP address has the correct value in the Resource Details tab of the server to be registered.

- When registering a newly-mounted PRIMERGY BX 900 server, the recognition of this server's Admin LAN MAC address may take time and cause registration failures (showing error message number 61142).
  In such cases, after the registration has failed, right-click the target server and select [Update] from the popup menu to request an update of hardware properties. This will update the MAC address to the correct value. This may also take a few minutes to obtain hardware information and update internal properties.
  Confirm that the correct MAC address is displayed for this server in the [Resource Details] tab before registering the server again.

- A server running a VM host can still be registered as a physical OS if its Server OS category is set to "Windows/Linux". A VM host server that was mistakenly registered as a physical OS should be deleted and re-registered as a VM host.

3. Click the <OK> button.

   The registered server will be displayed under the resource tree.

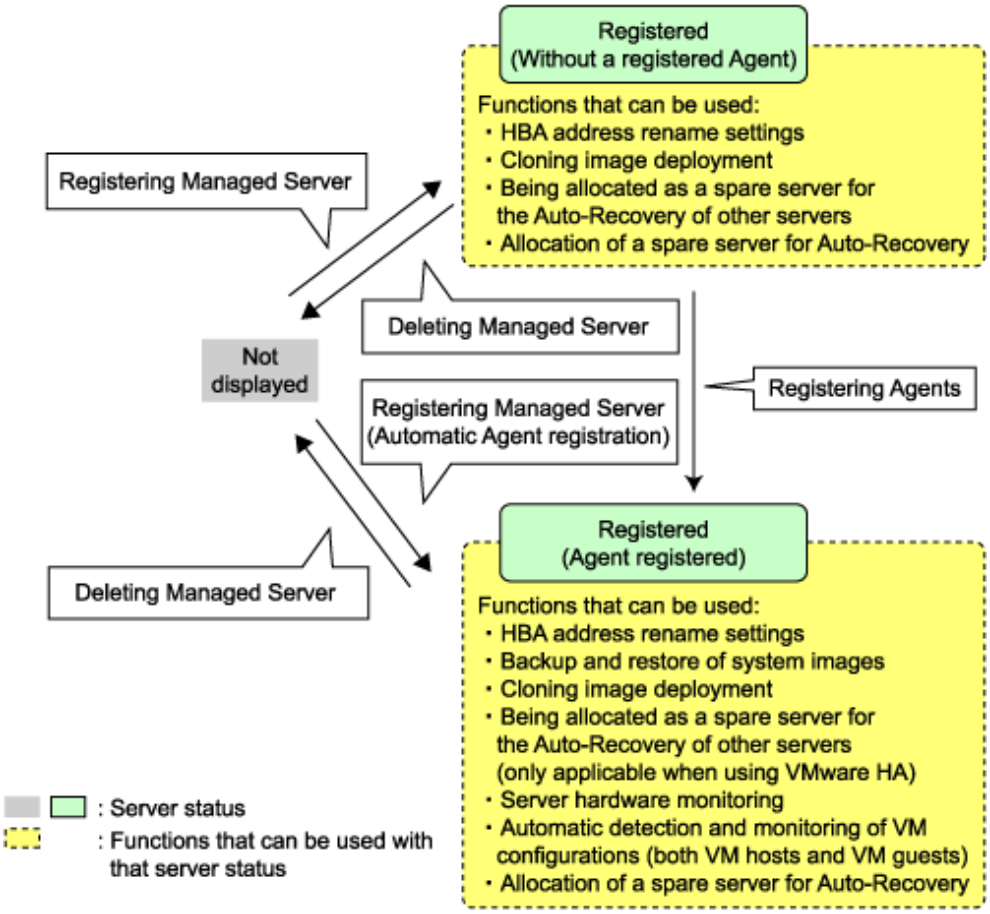
Note

- If a server on which an Agent was registered is shown as "unknown" in the resource tree, refer to "15.3 "unknown" Server Status" in the "ServerView Resource Coordinator VE Operation Guide" to fix its status.
- When an Agent is registered on a VM host, all VM guests running on that VM host are also registered automatically. Whenever a VM guest is created, modified, deleted or moved on a registered VM host, the changes are automatically updated in the resource tree.
- The VM guest name displayed in the RC console is either the VM name defined in its virtualization software or the hostname defined in the guest OS.
  The timing at which the hostname of a guest OS is detected and displayed varies according the virtualization product used. Refer to "A.3 Functional Differences between Products" for details.
- It is not recommended to use duplicate names for physical OS's, VM hosts, and VM guests. Otherwise, these resources cannot be managed from the command-line.
- When registering a server on which the Agent was installed, it is necessary to either reboot the server or restart its "Deployment service" (explained in the "5.2 Agent" section) after server registration. This step has to be done before running any image operation (system image backup or cloning image collection).
  For information on re-starting Agents, refer to the "5.2 Agent" section.

6.1.2.2 Registering Rack-Mount or Tower Servers

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

Figure 6.2 State transition diagram for managed servers



Use the following procedure to register rack-mount or tower servers:

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

   The [Register Server] dialog is displayed.

2. In the [Register Server] dialog, enter the following items.

   Input items differ depending on whether the "Register agent" checkbox is selected, as described below. If selected, Resource Coordinator VE will attempt to detect and register its Agent after server registration. Otherwise, the Agent won't be detected, but can later be registered if required.

   With Agent registration

   The following input items are required.

   - Physical server name
   - Remote Management Controller
     - IP address
     - User name
     - Password
   - Server management software (ServerView)
     - Association with server management software (ServerView)
     - SNMP community
   - Admin LAN
     - IP address

    - MAC address (NIC1)
- SAN boot
    - MAC address (NIC2)

Without Agent registration

The following input items are required.

- Physical server name
- Remote Management Controller
    - IP address
    - User name
    - Password
- Server management software (ServerView)
    - Association with server management software (ServerView)
    - SNMP community
- Admin LAN
    - IP address
- Server OS
    - Category

Physical server name

Enter a name to assign to this physical server.
Enter no more than 15 characters, including alphanumeric characters or hyphens ("-"). This name should start with an alphabet character.

Remote Management Controller

IP Address

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

User name

Enter the name of a remote management controller user account with administrative authority over this server.
Enter no more than 16 characters, including alphanumeric characters or symbols (ASCII characters 0x20 to 0x7e).

Password

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

Server management software (ServerView)

Association with server management software (ServerView)

For PRIMERGY servers
Select "Enable" and enter a SNMP community.

For servers other than PRIMERGY servers
Select "Disable".
By default, "Enable" is selected.

SNMP community

Enter the SNMP community that was set on this server.
Select "public", or enter an arbitrary string.
Enter no more than 32 characters, including alphanumeric characters, underscores ("_") or hyphens ("-").

Admin LAN

IP address

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

Admin LAN MAC address (NIC1)

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

SAN boot

MAC address (NIC2)

Enter the MAC address of the second Admin LAN network interface. This network interface will be used by the HBA address rename setup service.
Enter a MAC address in either one of the following two formats: hyphen-delimited ("xx-xx-xx-xx-xx-xx"), or colon-delimited ("xx:xx:xx:xx:xx:xx").
This field can be omitted when not using the HBA address rename setup service.

Server OS

Category

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

For a Physical OS
Select "Windows/Linux".

For a VM host
Select "VM Host" and enter the VM host login account information.
This login account information will be used by Resource Coordinator VE to control and communicate with the registered VM host.

User name

Enter the name of a user account with administrative authority over this VM host.

Password

Enter the password of the above VM host user account.

Note

- For details about the network interface(s) used on the Admin LAN, refer to "3.2.1 Network Configuration".
  If an incorrect network interface is used, Resource Coordinator VE will use a wrong MAC address for the Admin LAN.
  An Admin LAN IP address is required even when registering a spare server.
  Enter an IP address that does not conflict with the IP address of any other managed server on the Admin LAN.
- A server running a VM host can still be registered as a physical OS if its Server OS category is set to "Windows/Linux". A VM host server that was mistakenly registered as a physical OS should be deleted and re-registered as a VM host.

3. Click the <OK> button.

   The registered server will be displayed under the resource tree.

Note

- If a server on which an Agent was registered is shown as "unknown" in the resource tree, refer to "15.3 "unknown" Server Status" in the "ServerView Resource Coordinator VE Operation Guide" to fix its status.

- After registering the Agent, please verify that the information registered for the remote management controller is correct. This can be verified by trying out power operations (from Resource Coordinator VE) against that server. Refer to "Chapter 6 Power Control" in the "ServerView Resource Coordinator VE Operation Guide" for details on power operations.
- When using HBA address rename setup service, please confirm that the registered server can boot properly using the HBA address rename setup service.
  If the server can not boot properly, make sure that the specified MAC address (NIC2) is correct.
- When an Agent is registered on a VM host, all VM guests running on that VM host are also registered automatically. Whenever a VM guest is created, modified, deleted or moved on a registered VM host, the changes are automatically updated in the resource tree.
- The VM guest name displayed in the RC console is either the VM name defined in its virtualization software or the hostname defined in the guest OS.
  The timing at which the hostname of a guest OS is detected and displayed varies according its virtualization software. Refer to "A.3 Functional Differences between Products" for details.
- It is not recommended to use duplicate names for physical OS's, VM hosts, and VM guests. Otherwise, these resources cannot be managed from the command-line.
- When registering a server on which the Agent was installed, it is necessary to either reboot the server or restart its "Deployment service" (explained in the "5.2 Agent" section) after server registration. This step has to be done before running any image operation (system image backup or cloning image collection).
  For information on re-starting Agents, refer to the "5.2 Agent" section.

6.1.3 Registering LAN Switches

This section explains how to register LAN switches.

The following features are available for LAN switches.

- **LAN switch blades within a blade chassis (PRIMERGY BX series)**
  - Automatic VLAN settings (port VLAN or tagged VLAN)
  - Visualization of network links between server blades and LAN switch blades (within a chassis)
- **External LAN switches (LAN switches located outside of a blade chassis)**
  - Visualization of network links between LAN switches
  - Visualization of network links between LAN switches and LAN switch blades

Visualization of network links between LAN switches is available even if no LAN switch blade was registered. However, no physical links will be displayed unless two or more LAN switches were registered.

6.1.3.1 Registering LAN Switch Blades

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

Use the following procedure to register a LAN switch blade.

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

   The [Register LAN Switch] dialog is displayed.

2. In the [Register LAN Switch] dialog set the following items:

   LAN switch name

   Enter the name to assign to this LAN switch blade.
   Enter no more than 15 characters, including alphanumeric characters (upper or lower case), underscores ("_") or hyphens ("-").

   Admin LAN (IP address)

   Enter the Admin LAN IP address that was set on this LAN switch blade.
   Use standard dot notation.

Example

100.100.100.100

User name

Enter the name of a telnet user account that can log in to this LAN switch blade.

Password

Enter the password of the above telnet user account.

Administrative password

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

If the user name and the password of the administrator account were set in "User name" and "password", simply re-enter the same password in this field. In this case, Resource Coordinator VE does not check whether the password entered here matches the password set on the LAN switch blade.

SNMP Community

Enter the SNMP community that was set on this LAN switch blade.
Select either "public", or enter any name.
Enter no more than 32 characters, including alphanumeric characters, underscores ("_") or hyphens ("-").

3. Click the <OK> button.

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

Note

A telnet connection is made when registering a LAN switch blade. Some models may restrict the number of simultaneous connections. In this case, log out from other telnet connections.

6.1.3.2 Registering LAN Switches (Non-Blade Switches)

Use the following procedure to register LAN switches:

1. Discover LAN switches. Refer to [Discovery] for instructions.
2. Register LAN switches displayed in the network resource tree. Refer to [Registration] for instructions.

Discovery

1. From the RC console menu, select [Tools]-[Topology]-[LAN Switches].

   The [Discover LAN Switches] dialog is displayed.

2. In the [Discover LAN Switches] dialog set the following items:

   Start address

   Enter the start IP address of the network where to discover LAN switches.
   Use standard dot notation.

   Example

   100.100.100.100

Subnet mask

Enter the subnet mask of the network where to discover LAN switches.
Use standard dot notation.

Example

255.255.255.0

Addresses in range

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

Example

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

SNMP Community

Enter the SNMP community that was set on this LAN switch.
Select either "public", or enter any name.
Enter no more than 32 characters, including alphanumeric characters, underscores ("_") or hyphens ("-").

3. Click the <OK> button.

Resource Coordinator VE starts scanning for LAN switches within the specified network range.
Discovered LAN switches will be displayed under the resource tree with an "unregistered" status.

Registration

1. In the RC console resource tree, right-click a discovered LAN switch, and select [Register]-[LAN switch] from the popup menu.
The [Register LAN Switch] dialog is displayed.

2. In the [Register LAN Switch] dialog, set the following items:

LAN switch name

Enter the name to assign to this LAN switch.
Enter no more than 32 characters, including alphanumeric characters (upper or lower case), underscores ("_"), hyphens ("-") or periods (".").
By default, the name of a discovered LAN switch will be set to its system name or to its IP address if the system name could not be detected.

SNMP Community

Enter the SNMP community that was set on this LAN switch.
Select "public", or enter an arbitrary string.
Enter no more than 32 characters, including alphanumeric characters, underscores ("_") or hyphens ("-").

3. Click the <OK> button.

The registered LAN switch will be displayed under the resource tree.

Note

It is possible to set an automatically detected IP address to another unregistered LAN switch. However, this will result in the Resource Coordinator VE configuration being inconsistent with the actual network configuration.

If a LAN switch was registered with the IP address of another network device, delete the registered LAN switch following the instructions given in "6.4.3.2 Deleting LAN Switches (Non-Blade Switches)", then perform "Discover" and "Register" again.

6.1.4 Registering VM Management Software

This section explains how to register VM management software.

Registration of VM management software (such as VMware vCenter Server, etc) is necessary to enable VM guest migrations.

Use the following procedure to register VM management software:

1. From the RC console menu, select [Settings]-[VM Management Software].

   The [Configure VM Management Software] dialog is displayed.

2. In the [Configure VM Management Software] dialog, enter the following items.

   Location

   Select the location of this VM management software installation.

   - If VM management software is installed on the Admin Server

     Select "Admin Server".

   - Any other case

     Select "Other server".
     Selecting this option activates the IP address field. Enter the IP address of the server on which VM management software is installed.

     By default, "Admin Server" is selected.

   IP address

   Enter the IP address of the server on which VM management software is installed. If "Admin Server" was selected, this field is disabled and shows the IP address of the Admin Server.
   Use standard dot notation.

   Example

   100.100.100.100

   User name

   Enter the name of a VM management software user account with administrative authority.
   Enter no more than 84 characters, including alphanumeric characters or symbols (ASCII characters 0x20 to 0x7e).

   Password

   Enter the password of the above VM management software user account.
   Enter no more than 128 characters, including alphanumeric characters or symbols (ASCII characters 0x20 to 0x7e).

3. Click the <OK> button.

   VM management software is registered with the entered information.

6.1.5 Registering Power Monitoring Devices

This section explains how to register a power monitoring device.

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

Use the following procedure to register power monitoring devices.

1. In the RC console resource tree, right-click "Power Monitoring Devices" and select [Register]-[Power Monitoring Device] from the popup menu.

   The [Register Power Monitoring Devices] dialog is displayed.

2. The following items are set in the [Register Power Monitoring Devices] dialog:

   Device name

   Enter a name to assign to this power monitoring device. When exporting power consumption data, use this name to select devices for which to export data.
   Enter no more than 15 characters, including alphanumeric characters or hyphens ("-").This name should start with an alphabet character.

   Admin LAN (IP address)

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

   SNMP Community

   Enter the SNMP community that was set on this power monitoring device.
   Select "public", or enter an arbitrary string.
   Enter no more than 32 characters, including alphanumeric characters, underscores ("_") or hyphens ("-").
   This SNMP community will be used to collect power consumption data from this device (via SNMP protocol).

   Voltage

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

   Comment

   Enter a comment that describes this power monitoring device.
   Enter no more than 128 characters.

   Note

   Line breaks are counted as one character.

3. Click the <OK> button.

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

If collection of power data is disabled in the option settings, data will not be collected even if power monitoring devices are registered. Change data collection settings according to "6.3.6.1 Changing Environmental Data Settings".

Use the following procedure to enable collection of environmental data.

1. From the RC console menu, select [Tools]-[Options].

   The [Options] dialog is displayed.

2. Select "Environmental Data" category title from the [Options] dialog. Change the following items from the displayed "Environmental Data" area.

   Data to collect

   Select the "Power" checkbox.

3. Click the <Apply> button.

   Environmental Data collection will be activated.

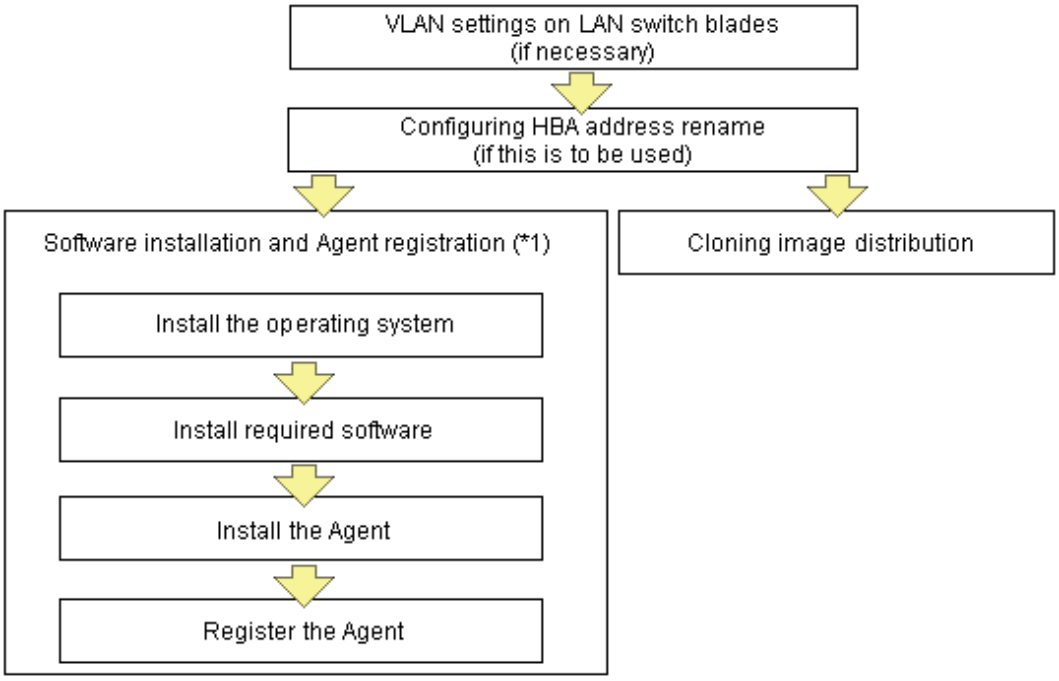
Note

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

6.2 Configuring the Operating Environment of Managed Servers

This section explains how to install software to the registered managed servers and set up their operating environment.

Figure 6.3 Procedure for setting up operating environments



*1: These settings can be omitted for resources that have already been installed or registered.

6.2.1 Configuring VLANs on LAN Switches

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

6.2.1.1 Configuring VLANs on external ports

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

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

   The [VLAN Settings] dialog is displayed.

2. In the [VLAN Settings] dialog, set the following items.

   VLAN ID

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

   Adding a new VLAN ID

   a. Under VLAN, select "Create new".

b. Enter a VLAN ID number.
Refer to the LAN switch's manual for details on VLAN IDs.

Modifying an existing VLAN ID

a. Under VLAN, select "Change".

b. Select a VLAN ID.

VLAN Type

Under Port List, select the VLAN type ("Untagged" or "Tagged") to be used by each port.

3. Click the <OK> button.

6.2.1.2 Configuring VLANs on internal ports

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

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

   The [Network Settings] dialog is displayed.

2. In the [Network Settings] dialog, select the index of the network interface for which to assign a VLAN ID, and click the <Setting> button.

   The [VLAN Configuration] dialog is displayed.

3. In the [VLAN Configuration] dialog, set the following items and click the <OK> button.

   VLAN ID (Port)

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

   VLAN ID (Tagged)

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

   Multiple VLAN IDs can be entered by separating them with commas (",").

   Note that the VLAN settings are not applied onto the LAN switch blade at this stage. To configure VLANs for multiple network interfaces, repeat steps 2 and 3.

4. Confirm the configuration set in the [Network Settings] dialog and click the <OK> button.

   VLAN settings are applied to the related LAN switch blade.

Note

The VLAN configuration of a registered LAN switch blade should be set from the RC console instead of the LAN switch's own Web-based and command-based interfaces.

6.2.2 Configuring HBA address rename

Use the following procedure to configure HBA address rename settings.
The HBA address rename function allows the Admin Server to control the WWNs set on a managed server's HBAs. During maintenance or switchover operations, a replacement server (or HBA) can inherit the WWN configuration set on a replaced server (or HBA). With this feature, the traditionally necessary re-configuration of storage devices is no longer required.
Use of the HBA address rename function requires registering specific settings for each server in advance.

Note

The HBA address rename function cannot be enabled for servers on which recovery settings were already configured. Cancel any existing recovery settings before enabling the HBA address rename function on a server.

1. Storage settings

Refer to "3.7 Configuring the Storage Environment" to configure storage devices.
When altering the configuration of a storage device already used by active servers, make sure to power off those servers before performing any configuration change.

2. Settings for the HBA address rename function

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

   The [HBA Address rename settings] dialog is displayed.

2. In the [HBA Address rename settings] dialog, set the following items:

   WWNN

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

   HBA ports

   Specify the following values according to the system configuration.

   - To create a single-path configuration, specify "1".
     Refer to "Figure 6.4 Procedures for single-path configurations" for details.
   - To create a multi-path configuration, specify "2".
     However, it is necessary to specify "1" during installation of the operation system. Specify "2" and reconfigure HBA address rename settings after setting up the multi-path driver.
     Refer to "Figure 6.5 Procedures for multi-path configurations" for details.

Figure 6.4 Procedures for single-path configurations

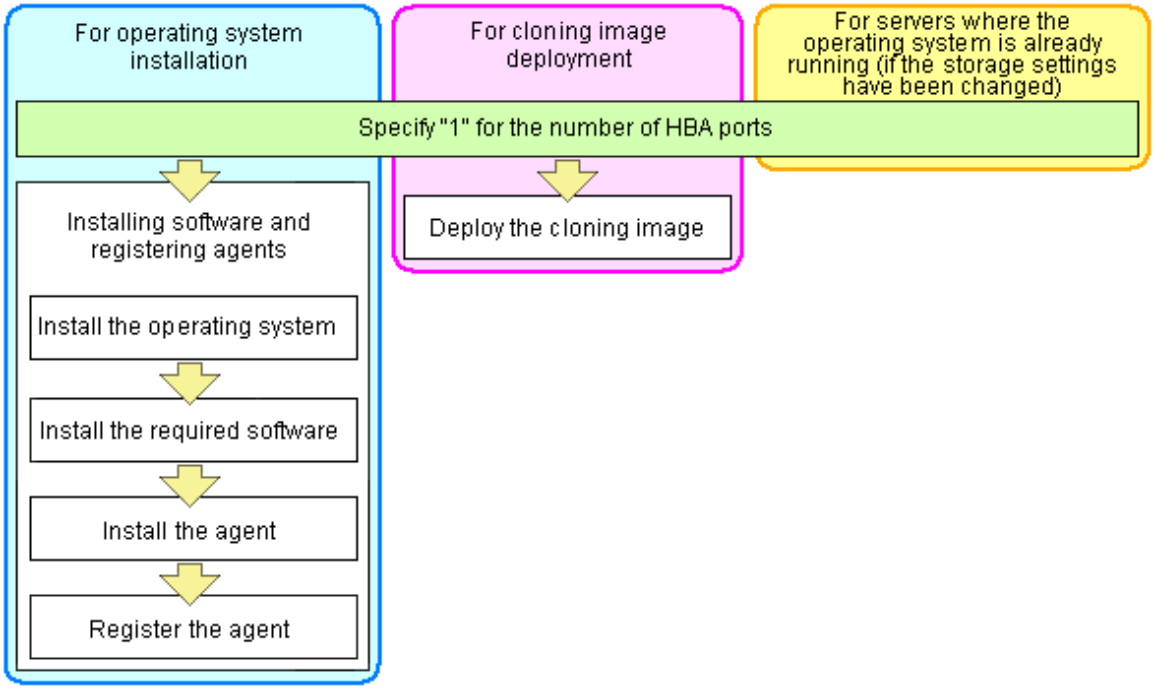
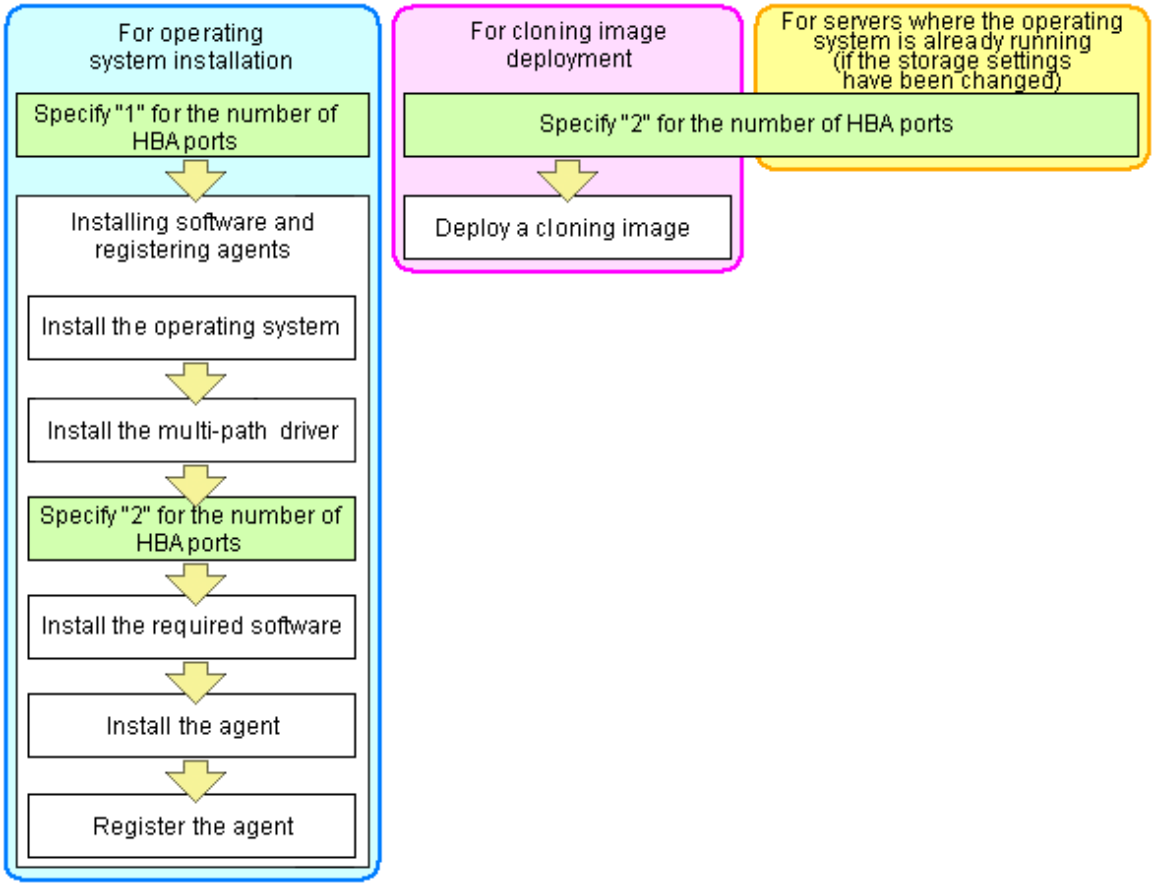


Figure 6.5 Procedures for multi-path configurations



Example

For a server with two HBA ports, use the HBA address rename function as follows.

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

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

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

Values actually set by the Admin Server on the HBA (WWPNs are generated automatically)

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

Information

WWN settings are applied to managed servers during server startup.

3. Check the server's restart checkbox if the server is to be restarted.

Information

Select server restart in the following cases.

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

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

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

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

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

4. Click the <OK> button.

5. Restart HBA address rename setup service.
   The HBA address rename setup service must be running to use the HBA address rename function. Refer to "6.2.2.1 Settings for the HBA address rename setup service" for details.

6.2.2.1 Settings for the HBA address rename setup service

When using the HBA address rename function, the Admin Server sets the WWN of managed servers during their startup sequence. This WWN is kept by managed servers until powered off.

However, a managed server won't be able to receive its assigned WWN unless it can communicate with the Admin Server. If communication with the Admin Server fails, because of problems on the Admin Server or a failure of the managed server's NIC1, the managed server won't start up properly as its HBA will not be set up with the correct WWN.
This can be avoided by using the HBA address rename setup service, which acts as a backup service in case of communication issues between the Admin Server and managed servers. This service, which must run on a server other than the Admin Server, can set up managed servers HBAs WWNs in the same way the Admin Server does.

This service must be running when using HBA address rename.

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

1. Open the [Start and stop of HBA address rename setting service] dialog.

   [Windows]
   Select [Start]-[All programs]-[Resource Coordinator VE]-[HBA address rename setup service].
   The [Start and stop of HBA address rename setting service] dialog is displayed.

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

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

The [Start and stop of HBA address rename setting service] dialog is displayed.

2. In the [Start and stop of HBA address rename setting service] dialog, enter the following items.

   Status

   The status of the service is displayed. "Stopping" is displayed if the service is not running, and "Operating" is displayed if the service is running.

   IP address of Admin Server

   Enter the IP address of the Admin Server.

   Port Number

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

   The Latest synchronous time

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

3. To start this service, click the <Start> button.
   To stop this service, click the <Stop> button.
   To cancel, click the <Cancel> button.

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

Note

- This service should be kept running at all times.
- Start this service on only one server for each Admin Server.
- OS administrator privileges are required to start and stop this service.
- This service does not operate on the server where the Manager is installed.

6.2.3 Software Installation and Agent Registration

Use the following procedure to install required software and register a server Agent.

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

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

1. Install the operating system

   a. Install the operating system on the managed server.

   b. Set up the Admin LAN.

      Set the Admin LAN IP address that was chosen for this server in "3.2.2 IP Addresses (Admin LAN)", as well as its corresponding network mask and default gateway.

   Using storage devices in multi-path configurations

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

- When using SAN boot together with the HBA address rename function, the number of paths to be used should be set to the "HBA ports" option of the HBA address rename function (refer to step 2 in "6.2.2 Configuring HBA address rename").
  The server is automatically restarted using a multi-path configuration.

Note

The server name (computer name for [Windows/Hyper-V] or a system node name for [Linux/VMware]) defined during OS installation should be set according to the following guidelines.

[Windows/Hyper-V]
Enter no more than 63 characters, including alphanumeric characters, underscores ("_") or hyphens ("-").
The server name cannot be composed solely of numbers.

[Linux/VMware]
Enter no more than 64 characters, including alphanumeric characters as well as the following symbols.

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

As the computer name [Windows] or the system node name [Linux/VMware] is also used as the server's host name, it is recommended to use only the characters prescribed by RFC (Request For Comment) 952:

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

It is recommended not to use duplicate names for physical OS's, VM hosts and VM guests. Otherwise, Resource Coordinator VE commands will not function properly.

2. Install required software

   Install the software packages that are required for a managed server.
   Refer to "1.1.2.2 Required Software" of the "ServerView Resource Coordinator VE Installation Guide" for information on required software.

3. Install the Resource Coordinator VE Agent

   Refer to "2.2 Agent Installation" of the "ServerView Resource Coordinator VE Installation Guide".

4. Register the Agent

   Register the Agent from the RC console while the target server is running.

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

      The [Agent registration] dialog is displayed.

   b. Select the server OS type (physical OS, VM host).

      - For a Physical OS

        Select "Windows/Linux".

      - For a VM host

        Select "VM host", and enter the VM host login account information.
        This login account information will be used by Resource Coordinator VE to control and communicate with the registered VM host.

      User name

      Enter the name of a user account with administrative authority over this VM host.

Password

Enter the password of the above VM host user account.

c. Click the <OK> button.

The Admin Server starts to monitor and display server Information obtained from the agent.

Note

- If a server on which an Agent was registered is shown as "unknown" in the resource tree, refer to "15.3 "unknown" Server Status" in the "ServerView Resource Coordinator VE Operation Guide" to fix its status.
- When an Agent is registered on a VM host, all VM guests running on that VM host are also registered automatically. Whenever a VM guest is created, modified, deleted or moved on a registered VM host, the changes are automatically updated in the resource tree.
  The VM guest name displayed in the RC console is either the VM name defined in its virtualization software or the hostname defined in the guest OS.
  The timing at which the hostname of a guest OS is detected and displayed varies according its virtualization software. Refer to "A.3 Functional Differences between Products" for details.
- When registering a server on which the Agent was installed, it is necessary to either reboot the server or restart its "Deployment service" (explained in the "5.2 Agent" section) after server registration. This step has to be done before running any image operation (system image backup or cloning image collection).
  For information on re-starting Agents, refer to the "5.2 Agent"section.
- A server running a VM host can still be registered as a physical OS if its selected Server OS category is set to "Windows/Linux". A VM host server that was mistakenly registered as a physical OS should be deleted and re-registered as a VM host.

6.2.4 Cloning Image Distribution

For the second and subsequent servers, operating systems are created using the cloning image collected from the first server.

Refer to "Chapter 8 Cloning [Windows/Linux]".

6.3 Modifying Settings

This section explains how to change settings for the Admin Server or resources registered on the Admin Server.

6.3.1 Changing Admin Server Settings

This section explains how to change the settings for the Admin Server.

6.3.1.1 Changing the Admin IP Address

Use the following procedure to change the IP address used on the Admin LAN by the Admin Server.

Change procedure

1. Log in to the Admin Server with an OS administrator account.
2. Stop the Manager.

   Refer to "5.1 Manager" for details on how to stop the Manager.
3. Change the SNMP trap destination set for the management blade and LAN switch blades.

   Set the SNMP trap destination to the new IP address of the Admin Server.

Note

Depending on the LAN switch blade used, setting an SNMP trap destination may restrict SNMP access to that switch blade.
In a clustered Manager configuration, set the physical IP addresses of both the primary and secondary nodes as SNMP trap destinations.
If the LAN switch blade is set to only grant access from known IP addresses, be sure to give permissions to the physical IP addresses of both the primary and secondary cluster nodes, as is done with trap destination settings.
Refer to the manual of the LAN switch blade used for details.

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

   Change the IP address following the instructions given in the operating system's manual.
   If the Admin LAN has been made redundant, change the admin IP address settings of the following LAN redundancy software.

   - PRIMECLUSTER GLS
   - BACS
   - Intel PROSet

   Refer to the manual of each product for usage details.
   In a clustered Manager configuration, change the cluster IP address according to the instructions given in "Changing the IP Address of a Clustered Manager".

5. Change the IP address registered as the Manager's Admin IP address.

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

   [Windows]

   ```
   >"Installation folder\Manager\bin\rcxadm" mgrctl modify -ip IP_address <RETURN>
   ```

   [Linux]

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

   In a clustered Manager configuration, refer to "Registering the Admin IP Address of a Clustered Manager" for details on how to change the Admin IP address registered for the Manager.

6. Log in to the Admin Server with an OS administrator account.

7. Change ServerView Agent settings on the managed server.

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

8. Stop the Agent on managed servers. [Windows/Linux] [Hyper-V]

   Refer to "5.2 Agent" for details on how to stop the Agent.

9. Change Agent settings.

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

   [Windows/Hyper-V]

   ```
   >"Installation folder\Agent\bin\rcxadm" agtctl modify -manager IP_address <RETURN>
   ```

   [Linux]

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

10. Restart the Agent on managed servers. [Windows/Linux] [Hyper-V]

    Refer to "5.2 Agent" for details on how to restart the Agent.

    Repeat steps 6 to 11 for each managed server on which the Agent is running.

11. Restart the Manager.

    Refer to "5.1 Manager" for details on how to restart the Manager.

12. Re-configure the HBA address rename setup service.

    When using the HBA address rename function, change the IP address of the Admin Server that is set for the HBA address rename setup service according to "6.2.2.1 Settings for the HBA address rename setup service".

13. Back up managed servers.

    If system image backups were already collected, it is recommended to update those images in order to reflect the changes made above. Refer to "8.2 Backing Up System Images" in the "ServerView Resource Coordinator VE Operation Guide" for details on system image backup.

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

14. Re-collect cloning images. [Windows/Linux]

    If cloning images were already collected, it is recommended to update those images to reflect the changed made above. Refer to "8.2 Collecting a Cloning Image" for details on cloning image collection.

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

Changing the IP Address of a Clustered Manager

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

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

[Linux]

1. Stop the Manager's cluster service.

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

2. Log in to the Admin Server's primary node.

   Log in to the operating system of the Admin Server's primary node with administration privileges.

3. Mount the shared disk on the primary node.

   Mount the Admin Server's shared disk on the primary node.

4. Change the logical IP address.

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

   Refer to the PRIMECLUSTER Global Link Services manual for details.

5. Activate the logical IP address.

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

   Refer to the PRIMECLUSTER Global Link Services manual for details.

Registering the Admin IP Address of a Clustered Manager

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

[Windows]

1. Cancel registry replication settings.

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

   - For x64 architectures

     SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard\DHCP

   - For x86 architectures

     SOFTWARE\Fujitsu\SystemcastWizard\DHCP

   Use the following procedure to remove the registry key.

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

      The [PXE Services Properties] dialog is displayed.

   b. In the [Registry Replication] tab, select the above registry key and click the <Delete> button.

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

   c. After removing the registry key, click the <Apply> button.

   d. Once settings are applied, click the <OK> button to close the dialog.

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

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

   >"*Installation_Folder***Manager\bin\rcxadm**" **mgrctl modify -ip** *IP_address* <RETURN>

3. Restore registry replication settings

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

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

      The [PXE Services Properties] dialog is displayed.

   b. In the [Registry Replication] tab, click the <Add> button.

      The [Registry Key] dialog is displayed.

   c. Restore the registry key deleted in step 1 in "Root registry key" and click the <OK> button.

   d. After completing registry key settings, click the <Apply> button.

   e. Once settings are applied, click the <OK> button to close the dialog.

4. Assign the Manager shared disk and IP address to the secondary node.

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

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

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

6. Assign the Manager shared disk and IP address to the primary node.

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

7. On the primary node, take the Manager shared disk and IP address offline.

[Linux]

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

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

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

2. De-activate the Admin Server's logical IP address.

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

   Refer to the PRIMECLUSTER Global Link Services manual for details.

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

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

   Refer to the PRIMECLUSTER Global Link Services manual for details.

4. Un-mount the shared disk.

   Un-mount the shared disk from the primary node.

5. Log in to the Admin Server's secondary node.

   Log in to the operating system of the Admin Server's secondary node with administration privileges.

6. Change the logical IP address.

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

   Refer to the PRIMECLUSTER Global Link Services manual for details.

7. Change the cluster configuration.

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

   After completing the configuration, save it and execute the following commands:

   - Configuration-Generate
   - Configuration-Activate

8. Start the Manager's cluster service.

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

6.3.1.2 Changing Port Numbers

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

[Windows]

- Manager services
  - Resource Coordinator Manager
  - Resource Coordinator Task Manager
  - Resource Coordinator Web Server (Apache)
  - Resource Coordinator Sub Web Server (Mongrel)
  - Resource Coordinator Sub Web Server (Mongrel2)
  - Systemwalker MpWksttr

- Deployment services
  - Deployment Service
  - TFTP Service
  - PXE Services

[Linux]

- Manager services
  - rcxmanager
  - rcxtaskmgr
  - rcxmongrel1
  - rcxmongrel2
  - rcxhttpd
- Deployment services
  - scwdepsvd
  - scwpxesvd
  - scwtftpd

Change the ports used by the above services if there is a possibility that they will conflict with other applications or services.
For Windows operating systems, an ephemeral port may conflict with a Resource Coordinator VE service if the maximum value allowed for ephemeral ports (5000 by default) was changed. In this case, change the port numbers used by Resource Coordinator VE services to values greater than the maximum ephemeral port value.

This section explains how to change the ports used by Resource Coordinator VE services.
Refer to the ServerView Operations Manager manual for information on how to change the ports used by ServerView Operations Manager.
The ports used for SNMP communication and server power control are defined by standard protocols and fixed at the hardware level, thus can not be changed.

Refer to "Appendix C Port List", for details on the ports used by Resource Coordinator VE.
When using a firewall on the network, firewall settings should be updated to match the new port definitions and allow communications for any modified port.

Manager services

Use the following procedure to change the Admin Server ports used by Manager services:

1. Stop Manager services.

   Refer to "5.1 Manager" for details on how to stop Manager services.

2. Change port numbers.

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

   [Windows]

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

   [Linux]

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

   Refer to "5.6 rcxadm mgrctl" of the "ServerView Resource Coordinator VE Command Reference" for details on this command and the service names that can be passed in the *name* parameter.

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

3. Restart Manager services.

   Refer to "5.1 Manager" for details on how to restart Manager services.

Note

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

  - Admin Client

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

  - HBA address rename setup service

    If the HBA address rename setup service is running, change the port number used to communicate with the Admin Server to the "rcxweb" port according to "6.3.3 Changing Settings for the HBA Address Rename Setup Service".

  [Windows]

  - Change the RC console shortcut on the Manager

    1. Open the following folder on the Admin Server.
       Installation folder\Manager
    2. Right click the "RC Console" icon, and select [Properties] from the popup menu.
    3. In the [Web Document] tab, change the port number set in the "URL" field (as shown below).

       URL: https://localhost:23461/

    4. Click the <OK> button.

- When changing the "nfagent" port, the following ports on managed servers should be set to the same value.

  Set the "nfagent" port set on each managed server to the same value, according to the instructions given in "6.3.2.6 Changing Port Numbers".
  The system image and cloning images collected before the change can no longer be used, and should be deleted.
  If necessary, re-collect system images and cloning images.

Deployment services

Use the following procedure to change the ports used by deployment services.

[Windows]

1. Change port numbers.

   a. Open the Windows Registry Editor, and search for the following subkey:

      - When using a 32-bit version of Windows:

        Key name: HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\SystemcastWizard\CLONE

      - When using a 64-bit version of Windows:

        Key name: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard\CLONE

   b. Select "PortBase" from the registry entries under this subkey.

   c. From the menu, select "Edit"-"Modify"

      The "Edit DWORD Value" dialog is displayed.

d. In the "Edit DWORD Value" dialog, select the "Decimal" base, and enter a new port value in "Value data".

   This port value will define the first port of the range used by deployment services.

   However, because deployment services can use up to 16 port numbers, ensure that all ports included between "PortBase" (defined here) and "PortBase+15" are not conflicting with any other application or service. Moreover, be sure to set a value lower than 65519 for "PortBase" so that the highest port number ("PortBase+15") does not exceed the largest valid port number (65534).

e. Click the <OK> button.

In a clustered Manager configuration, change port numbers on both the primary and secondary node.

2. Restart the server on which the port number has been changed.

[Linux]

1. Change port numbers.

   Edit the following file: /etc/opt/FJSVscw-common/scwconf.reg.

   In PortBase (under HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\SystemcastWizard\CLONE), set the first value of the port number to be used by deployment services. This value should be entered in hexadecimal format. To avoid conflicts with ephemeral ports, use a value not included in the ephemeral port range defined by "net.ipv4 local port range".

   This ensures that deployment services will use ports outside of the range defined by net.ipv4.ip_local_port_range for image operations.

   However, because deployment services can use up to 16 port numbers, ensure that all ports included between "PortBase" (defined here) and "PortBase+15" are not conflicting with any other application or service. Moreover, be sure to set a value lower than 65519 for "PortBase" so that the highest port number ("PortBase+15") does not exceed the largest valid port number (65534).

   In a clustered Manager configuration, change port numbers on both the primary and secondary node.

2. Restart the server on which the port number has been changed.

Information

Deployment services allow managed servers to boot from the network using a dedicated module stored on the Admin Server during backup, restore or cloning.
Note that changing port numbers on the Admin Server alone is enough to support communication during the above image operations. Therefore, no additional configuration is required on the managed servers.

6.3.1.3 Changing the Maximum Number of System Image Versions

Use the following procedure to change the maximum number of system image versions.

1. Change the maximum number of system image versions.
2. Confirm the maximum number of system image versions.

   Refer to "5.4 rcxadm imagemgr" of the "ServerView Resource Coordinator VE Command Reference" for details.

Note

If the specified limit is smaller than the number of existing system image versions, older versions will not be deleted automatically. In this case, backing up a new system image, will only delete the oldest version.
Delete unused image versions manually if they are no longer necessary. Refer to "8.5 Deleting a System Image" in the "ServerView Resource Coordinator VE Operation Guide" for details.

If the RC console was already opened, refresh the Web browser after changing the maximum number of system image versions.

6.3.1.4 Changing the Maximum Number of Cloning Image Versions

Use the following procedure to change the maximum number of cloning image versions.

1. Change the maximum number of cloning image versions.
2. Confirm the maximum number of cloning image versions.

   Refer to "5.4 rcxadm imagemgr" of the "ServerView Resource Coordinator VE Command Reference" for details.

Note

If the specified limit is smaller than the number of existing cloning image versions, older versions will not be deleted automatically. In this case, collecting a new cloning image version will require selecting a previous image version for deletion.
Delete unused image versions manually if they are no longer necessary. Refer to "8.5 Deleting a Cloning Image" for details.

If the RC console was already opened, refresh the Web browser after changing the maximum number of cloning image versions.

6.3.1.5 Changing the Image Folder Location

Use the following procedure to change the location (path) of the image files folder.

1. Select the [Image List] tab in the RC console and confirm the current image list.
2. Log on to the Admin Server as the administrator.
3. Stop manager services.

   Refer to "5.1 Manager" for details.
4. Change the location of the image folder.

   Refer to "5.4 rcxadm imagemgr" of the "ServerView Resource Coordinator VE Command Reference" for details.
   It may take time to execute the command because image files will be copied during this operation.

   In a clustered Manager configuration, refer to "Clustered Manager Configuration" for details on how to change the image folder location.
5. Start manager services.

   Refer to "5.1 Manager" for details.
6. Select the [Image List] tab in the RC console and confirm the image list is same as before.

Clustered Manager Configuration

Settings differ depending on the operating system used for the Manager.

[Windows]

1. Cancel registry replication settings.

   Bring online the shared disk and IP address, and take all other resources offline.
   Next, remove the following registry key from the registry replication settings set for the "Deployment Services" cluster resource.

   - For x64 architectures

     SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard\ResourceDepot

   - For x86 architectures

     SOFTWARE\Fujitsu\SystemcastWizard\ResourceDepot

   Use the following procedure to remove the registry key.

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

      The [Deployment Service Properties] dialog is displayed.

b. In the [Registry Replication] tab, select the above registry key and click the <Delete> button.

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

c. After removing the registry key, click the <Apply> button.

d. Once settings are applied, click the <OK> button to close the dialog.

2. Change the location of the image files folder.

   Change the location of the image files folder according to the instructions given in "5.4 rcxadm imagemgr" of the "ServerView Resource Coordinator VE Command Reference".
   Because image files are actually copied over to the new location, this step may take some time to complete.

   Run the "rcxadm imagemgr" command from either node of the cluster resource.
   The new location should be a folder on the shared disk.

3. Restore registry replication settings.

   Restore the registry key deleted in step 1 to the registry replication settings of the "Deployment Service" resource.
   Use the following procedure to restore the registry key.

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

      The [Deployment Service Properties] dialog is displayed.

   b. In the [Registry Replication] tab, click the <Add> button.

      The [Registry Key] dialog is displayed.

   c. Restore the registry key deleted in step 1 in "Root registry key" and click the <OK> button.

   d. After completing registry key settings, click the <Apply> button.

   e. Once settings are applied, click the <OK> button to close the dialog.

[Linux]

1. Mount the shared disk on the primary node.

   Log in to the primary node with OS administrator privileges and mount the Admin Server's shared disk.

2. Change the location of the image files directory.

   Change the location of the image files directory according to the instructions given in "5.4 rcxadm imagemgr" of the "ServerView Resource Coordinator VE Command Reference".

   Because image files are actually copied over to the new location, this step may take some time to complete.

   Run the "rcxadm imagemgr" command on the primary node.

   The new location should be a directory on the shared disk.

3. Un-mount the shared disk from the primary node.

   Un-mount the shared disk (mounted in step 1) from the primary node.

6.3.2 Changing Chassis and Managed Servers Settings

This section explains how to change the settings for the chassis and the managed server. If collecting the system images and cloning images of the Admin Server, collect the backup and cloning images after completing changes in the managed server settings.
Refer to "8.2 Backing Up System Images" in the "ServerView Resource Coordinator VE Operation Guide" for details on how to perform a backup. Refer to "8.2 Collecting a Cloning Image" for details on how to collect cloning mages.

Note

- To change VM guest settings, use the management console of the server virtualization software used.
- A managed server that has already been registered cannot be moved to a different slot.
  To move a managed server to a different slot, first delete the server, then move it to a different slot and register it again.

6.3.2.1 Changing Chassis Names

Use the following procedure to change the name of a registered chassis.

From the RC console, right-click the target chassis, select [Modify]-[Registration Settings] from the popup menu, and change the "chassis name" item.

The chassis name should start with a letter and can be up to 10 alphanumeric characters or hyphens ("-").

6.3.2.2 Changing Server Names

Names of physical OS's, VM hosts and VM guests can be changed by a user with administrative authority. Once changed, new names are automatically reflected in the RC console.

Use the following procedure to change the name of a physical server.

1. From the RC console, right-click the target server, and select [Modify]-[Registration Settings] from the popup menu, and change the "physical server name".

   In the physical server name, the first character must be a letter and can be up to 15 alphanumeric characters or hyphens ("-").

2. If the network parameter automatic setting function is used in the deployment of the cloning images, the "physical server name" set in the definition file must also be changed.

   Refer to "8.6 Network Parameter Auto-Configuration for Cloning Images" for details on the network parameter automatic setting function.

6.3.2.3 Changing Admin IP Addresses

This section explains how to change admin IP addresses.

To change the IP addresses of remote management controllers, refer to "6.3.2.5 Changing Remote Management Controller Settings".

Chassis

Use the following procedure to change the IP address of a chassis.

1. Change the IP address of set on the management blade.
2. From the RC console, right-click the target chassis, select [Modify]-[Registration Settings] from the popup menu, and change the "Admin LAN (IP address)" item.

Managed servers

Use the following procedure to change the IP address of a managed server.
This procedure is not required when changing only the public IP address of a server. However, it is still required when using the same address for both the Admin and public IP address.

1. Log in to the Admin Server with an OS administrator account.

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

   Change the IP address according to the OS manual.
   If the Admin LAN has been made redundant, change the admin IP address set in the following tools or products.

   Refer to the manual of each product for usage details.

   [Windows]
   PRIMECLUSTER GLS
   BACS
   Intel PROSet

   [Linux]
   PRIMECLUSTER GLS: "NIC switching mode (Physical IP address takeover function)".

3. Restart the managed server.

4. From the RC console, right-click the target server, select [Modify]-[Registration Settings] from the popup menu, and change the "Admin LAN (IP address)" item.

6.3.2.4 Changing SNMP Communities

This section explains how to change SNMP community settings.

- For blade servers

  Use the following procedure to change SNMP community used by chassis and managed servers.

  1. Change the SNMP community set on the management blade.

     The new SNMP community should have Read-Write permission.

  2. Change the SNMP community set on the managed server.

     Use the same SNMP community for both the management blade and the managed servers. Follow the instructions in the ServerView Agent's manual to change the SNMP community used by a managed server.
     The new SNMP community should have Read-Write permission.

  3. From the RC console, right-click the target server, select [Modify]-[Registration Settings] from the popup menu, and change the "SNMP community" item.

  4. Click the <OK> button.

     The SNMP community is changed.

- For Rack-mount or tower servers

  Use the following procedure to change the SNMP community used by PRIMERGY servers. For servers other than PRIMERGY servers, changing SNMP communities doesn't require any configuration change in Resource Coordinator VE.

  1. Change the SNMP community set on the managed server.

     Follow the instructions in the ServerView Agent's manual to change the SNMP community used by a managed server.

  2. From the RC console, right-click a managed server, select [Modify]-[Registration Settings] from the popup menu, and change the "SNMP community" item.

  3. Click the <OK> button.

     The SNMP community is changed.

6.3.2.5 Changing Remote Management Controller Settings

This section explains how to change remote management controller settings.

Use the following procedure to change remote management controller settings.

1. Change settings on the remote management controller.
   If the user account is changed, it should still have administrator authority.

2. From the RC console, right-click the target server, select [Modify]-[Registration Settings] from the popup menu, and change the "IP address" of the "Remote management controller". To modify user account information, select "Modify user account", and change the "User name" and "Password" of the "Remote management controller".

6.3.2.6 Changing Port Numbers

This section explains how to change port numbers.
When changing port numbers of the agent, the "nfagent" port of the manger must also be changed. Change this according to information in "6.3.1.2 Changing Port Numbers". Refer to "Appendix C Port List" for details on port numbers.

Use the following procedure to change the port numbers for managed servers:

1. Change the port numbers.

   [Windows/Hyper-V]
   Use a text editor (such as Notepad) to change the following line in the *Windows_system_folder*\system32\drivers\etc\services file.

   ```
   # service name  port number/protocol name
   nfagent         23458/tcp
   ```

   [Linux/VMware]
   Use a command such as vi to change the following line in the /etc/services file.

   ```
   # service name  port number/protocol name
   nfagent         23458/tcp
   ```

2. Restart the server in which the port number has been changed.

6.3.2.7 Changing VM Host Login Account Information

This section explains how to change VM host login account information.
If the login account information (user name and password) of the VM host entered when the VM host was registered is changed on the VM host, change the login account information of the VM host that was registered in Resource Coordinator VE.

The method for changing the VM host login account is shown below.

1. In the RC console resource tree, right-click the target VM host, and select [Modify]-[VM host login information] from the popup menu.

   The [Change Login Information] dialog is displayed.

2. Enter the login account information which was changed on the VM host.

   User name

   Enter the user name to log in to the VM host. The user name is specified by a user who has VM host administrator authority.

   Password

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

3. Click the <OK> button.

   VM host login information is changed.

6.3.2.8 Changing the VLAN Settings of a LAN Switch

The VLAN settings of the LAN switch blade ports connected to the physical servers can be reconfigured normally within Resource Coordinator VE.
Refer to "6.2.1.2 Configuring VLANs on internal ports" for details on how to configure these settings.

6.3.2.9 Changing HBA address rename Settings

The WWNs and HBA ports that are set by HBA address rename can be reconfigured normally within Resource Coordinator VE.
Refer to "6.2.2 Configuring HBA address rename" for details on how to configure these settings.

6.3.3 Changing Settings for the HBA Address Rename Setup Service

This section explains how to change settings for the HBA address rename setup service. Such settings include the Admin Server IP address, the port used to communicate with the Admin Server, and the IP address of the HBA Address Rename Server.

6.3.3.1 Changing the IP Address of the Admin Server

This section explains how to change the IP address of the Admin Server.
When this setting is changed, the HBA address rename setup service automatically checks whether it can communicate with the new Admin Server IP address.
Changing this setting also requires changing the IP address set on the Admin Server beforehand.

Change the IP address of the Admin Server according to "6.3.1.1 Changing the Admin IP Address", and change the admin IP address for the HBA address rename setup service according to step 12.

6.3.3.2 Changing the Port Number Used to Communicate with the Admin Server

This section explains how to change the port used between the HBA address rename setup service and the Admin Server.
The HBA address rename setup service used the "rcxweb" port to communicate with the Admin Server.
When this setting is changed, the HBA address rename setup service automatically checks whether it can communicate with the new Admin Server IP address.
Changing this setting also requires changing the port on the Admin Server side beforehand.

Use the following procedure to change the port numbers used to communicate with the Admin Server:

1. Change the port number of the Manager.

   Change the "rcxweb" port number according to the instructions given in "6.3.1.2 Changing Port Numbers".

2. Change the port number of the HBA address rename setup service.

   Refer to "6.2.2.1 Settings for the HBA address rename setup service", and change the port to the same port number.

6.3.3.3 Changing the IP Address of the HBA Address Rename Server

This section explains how to change the IP address of the HBA address rename server.
Use the following procedure to change the IP address of the HBA address rename server.

1. Log in to the HBA address rename server with administrator authority.
2. Stop the HBA address rename setup service.

   Stop the HBA address rename setup service according to "6.2.2.1 Settings for the HBA address rename setup service".

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

   Change the IP address following the instructions given in the operating system's manual.

4. Restart the HBA address rename setup service.

   Restart the HBA address rename setup service according to "6.2.2.1 Settings for the HBA address rename setup service".

6.3.4 Changing LAN Switch Settings

This section explains how to change LAN switch settings.

6.3.4.1 Changing LAN Switch Basic Settings

This section explains how to change LAN switch basic settings.
The following settings can be changed.

- LAN switch name (node name for management purposes)
- Admin LAN (IP address)
- User name (LAN switch blade only)
- Password (LAN switch blade only)
- Privileged password (LAN switch blade only)
- SNMP community

Complete the changes to the settings on the target LAN switch before performing this procedure.

Use the following procedure to change LAN switch settings:

1. In the RC console resource tree or network resource tree, right-click the target LAN switch name and select [Modify]-[Registration Settings] from the popup menu.

   The [Modify LAN Switch] dialog is displayed.

2. Edit the information in the [Modify LAN Switch] dialog and click the <OK> button.

   The settings for the LAN switch are changed with the entered information.

Note

It is possible to set the IP address of the target switch to another unregistered LAN switch. However, this will result in the Resource Coordinator VE configuration being inconsistent with the actual network configuration.
If the IP address of the target switch is set to the same address as that of another unregistered LAN switch unexpectedly, change back the target LAN switch IP address to its original value according to the instructions given in this section.
If there are more then one LAN switches with inconsistent IP address configurations, delete all registered LAN switches according to "6.4.3.2 Deleting LAN Switches (Non-Blade Switches)" first, then perform "Discover" and "Register" according to "6.1.3.2 Registering LAN Switches (Non-Blade Switches)".

6.3.4.2 Changing VLANs set on External LAN Switch Ports

VLAN types and IDs set on the external ports of a managed LAN switch blade can be changed.

Changing VLAN IDs

This explains how to change VLAN IDs set on the external ports of a LAN switch.

- Port VLAN

  Use the following procedure to change VLAN IDs:

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

   The [VLAN Settings] dialog is displayed.

2. In the [VLAN Settings] dialog, set the following items.

   VLAN ID

   Select "Change" in the VLAN information and select the VLAN ID that has been changed.

   VLAN Type

   Select "Untagged" from the VLAN type port number to be set from the port list.

3. Click the <OK> button.

   VLAN ID is changed.

- Tagged VLAN

  First delete the VLAN ID was set on the desired LAN switch blade port before setting the new VLAN ID.

  Use the following procedure to change VLAN IDs:

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

     The [VLAN Settings] dialog is displayed.

  2. In the [VLAN Settings] dialog, set the following items.

     VLAN ID

     Select "Change" in the VLAN information and select the VLAN ID to be changed.

     VLAN Type

     In the port list, select "None" as the VLAN type set for the desired port.

  3. Click the <OK> button.

     The VLAN ID set for the selected LAN switch blade port is released.

  4. Repeat step 1 and set the new VLAN ID in the "VLAN Settings" dialog.

     VLAN ID

     Select "New" or "Change" in the VLAN information and select the VLAN ID to be changed.

     VLAN Type

     Select "Tagged" from the VLAN type port number to be set from the port list.

  5. Click the <OK> button.

     The VLAN ID is changed.

Changing VLAN types

This section explains how to change the types of VLAN (port or tagged VLAN) set on the external ports of a LAN switch.

Use the following procedure to change VLAN types:

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

   The [VLAN Settings] dialog is displayed.

2. In the [VLAN Settings] dialog, select "Change" in the VLAN information to select the VLAN ID.

3. In the port list, select the appropriate VLAN type ("Untagged" or "Tagged") to be set to the desired port.

4. Click the <OK> button.

   The VLAN type is changed.

Deleting VLAN IDs

This section explains how to delete VLAN IDs.

- Deleting VLAN IDs from LAN switches

  Use the following procedure to delete VLAN IDs:

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

     The [VLAN Settings] dialog is displayed.

  2. In the [VLAN settings] dialog, select "Change" in the VLAN information and select the VLAN ID to delete.

  3. Click the <Delete> button.

     The VLAN ID is deleted.

- Deleting VLAN IDs from LAN switch ports

  Use the following procedure to delete VLAN IDs:

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

     The [VLAN Settings] dialog is displayed.

  2. In the [VLAN Settings] dialog, set the following items.

     VLAN ID

     Select "Change" in the VLAN information and select the VLAN ID to be deleted.

     VLAN type

     Select "None" from the VLAN type port number to be deleted from the port list.

  3. Click the <OK> button.

     The VLAN ID is deleted.

6.3.4.3 Re-discovering LAN Switches

Newly added LAN switches can be discovered by re-executing LAN switch discovery.
Refer to "Discovery" in "6.1.3.2 Registering LAN Switches (Non-Blade Switches)" for details on LAN switch discovery.

6.3.5 Changing VM Management Software Settings

This section explains how to change VM management software settings.

The following settings can be changed.

- Location
- IP address
- User name
- Password

Complete re-configuration within the VM management software admin console before performing this procedure.

Use the following procedure to change VM management software settings:

1. From the RC console menu, select [Settings]-[VM management software].

   The [Configure VM management software] dialog is displayed.

2. In the [Configure VM management software] dialog, enter the following items.

   Location

   If VM management software is installed on the Admin Server, select "Admin Server". Otherwise, select "Other server".

   IP address

   If "Other Server" was selected, enter the IP address of the server on which VM management software is installed.

   User name

   Enter the name of a VM management software user account.

   Password

   Enter the password of the above VM management software user account.

3. Click the <OK> button.

   VMware management software settings are changed.

6.3.6 Changing Power Monitoring Environment Settings

This section explains how to change power monitoring environment settings.

Power environment settings include power monitoring device settings and collection settings.

6.3.6.1 Changing Environmental Data Settings

Use the following procedure to change environmental data settings:

1. From the RC console menu, select [Tools]-[Options].

   The [Options] dialog is displayed.

2. In the [Options] dialog, select the "Environmental Data" category title.

   The "Environmental Data" area is displayed.

3. In the "Environmental Data" area, change the following items.

   Data to collect

   Select "Power", to start collecting power consumption data.

   Polling interval (in minutes)

   Enter the time interval of the data collection (1-6 or 10).

   The number of devices that can be monitored simultaneously depends on the value of this polling interval and the load put on the Admin Server.

   Table 6.1 Polling interval

Polling interval	Number of devices that can be monitored simultaneously
5 minutes	Up to 40 devices
10 minutes	Up to 60 devices

   Use a polling interval of 5 minutes or longer when monitoring chassis and servers. Use a polling interval of 10 minutes if monitoring more than 40 devices.

Data storage period

Enter storage periods for each collection rate. Data older than the configured storage period will be deleted everyday.

Enlarging data storage periods reduces the number of devices that can be monitored simultaneously.

Use the default storage period values when monitoring chassis and servers.

4. Click the <Apply> button.

Note

If the "Power" checkbox under "Data to collect" is unselected, the collection of power consumption data (including the calculation of hourly, daily, and other summarized data) will not be performed anymore.

6.3.6.2 Changing Power Monitoring Devices

The following settings can be changed:

- Device name
- Admin LAN (IP address)
- SNMP community
- Voltage
- Comment

Complete setting modifications on the actual power monitoring device before performing this procedure.

Use the following procedure to change power monitoring device settings:

1. From the RC console, right-click the power monitoring device, then select [Modify]-[Registration Settings] from the popup menu.

   The [Modify Power Monitoring Device] dialog is displayed.

2. Edit the items to be changed in the [Modify Power Monitoring Device] dialog and click the <OK> button.

   The power monitoring device settings will be changed with the entered information.

6.4 Deleting Resources

This section explains how to delete resources.

The managed server and the LAN switch can be registered and deleted for one resource in the same chassis.
Note that operation to the server cannot be performed while the LAN switch is being registered and removed.
If the operation is performed simultaneously for multiple resources, one of the following messages is displayed.
In this case, wait until the process is completed then execute it again.

FJSVrcx:ERROR:67210: *LAN switch name*(LAN switch):is busy

or

FJSVrcx:ERROR:67210: *Managed server name* (physical server):is busy

6.4.1 Deleting Chassis

This section explains how to delete chassis.

Use the following procedure to delete the chassis.

1. In the RC console resource tree, right-click the target chassis, and select [Delete] from the popup menu.

   The [Delete Resource] dialog is displayed.

2. Click the <OK> button.

   The target chassis is deleted from the resource tree.

Note

If blade servers within the chassis were already registered, delete these blade servers before deleting the chassis.
If LAN switches have been registered, delete all LAN switches before deleting the chassis.

6.4.2 Deleting Managed Servers

This section explains how to delete managed servers.

Use the following procedure to delete managed servers.

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

   The [Delete Resource] dialog is displayed.

   If a VM host is running on the server to be deleted, any VM guests running on that host are also deleted from the resource tree at the same time. The VM guests to be deleted appear in the [Delete Resource] dialog, so check that it is safe to delete them.

2. Click the <OK> button.

   If a physical OS or VM host exists on the target server and HBA address rename is set, the server will be powered off when the resource is deleted.
   The target server is un-registered.

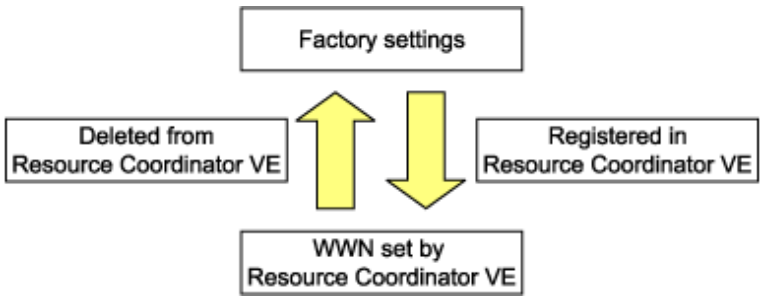
   When deleting a PRIMERGY BX server, the deleted server will still be displayed in the resource tree as "not registered".

Note

When deleting servers, Resource Coordinator VE does not delete the host affinity settings of a storage unit or the zoning settings of a Fibre Channel switch. Use storage management software (such as ETERNUS SF Storage Cruiser) to delete these settings.

Information

- If HBA address rename has already been set up on the managed server, the HBA WWN is reset to the factory default.
  Power to the managed server is turned on temporarily when this occurs.



- VM guests can be deleted using the management console of the server virtualization software used. Doing so will automatically delete those VM guests from Resource Coordinator VE as well.
- If the same storage device volume is to be used to operate the target server after the server has been deleted, use storage management software such as ETERNUS SF Storage Cruiser to reset the storage host affinity and fibre channel switch zoning with the factory default WWN.

- Any system images backed up from the target server are also deleted automatically.
- After the server has been deleted, the maintenance LED is switched OFF automatically.
- Deleting a server on which both the HBA address rename function and a VM high-availability feature (provided by the virtualization software used) are enabled will produce the following behavior. The server will be powered off, causing the high-availability feature to trigger its VM recovery process. To avoid interruption of hosted applications during server deletion, it is recommended to move VM guests to another server beforehand. For more details on the high-availability features available for each server virtualization product, refer to "A.2 Configuration Requirements".

6.4.3 Deleting LAN Switches

This section explains how to delete LAN switches.

As described below, the deletion method differs according to the type of LAN switch to delete.

- Deleting LAN switch blade
- Deleting LAN switch

6.4.3.1 Deleting LAN Switch Blades

This section explains how to delete LAN switch blades.

Use the following procedure to delete LAN switch blades.

1. In the RC console resource tree, right-click the target LAN switch blade and select [Delete] from the popup menu.

   The [Delete Resource] dialog is displayed.

2. Click the <OK> button.

   The target LAN switch blade is un-registered.

6.4.3.2 Deleting LAN Switches (Non-Blade Switches)

This section explains how to delete LAN switch.

Use the following procedure to delete LAN switches.

1. In the RC console resource tree, right-click the target LAN switch and select [Delete] from the popup menu.

   The [Delete Resource] dialog is displayed.

2. Click the <OK> button.

   The target LAN switch is un-registered.

6.4.4 Deleting VM Management Software

This section explains how to delete VM management software.

Use the following procedure to delete VM management software.

1. From the RC console menu, select [Settings]-[VM management software].

   [VM management software] dialog is displayed.

2. In [VM management software] dialog, select "VM Management Software Deletion".
3. Click the <OK> button.

   The target VM management software is un-registered.

6.4.5 Clearing the Power Monitoring Environment

This section explains how to clear the power monitoring environment.

Clearing the power monitoring environment is done by deleting power monitoring targets and cancelling collection settings.

6.4.5.1 Deleting Power Monitoring Devices

This section explains how to delete power monitoring devices.
Use the following procedure to delete power monitoring devices:

1. In the RC console resource tree, right-click the target power monitoring device and select [Delete] from the popup menu.

   The [Delete Resource] dialog is displayed.

2. Click the <OK> button.

   The target power monitoring device is deleted from the resource tree.

6.4.5.2 Canceling Collection Settings for Power Monitoring Environments

This section explains how to cancel the collection of power consumption data.
Use the following procedure to cancel the collection of power consumption data.

1. From the RC console, select [Tools]-[Options].

   The [Options] dialog is displayed.

2. In the [Options] dialog, click the [Environmental Data] category title, and change the following items.

   Data to collect

   Remove the check mark from the "Power" checkbox.

3. Click the <Apply> button.

   Collection of environmental data is canceled.

Chapter 7 Pre-configuration

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

7.1 Overview

Using the Pre-configuration function, it is possible to create system definition files that can be later used to setup a Resource Coordinator VE environment. Importing system configuration files makes it easy to perform various registration settings in one operation. This prevents the operating mistakes induced by sequences of individual, manual configuration steps.

The pre-configuration function can be used in the following situations.

- New installation

  From a traditional work office (or another off-site location), define the various parameters required for Resource Coordinator VE and record them in a system configuration file. Next, send this definition file to your actual system location (machine room), and import the file into Resource Coordinator VE using the import functionality of the RC console. This single operation will automate the registration of all the servers defined in the system configuration file.

- Backing up a system configuration

  Using the export functionality of the RC console, the current Resource Coordinator VE configuration can be exported to a system configuration file. This configuration file can then be used as a backup of the current configuration.

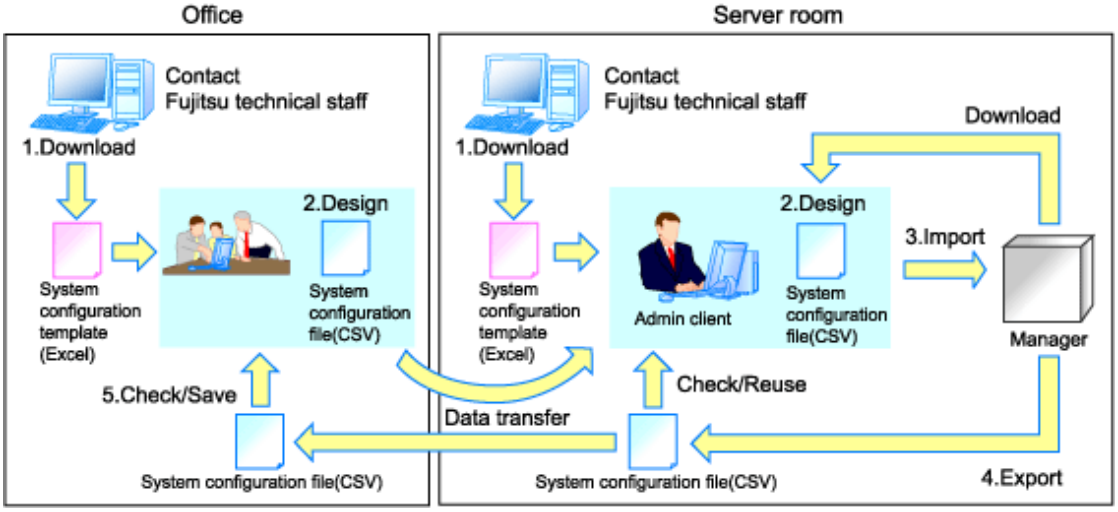
- Batch re-configuration

  The registration settings of already registered resources can be modified easily by exporting the current configuration to a system configuration file and editing the desired configuration items before re-importing that configuration file. The actual re-configuration is then performed as a single import operation.

- Re-use of existing configurations

  Once a system has been fully setup, its configuration can be exported and re-used as a basis for the design of other systems. This makes it easy to design various systems located in different sites.

Figure 7.1 Examples of use



Only system configuration files in CSV format can be imported or exported. Refer to "Appendix D Format of CSV System Configuration Files" for details on the system configuration file's format.
Resource Coordinator VE provides a sample in CSV format. An Excel template (hereafter called "system configuration template") is also available from the ServerView Resource Coordinator VE home page. This system configuration template makes it easy to create system configuration files in CSV format.

The system configuration files imported by the system configuration template or the RC console should start with a "RCXCSV,V1,0", "RCXCSV,V2.0" or "RCXCSV,V3.0" descriptor as their first line.

Similarly, system configuration files, created by the system configuration template or exported from the RC console always start with a "RCXCSV,V3.0" descriptor as their first line.

The following operations, usually performed from the RC console, can be equally performed using the pre-configuration function.

- Registering resources:
  - "Chapter 6 Setup"
    - "6.1.1 Registering Chassis"
    - "6.1.2 Registering Managed Servers"
    - "6.1.3 Registering LAN Switches"
    - "6.1.4 Registering VM Management Software"
    - "6.1.5 Registering Power Monitoring Devices" (*1)
    - "6.2.1 Configuring VLANs on LAN Switches"
    - "6.2.2 Configuring HBA address rename" (*2)
  - "Chapter 9 Server Switchover Settings"
    - "9.6 Server Switchover Settings"
- Modifying resources:
  - "Chapter 6 Setup"
    - "6.3.1.1 Changing the Admin IP Address" (*3)
    - "6.3.2.2 Changing Server Names"
    - "6.3.2.3 Changing Admin IP Addresses" (*3)
    - "6.3.2.4 Changing SNMP Communities"
    - "6.3.2.5 Changing Remote Management Controller Settings"
    - "6.3.2.7 Changing VM Host Login Account Information"
    - "6.3.2.8 Changing the VLAN Settings of a LAN Switch"
    - "6.3.2.9 Changing HBA address rename Settings" (*2)
    - "6.3.4 Changing LAN Switch Settings"
    - "6.3.5 Changing VM Management Software Settings"
    - "6.3.6 Changing Power Monitoring Environment Settings"
  - "Chapter 9 Server Switchover Settings"
    - "9.7 Changing Server Switchover Settings"

*1: To start collecting environment data, the collection settings should be manually set from the RC console's option dialog.
*2: Restart all the managed servers that were either registered or modified following an import operation.
*3: The pre-configuration's scope of configuration is the same as that of the RC console.

Moreover, the pre-configuration function can perform the same labels and comments settings as those available in BladeViewer. Those settings are described in "3.6.1 Listing and Editing of Labels and Comments" and "Chapter 3 BladeViewer" in the "ServerView Resource Coordinator VE Operation Guide".

Note

The following operations cannot be performed by the pre-configuration function, and should be performed from the RC console.

- Deleting registered resources from Resource Coordinator VE

- Changing the name of a registered chassis, physical server (only for servers other than PRIMERGY BX servers) or a power monitoring device
- Discovering, registering or the changing registration settings of a LAN switch
- Detecting physical link information from a LAN switch

7.2 Importing the System Configuration File

This section explains how to import a system configuration definition file (saved in CSV format) from the RC console.

Use the following procedure to import a system configuration definition file.

1. Prepare a system configuration file in CSV format.

   Point

   - The system configuration template in Excel format cannot be directly imported into Resource Coordinator VE. Use the template's save to CSV function to produce a system configuration file in CSV format before importing.
   - Only system configuration files beginning with "RCXCSV,V1.0", "RCXCSV,V2.0" or "RCXCSV,V3.0" in their first line can be imported. For details of the file format, refer to "Appendix D Format of CSV System Configuration Files".
   - When importing system configuration files which begins with "RCXCSV,V1.0" in the first line, the agent cannot automatically be registered. Moreover, the registration fails in case that a spare server is defined to a VM host in the system configuration file.
     For details on upgrading from Systemwalker Resource Coordinator Virtual server Edition V13.2, refer to "Chapter 4 Upgrading from Earlier Versions" in the "ServerView Resource Coordinator VE Installation Guide".

2. Open the RC console and log in. Refer to "5.3 RC Console" for details.
3. In the RC console, select the [File]-[Import] menu item.

   The [Import system configuration file] dialog is displayed.

4. Specify the system configuration file prepared in step 1, then click <OK>. The import processing will start. The system configuration file is verified first. Next, resources are imported one by one, following the order defined by the system configuration file.

   The processing of resource registration or change is executed after the verification. The process status is displayed in the Recent Operations area of the RC console. The <Cancel> button interrupts the import process after completing the current processing. Note that the processing performed up to the error point is effective in the system.

   Point

   The "SpareServer", "ServerAgent" and "ServerVMHost" sections must meet the conditions below when performing pre-configuration.

   a. Spare server section ("SpareServer")

      - In case that the specified spare server has no operating system installed.

        The physical server which is defined as a spare server must not be defined in "ServerWWNN", "ServerAgent" or "ServerVMHost" sections.

      - In case that the specified server is a VM host.

        The physical server which is defined as a spare server must already be registered for the Resource Coordinator VE agent.

      If the above conditions are not meet, divide the section as different CSV files, and import them one by one.

   b. Agent section ("ServerAgent" or "ServerVMHost")

      - The agent of the Resource Coordinator VE must already be installed in the managed server.
      - An operating system must be running on the managed server.

- The agent of the target physical server must be registered, or the agent registration section is defined in the system configuration file.

5. When the import is completed successfully, a message is displayed in the Recent Operations area.

Point

- Error handling

  The processing of resource registration or change is executed after the verification of the system configuration file during import.

  If an error occurs during verification process, which means some invalid value existing in the system configuration file, an error message is displayed only in the event log. Correct the system configuration file, and import it again.
  Invalid content also includes the invalid section headers.
  If there is an error message displayed, but the values in the specified line are all correct, check whether the section header is correct or not.

  If an error occurs during registration and change process, an error message is displayed to both the Recent Operations area and the event log. In this case, the process is finished up to the previous line setting, that is, before the system configuration file line number which message is displayed. Correct the system configuration file and rectify the problem, then import it again. The process will resume from it last stopped.

- Import log file

  The import log is saved on the following location. In case that an error occurs in the verification step, which means the processing of registration or changing the resource does not start yet, no log file is created.

  [Windows]
  Installationfolder\Manager\var\log\config.log

  [Linux]
  /var/opt/FJSVrcvmr/log/config.log

- Backing up the manager prior to import automatically

  When import operation is performed by user, exporting is automatically executed also. The export file is saved as the backup of the manager configuration. Use this file to return to the previous value if an input error in the system configuration file. Note that the backup can store the latest five generations.

  The system configuration file backup can be stored as following.

  [Windows]

  Folder

  Installationfolder\Manager\var\config_backup

  File name

  rcxconf-*YYYYMMDDHHMMSS*.csv (the date and time are shown in *YYYYMMDDHHMMSS*)

  [Linux]

  Directory

  /opt/FJSVrcvmr/var/config_backup

  File name

  rcxconf-*YYYYMMDDHHMMSS*.csv (the date and time are shown in *YYYYMMDDHHMMSS*)

6. If the import complete successfully, perform the following procedures if required.

   - If HBA address rename is set, then restart the relevant managed server.
   - If the agent is registered, perform either one of the following to enable further backup or cloning operations.
     - Restart the managed server.
     - Restart the "Deployment service" described in "5.2 Agent".

7.3 Exporting the System Configuration File

Use the following procedure to export the system configuration file in CSV format from the RC console.

1. Open the RC console and login. Refer to "5.3 RC Console" for details.
2. In the RC console, select the [File]-[Export] menu item.
3. The export process starts automatically.
4. When the process complete successfully, the [File Download] dialog is displayed.

   The <Save> button brings up the [Save As] dialog, where you are prompted for the folder and file name in which to save the file. Note that the system configuration file can be exported only in the CSV format.

   The <Open> button opens the file with the application (such as Excel) associated to CSV files.

   The <Cancel> button cancels the export.

Note

If any server is in switchover state, the server name is enclosed in parentheses, such as "(name)".

Point

Error handling

If an error occurs, an error message is displayed. Follow the message diagnostic to resolve the problem.

Chapter 8 Cloning [Windows/Linux]

This chapter explains how to use the server cloning function.

8.1 Overview

Cloning is a function used to deploy a cloning image collected from a single managed server (source server) to other managed servers (destination servers).

This function shortens the time required for an initial installation as it can be used to install the same operating system and software on multiple servers.
Software maintenance can also be performed quickly and easily by deploying a cloning image collected from a server on which patches and software have already been applied, added, or modified.

The information below is not copied when the cloning image is collected from the Admin Server; and will be automatically reconfigured when the cloning image is deployed. This enables a single cloning image to be deployed to different servers.

- Host name
- IP address and subnet mask of the Admin LAN
- Default gateway of the Admin LAN

Settings other than the above (such as those for applications and middleware) are not automatically reconfigured, please set them manually before and after the cloning operation when necessary.

The Public LAN settings (IP address and redundancy settings) for servers to which the cloning image is deployed can be configured easily by using the network parameter auto-configuration function.
Refer to "8.6 Network Parameter Auto-Configuration for Cloning Images" for details on the network parameter auto-configuration function.

Note

- When cloning servers, only content from the boot disk (first disk recognized by the BIOS on managed servers) is actually cloned. Data disks content (second disk onwards) can not be cloned. It is recommended to use other backup software, or copy features available in storage systems for such purposes.
  Note that all partitions (Windows drives or Linux partitions) included in the boot disk will be cloned.

  Table 8.1 Cloning target examples

Disk	Windows drive	Cloning Target
First disk	C:	Yes
	E:	Yes
Second disk	D:	No
	F:	No

- Because managed servers are restarted during the cloning process, it is required to stop all applications running on those servers beforehand.
- The first partition must be a primary partition.
- The cloning function only supports the following file systems on managed servers. Note that LVM partitions are not supported.
  - NTFS
  - ext3
  - LinuxSwap
- Source and destination servers must meet the following conditions:
  - All server models must be identical.

- The hardware configuration of each server must be identical, including optional cards and the slots they are mounted in.
- The same BIOS settings must have been made for all servers according to the procedure in "BIOS Settings for Managed Servers" in "3.5 Configuring the Server Environment".
- All servers must use the same redundancy configuration (if any) and the same number of redundant paths for LAN and SAN connections. All servers must also be able to access the same network and storage devices.
  Note that LAN switches and fiber channel switches set with cascading connections are seen as single devices.

- Some applications may require manual adjustments to function properly after cloning. If necessary, manually perform such adjustments before or after the cloning process.
- No more than four image processes can be executed simultaneously (image processes include backup and restore of system images, as well as collection and deployment of cloning images). If five or more processes are requested, the fifth and subsequent processes are placed on standby.
  Restore operations executed during a server switchover or failback process are also placed on standby if four image processes are already running. It is therefore recommended to restrict the number of simultaneous image processes to no more than three and keep slot(s) open for high-priority requests, such as automatic (Auto-Recovery) or manual switchovers.
- Software that needs to connect to an external server upon OS startup may not run properly after the collection or deployment of a cloning image.
  In this case, restart the operating system after collecting or deploying the cloning image.
- For servers on which the Watchdog function is enabled, cloning operations on that server may be aborted by an automatic restart or shutdown. The Watchdog is a function which automatically restarts or shuts down non-responsive servers when their operating system does not respond for a given period of time.
  It is therefore highly recommended to disable the Watchdog function before a cloning operation.
  Refer to the server manual for details on the Watchdog function.
- For servers (Windows Server 2008) using a Multiple Activation Key (MAK) for Volume Activation, the activation utility (sysprep) can only be run up to three times.
  Because this activation utility (sysprep) is run each time a cloning image is deployed, such an image (one collected from a MAK-activated server) can not be (re-)collected and deployed more than four times (this count is increased each time an image is updated or re-collected as a new image). It is therefore not recommended to re-collect cloning images from image-deployed servers, but rather to collect a new image from a dedicated (freshly installed) master server.
- Cloning of servers running a SUSE Linux Enterprise Server operating system is not supported.

8.2 Collecting a Cloning Image

This section explains how to collect a cloning image from a source server. Collected cloning images can later be used for the deployment of other servers.

A cloning image can be collected only from a managed server on which the Agent was registered.
Refer to "6.2.3 Software Installation and Agent Registration" for details on registering Agents.

Cloning images cannot be collected from VM hosts or VM guests.

Preparations

Install the desired operating system and necessary applications on the source server from which to collect a cloning image.
Additionally, apply any required patches and other necessary settings.
Make sure that the source server operates properly after those steps.

- Make sure that the DHCP client has been enabled on the source server.
- The number of cloning image versions that can be kept for a given cloning image (identified by its name attribute) is limited. When collecting a new cloning image while this limit has already been reached, select the version to be deleted.
  By default, this limit is set to 3 versions per cloning image.
  This limit can be changed by following the instructions given in "6.3.1.4 Changing the Maximum Number of Cloning Image Versions".

- When deploying cloning images, the destination server temporarily starts up with its hostname set to either the physical server name or the source server's hostname. Some programs may experience problems when started with a different hostname. If such programs have been installed, configure their services not to start automatically. This has to be configured before collecting the cloning image.
- To use network parameter auto-configuration function, check the operation before performing collection.
  For details, refer to "8.6.1 Operation Checks and Preparations".

[Windows]

- Enable NetBIOS over TCP/IP
- A volume license is required for cloning, and must be entered during the installation of Resource Coordinator VE Agent. Refer to "2.2.1.2 Collecting and Checking Required Information" and "2.2.2 Installation [Windows/Hyper-V]" in the "ServerView Resource Coordinator VE Installation Guide" for details.

  If no volume license is entered during the Agent installation, or if this information is changed after installation, edit the following license configuration file on the source server. Note that the structure and location of this file depend on the version of Windows that is being used.

  - In Windows Server 2003

    Installation folder\Agent\scw\SeparateSetting\sysprep\sysprep.inf

    Edit the following line to enter a valid product ID.

ProductID=*Windows product key* (*1)

    *1: 5-digit values separated by hyphens

    Example

ProductID=11111-22222-33333-44444-55555

    Note

    An invalid product ID (invalid format or invalid value) will cause an error the next time a cloning master (collected from this server) will be deployed. Make sure to enter a valid product ID when editing the definition file.

  - In Windows Server 2008

    Installation folder\Agent\scw\SeparateSetting\ipadj\activation.dat

    In the [ActivationInfo] section, set the following parameters using a "parameter=value" syntax.
    Refer to the following table for details on each parameter.

    Table 8.2 Structure of the Definition File

Format	Parameter	Value
KMS	.cmd.remotescript.1.params.kmscheck (Mandatory)	KMS host search type. Select one of the following. ・ "AUTO": Automatic search ・ "MANUAL": Specify the KMS host If "MANUAL" is set, make sure that the cmd.remotescript.1.params.kmsname is set.
	.cmd.remotescript.1.params.kmsname	Host name (FQDN), computer name or IP address of the KMS host
	.cmd.remotescript.1.params.kmsport	KMS host port number. The default is 1688.

Format	Parameter	Value
MAK	.cmd.remotescript. 1.params.makkey (Mandatory)	MAK key
Common	.cmd.remotescript.1.params.ieproxy	Host name (FQDN) and the port number of the proxy server. The host name and port number are separated by a colon (":").
	.cmd.remotescript. 1.params.password	Administrator password. An existing password setting will be displayed as an encrypted character string. To change this password, rewrite it in plain text, delete the following "encrypted=yes" line, and follow the encryption procedure described below. If this parameter is not set, the password will be re-initialized.
	encrypted	The encryption status of the Administrator password. "yes" means that the password is encrypted. If this line exists, the rcxadm deployctl command will not function.

Example

- With KMS (automatic search)

  [ActivationInfo]

  .cmd.remotescript.1.params.kmscheck=AUTO
  .cmd.remotescript.1.params.ieproxy=proxy.activation.com:8080
  .cmd.remotescript.1.params.password=PASSWORD

- With KMS (manual settings)

  [ActivationInfo]

  .cmd.remotescript.1.params.kmscheck=MANUAL
  .cmd.remotescript.1.params.kmsname=fujitsu.activation.com
  .cmd.remotescript.1.params.kmsport=4971
  .cmd.remotescript.1.params.ieproxy=proxy.activation.com:8080
  .cmd.remotescript.1.params.password=PASSWORD

- With MAK

  [ActivationInfo]

  .cmd.remotescript.1.params.makkey=11111-22222-33333-44444-55555
  .cmd.remotescript.1.params.ieproxy=proxy.activation.com:8080
  .cmd.remotescript.1.params.password=PASSWORD

  When changing the Administrator password, execute the following command. This command will encrypt the .cmd.remotescript.1.params.password parameter and add an "encrypted=yes" line to show that it is encrypted.
  Refer to "5.3 rcxadm deployctl" in the "ServerView Resource Coordinator VE Command Reference" for details.

  > "*Installation folder***Agent\bin\rcxadm**" **deployctl passwd -encrypt** <RETURN>

- With MAK (already encrypted password)

  [ActivationInfo]

  .cmd.remotescript.1.params.makkey=11111-22222-33333-44444-55555
  .cmd.remotescript.1.params.ieproxy=proxy.activation.com:8080

```
.cmd.remotescript.1.params.password=xyz123456
encrypted=yes
```

Collecting a Cloning Image

Use the following procedure to collect a cloning image from a source server:

1. Put the source server into maintenance mode.

   a. In the RC console resource tree, right-click the source server (or its physical OS), and select [Maintenance Mode]-[Set] from the popup menu.

      The [Set Maintenance Mode] dialog is displayed.

   b. Click the <OK> button.

      The source server is put into maintenance mode.

2. Stop all operations running on the source server.

   When a cloning image is collected, the source server is automatically restarted. Therefore, all operations running on the source server should be stopped before collecting the image.
   Cancel any Admin LAN or Public LAN redundancy settings.
   However, there is no need to cancel Public LAN redundancy settings made via the network parameter auto-configuration function.
   The following settings are disabled during cloning image collection, which may result in services failing to start on server startup. To avoid this, automatic startup should be disabled for any service that depends on the following settings.

   - Hostname
   - IP address and subnet mask for the Admin LAN
   - Default gateway for the Admin LAN

3. Collect a cloning image.

   a. In the RC console resource tree, right-click the physical OS of the source server and select [Cloning]-[Collect] from the popup menu.
      The [Collect a Cloning Image] dialog is displayed.

   b. In the [Collect a Cloning Image] dialog, set the following parameters:

      Cloning Image Name

      Enter a name to identify the collected cloning image.

      New
      When creating a new cloning image, select "New" and enter a new cloning image name.
      The cloning image name can be up to 32 characters long, and can contain alphanumeric characters and the underscore ("_") character.

      Update
      When updating an existing cloning image, select "Update" and select a cloning image from the list.

      The maximum number of versions that can be stored at one time for a cloning image is limited.
      If the selected cloning image has already reached this limit, it is necessary to delete one of its existing versions in order to create a new cloning image. This can be done directly in this dialog by selecting the version to be deleted from the displayed list.
      The selected version will be automatically deleted when collection of the new cloning image completes.
      By default, the maximum number of stored image versions is set to 3.
      This setting can be changed by following the instructions given in "6.3.1.4 Changing the Maximum Number of Cloning Image Versions".

Comments (Optional)

Enter a comment that identifies the cloning image.
A comment can be of no more than 128 characters. Percents ("%), backslashes ("\"), double quotes ("), and linefeed characters are not allowed.

If [Update] was selected for the "Cloning Image Name" option, the comment of the most recent image version is displayed.
If no comment is specified, a hyphen ("-") will be displayed in the RC console.

It is recommended to enter comments with information such as hardware configuration (server model, disk size, and number of network interfaces), software configuration (names of installed software and applied patches), and the status of network parameter auto-configuration function.

"Release Maintenance Mode after collection" option

Enable this option to automatically release the source server from maintenance mode after image collection and maintenance work. If this option disabled, maintenance mode should be released manually after collecting the cloning image.

c. Click the <OK> button.

A cloning image is collected from the selected source server.

4. Restart applications on the source server.

Restore the settings of any service whose startup settings were changed in step 2 and start these services.
Restore any Admin LAN or Public LAN redundancy settings that may have been canceled in step 2.
Check that applications are running properly on the source server.

5. Release the source server from maintenance mode.

This step is not required if the "Release Maintenance Mode after collection" option was enabled in the [Collect a Cloning Image] dialog.

a. In the RC console, right-click the source server (or its physical OS), and select [Maintenance Mode]-[Release] from the popup menu.

The [Release Maintenance Mode] dialog is displayed.

b. Click the <OK> button.

The source server is released from maintenance mode.

Note

- While a cloning image is being collected, no other operations can be performed on that image or other versions of that image (images sharing the same image name).
- Communication errors between the admin and source servers (resulting in an image collection failure or an "unknown" status on the source server) may be caused by improper use of the network parameter auto-configuration function (described in "8.6 Network Parameter Auto-Configuration for Cloning Images"). Examples of improper use are given below.
  - Auto-configuration settings were made for the Admin LAN (the network parameter auto-configuration function shouldn't be used on the Admin LAN).
  - Auto-configuration settings were made for the Public LAN using IP addresses contained within the Admin LAN subnet range.

Log in to the source server and check for the presence of such settings in the network parameter definition file.
If incorrect settings were made, use the following recovery procedure to fix communication errors.

1. Fix network settings on the source server

Run the "rcxadm lanctl unset" command described in "8.6.3 Clearing Settings" to reset network settings back to their original values.

If the Admin LAN IP address is not set on the source server, set it manually to restore communications between the Admin Server and the source server.

2. Re-collect the cloning image

   Correct any errors found in the source server's network parameter definition file and re-collect the cloning image from the source server.

3. Delete faulty cloning images

   Delete any cloning image that was collected with incorrect network parameters.

8.3 Deploying a Cloning Image

Once collected, cloning images can be deployed to one or more destination servers.

Cloning images collected from the source server can only be deployed to destination servers which satisfy the following conditions:

- Destination servers should be in either "normal", "warning", "unknown" or "stop" status.
- Destination servers should have been put into maintenance mode.
- Destination servers should be of the same model as the source server.
- Destination servers should not be used as spare server(s) for other servers.

Cloning images cannot be deployed to servers where VM hosts or VM guests are running.

Preparation

It is recommended to back up destination servers before deploying cloning images, as this will simplify the recovery procedure in case of the deployed cloning image is faulty.
Refer to "8.2 Backing Up System Images" in the "ServerView Resource Coordinator VE Operation Guide" for details on backing up servers.

Note

- Cloning images cannot be deployed to servers that have been set up as spare servers for other managed servers. Cancel any such settings before deploying a cloning image.
- VLAN settings (on adjacent LAN switch ports) cannot be deployed during server cloning. LAN switch VLAN settings should be set up before deploying a cloning image.
  Refer to "6.2.1 Configuring VLANs on LAN Switches" for details on how to configure VLAN settings on LAN switches.
- When deploying a cloning image back to its source server, the source server should be backed up before deployment.
  For details on server backup, refer to "8.2 Backing Up System Images" of the "ServerView Resource Coordinator VE Operation Guide".

  If the deployed cloning image is faulty and causes deployment errors, use the following procedure to collect a new cloning image.

  1. Restore the system image that was backed up before cloning image deployment
  2. Fix any incorrect settings on the source server
  3. Collect a new cloning image
  4. Delete the faulty cloning image

Deploying a Cloning Image

Use the following procedure to deploy a cloning image to one or more destination servers:

1. Put the destination server(s) into maintenance mode (only for Agent-registered servers).

   a. In the RC console resource tree, right-click a destination server (or its physical OS), and select [Maintenance Mode]-[Set] from the popup menu.

      The [Set Maintenance Mode] dialog is displayed.

   b. Click the <OK> button.

      The selected destination server is put into maintenance mode.

   Repeat this step for each of the destination servers.

2. Deploy a cloning image.

   - Deploying a cloning image to a single destination server

     a. In the RC console resource tree, right-click the destination server (or its physical OS) and select [Cloning]-[Deploy] from the popup menu.

        The [Deploy a Cloning Image] dialog is displayed.
        A list of available cloning images is displayed in the [Deploy a Cloning Image] dialog.
        Only cloning images that have been collected from a server of the same model as the destination server are available for deployment.

     b. Select the cloning image to be deployed in the [Deploy a Cloning Image] dialog, and then set up the following items:

        Server name after deployment
        Enter the name of the server to which the cloning image is to be deployed.
        By default, the physical OS name is entered if the physical OS is registered. If the physical OS is not registered, the physical server name is entered.

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

        [Linux]
        A string composed of up to 64 alphanumeric characters, and the following symbols:

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

        
        Information

        Since the entered server name is also used as the hostname of the destination server, it is recommended that the server name be composed of the following character strings defined in RFC (Request For Comments) 952:

        - Alphanumeric characters

        - Hyphens, ("-")

        - Periods, (".") [Linux]

        "Release from Maintenance Mode after deployment" option
        Enable this option to automatically release the destination server from maintenance mode after cloning image deployment.
        If this option disabled, maintenance mode should be released manually after deployment.

     c. Click the <OK> button.

        The cloning image is deployed to the selected target servers.

   - Deploying a cloning image to multiple destination servers

     a. In the RC console, open the [Image List] tab.

        A list of cloning image is displayed.

b. From this list, right-click a cloning image and select [Deploy] from the popup menu.

   The [Deploy a Cloning Image] dialog is displayed.
   A list of destination servers satisfying deployment conditions are displayed in the [Deploy a Cloning Image] dialog.

c. Select destination servers from the list, and set up the following items:

   "Release from Maintenance Mode after deployment" option
   Enable this option to automatically release destination servers from maintenance mode after cloning image deployment.
   If this option disabled, maintenance mode should be released manually after deployment.

   The "Server Name" column displays the names of each destination servers.
   By default, server names (computer name or hostname) or physical server names are displayed.
   The names specified in this column will be assigned to destination servers as their computer names (for Windows systems) or system node names (for Linux systems).

   Those names can be changed using the following procedure.

   1. Double-click the "Server Name After Deployment" cell of a server.

   The "Server Name After Deployment" cell becomes editable.

   2. Enter a new server name.

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

   [Linux]
   A string composed of up to 64 alphanumeric characters, and the following symbols:

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

   Since the entered server name is also used as the hostname of its corresponding destination server, it is recommended to use only characters defined in RFC (Request For Comments) 952:

   - Alphanumeric characters

   - Hyphens, ("-")

   - Periods, (".") [Linux]

d. Click the <OK> button.

   The cloning image is deployed.

3. Restart applications on the destination server(s).

   If necessary, make redundancy settings for the Admin LAN and Public LAN.
   After deployment, destination servers are set to use the Admin Server as their default gateway. Re-configure such network settings if necessary.
   Check that applications are running properly on destination servers.
   At this point, if an application is still using the source server's hostname or IP address (e.g. within application-specific settings or configuration file), manually update such settings with the destination server values.

4. Release maintenance mode.

   This step is not required if the "Release from Maintenance Mode after deployment" option was enabled in the [Deploy a Cloning Image] dialog.

   a. In the RC console resource tree, right-click a destination server (or its physical OS) and select [Maintenance Mode]-[Release] from the popup menu.

      The [Release Maintenance Mode] dialog is displayed.

   b. Click the <OK> button.

      The selected destination server is released from maintenance mode.

Repeat this step for each of the destination servers.

Note

- When deploying a cloning image that was collected from a Windows server, the following information is reset on each destination server. This is a result of the execution of Microsoft's System Preparation (Sysprep) tool.
  If necessary, restore the following settings to their original values after the cloning image has been deployed:
  - Desktop icons and shortcuts
  - Drive mappings
  - The [Startup and Recovery] settings accessed from the [Advanced] tab of the [System Properties] dialog
  - Virtual memory settings
  - TCP/IP-related settings
  - The "Country/region" settings in the locations defined in the "Phone and Modem Options".
  - Disk quota settings
  - Storage Provider settings
  - Microsoft Internet Explorer settings (RSS feeds subscription information, information stored by the Autocomplete function, saved passwords)
  - Microsoft Outlook Express settings (mail/directory server passwords)
  - Network card driver settings (drivers without a digital signature should be replaced by the latest updated drivers with a digital signature)
  - Access rights to the '\Documents and Settings\Default User' folder
- While a cloning image is being deployed, collection and deletion cannot be performed simultaneously on the cloning images with the same name.
- If a cloning image is deployed to a system with a larger disk capacity than the disk space required for the cloning image, any excessive disk space becomes unused disk space. This unused disk space can be used for other purposes.
- Destination servers are rebooted several times during image deployment. Make sure that deployment has completed before restarting operations and making further settings.
- The number of reboots during deployment increases when using the HBA address rename function.
- Communication errors between the admin and destination servers (resulting in an image deployment failure or an "unknown" status on the destination server) may be caused by improper use of the network parameter auto-configuration function (described in "8.6 Network Parameter Auto-Configuration for Cloning Images"). Examples of improper use are given below.
  - Auto-configuration settings were made for the Admin LAN (the network parameter auto-configuration function shouldn't be used on the Admin LAN).
  - Auto-configuration settings were made for the Public LAN using IP addresses contained within the Admin LAN subnet range.

  Log in to the destination servers on which errors happened and check for the presence of such settings in the network parameter definition file.
  If incorrect settings were made, perform the following operations to fix communication errors.

  1. Fix network settings on destination servers

     Perform the following for each of the destination servers.

     - If the source and destination servers are the same

       Restore the system images backed up before deployment.

     - If the destination server is different from the source server

       Run the "rcxadm lanctl unset" command described in "8.6.3 Clearing Settings" to reset network settings back to their original values.

If the Admin LAN IP address is not set on the source server, set it manually to restore communications between the Admin Server and the source server.

2. Re-collect the cloning image

   Correct any errors found in the network parameter definition file and re-collect the cloning image.

3. Re-deploy the cloning image to destination servers

   Re-deploy the cloning image to the destination servers for which deployment failed.

4. Delete faulty cloning images

   Delete any cloning image that failed to deploy, or that was collected with incorrect network parameters.

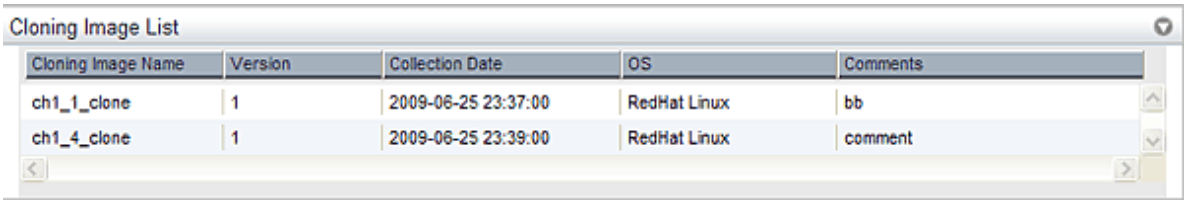
- If Windows Server 2008 activation failed during deployment, "Message Number 47233" is displayed. This message indicates that deployment of Windows Server 2008 completed but that activation failed. Refer to "Message Number 47233" in the "ServerView Resource Coordinator VE Messages" guide for details on an appropriate corrective action.
- When a 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 when ports with different speeds co-exist in the same network, or multiple image operations are run simultaneously.

8.4 Viewing Cloning Images

This section explains how to display collected cloning images.

Open the [Image List] tab in the RC console.
A list of cloning images is displayed under "Cloning Image List" in the lower part of the screen.
Use this list to manage the cloning images used by Resource Coordinator VE.

Figure 8.1 Cloning Image List area



Refer to "2.5.4 [Image List] tab" for details on the Cloning Image List.

8.5 Deleting a Cloning Image

This section explains how to delete a cloning image.

Deleting a Cloning Image

Use the following procedure to delete a cloning image:

1. Open the [Image List] tab in the RC console.

   A list of cloning image is displayed under "Cloning Image List".

2. In this list, right-click the name of the cloning image to delete and select [Delete] from the popup menu.

   The [Delete a Cloning Image] dialog is displayed.

3. In the [Delete a Cloning Image] dialog, click the <OK> button.

   The selected cloning image is deleted.

Note

While the cloning image is being deleted, no operations can be performed on other versions of the same cloning image (images that share the same image name).

8.6 Network Parameter Auto-Configuration for Cloning Images

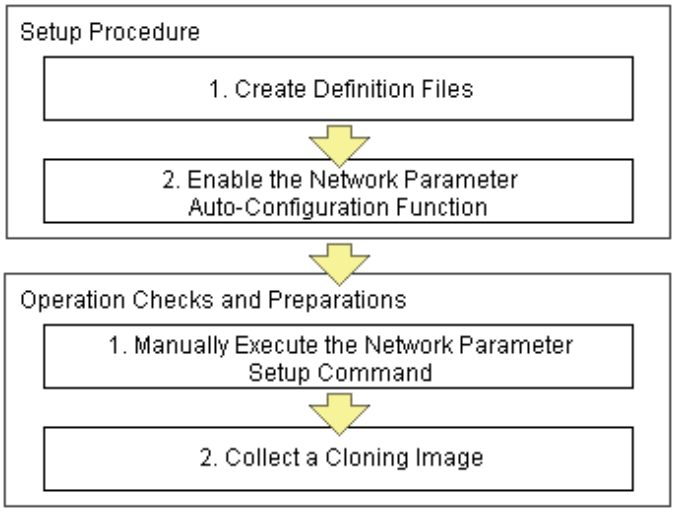
This section explains the network parameter auto-configuration function for cloning images.

Defining Public LAN network parameters for each managed server before collecting cloning images enables automatic configuration of the cloned servers' Public LAN network interfaces when later deploying those cloning images.
This speeds up the deployment of multiple servers, as Public LAN IP addresses no longer need to be manually and separately configured on each cloned server.

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

- When not using LAN redundancy
  - IP address
  - Subnet mask
- When using LAN redundancy [Linux]
  - The "NIC switching mode (Physical IP address takeover function)" of PRIMECLUSTER Global Link Services

Figure 8.2 Setup Procedure When Using the Network Parameter Auto-configuration Function



Note

[Windows/Linux]
The network parameter auto-configuration function cannot be used on the Admin LAN. If used, deployment commands may fail when deploying new servers may fail, or communication issues may occur during collection or deployment of cloning images.

[Linux]
When using LAN redundancy, cancel any network redundancy settings that were made on managed servers using PRIMECLUSTER Global Link Services before deploying new servers.
If not cancelled, deployment commands may fail when deploying new servers. Moreover, the manually set redundancy configuration will be automatically cancelled during the cloning process. This may cause communication issues during the execution of deployment commands, or the collection of cloning images.
Once the deployment of new servers has completed, redundancy network configurations (for the Admin LAN or other networks) that are not handled by the network parameter auto-configuration feature should be set up manually.

PRIMERGY Global Link Services can not be used to enable Admin LAN redundancy on servers running a SUSE Linux Enterprise Server operating system.

Setup Procedure

Use the following procedure to set up network parameters for a Public LAN:

Point

Using a specific managed server (reference server) to collect and update cloning images is recommended in order to centrally manage the network parameters definition files.

1. **Create Definition Files**

   This section explains how to setup the following definition files.

   - FJSVrcx.conf
   - ipaddr.conf

   Create those definition files under the following folder on the reference server:

   [Windows]
   Installation folder\Agent\etc\FJSVrcx.conf
   Installation folder\Agent\etc\ipaddr.conf

   [Linux]
   /etc/FJSVrcx.conf
   /etc/opt/FJSVnrmp/lan/ipaddr.conf

   Sample configuration of the definition file (FJSVrcx.conf)

   ```
   admin_LAN=192.168.1.11
   hostname=node-A
   ```

   - admin_LAN

     Enter the IP address used by the reference server on the Admin LAN.

   - hostname

     Enter the physical server name of the reference server.

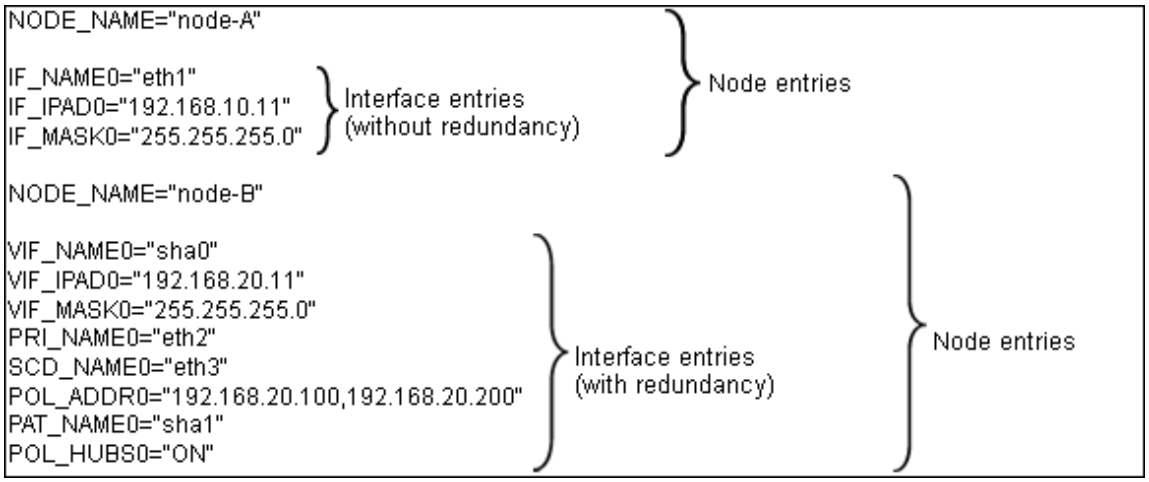
   Format of the definition file (ipaddr.conf)

   The definition file is made up of the following entries:

   - One or more node entries

- One or more interface entries (with or without redundancy) under each node entry

Figure 8.3 Sample configuration of the definition file (ipaddr.conf)



Refer to the following sample file for details of how to set the definition file (ipaddr.conf).

[Windows]
Installation folder\Agent\etc\ipaddr.sample_en

[Linux]
/etc/opt/FJSVnrmp/lan/ipaddr.sample_en

Note

Blank characters and comment lines (lines starting with a comment symbol (#) are ignored.

Each entry is identified by a keyword and must be set with an appropriate value. The expected content of each entry is explained below.

- Node Entries

  The following table explains the how to define each node entry.

  Table 8.3 Node entry settings

Setting	Keyword	Expected Value	Description
Managed server name	NODE_NAME	Physical server name	Physical server name that was set when registering the server.

  ## Note

  Specify additional entries for any node (server) that may be added in the future (one entry per server).

- Interface Entries (Without Redundancy Settings)

  The following table explains how to define each interface entry.
  Keywords for interface entries should be appended with a number comprised between 0 and 99.

  ## Note

  The number appended to each entry's keyword should start with 0 and increase incrementally.

Table 8.4 Interface entry settings (without redundancy)

Setting	Keyword	Expected Value	Description
Interface name	IF_NAME	Interface name	Specify the interface name as displayed by the operating system (*1) <Example> [Windows] Local area connection 2 [Linux] eth*X* (where *X* is an integer equal to or greater than 0)
IP address	IF_IPAD	IP address in xxx.xxx.xxx.xxx format	-
Subnet mask	IF_MASK	Subnet mask in xxx.xxx.xxx.xxx format	-

*1: As Windows allows interface names to be changed, ensure that the names defined here match those displayed in Windows.

- Interface Entries (with Redundancy Settings) [Linux]

  The following table explains how to define each interface entry.
  Keywords for interface entries should be appended with a number comprised between 0 and 99.

  This setting uses the "NIC switching mode (Physical IP address takeover function)" of the PRIMECLUSTER Global Link Services product, which requires a virtual interface set with its own IP address.

  Within a same node entry, it is possible to define interface entries both with and without redundancy settings as long as interface names differ.

Note

The number appended to each entry's keyword (including both entries with and without redundancy settings) should start with 0 and increase incrementally.

Interface entries with redundancy settings are only activated with Linux. With Windows, these interface entries will be ignored.

Table 8.5 Interface entry settings (with redundancy)

Setting	Keyword	Expected Value	Description
PRIMECLUSTER GLS virtual interface name	VIF_NAME	sha*X*	*X* is an integer between 0 and 255.
IP address specified for virtual interface	VIF_IPAD	IP address in xxx.xxx.xxx.xxx format	-
Subnet mask	VIF_MASK	Subnet mask in the format xxx.xxx.xxx.xxx	-
Name of primary interface	PRI_NAME	Interface name (eth*X*)	*X* is an integer equal to or greater than 0. This setting specifies the primary interface name when a pair of interface names exists. <Example> eth2

Setting	Keyword	Expected Value	Description
Name of secondary interface	SCD_NAME	Interface name (eth *Y*)	*Y* is an integer equal to or greater than 0. This setting specifies the secondary interface name when a pair of interface names exists. <Example> eth3
IP address of monitored destination	POL_ADDR	IP address in xxx.xxx.xxx.xxx format	Up to two IP addresses can be specified, separated by a comma. When hub-to-hub monitoring is to be performed, specify two monitored destinations. Hub-to-hub monitoring will not be performed if only one destination is specified. In this case, the value specified in POL_HUBS (whether to perform hub-to-hub monitoring) will not be referenced.
Virtual interface name for standby patrol	PAT_NAME	sha *Y*	*Y* is an integer between 0 and 255. Specify a name that is different from the virtual interface name. Do not set anything unless standby patrolling is set.
Hub-to-hub monitoring ON/OFF	POL_HUBS	ON/OFF	Specify "ON" to enable hub-to-hub monitoring, or "OFF" otherwise. This setting is valid only if two monitoring destinations are specified. If only one monitoring destination is specified, this setting is disabled (set to "OFF").

Refer to the PRIMECLUSTER Global Link Services manual for details on each setting.

2. **Enable the Network Parameter Auto-Configuration Function**

   Enable the network parameter auto-configuration function by executing the following command:
   Execute this command from a managed server.

   [Windows]

   ```
   >Installation_folder\Agent\bin\rcxadm lanctl enable <RETURN>
   ```

   [Linux]

   ```
   # /opt/FJSVrcxat/bin/rcxadm lanctl enable <RETURN>
   ```

   Refer to "5.5 rcxadm lanctl" of the "ServerView Resource Coordinator VE Command Reference" for details on this command.

8.6.1 Operation Checks and Preparations

Use the following procedure to actually apply the definition file's settings on the reference server and prepare a cloning image to be used for further server deployments. The definition file's settings applied from the definition file should be validated before image collection by checking the reference server's behavior and configuration.

1. **Execute the Network Parameter Setup Command**

   Execute the network parameter configuration command on the reference server holding the prepared definition file and check that the defined settings are applied correctly.

   ### Executing the Command

   Before collecting the cloning image, run the following command to apply the definition file and verify that the defined settings are actually reflected on the reference server. This command also activates network parameter auto-configuration for any cloning image subsequently collected. Once this command has been executed, collecting a cloning image from the reference server and deploying it to other servers will automatically perform the network configuration that was described in the definition file.

   [Windows]

   ```
   >"Installation_folder\Agent\bin\rcxadm" lanctl set <RETURN>
   ```

   [Linux]

   ```
   # /opt/FJSVrcxat/bin/rcxadm lanctl set <RETURN>
   ```

   Refer to "5.5 rcxadm lanctl" of the "ServerView Resource Coordinator VE Command Reference" for details on this command.

   ### Validating Settings (Without LAN Redundancy)

   Use a command provided by the operating system ("ipconfig" for Windows and "ifconfig" for Linux) to confirm that network interface settings (without redundancy) were correctly applied.

   ### Validating Settings (With LAN Redundancy) [Linux]

   Use the following commands to confirm that network interface settings (with redundancy) were correctly applied.

   - Using the /opt/FJSVhanet/usr/sbin/dsphanet command

     ```
     # /opt/FJSVhanet/usr/sbin/dsphanet <RETURN>
     [IPv4,Patrol]
      Name       Status   Mode CL   Device
     +----------+--------+----+----+-------------------------------------------------+
      sha0       Active    e   OFF  eth0(ON),eth1(OFF)
      sha2       Active    p   OFF  sha0(ON)
      sha1       Active    e   OFF  eth2(ON),eth3(OFF)
     [IPv6]
      Name       Status   Mode CL   Device
     +----------+--------+----+----+-------------------------------------------------+
     ```

     Items to confirm

     - The status of the virtual interface must be "Active".

     - When the standby patrol function is used ("p" mode), the status of the virtual interface set in standby patrol ("sha2" in the output example above) must be "Active".

   - Using the /opt/FJSVhanet/usr/sbin/dsppoll command

     ```
     # /opt/FJSVhanet/usr/sbin/dsppoll <RETURN>


      Polling Status    =  ON
      interval(idle)    =   5( 60)
      times             =   5
      repair_time       =   5
      link detection    =  NO
      FAILOVER Status   = YES


      Status  Name  Mode Primary Target/Secondary Target            HUB-HUB
     +------+------+----+-----------------------------------------+-------+
     ```

```
   ON    sha0    e    192.168.1.101(ON)/192.168.1.102(WAIT)        ACTIVE
   ON    sha1    e    192.168.1.101(ON)/192.168.1.102(WAIT)        ACTIVE
```

Items to confirm

- The monitoring status (Polling Status) must be "ON" (monitoring in progress).

- If one monitoring destination is specified, the status of that destination (Primary Target) must be "ON" (monitoring in progress).

- If two monitoring destinations are specified, the status of the primary destination (Primary Target) must be "ON" (monitoring in progress) and the status of the secondary destination (Secondary Target) must be "WAIT" (on standby).

- When hub-to-hub monitoring is set to ON, the status (HUB-HUB) must be "Active" (monitoring in progress).

If the interface settings have not been configured correctly, clear the settings using the rcxadm lanctl unset command, and then correct the definition file before executing the rcxadm lanctl set command again.
If anything (including user-defined checks) does not turn out as expected even though the settings were applied correctly, check the network connections and the monitoring target, and take appropriate action.

Another test is to either deactivate the port on the LAN switch blade corresponding to the network interface where communications are actually being performed, or disconnect the cable from an external port on the LAN switch blade, to check whether the spare network interface automatically takes over communication. If the standby patrol function is enabled, check the port status or check that the status of the standby network interface changes to "WAIT" after reconnecting the cable.

2. **Collect a Cloning Image**

   Collect a cloning image from the managed server checked in step 1.

   Refer to "8.2 Collecting a Cloning Image" for details on how to collect a cloning image.

   Note

   [Linux]

   When a cloning image is collected, any LAN redundancy settings on managed servers are canceled, and only network parameters for the Public LAN are set up again when collection completes. If LAN redundancy has been set up for the Admin LAN, set the LAN redundancy settings again manually.

8.6.2 Maintenance

If the network parameter auto-configuration function fails, an error message is output together with error details to the following file:

[Windows]
Installation_folder\Agent\var\log\error_lan.log

[Linux]
/var/opt/FJSVnrmp/logs/error_lan.log

Refer to the "ServerView Resource Coordinator VE Messages" guide for details on message meanings and appropriate corrective actions.
The file size limit is 32 KB and only one version is maintained. Old logs will have the extension ".old" appended to the file name and remain in the same directory.

8.6.3 Clearing Settings

This section explains how to disable the network parameter auto-configuration function and clear the settings that were applied.

Disabling the Network Parameter Auto-Configuration Function

The network parameter auto-configuration function of the cloning image being collected can be disabled by executing the following command.
After disabling it, collect a new cloning image to update the existing image.

[Windows]

```
>"Installation_folder\Agent\bin\rcxadm" lanctl disable <RETURN>
```

[Linux]

```
# /opt/FJSVrcxat/bin/rcxadm lanctl disable <RETURN>
```

Clearing Network Parameter Settings

If network settings must be added or changed due to the addition of a new server, first clear the existing settings. Clear the network parameter settings of managed server by executing the following command:

[Windows]

```
>"Installation_folder\Agent\bin\rcxadm" lanctl unset <RETURN>
```

[Linux]

```
# /opt/FJSVrcxat/bin/rcxadm lanctl unset <RETURN>
```

Refer to "5.5 rcxadm lanctl" of the "ServerView Resource Coordinator VE Command Reference" for details on this command.

Note

[Windows/Linux]
Network parameter settings for interfaces not designated in the definition file cannot be released.

[Linux]
When this command is executed, any LAN redundancy settings for managed servers are unset. If LAN redundancy settings have been made for the Admin LAN, configure these LAN redundancy settings again manually.

8.6.4 Modifying the Operating Environment

Use the following procedures to modify the operating environment.

Deploying New Managed Servers with Automated Public LAN Configuration

Use the following procedure to add new managed servers and automate their Public LAN settings using the network parameter auto-configuration function:

1. Register the newly added servers.
2. Perform the following procedure on a reference server chosen between already running servers:
   a. Clear the network parameter settings

      Cancel the network parameter settings by executing the rcxadm lanctl unset command.

   b. Edit the definition file.

      Set up a node entry in the definition file (ipaddr.conf) with the server name, interface entries and other information for the server to be added.

   c. Manually execute network parameter settings

      Execute the rcxadm lanctl set command to apply the network parameters and make sure that the resulted configuration (induced from the definition file) is correct.

   d. Collect the cloning image again.

3. Deploy the collected cloning image to the newly added servers.

Modifying Existing Public LAN Configuration

If network settings must be modified due to the addition or removal a Public LAN, or a change of IP address; perform the following on an arbitrary reference server (chosen between already running servers).

1. Execute the rcxadm lanctl unset command to clear the network parameters configuration.
2. Edit the definition file to add, modify or delete network parameters.
3. Execute the rcxadm lanctl set command to apply the network parameters and make sure that the resulted configuration (induced from the definition file) is correct.
4. Collect a new cloning image from the reference server.

Chapter 9 Server Switchover Settings

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

9.1 Overview

Server switchover is a feature that allows the user to switch over applications from a primary server to a predefined spare server when the primary server fails or is stopped for maintenance.
It can also perform Auto-Recovery, which automatically switches applications over to a spare server when a hardware failure is detected on the primary server.

Server switchover can be realized through two different methods, as described below. The switchover method used by a given server is automatically selected when configuring its recovery settings. If HBA address rename settings were already made when applying recovery settings, the HBA address rename method will be automatically selected. Otherwise, the backup and restore method will be selected.

However, each method has its own restrictions regarding the supported hardware environment. Refer to the "Note" in "1.2 Hardware Environment" of the "ServerView Resource Coordinator VE Installation Guide" for details on the hardware environments supported by each switchover method.

- Backup and restore method

  In a local boot environment, this method restores a system image backup to a spare server, which is then automatically started up. This method is used when no HBA address rename settings have been made to the primary server.
  After switchover, the operating system and its applications will resume on the spare server from the state they were in at the last system image backup. Note that only the content of the first local disk (or boot disk) as seen by the BIOS of the managed server is subject to a backup or restore operation, including all partitions (Windows drives or Linux partitions) present on the boot disk. However, since additional disks (disks used as data disks), are not subject to backup and restore, their content can not be made accessible to the spare server with a server switchover. When using more than one local disk, backup and restore of such additional data disks should be performed using external backup software.

- HBA address rename method

  In a SAN boot environment, this method sets the WWN of a spare server's HBA to the same value as that originally set on the primary server. This allows the spare server to connect to and boot from the same boot disk that was used by the primary server. This method is used when HBA address rename settings have been made on the primary server. Because this method automatically starts the spare server from the primary server's boot disk, applications can be resumed without users being aware of the hardware replacement that occurred.

The HBA address rename method is also referred to as an I/O virtualization method.

For PRIMERGY BX servers, the network configuration (VLAN IDs of adjacent LAN switch ports) of the primary server will be inherited by the spare server. This is true for all methods of server recovery.

After two servers have been switched over, a failback operation can switch them back to their original configuration using the same switchover method. Conversely, server takeover is the operation that appoints the activated spare server as the new primary server instead of switching back servers to their original configuration.

Note

- Auto-Recovery occurs when a hardware failure is detected. However, it does not occur when the operating system has stopped as a result of a software error or when the operating system is automatically rebooted.
  Refer to "9.3 Server Switchover Conditions" for details on server switchovers.
  Furthermore, since the Auto-Recovery is driven by a hardware failure, it prioritizes a fast recovery to a spare server instead of collecting an OS memory dump (which would be used to troubleshoot an OS failure). Thus, even if a memory dump was set to be collected in the event of an OS failure, server recovery will take precedence and the memory dump will not be collected.

- Server switchover can be realized by either one of the following methods: Backup and restore method or HBA address rename method.

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

- It is not possible to specify spare servers for individual VM guests. It is either possible to store VM guests on a SAN or NAS shared disk and assign a spare server to the VM host, or use the VM high-availability feature provided by the server virtualization software used.
  Refer to "A.3 Functional Differences between Products" for details on the different high-availability features available in each server virtualization product.
  For individual VM hosts, server switchover can be realized either from Resource Coordinator VE or from the high-availability feature provided with the server virtualization software used.

When using HBA address rename, a spare server can be shared between servers running physical OS's and those running VM hosts by combining the following settings.
Refer to "Figure 9.3 Sharing a spare server between physical OS's and VM guests" in "9.2 Configuration" for details.

a. Specify a VM host that doesn't run any VM guests as the spare server used to recover VM guests within the high-availability feature of the server virtualization software used.

b. Specify the physical server running the above VM host as the spare server of other physical OS's.

Once the above settings have been made, a server failure will trigger the following recovery operations. If the failed server was running a physical OS, Resource Coordinator VE will shut down the VM host on the spare server and switch the failed physical OS over to the spare server. If the failed server was a VM host running VM guests, the high-availability feature provided with the server virtualization software will recover the VM guests on the spare VM host server. Since physical OS's and VM guests share a common spare server, the two types of recovery described above can perform together: once one type of recovery occurs on a spare server, the other type of recovery can no longer be performed on that same spare server.

Information

- Server switchover based on backup and restore takes approximately 3 minutes, plus the time required to restore the system image. Image restoration time depends on different factors such as disk space and network usage, but as an estimate, a disk of 73GB will take 30 to 40 minutes (the transfer of the system images takes between 10 to 20 minutes, while system restarts and other configuration changes take another 20 minutes).
- Server switchover based on HBA address rename takes approximately 5 minutes, plus the time required to start up the original operating system and services on the spare server. If a VM host was running on the spare server, the time required to shutdown the spare server must also be included.

9.2 Configuration

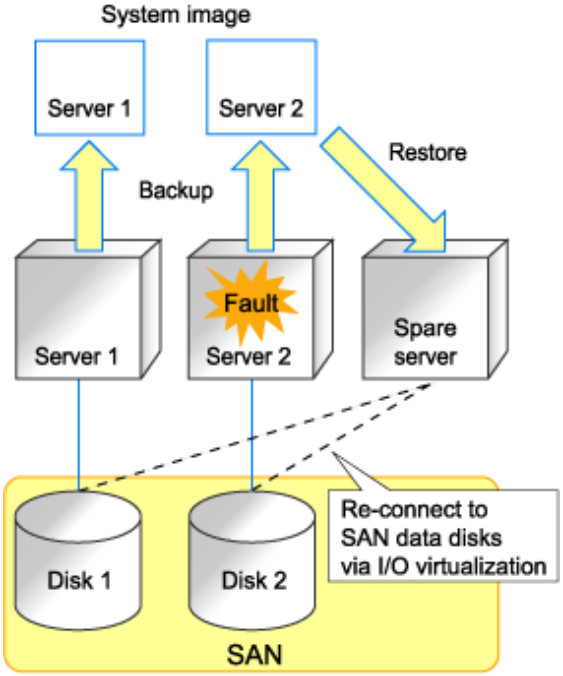
This section provides examples of switchover configurations for each different switchover method.

Each method has its own restrictions regarding the supported hardware environment. Refer to the "Note" in "1.2 Hardware Environment" of the "ServerView Resource Coordinator VE Installation Guide" for details on the hardware environments supported by each switchover method.

- Spare server configuration for local-boot servers

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

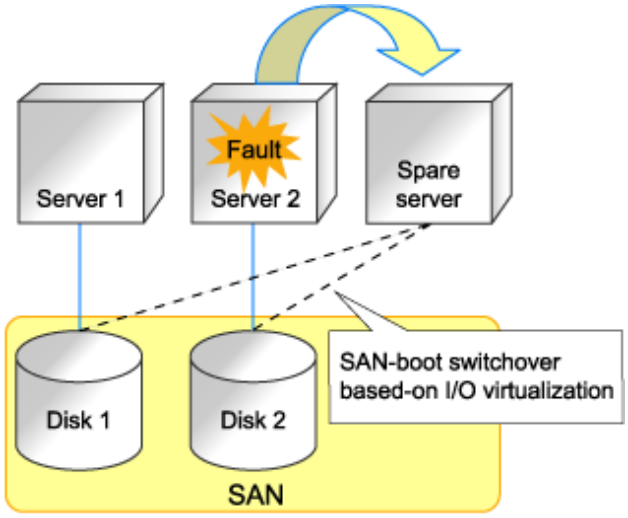
Figure 9.1 Spare server configuration for local-boot servers



- Spare server configuration for SAN-boot servers

  At least one spare server should be set aside for servers in a SAN boot environment.
  When a primary server fails, the WWN set on its HBA is inherited by the spare server, which can then access and start up from the same boot disk. One or more spare server can be shared by multiple primary servers.

Figure 9.2 Spare server configuration for SAN-boot servers

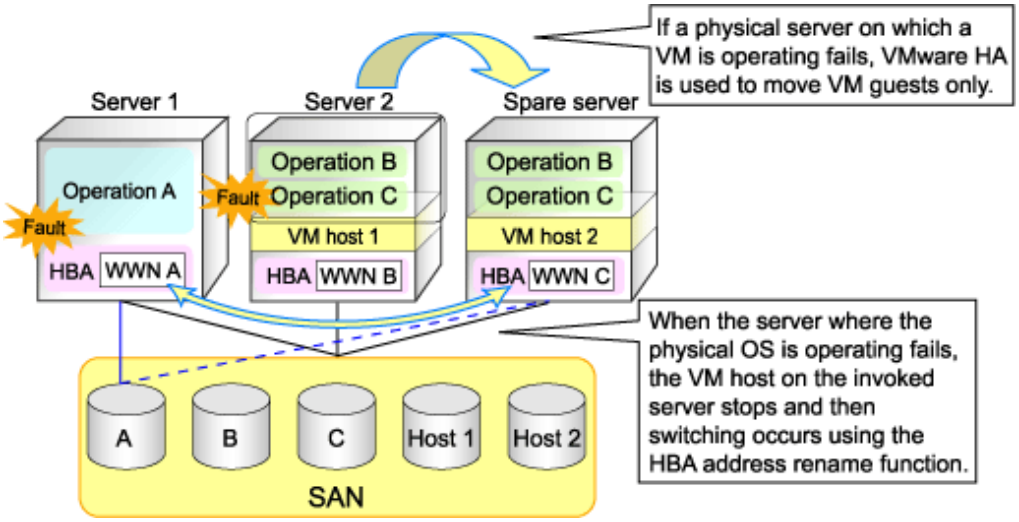


For spare server configurations based on I/O virtualization, one or more spare servers can be shared by multiple physical OS's and VM guests (using the high-availability feature provided with their server virtualization software). For details on the server virtualization products supporting this configuration, refer to "A.1 Supported Functions".

In this case, spare servers should be set up as a VM hosts booting from a SAN, so that when a physical server hosting VM guests experiences a failure, the high-availability feature provided with their virtualization software can be used to transfer the VM guests to this spare VM host.

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

Figure 9.3 Sharing a spare server between physical OS's and VM guests



Note

A spare server cannot be shared by a local boot server and a SAN boot server.

9.3 Server Switchover Conditions

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

Conditions for Spare Servers

The spare server must be identical to the active server in the ways listed below.
If these conditions are not satisfied, allocation of a spare server may not be possible, server switchover may fail, or the server may malfunction after the switchover is completed.

- Identical server model
- Identical server hardware configuration

  Add-on cards, the slots they are mounted in, and the number, size, and RAID configuration of local disks, must be the same.
  There are no other hardware conditions for the spare server (such as memory capacity, number of CPUs and CPU clock speed). However, the hardware configuration of the spare server must be capable of running the operating system and applications running on the primary server.
- Identical BIOS settings

  The same settings must be used for the primary and spare servers. Refer to "BIOS Settings for Managed Servers" in "3.5 Configuring the Server Environment" for details.
- Identical LAN and SAN access scope

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

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

If a spare server is shared by a physical OS and one or more VM guests (using the high-availability feature provided with their server virtualization software), the spare server must be configured for SAN boot using I/O virtualization.
Refer to "Figure 9.3 Sharing a spare server between physical OS's and VM guests" in "9.2 Configuration" for details.

Also, if more than two local disks are connected to a spare server in a backup/restore configuration, and if the partitioning of the disks coming after the first in the boot order is different than the first disk, a warning message may be displayed at restart, or the operating

system may not restart, causing any switchovers initiated to fail. After configuring the spare server, verify that it is operating properly by performing a switchover and failback.
If the operation fails, configure the partitions other than the first boot disk of the spare server to match the configuration of the primary server, or set up the primary server configuration so that it does not depend on any disk other than the first, using automatic service startups and re-labeling the Windows drives as necessary.

Conditions for Server Switchover

The following conditions must be satisfied for a server switchover or Auto-Recovery to succeed:

- The server configuration cannot already be switched over (the primary server must be the active server).
- The status of the spare server must be "normal", "warning" or "stop". If a VM host has been installed on the spare server(for VMware HA), its status must be either "normal" or "warning".
- If a spare server is shared by a physical OS and a VM guest (using the high-availability feature provided with its server virtualization software), there must be no VM guests on the spare server.
- If a spare server is shared by more than one active server, none of the other primary servers may be switched over to that spare server.
- If the server is in a local boot environment, its system image must have been backed up.

Conditions for Server Failback

The following conditions must be satisfied for server failback to succeed:

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

9.4 Conditions Required for Auto-Recovery

A server for which Auto-Recovery was enabled will be automatically switched over to its spare server if Resource Coordinator VE detects both a failure from the server hardware and determines that its physical OS (or VM host) has stopped. These two conditions are detailed below.

- Detecting hardware failures from servers

  A hardware failure can be detected from specific SNMP traps sent to the Admin Server from either the ServerView Agent or the server management unit. Alternatively, Resource Coordinator VE can detect a failure by periodically polling the status of each managed server.

  Detectable hardware failures

  - CPU faults
  - Memory errors
  - Fan failures
  - Temperature abnormalities

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

  A physical OS (or VM host) is seen to have abnormally stopped when the following conditions are met:

  - An abnormal server status is obtained from a server management unit, and it is not possible to communicate with either the ServerView Agent or the Resource Coordinator VE Agent.

Note

- Because the range of hardware failures that can be detected from rack-mount and tower servers is limited, Auto-Recovery can not be enabled for such servers. Instead, it is recommended to perform manual switchovers whenever necessary.
- Auto-Recovery is not triggered on servers that are in maintenance mode.
- Even if a hardware failure is detected, Auto-Recovery will not be triggered if no response is received from the target server. In such cases, shutting down (or restarting) the server will (temporally) stop the operating system, triggering an automatic switchover as the conditions for Auto-Recovery will be met. Under such conditions, automatic switchovers can be prevented by setting the server to maintenance mode before shutdown (or restart).

9.5 Status Display

Current recovery settings can be confirmed by selecting a physical OS or VM host in the resource tree of the RC console and from the spare server information displayed in the [Resource Details] tab.

The following information is displayed:

Primary server

Displays the name of the physical server that will be replaced when server switchover occurs.

Active server

Displays the name of the physical server that is currently running.

Server switchover method

Displays the specified server switchover method.

Automatic server recovery

Shows whether automatic server recovery is enabled or not.

Automatic network re-configuration

Shows whether network settings will be automatically adjusted during server switchover.

Spare server

Displays the name of the physical server that will replace the current active server when server switchover occurs.
More than one spare server will be displayed if more than one has been specified.

9.6 Server Switchover Settings

Use the following procedure to configure server switchover settings:

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

   The [Spare server settings] dialog is displayed.

2. In the [Spare server settings] dialog, set the following parameters:

   Spare server

   From the spare server list, select the checkbox in the "Selection" column of the server that is to be used as the spare server.
   One or more spare servers can be specified, including spare servers from different chassis.

   If more than one is specified, an unused spare server will be selected from the list of available candidates when a server switchover occurs.

Information

A server for which any of the operations listed below have been performed is either currently set as an active server or is in the process of being set as an active server. Therefore, it cannot be used as a spare server. However, in configurations in which a spare server is shared between physical OS's and VM guests (using the high-availability feature provided with their server virtualization software), a server running a VM host can be set as a spare server if its status is either "normal" or "warning".

- Agent registration
- I/O virtualization
- Server switchover settings

To change a server with the above settings to a spare server, the server must be deleted and then reregistered. Note that if the server is registered while it is running, an agent will be registered automatically. For this reason it should be registered while it is stopped. Refer to "6.1.2 Registering Managed Servers" for details on server registration.

To delete a spare server that has been added, refer to "9.8 Canceling Server Switchover Settings".

"Local-boot with SAN data (Backup and restore method)" checkbox

This checkbox is available only for servers on which HBA address rename settings have been made, and disabled otherwise.
Select this option for servers that boot from a local disk while using SAN storage to store data. If selected, spare server(s) will also be able to boot locally and access the same SAN storage data space after a switchover.
Do not select this option for servers that boot from a SAN disk.

"Apply network settings when the server is switched over" checkbox

Select this option to enable automatic adjustment of VLAN ID settings during a server switchover. If selected, the internal LAN switch ports connected to the spare server will be set with the same VLAN settings as those of the ports connected to the primary server.
This option is selected by default.
This feature is available only for PRIMERGY BX servers.

Note

Do not select this option if VLAN settings are to be manually adjusted from the LAN switch's management interface (either graphical or command-line interface).

"Automatically switch over when a server fault is detected" checkbox

Select this option to enable Auto-Recovery.
If selected, the primary server will be automatically switched over with a spare server upon failure. Server failures are detected when the server's status changes to "error" or "fatal" and its operating system stops functioning.
Do not select this option if primary servers are to be manually switched over.
Note that this option is selected by default.
This feature is available only for PRIMERGY BX servers.

3. Click the <OK> button.

   The server switchover settings are configured.

Point

The conditions specified in "9.3 Server Switchover Conditions" must be satisfied for a server switchover to execute correctly.
Once settings are complete, perform switchover and failback on each spare server that has been set up to verify that these operations can be executed correctly.
Refer to "Chapter 10 Server Switchover" in the "ServerView Resource Coordinator VE Operation Guide" for details on switchover and failback methods.

[VM host]
The automatic startup of VM guests after the switchover of their VM host depends on their virtual machines' startup configuration within the server virtualization software used.

Refer to the manual of each server virtualization product for details.

According to the server virtualization product used, a newly created VM guest may require some re-configuration before running a server switchover.

Refer to "A.2 Configuration Requirements" for details on such settings.

9.7 Changing Server Switchover Settings

The procedure used to change server switchover settings is the same as that described in "9.6 Server Switchover Settings".
Refer to "9.6 Server Switchover Settings" for details.

9.8 Canceling Server Switchover Settings

Use the following procedure to cancel server switchover settings.

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

   The [Spare server settings] dialog is displayed.

2. In the [Spare server settings] dialog, deselect the checkbox in the "Selection" column for the desired spare server.

3. Click the <OK> button.

   The selected spare server is no longer set as a spare server.

Chapter 10 Saving Environment Settings

This chapter explains how to save environment settings.

The configuration of a Resource Coordinator VE setup can be saved to guard against unexpected problems. Use the pre-configuration export function and the troubleshooting data collection command (rcxadm mgrctl snap) to save settings.
This troubleshooting data can be used in conjunction with the data later collected when a problem occurs for a more effective investigation, and should therefore be stored with caution.

See

- Refer to "7.3 Exporting the System Configuration File" for details on the pre-configuration function.
- Refer to "15.1 Types of Troubleshooting Data" in the "ServerView Resource Coordinator VE Operation Guide" for details on the collection of troubleshooting data.
- Refer to "5.6 rcxadm mgrctl" in the "ServerView Resource Coordinator VE Command Reference" for details on the troubleshooting data collection command.

Appendix A Server Virtualization Products

This appendix details the functions available for each server virtualization product managed in Resource Coordinator VE.

A.1 Supported Functions

Resource Coordinator VE provides the following functions for managed servers running server virtualization software.

Functions related to server virtualization software

Table A.1 Functions related to VM Hosts

Function	Server Virtualization Product		
	VMware	Hyper-V	Xen
Monitoring	Yes	Yes (*1)	Yes
Power control	Yes	Yes	Yes
Server switchover, failback, takeover (based on backup and restore) (*2)	Yes	Yes	Yes
Server switchover, failback and takeover (based on I/O virtualization)	Yes	Yes	Yes
Sharing of spare servers between physical OS's and VM guests (based on I/O virtualization) (*3)	Yes	-	-
Backup and restore (*2)	Yes	Yes	Yes
Cloning	-	-	-
VM maintenance mode settings	Yes (*4)	-	-
Launch of VM management console	Yes	Yes	-
Network map	Yes	Yes	-

*1: Must be set to allow remote management. Refer to "A.2 Configuration Requirements" for details.
*2: Not supported for VMware vSphere 4.
*3: Spare servers can only be shared between physical OS's and VM guests when using the I/O virtualization switchover method.
*4: Only available from the command-line.

Table A.2 Functions related to VM Guests

Function	Server Virtualization Product		
	VMware	Hyper-V	Xen
Monitoring (*1)	Yes (*2)	Yes	Yes (*2)
Power control (*2)	Yes	Yes	Yes (*3)
Migration between physical servers	Yes (*4)	-	Yes
Launch of VM management console	Yes	Yes	-

*1: VM guests are automatically detected after VM host registration. The result of further VM guest creation, modification, removal or migration is also automatically reflected in Resource Coordinator VE.
*2: Depending on the virtualization software used, this function may require specific settings. Refer to "A.2 Configuration Requirements" for details.
*3: An error may happen when using the high-availability function of a server virtualization software. Refer to "A.3 Functional Differences between Products" for details.
*4: A VM management software (such as VMware vCenter Server) must be registered to enable this feature.

Attributes of VM Hosts and VM Guests

Table A.3 General Area

Function	Server Virtualization Product		
	VMware	Hyper-V	Xen
Server name	Yes	Yes	Yes
Admin LAN IP address (*1)	Yes	Yes	Yes
Status	Yes	Yes	Yes
Type	Yes	Yes	Yes
OS	Yes	Yes	Yes
Physical server name (*1)	Yes	Yes	Yes

*1: Not displayed for VM guests.

Table A.4 VM Host Information Area

Function	Server Virtualization Product		
	VMware	Hyper-V	Xen
VM type	Yes	Yes	Yes
VM software name	Yes	Yes	Yes
VM software VL	Yes	Yes	Yes
Number of VM guests	Yes	Yes	Yes
VM management software	Yes	-	-
VM Guests	Yes	Yes	Yes

Table A.5 VM Guest Information Area

Function	Server Virtualization Product		
	VMware	Hyper-V	Xen
VM type	Yes	Yes	Yes
VM host name	Yes	Yes	-
VM name	Yes	Yes	Yes
VM management software	Yes	-	-

A.2 Configuration Requirements

This section describes the settings required to properly configure each different virtualization product for use with Resource Coordinator VE.

Configuration Requirements for Each Server Virtualization Product

The required configuration differs with each server virtualization product. For details on the configuration of each virtualization product refer to the manual of each product.

[VMware]
Installation of VMware Tools is required to properly display the hostnames of guest OS's and enable their remote shutdown via the power control functions of Resource Coordinator VE. Install VMware Tools after installing an operating system in a VM guest.

[Hyper-V]
Use the following procedure to enable remote management in Hyper-V.

1. Enable remote control in WMI settings.

    a. In each VM host, access the Control Panel and open the [Administrative Tools]-[Computer Management].
    The [Computer Management] dialog is displayed.
    From the [Computer Management] dialog, open [Services and Applications], right-click on [WMI Control] and select [Properties].
    The [WMI Control Properties] dialog is displayed.

    b. In the [WMI Control Properties] dialog, open the [Security] tab, select [Root]-[virtualization] and click on the <Security> button.

    The [Security for ROOT\virtualization] dialog is displayed.

    c. In the [Security for ROOT\virtualization] dialog, select the VM host's user name, select the "Allow" checkbox for "Remote Enable" and click the <OK> button.

2. Configure the Windows Firewall to enable remote WMI management.

    a. In each VM host, run the "GPedit.msc" command.

    The [Local Group Policy Editor] dialog is displayed.

    b. In the [Local Group Policy Editor] dialog, open the following folder.

    [Computer Configuration]-[Administrative Templates]-[Network]-[Network Connections]-[Windows Firewall]

    c. 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.

    d. In the displayed screen, right-click "Windows Firewall: Allow inbound remote administration exception" and select [Properties].

    The [Windows Firewall: Allow inbound remote administration exception] dialog is displayed.

    e. Select "Enabled" and click the <OK> button.

3. Configure DCOM

    a. In each VM host, run the "Dcomcnfg.exe" command.

    The [Component Services] dialog is displayed.

    b. In the [Component Services] dialog, expand [Component Services]-[Computers], right-click [My Computer] and select [Properties].

    The [My Computer Properties] dialog is displayed.

    c. In the [My Computer Properties] dialog, open the [COM Security] tab.

    d. Click the <Edit Limits> button under "Launch and Activation Permissions".

    The [Launch and Activation Permission] dialog is displayed.

    e. In the [Launch and Activation Permission] dialog, select the VM host's user name under "Groups or user names:", and select the "Allow" checkbox for "Remote Activation" and click the <OK> button.

    f. Click the <Edit Limits> button under "Access Permissions".
    The [Access Permission] dialog is displayed.

    g. In the [Access Permission] dialog, select "ANONYMOUS LOGON" under "Groups or user names:", select the "Allow" checkbox for "Remote Access" and click the <OK> button.

[Xen]
Installation of XenServer Tools is required to enable remote shutdown of VM guests via the power control functions of Resource Coordinator VE. Install VMware Tools after installing an operating system in a VM guest.

Note

[Hyper-V]
If a VM host belongs to a domain, make sure that its hostname can be properly resolved by the Admin Server (from the VM host IP address).
If host name resolution fails, perform the necessary DNS (or hosts file) settings to enable host name resolution.

[Xen]

- Make sure that each VM host is able to resolve the hostname of the Admin Server from its IP address (on the Admin LAN).
  If host name resolution fails, perform the necessary DNS (or hosts file) settings to enable host name resolution.
- When using Citrix XenServer with a resource pool, confirm that a home server is set for each VM guest.
  If no home server is set, Resource Coordinator VE is only able to recognize active VM guests. Refer to "A.3 Functional Differences between Products" for details.
- When using Citrix Essentials for XenServer with a resource pool, high-availability should be enabled for that resource pool.
  If high-availability is not enabled, and the pool master become unreachable, Resource Coordinator VE won't be able to control or get information from the VM hosts and VM guests placed in that resource pool. If VM guest statuses become out-of-date, or operations on VM hosts or VM guests fail, check the status of the pool master. If the pool master is not reachable, resolve any communication problem that may prevent the Manager from communicating with it (if necessary, change the pool master to a VM host that is always accessible from the Manager).
  Refer to the Citrix XenServer manuals for details on resource pool configurations.

Configuration Requirements for VM Guest Switchovers

Depending on the virtualization product being used, the following settings should be made to enable switchover of a newly created VM guest.

[VMware]
The VM guest's UUID must be changed.
Perform the following settings before switchover of a VM guest.

From the VM management client, add the following parameter to the guest's virtual machine configuration.

```
Name         Value
uuid.action  keep
```

Refer to the help section of the VM management client for details on how to add parameters to a virtual machine configuration.

Without this setting, a confirmation dialog is shown each time a virtual machine is started after being moved to a different VM host. Enabling this setting will prevent such confirmation dialogs from being shown, and the virtual machine will be set to always keep its UUID when moved between different servers.

[Hyper-V]
No specific configuration is required.

[Xen]
No specific configuration is required.

Integration with VM Management Consoles

[VMware]
VMware Infrastructure Client or VMware vSphere Client should be installed on the Resource Coordinator VE Admin Client.

[Hyper-V]
Hyper-V Manager should be installed on the Resource Coordinator VE Admin Client.

A.3 Functional Differences between Products

This section describes the functional differences of each server virtualization product when used with Resource Coordinator VE.

Display of VM Guest Names

The names of VM guests displayed in Resource Coordinator VE vary according to the server virtualization product used.

[VMware]
The RC console displays either a VM guest's VM name (as defined within VMware), or the hostname of its guest OS.
The guest OS hostname is displayed only after VMware Tools have been installed and the VM guest has been restarted once. The following conditions illustrate this behavior.

- VMware Tools were not installed yet: the VM name is displayed.
- VMware Tools were installed, but the VM guest wasn't restarted yet: the VM name is displayed.
- VMware Tools were installed, and the VM guest restarted: the hostname of the guest OS is displayed.

If symbols were used in the VM name, those may be shown as percents ("%") or a pair of hexadecimal characters (example: "%5c"). Such behavior is similar to that of some parts of VMware's management console.

[Hyper-V]
The RC console displays either a VM guest's VM name (as defined within Hyper-V), or the hostname of its guest OS.
The guest OS hostname is displayed after the VM guest has been started up at least once.

[Xen]
The RC console displays the Xen VM names obtained at the time of VM host registration.
Once a VM guest is registered, VM name changes made from the Xen administration client will not be reflected in the RC console.

VM Guest Shutdown [Xen]

When using Citrix XenServer in a high-availability configuration, VM guests can not be shut down if the automatic reboot option (for VM guests) is enabled.
Refer to the Citrix XenServer manual for details on this option.

High-Availability Features of Each Product

Each server virtualization product provides its own high-availability feature. For details about such features, refer to the manual of each product.

Table A.6 High-availability features of each product

Server Virtualization Product	High-availability feature
VMware	VMware HA
Hyper-V	None (*1)
Xen	HA

*1: Hyper-V doesn't provide a high-availability feature itself, but an equivalent feature is provided by a separate Microsoft product.

Sharing of spare servers between physical servers and VM guests

Resource Coordinator VE allows sharing of spare servers between physical servers and VM guests by combining its own spare server functionality with the high-availability features available in each server virtualization product. This can be done using the following procedure.

a. Choose a VM host that is not running any VM guest, and set it as a VM guest recovery server using the high-availability feature of the virtualization product used.

b. In Resource Coordinator VE, set the server chosen in a. as the spare server of other physical servers.

Refer to "A.1 Supported Functions" for details on which virtualization product can be used to share a common spare server with Resource Coordinator VE.

Backup and restore of VM hosts when VM guests are stored on their boot disk

Depending on the virtualization product used, the behavior of backup and restore functions differs whether or not VM guests are stored on the VM host's boot disk.

[VMware]
VM guests are not included in the VM host's backup and restore.

[Hyper-V]
VM guests are included in the VM host's backup and restore. However, only the data stored on the VM host's boot disk is subject to backup and restore.

[Xen]
VM guests are included in the VM host's backup and restore. However, only the data stored on the VM host's boot disk is subject to backup and restore.

Table A.7 Backup and restore behavior for each virtualization product

Disk	Partition	Backup and Restore Target		
		VMware	Hyper-V	Xen
First disk	VM host	Yes	Yes	Yes
	swap	No (*1)	-	No (*1)
	VM guest	No (*2)	Yes	Yes
	Data	Yes	Yes	Yes
Second disk	VM guest	No	No	No
	Data	No	No	No

*1: The data inside the swap partition is not backed up. On restoration, only the swap partition's configuration is restored.

*2: VMFS partitions are not subject to backup and restore.

VM Guest Migration

Migration of VM guests is supported for VMware and Xen environments. For VMware environments, VMware vCenter Server should be registered as a VM management software to enable migrations.

Depending on the server virtualization software used, the following remarks apply.

[VMware]
None.

[Xen]
With Citrix XenServer, a migrated VM guest may be temporally suspended before migration. Refer to the Citrix XenServer manual for details on the migration process and the conditions behind this behavior.

The terminology used to describe different types of migration may differ depending on each virtualization vendor. For unification purposes, Resource Coordinator VE uses the following terminology.

Table A.8 Migration Terminology

Resource Coordinator VE terminology	VMware Terminology	Description
Live migration	VMotion	Migration of an active virtual machine (without interruption)
Cold migration	Cold migration	Migration of a powered off virtual machine

VM Guest Statuses

Displayed VM guest statuses may differ depending on the configuration of its server virtualization environment.

[VMware]

- If no VM management software was registered in Resource Coordinator VE

  VM guest statuses can be either one of the following: "normal", "unknown" or "stop".

- If a VM management software was registered in Resource Coordinator VE

  VM guest statuses can be either one of the following: "normal", "warning", "error", "unknown" or "stop".

[Hyper-V]
VM guest statuses can be either one of the following: "normal", "unknown" or "stop".

[Xen]
VM guest statuses can be either one of the following: "normal", "unknown", "stop" or "error".

VM Maintenance Mode

VM maintenance mode settings are only available for VMware environments.

The terminology used to describe VM maintenance mode may differ depending on each virtualization vendor. Refer to the manual of each product for details on VM maintenance mode settings and their requirements.

Table A.9 VM Maintenance Mode Terminology

Server Virtualization Product	Vendor Terminology
VMware	Maintenance mode
Hyper-V	None
Xen	Maintenance mode

Migration Conflicts

A VM guest migration may fail if another migration was already launched from outside (*1) or Resource Coordinator VE. In such cases, select [Operation]-[Update] from the RC console menu to refresh the screen and check that the VM guest is not already being migrated.

[Xen]
With Citrix XenServer, "Home server" should be set for VM guests running on the VM hosts registered in the resource pool. Otherwise, powered off VM guests will no longer be recognized by Resource Coordinator VE. If a VM guest is no longer displayed in the RC console after a screen update, confirm that "Home server" is set.

*1: This may happen when using an automatic migration feature within the server virtualization software, or when a migration was run directly from a VM management console. Refer to the virtualization software manual for details on automatic migration features.

Notes on Resource Pool Usage [Xen]

When using Citrix Xen Server with a resource pool, the pool master should always be accessible from the Resource Coordinator VE Manager. Otherwise, the statuses of VM hosts and VM guests belonging to that resource pool will change to "unknown", and the affected VM guests will no longer be manageable from Resource Coordinator VE. In such cases, check the status of the pool master, and resolve any communication problem that may prevent the Manager from communicating with it (if necessary, change the pool master to a VM host that is always accessible from the Manager).

When using Citrix XenServer in a high-availability configuration, the pool master is automatically changed to another VM host if it becomes unreachable. As a result, VM guests can then be controlled normally from Resource Coordinator VE.

Refer to the Citrix XenServer manual for details on the resource pool and high availability configurations.

Appendix B 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 ports.
For other 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 B.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. Refer to the chassis hardware manual for details.

Table B.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.

- A LAN switch directly connected to a PRIMERGY BX 600 LAN pass-thru blade
- A LAN switch directly connected to a rack-mount or tower server

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.

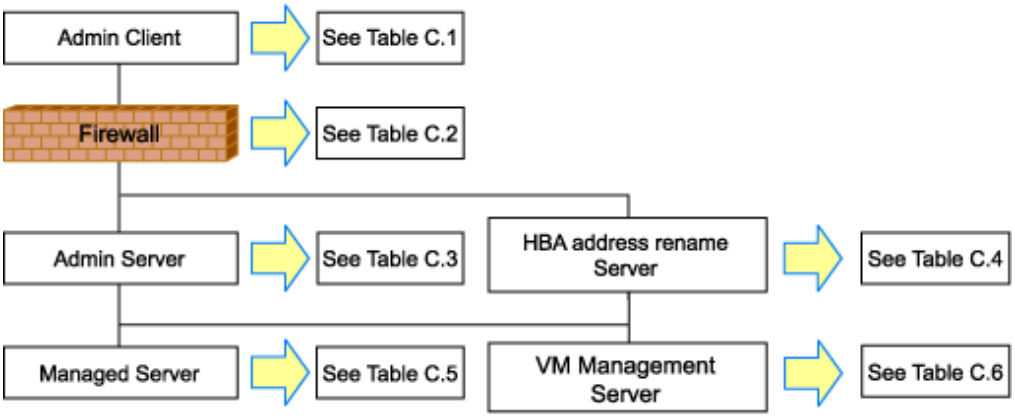
Reference	Product Name
PG-SW104	PRIMERGY BX600 Switch Blade (1Gbps) PRIMERGY BX600 Ethernet Switch 1GB 10/6(SB9)
PG-SW105	PRIMERGY BX600 Switch Blade (10Gbps) PRIMERGY BX600 Ethernet Switch 1GB 10/6+2 (SB9)
PG-SW106	Cisco Catalyst Blade Switch 3040 PRIMERGY BX600 Ethernet Switch 1GB 10/6 (Cisco CBS 3040)
PG-SW107	PRIMERGY BX600 Switch Blade (1Gbps) PRIMERGY BX600 Ethernet Switch 1GB 30/12 (SB9F)

Appendix C Port List

This appendix describes the ports used by Resource Coordinator VE.

The following figure shows the connection configuration of Resource Coordinator VE components.

Figure C.1 Connection configuration



Resource Coordinator VE ports should be set up during the system configuration of each related server.
Refer to "6.3.1.2 Changing Port Numbers" or "6.3.2.6 Changing Port Numbers" for details on how to configure the ports used by Resource Coordinator VE.
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 Coordinator VE. Communications should be allowed for each of these ports for Resource Coordinator VE to operate properly.

Table C.1 Admin Client

Function overview	Source				Destination				Protocol
	Server	Service	Port	Change	Server	Service	Port	Change	
RC console	Admin Client	-	Variable value	Not possible	Admin Server	rcxweb	23461	Possible	tcp
ServerView Operations Manager (*1)						http	3169		

Table C.2 Firewall

Function overview	Direction	Source		Destination		Protocol
		Server	Port	Server	Port	
RC console	One-way	Admin Client	Variable value	Admin Server	23461	tcp
ServerView Operations Manager (*1)					3169	

Table C.3 Admin Server

Function overview	Source				Destination				Protocol
	Server	Service	Port	Change	Server	Service	Port	Change	
RC console	Admin Client	-	Variable value	Not possible	Admin Server	rxcweb	23461	Possible	tcp
ServerView Operations Manager (*1)						http	3169		
Internal control	Admin Server	-	Variable value	-	Admin Server	nfdomain	23457	Possible	tcp

Function overview	Source				Destination				Protocol
	Server	Service	Port	Change	Server	Service	Port	Change	
		-	Variable value	-		rcxmgr	23460	Possible	tcp
		-	Variable value	-		rcxtask	23462	Possible	tcp
		-	Variable value	-		rcxmongrel 1	23463	Possible	tcp
						rcxmongrel 2	23464	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
ServerView Agent (*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 to 14989	-	Admin Server	-	14974 to 14989	-	tcp udp
Restore, cloning (deployment)	Managed server	-	Variable value	-	Admin Server	-	14974 to 14989	-	tcp udp
Monitoring server power states	Admin Server	-	-	-	Managed server	-	-	-	ICMP (*2)

Function overview	Source				Destination				Protocol
	Server	Service	Port	Change	Server	Service	Port	Change	
VMware ESX, vCenter Server (*3)	Admin Server	-	Variable value	-	Managed server, vCenter Server	-	443	Not possible	tcp
LAN switch discovery	Admin Server	-	-	-	LAN switch	-	-	-	ICMP

Table C.4 HBA Address Rename Server

Function overview	Source				Destination				Protocol
	Server	Service	Port	Change	Server	Service	Port	Change	
HBA address rename setup service	HBA address rename server	-	Variable value	Not possible	Admin Server	rcxweb	23461	Possible	tcp
		bootps	67	Not possible	Managed server	bootpc	68	Not possible	udp
		pxe	4011	Not possible					
		tftp	69	Not possible		-	Variable value	-	udp

Table C.5 Managed Server

Function overview	Source				Destination				Protocol
	Server	Service	Port	Change	Server	Service	Port	Change	
Monitoring and controlling resources	Admin Server	-	Variable value	-	Managed server (Physical OS)	nfagent	23458	Possible	tcp
					Managed server (VMware)	https	443	Not possible	tcp
					Managed server (Xen)	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
ServerView Agent (*1)	Admin Server	-	Variable value	-	Managed server	snmp	161	Not possible	tcp udp
	Managed server	-	Variable value	-	Admin Server	snmptrap	162	Not possible	udp

Function overview	Source				Destination				Protocol
	Server	Service	Port	Change	Server	Service	Port	Change	
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 (*3)	Admin Server	-	Variable value	-	Managed server	-	443	Not possible	tcp

Table C.6 VM Management Server (VMware vCenter Server)

Function overview	Source				Destination				Protocol
	Server	Service	Port	Change	Server	Service	Port	Change	
vCenter Server	Admin Server	-	Variable value	-	vCenter Server	-	443	Not possible	tcp

*1: Required for PRIMERGY servers.
*2: ICMP ECHO_REQUEST datagram.
*3: Required when running VMware ESX on managed servers.

Appendix D Format of CSV System Configuration Files

This appendix explains the format of the CSV system configuration files used by Resource Coordinator's pre-configuration function.

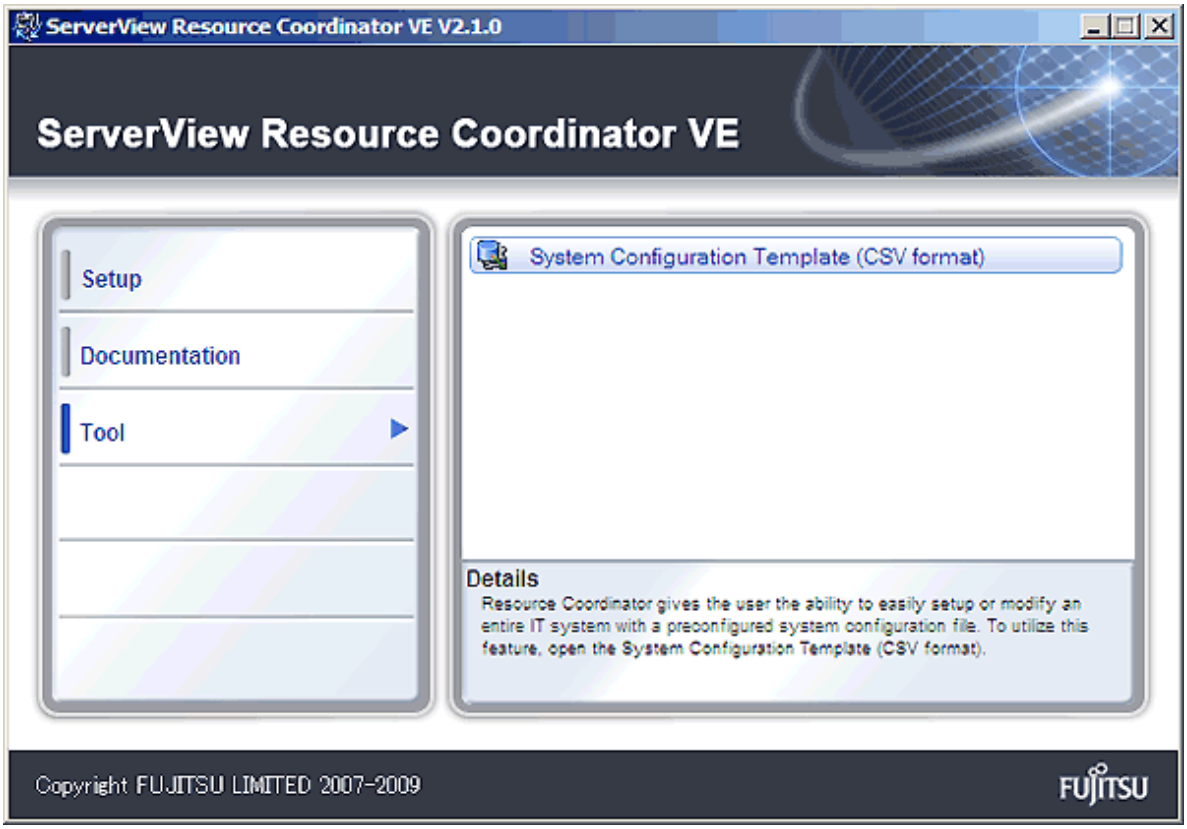
D.1 Obtaining the System Configuration File (CSV Format)

The system configuration files can be obtained as follows.

- From the Autorun dialog of the Resource Coordinator VE CD-ROM [Windows].

  Place the Resource Coordinator VE CD-ROM in a CD-ROM drive. This will display the Autorun dialog shown below. Select "Tool" and click "System Configuration Template (CSV format)". The CSV file will be opened from the associated application (such as Excel). Check the file content and save it.

  Figure D.1 Autorun Dialog



Information

If the above window does not open, execute "RcSetup.exe" from the CD-ROM drive.

- From the Resource Coordinator VE CD-ROM

  Insert the Resource Coordinator VE CD-ROM in a CD-ROM drive and copy the following file.

  [Windows]
  CD_drive:\template\ja\template.csv

  [Linux]
  CD_mount_point/template/ja/template.csv

- From the RC console

  The System Configuration Template can be obtained from a Resource Coordinator VE installation.

1. Open and log in to the RC console according to the instructions given in "5.3 RC Console".
2. Select [File]-[Download Template]-[CSV format] from the RC console.
3. Click the <Save> button in the [File download] dialog.
4. Specify the destination directory and the file name, then click the <Save> button.

D.2 File Format

The system configuration files (CSV format) used for pre-configuration are comma (",") delimited.
The format of each line is given below:

- File format definition

  The first line of the file must begin with the following:

  ```
  RCXCSV,V3.0
  ```

  Note

  Refer to the "Systemwalker Resource Coordinator Virtual server Edition V13.2 Setup Guide" for details on RCXCSV V1.0 system configuration files, and to the "Systemwalker Resource Coordinator Virtual server Edition V13.3 Setup Guide" for details on RCXCSV V2.0 system configuration files. Although RCXCSV1.0, RCXCSV V2.0 and RCXCSV3.0 have different formats, those formats are retro-compatible (the RCXCSV V3.0 and RCXCSV V2.0 formats include all the information defined by the RCXCSV V1.0 format).
  As detailed below, some sections (described in "D.3 Resource Definitions") are only available with the latest format(s).

  - RCXCSV V2.0 and later

    "LanSwitchNet", "ServerAgent", "ServerVMHost", "PowerDevice", "Memo"

  - RCXCSV V3.0

    "VMManager"

- Comments

  The following lines are assumed to be comments and are skipped:

  - Lines that begin with the symbol ("#")

    Example

    ```
    #Development environment definition
    ```

  - Lines that consist of only blank spaces (" "), tab characters or linefeed code
  - Lines that contain only commas (",")
  - Unrecognized resource definition

- Resource definitions

  Create the resource definition using the following format. Describe the same type of resource in the same section. Optional section can be omitted.

  - Resource definition format

    ```
    [Section name]
    Section header
    Operation column, Parameter [,parameter]...
    ```

- Section name

  This describes the resource type.

- Section header

  This describes the parameter type unique to the resource.

  Note

  Do not enter any comments between the section name and section header.

- Operation Column

  This describes the operation type for the resource. The following characters can be used in the operation column.

  "new": registration
  "change": change
  "-": do nothing

- Parameter

  This describes the parameter value to be set.

  Note

  The order of operation and parameter columns should follow the order defined in "Section header" under "D.3 Resource Definitions".

Allowed Characters

Refer to "D.3 Resource Definitions" for details on the characters allowed for each resource definition. Optional parameters can be omitted by using hyphens ("-").
However, hyphens ("-") are seen as valid characters for user names, passwords and SNMP communities. Note that if extra commas (",") are added to the end of a line, those will be simply ignored without errors.

Backslashes ("\") and double quotations (") will be displayed differently in the RC console from how they appear in the system configuration file.
Refer to the following table for details on such differences.

Table D.1 Differences between system configuration files' contents and display in the RC console

Content of a system configuration file (CSV)	Display in the RC console
\\	\
\n	Line break
""	"
, (*1)	,

*1: The whole value must be enclosed by double quotations (").

Example

- CSV content

```
"a\nb,\\n"
```

- Display in the RC console

```
a
b,\n
```

Order of section definition

Section order, section name and omission possible or not possible are shown below.
The section indicated as "Required" must be described in the system configuration file. Moreover, the section definition order is fixed.

Table D.2 Section order

Order	Section name	Required/Optional
1	Chassis	Optional
2	LanSwitch	Optional
3	LanSwitchNet	Optional
4	Server	Required
5	ServerNet	Optional
6	ServerWWNN (*1)	Optional
7	SpareServer (*1)	Optional
8	VMManager	Optional
9	ServerAgent (*2, *3)	Optional
10	ServerVMHost (*2, *3)	Optional
11	PowerDevice	Optional
12	Memo (*2)	Optional

*1: When loading from the system configuration template in the Excel format, the operation column information will be skipped.
*2: When loading from the system configuration template in the Excel format, the whole section will be skipped.
*3: Do not enter the information of the same physical server both in the "ServerAgent" and "ServerVMHost" section.

System backup information is automatically added to the end of the system configuration file when exporting in the CSV format. The sections after the line below contain the backup information. The backup information is skipped when loading from the system configuration template in the Excel format.

```
#Do not edit the following information, which is used to recover the manager.
```

Do not modify the backup information, as it is automatically created. Note that these sections do not have to be defined if the system configuration file is created for new system configuration.

- Importing a system configuration file in a format older than "RCXCSV,V3.0" and exporting it again will produce a file in "RCXCSV,V3.0" format.
- If a system configuration file (CSV format) is imported and then exported, the line order after export may differ from the line order before import. The following information will also be deleted:
  - Comments lines
  - Strings enclosed in brackets "( )" indicating omitted values
  - Extra commas at the end of lines (",")

D.3 Resource Definitions

This section explains the resource definition information specified system configuration files.

Chassis management information

- **Section name**

  Enter [Chassis] as the section name.

- **Section header**

  operation

  Enter the resource operation type. Enter a hyphen ("-") to skip this line.

  chassis_name

  Enter the name that will be used to identify the chassis.
  Enter a string starting with an alphabet character, including no more than 10 alphanumerical characters and hyphens ("-").

  Note

  Chassis names should be unique between all chassis (chassis names are case-insensitive).

  ip_address

  Enter the same IP address as that set on the management blade.
  Enter a string of numeric values (between 0 and 255) and periods.

  Example

  10.20.30.40

  Note

  IP addresses should be unique between all resources.

  snmp_community_name

  Enter the same SNMP community (read-write permission) as that set on the management blade.
  Enter a string of no more than 32 alphanumerical characters, underscores ("_") and hyphens ("-").

LAN switch blade management information

- **Section name**

  Enter [LanSwitch] as the section name.

- **Section header**

  operation

  Enter the resource operation type. Enter a hyphen ("-") to skip this line.

  chassis_name

  Enter the chassis name (the value of "chassis_name" in [Chassis] section).

  slot_no

  Enter the slot number where the LAN switch blade is installed. Enter numeric characters (1-4).

Note

Resource Coordinator VE doesn't check the actual slot position of a LAN switch, nor does it confirm whether a LAN switch is actually mounted or not.

switch_name

Enter the resource name that will be used to identify the LAN switch blade.
Enter a string of no more than 15 alphanumeric characters, underscores ("_") and hyphens ("-").

Note

LAN switch blade names should be unique between all switch blades (switch names are case-sensitive).

ip_address

Enter the same IP address as that set on the LAN switch blade.
Enter a string of numeric values (between 0 and 255) and periods.

Example

10.20.30.40

Note

IP addresses should be unique between all resources.

snmp_community_name

Enter the same SNMP community (read-only permission) as that set on the LAN switch blade.
Enter a string of no more than 32 alphanumerical characters, underscores ("_") and hyphens ("-").

user_name

Enter the name of the user account used to remotely log into the LAN switch blade.
Enter a string of no more than 64 alphanumerical characters, underscores ("_") and hyphens ("-"). User names are case-sensitive.

passwd

Enter the password of the above user account.
Enter a string of no more than 80 alphanumerical characters and symbols (ASCII character codes: 0x20, 0x21 or 0x23 to 0x7e) and no double-quotations ("). Passwords entered in this field are seen as plain-text passwords.

passwd_enc

Enter "plain" if the password character string is plain, and enter "encrypted" if the password is encrypted.
Enter a string of no more than 80 alphanumerical characters and symbols (ASCII character codes: 0x20, 0x21 or 0x23 to 0x7e) and no double-quotations ("). Passwords entered in this field are seen as plain-text passwords.

privileged_passwd

Enter the admin password of the above user account.
Enter a string of no more than 80 alphanumerical characters and symbols (ASCII character codes: 0x20, 0x21 or 0x23 to 0x7e) and no double-quotations ("). Passwords entered in this field are seen as plain-text passwords.

privileged_passwd_enc

Enter "plain" if the privileged password character string is plain, and enter "encrypted" if the password is encrypted.

product_name

Enter the model of the LAN switch blade. Note that if a hyphen ("-") is entered, it is treated as "BX600 GbE Switch Blade 30/12".
One of the following models can be entered.

- PY CB Eth Switch/IBP 1Gb 36/12
- PY CB Eth Switch/IBP 1Gb 36/8+2
- BX600 GbE Switch Blade 30/12
- PRIMERGY BX600 GbE Switch 16/2x10Gb
- PRIMERGY BX600 GbE Switch 16x1Gb
- Cisco Catalyst Blade Switch 3040

LAN switch blade VLAN information

- **Section name**

Enter [LanSwitchNet] as the section name.

- **Section header**

operation

Enter the resource operation type. Enter a hyphen ("-") to skip this line.

chassis_name

Enter the chassis name (the value of "chassis_name" in [Chassis] section).

slot_no

Enter the slot number where the LAN switch blade is installed. Enter numeric characters (1-4).

port_no

Enter the port number of an external LAN switch blade port. Enter numeric characters. The port number that can be specified is different depending on the model type. Refer to the manual of the LAN switch blade to be used for details.

vlan_id (optional)

Enter the VLAN ID and tag type ("/T" for tagged or "/U" for untagged) to be assigned to the specified LAN switch blade port. Enter a VLAN ID followed by tag types. Multiple VLAN IDs can be specified when delimited by semi-colons (";"). Both tagged ("/T") and untagged ("/U") VLAN IDs can be used together, but only one untagged ("/U") type is allowed.

Example

10/U
10/U;20/T;30/T
10/T;20/T

Note

If a hyphen ("-") is entered, VLAN settings will not be performed.

Server management information (Required)

- **Section name**

  Enter [Server] as the section name.

- **Section header**

  operation

  Enter the resource operation type. Enter a hyphen ("-") to skip this line.

  chassis_name

  Enter the chassis name (the value of "chassis_name" in [Chassis] section).

  Note

  This field is only required for PRIMERGY BX servers.

  slot_no

  Enter the slot number where the server blade is installed. Enter numeric characters (1-18).

  Note

  This field is only required for PRIMERGY BX servers.
  Resource Coordinator VE doesn't check the actual slot position of a LAN switch, nor does it confirm whether a LAN switch is actually mounted or not.

  server_name

  Enter the resource name that will be used to identify the server. Enter a string of no more than 15 characters long, where the first character is a letter and the remaining characters are alphanumeric characters and hyphens ("-"). If enclosed by "( )", this server will be seen as being in a switched over state, and this line will be ignored when importing the system definition file.

  Note

  Server names should be unique between all servers (server names are case-insensitive).

  ip_address

  Enter the same IP address as that set within the server's operating system.
  Enter a string of numeric values (between 0 and 255) and periods.

  Example

  10.20.30.40

  Note

  IP addresses should be unique between all resources.

  mac_address

  Enter the MAC address of the Admin LAN network interface: NIC1 (Index1).
  Enter a string delimited by hyphens ("-") or colons (":") ("xx-xx-xx-xx-xx-xx" or "xx:xx:xx:xx:xx:xx").

hbaar_mac_address

Enter the MAC address of the network interface used for the HBA address rename setup service: NIC2 (Index2).
Enter a string delimited by hyphens ("-") or colons (":") ("xx-xx-xx-xx-xx-xx" or "xx:xx:xx:xx:xx:xx").

Note

This field is only required when using the HBA address rename setup service.

snmp_community_name

Enter the name of the SNMP community (read permission) assigned to this server.
Enter a string of no more than 32 alphanumerical characters, underscores ("_") and hyphens ("-").

Note

This field is only required when using the HBA address rename setup service.

ipmi_ip_address

Enter the IP address of this server's remote management controller.
Enter a string delimited by hyphens ("-") or colons (":") ("xx-xx-xx-xx-xx-xx" or "xx:xx:xx:xx:xx:xx").

Example

10.20.30.40

Note

IP addresses should be unique between all resources.

ipmi_user_name

Enter the name of a remote management controller user account with administrative privileges.
Enter a string of no more than 16 alphanumerical characters and symbols (ASCII character codes: 0x20 to 0x7e).

Note

If the name of the current administrator account on the remote management controller is longer than 16 characters, either create a new account or rename the current account (within 16 characters).

ipmi_passwd

Enter the password of the remote management controller user account.
Enter a string of no more than 16 alphanumerical characters and symbols (ASCII character codes: 0x20 to 0x7e).
If no password is set for this account, just leave this field blank.

Note

If the password of the current administrator account on the remote management controller is longer than 16 characters, either create a new account or change its password (within 16 characters).

ipmi_ passwd_enc

Enter "plain" if the password character string is plain, and enter "encrypted" if the password is encrypted.

Server blade VLAN information

- **Section name**

  Enter [ServerNet] as the section name.

- **Section header**

  operation

  Enter the resource operation type. Enter a hyphen ("-") to skip this line.

  server_name

  Enter the server name (the value of "server_name" in [Server] section).

  nic_no

  This is the index number of the server blade's network interface. Enter numeric characters (1-12).

  vlan_id (optional)

  Enter the VLAN ID and tag type ("/T" or "/U") to be assigned to the LAN switch blade port connected to this server's network interface.
  Enter a VLAN ID followed by tag types. Multiple VLAN IDs can be specified when delimited by semi-colons (";"). Both tagged ("/T") and untagged ("/U") VLAN IDs can be used together, but only one untagged ("/U") type is allowed.

  Example

  10/U
  10/U;20/T;30/T
  10/T;20/T

  Note

  If a hyphen ("-") is entered, VLAN settings will not be performed.
  Use the following NIC indexes to specify LAN expansion cards (if any was mounted).

  - PRIMERGY BX600 servers

    Index 7 or 8

  - PRIMERGY BX900 servers

    Indexes from 5 to 12

HBA address rename information of a server

- **Section name**

  Enter [ServerWWNN] as the section name.

- **Section header**

  operation

  Enter the resource operation type. Enter a hyphen ("-") to skip this line.

  server_name

  Enter the server name (the value of "server_name" in [Server] section).

  port_count

  This is the number of ports that use HBA address rename. Enter numeric characters (1-2).

wwnn

Enter the 16-digit hexadecimal WWNN string of the physical server which uses the HBA address rename function.
Enter a hexadecimal string using alphanumerical characters, with "20 0" as the first three characters.

Note

All WWNNs should be unique between all resources (WWNNs are case-insensitive).

Server switchover management information

- **Section name**

  Enter [SpareServer] as the section name.

- **Section header**

  operation

  Enter the resource operation type. Enter a hyphen ("-") to skip this line.

  server_name

  Enter the server name (the value of "server_name" in [Server] section).

  spare_server

  Enter the physical server name of a server to be assigned as a spare server.
  Multiple spare servers can be specified using semi-colons (";") as a delimiter. To remove current spare server settings, enter "-DELETE".

  vlan_switch (optional)

  Enter a value to indicate whether or not the VLAN settings will be automatically transferred to the spare server when a server switch over occurs. Enter "ON", "OFF" or a hyphen ("-").

  auto_switch (optional)

  This value defines whether or not to trigger an automatic switchover upon detection of a server failure. Enter "ON", "OFF" or a hyphen ("-").

  boot_type

  Enter the boot type of the server. Enter either one of the following strings.

  - "SAN" (for SAN-boot)
  - "local" (for local-boot)

VM management software information

- Section name

  Enter [VMManager] as the section name.

- **Section header**

  operation

  Enter the resource operation type. Enter a hyphen ("-") to skip this line.

  name

  Enter the name used to identify this VM management software. In ServerView Resource Coordinator VE V2.1, enter "vCenterServer".

ip_address

Enter the IP address used to connect to this VM management software.
Enter a string of numeric values (between 0 and 255) and periods.
If a hyphen ("-") is entered, this VM management software will be seen as being installed on the Admin Server.

Example

10.20.30.40

product

Enter the name of this VM management software. In ServerView Resource Coordinator VE V2.1, enter "vmware-vc".

login_name

Enter the name of the user account set for this VM management software.
Use a string of no more than 84 alphanumerical characters and symbols (ASCII character codes: 0x21 to 0x7e). When specifying a domain, use the following syntax: "*domain_name**user_name*".

login_passwd

Enter the password for this VM management software.
Use a string of no more than 128 alphanumerical characters and symbols (ASCII character codes: from 0x21 to 0x7e).

passwd_enc

Enter "plain" if the password character string is plain, and enter "encrypted" if the password is encrypted.

Server Agent management information

- **Section name**

Enter [ServerAgent] as the section name.
This is required when registering multiple Agents together (for Windows or Linux managed servers).

- **Section header**

operation

Enter the resource operation type. Enter a hyphen ("-") to skip this line.
The "change" operation can not be used for this section.

server_name

Enter the server name (the value of "server_name" in [Server] section).

VM host management information

- **Section name**

Enter [ServerVMHost] as the section name.
This is required when registering multiple Agents together (for VM host managed servers).

- **Section header**

operation

Enter the resource operation type. Enter a hyphen ("-") to skip this line.

server_name

Enter the server name (the value of "server_name" in [Server] section).

vm_login_name

Enter the name of the user account used to remotely log into the VM Host.

vm_login_passwd

Enter the password of the above user account.

vm_passwd_enc

Enter "plain" if the password character string is plain, and enter "encrypted" if the password is encrypted.

Power monitoring device information

- **Section name**

Enter [PowerDevice] as the section name.

- **Section header**

operation

Enter the resource operation type. Enter a hyphen ("-") to skip this line.

device_name

Enter the name that will be used to identify the power monitoring device (UPS or PDU).
Enter a string of no more than 15 alphanumerical characters and hyphens ("-"), starting with an alphabet character.

Note

Device names should be unique between all power monitoring devices (device names are case-sensitive).

ip_address

Enter the same IP address as that set on the power monitoring device.
Enter a string of numeric values (between 0 and 255) and periods.

Example

10.20.30.40

Note

IP addresses should be unique between all resources.

snmp_community_name

Enter the same SNMP community (read-only permission) as that set on the power monitoring device.
Enter a string of no more than 32 alphanumerical characters, underscores ("_") and hyphens ("-").

voltage

Enter the voltage (V) that is being supplied to the power monitoring device. Enter a number between 10 and 999.

Note

Power consumption data is calculated using the electrical current value obtained from the power monitoring device and its specified voltage.

comment (optional)

Entry any comments for the power monitoring device.
Enter a string of no more than 128 characters.

Note

Line breaks ("\n") are counted as one character.

Memo

- **Section name**

  Enter [Memo] as the section name.
  This is required when registering the labels and contact information (displayed in BladeViewer) using the pre-configuration function.

- **Section header**

  operation

  Enter the resource operation type. Enter a hyphen ("-") to skip this line.

  resource_type

  Enter the type of the resource for which to set this memo. Enter one of the following.

  - "physical_server" (if the physical server including the VM Host is specified)
  - "vm_guest" (if the VM Guest is specified)
  - "common" (if the contact information is specified)

  resource_name

  Enter the name of the resource name for which to set this memo. Enter one of the following.

  - Enter the server name (the value of "server_name" in [ServerAgent] section) or the VM Host name (the value of "server_name" in [ServerVMHost] section) if the value of "resource type" is "physical_server".
  - Enter only the registered VM Guest name if the value of "resource_type" is "vm_guest".
  - Do not enter anything if the value of "resource_type" is "common".

  label (optional)

  This label is used to identify the applications running on each server. Enter a string that contains up to 32 characters. Note that if the value of "resource_type" is "common", do not enter anything.

  Note

  Line breaks ("\n") are not available.

  comment (optional)

  This is a comment that can be set as an option for each application. If the "resource_type" is "common", this can be used for the contact details, maintenance or anything else.
  Enter a string that contains up to 256 characters.

D.4 Examples of CSV format

This section shows an example of the system configuration file in the CSV format.

```
RCXCSV V3.0

# ServerView Resource Coordinator VE V2.1
# System configuration file
# Author Fujitsu
```

[Chassis]
operation chassis_name ip_address snmp_community_name
- chassis01 192.168.3.150 public

[LanSwitch]
operation chassis_name slot_no switch_name ip_address snmp_community_name user_name passwd passwd_enc privileged_passwd privileged_passwd_enc product_name
- chassis01 1 switch-01 192.168.3.161 public admin admin plain admin plain BX600 GbE Switch Blade 30/12
- chassis01 2 switch-02 192.168.3.162 public admin admin plain admin plain BX600 GbE Switch Blade 30/12

[LanSwitchNet]
operation chassis_name slot_no port_no vlan_id
- chassis01 1 31 1/U;10/T;20/T
- chassis01 1 32 1/U
- chassis01 1 33 1/U
- chassis01 1 34 1/U
- chassis01 1 35 1/U
- chassis01 1 36 1/U
- chassis01 1 37 1/U
- chassis01 1 38 1/U
- chassis01 1 39 1/U
- chassis01 1 40 1/U
- chassis01 1 41 1/U
- chassis01 1 42 1/U
- chassis01 1 43 1/U
- chassis01 1 44 1/U
- chassis01 2 31 1/U;10/T;20/T
- chassis01 2 32 1/U
- chassis01 2 33 1/U
- chassis01 2 34 1/U
- chassis01 2 35 1/U
- chassis01 2 36 1/U
- chassis01 2 37 1/U
- chassis01 2 38 1/U
- chassis01 2 39 1/U
- chassis01 2 40 1/U
- chassis01 2 41 1/U
- chassis01 2 42 1/U
- chassis01 2 43 1/U
- chassis01 2 44 1/U

[Server]
operation chassis_name slot_no server_name ip_address mac_address hbaar_mac_address snmp_community_name ipmi_ip_address ipmi_user_name ipmi_passwd ipmi_passwd_enc
- chassis01 1 blade001 192.168.3.151
- chassis01 7 blade002 192.168.3.157
- chassis01 9 blade003 192.168.3.159
- rackmount001 192.168.3.200 00:E5:35:0C:34:ABpublic 192.168.3.199 admin admin plain
- rackmount002 192.168.3.202 00:E5:35:0C:34:ACpublic 192.168.3.201 admin admin plain

[ServerNet]
operation server_name nic_no vlan_id
- blade001 1 1/U;10/T;20/T
- blade001 3 1/U
- blade001 5 1/U
- blade002 1 1/U;10/T;20/T
- blade002 3 1/U

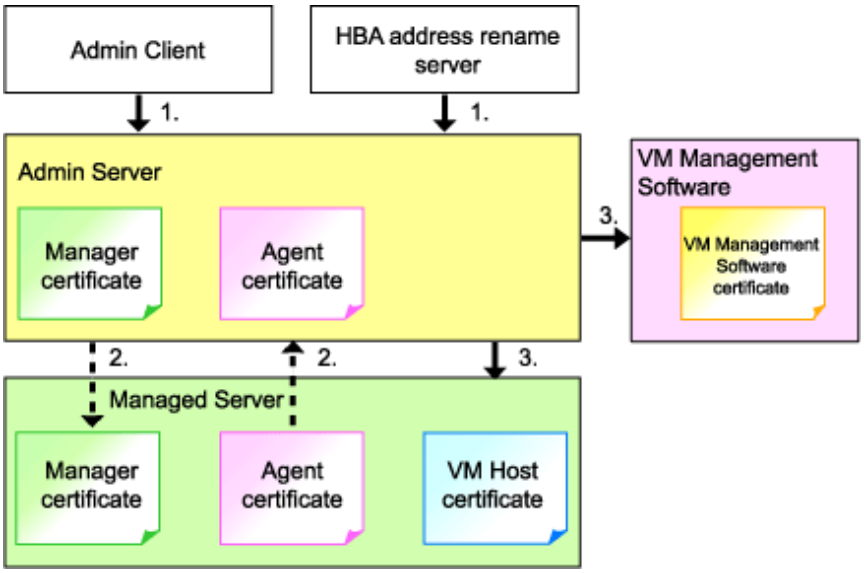
```
- blade002 5 1/U
- blade003 1 1/U
- blade003 3 1/U
- blade003 5 1/U
- blade001 2 1/U
- blade001 4 1/U
- blade001 6 1/U
- blade002 2 1/U
- blade002 4 1/U
- blade002 6 1/U
- blade003 2 1/U
- blade003 4 1/U
- blade003 6 1/U

[ServerWWNN]
operation server_name port_count wwnn
- blade001 1 20 00 00 17 42 51 00 01
- blade002 1 20 00 00 17 42 51 00 02

[SpareServer]
operation server_name spare_server vlan_switch auto_switch boot_type
- blade001 blade003 ON ON local

[VMManager]
operation name ip_address product login_name login_passwd passwd_enc
- vCenterServer 127.0.0.1 vmware-vc Administrator admin plain

[ServerAgent]
operation server_name
- blade001
- rackmount001
- rackmount002

[ServerVMHost]
operation server_name vm_login_name vm_login_passwd vm_passwd_enc
- blade002 admin admin plain

[PowerDevice]
operation device_name ip_address snmp_community_name voltage comment
- ups1 192.168.3.196 public 100 SmartUPS
- ups2 192.168.3.197 public 100 SmartUPS

[Memo]
operation resource_type resource_name label comment
- common TEL:0000-0000

#Backup configuration
#Do not edit the following information which is used to recover the manager.

[Parameter]
operation type name value
- MonitorParameter lifespan_daily 12
- MonitorParameter polling_interval 5
- MonitorParameter lifespan_monthly 60
- MonitorParameter lifespan_finest 1
- MonitorParameter power_monitored FALSE
- MonitorParameter lifespan_hourly 1
- MonitorParameter lifespan_annual 60
```

Appendix E HTTPS Communications

This appendix details the HTTPS communication protocol used by Resource Coordinator VE and its security features.

Resource Coordinator VE uses HTTPS communication for the three cases shown in the figure below.
Certificates are used for mutual authentication and for encrypting communication data.

Figure E.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 Coordinator VE (Manager or Agent) is first installed. Certificates of other communication targets are stored at different timings, as described below (refer to "Certificate Creation Timings"). 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 those renewed certificates differ from those stored on the Agent side (on managed servers), Agents are no longer 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. Refer to "3.1 Manager Uninstallation" and "2.1 Manager Installation" in the "ServerView Resource Coordinator VE Installation Guide" for details on how to backup and restore Agent certificates on the Admin Server.

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 VM host or VM management software. Those certificates are used to encrypt communications.

Certificate Creation Timings

Between the Admin Client and Admin Server, or between the HBA Address Rename Server and the Admin Server

Certificates are automatically obtained when establishing HTTPS connections. 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 when establishing HTTPS connections. They are not stored on the Admin Server.

Types of Certificates

Resource Coordinator VE 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 Coordinator VE 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

  Opening a browser and connecting to the Admin Server for the first time will produce a warning dialog regarding the security certificate received from the Admin Server.

- Address bar and Phishing Filter warning in Internet Explorer 7 or 8

  The background color of the address bar will become red and the words "Certificate error" will be displayed on its right side.
  The Phishing Filter will also show a warning on the status bar.

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. 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.
When using other servers as Admin Clients, use the following procedure to install the Admin Server's certificate on each client.

1. Create a certificate

   a. Open the command prompt on the Admin Server.

   b. Execute the following command to move to the installation folder.

      [Windows]

      ```
      >cd "Installation folder\Manager\sys\apache\conf" <RETURN>
      ```

      [Linux]

      ```
      # cd /etc/opt/FJSVrcvmr/sys/apache/conf <RETURN>
      ```

c. After backing up the current certificate, execute the certificate creation command bundled with Resource Coordinator VE (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 Coordinator VE. 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:\Program Files\Resource Coordinator VE" folder, and generating a certificate valid for 15 years (or 5479 days, using the -days 5479 option).

[Windows]

```
>cd "C:\Program Files\Resource Coordinator VE\Manager\sys\apache\conf" <RETURN>
>..\..\..\bin\rcxadm mgrctl stop <RETURN>
>copy ssl.crt\server.crt ssl.crt\server.crt.org <RETURN>
>copy ssl.key\server.key ssl.key\server.key.org <RETURN>
>..\bin\openssl.exe req -new -x509 -nodes -out ssl.crt\server.crt -keyout ssl.key\server.key -days 5479 -config
openssl.cnf <RETURN>
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.................++++++
.....................++++++
writing new private key to 'ssl.key\server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []: <RETURN>
State or Province Name (full name) []: <RETURN>
Locality Name (eg, city) [Kawasaki]: <RETURN>
Organization Name (eg, company) []: <RETURN>
Organizational Unit Name (eg, section) []: <RETURN>
Common Name (eg, YOUR name) [localhost]: IP address or hostname (*1) <RETURN>
Email Address []: <RETURN>

>..\..\..\bin\rcxadm.exe mgrctl start <RETURN>
```

[Linux]

```
# cd /etc/opt/FJSVrcvmr/sys/apache/conf <RETURN>
# /opt/FJSVrcvmr/bin/rcxadm mgrctl 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 ../ssl/openssl.cnf <RETURN>
Generating a 1024 bit RSA private key
.................++++++
.....................++++++
writing new private key to 'ssl.key/server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
```

What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) []: <RETURN>
State or Province Name (full name) []: <RETURN>
Locality Name (eg, city) [Kawasaki]: <RETURN>
Organization Name (eg, company) []: <RETURN>
Organizational Unit Name (eg, section) []: <RETURN>
Common Name (eg, YOUR name) [localhost]: *IP address or hostname* (*1) <RETURN>
Email Address []: <RETURN>

/opt/FJSVrcvmr/bin/rcxadm mgrctl start <RETURN>

*1: Enter the IP address to be entered in the Web browser or the host name (FQDN).

Example

IP address: 192.168.1.1
Host name: myhost.company.com

2. Add the certificate to the Web browser.

   Open the Resource Coordinator VE login screen following the instructions given in "5.3 RC Console".
   When opening the RC 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.

      - In Internet Explorer 6

        Double-click the key mark displayed in the status bar.

      - In Internet Explorer 7 or 8

        Open the "Certificate is invalid dialog" by clicking the "Certificate error" displayed in the address bar. This will open a "Certificate is not trusted" or " Certificate is invalid" message.
        Click the "Display 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 the <Install Certificate...> button.

   d. The [Certificate Import Wizard] dialog is displayed.

      Click the <Next>> button.

   e. Select "Place all certificates in the following store" and click the <Browse...> button.

   f. The [Select Certificate Store] dialog is displayed.

      Select the "Trusted Root Certification Authorities" and click the <OK> button.

   g. Click the <Next>> button.

   h. Check that "Trusted Root Certification Authorities" is selected and click the <Finish> button.

   i. Confirm the content displayed in the "Security Warning" dialog and click the "Yes" button.

   j. 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.

Appendix F Maintenance Mode

This appendix explains the maintenance mode available in Resource Coordinator VE and how to use it.

Maintenance mode is used during hardware maintenance of managed servers. It is also used during the installation and maintenance of physical OS's and VM hosts. Maintenance mode avoids unwanted error notifications and disables execution of Auto-Recovery upon server failure.

The following operations can be performed on a server in maintenance mode:

- Maintenance LED

  Maintenance LEDs can be turned on or off.

- Backup and restore

  System images can be backed up and restored.

- Cloning

  Cloning images can be collected and distributed.

Use the following procedures to set and release maintenance mode:

- Setting maintenance mode

  In the RC console resource tree, right-click the server (or the physical OS or VM host on the server) to put into maintenance mode, and select [Maintenance Mode]-[Set] from the popup menu.

- Releasing maintenance mode

  In the RC console resource tree, right-click the server (or the physical OS or VM host on the server) to put into active mode, and select [Maintenance Mode]-[Release] from the popup menu.

Appendix G Notes on Installation

Keep the following notes in mind when setting up a Resource Coordinator VE environment:

- The maximum of managed servers can be registered in Resource Coordinator VE is limited, and depends on the Resource Coordinator VE license bought.
  Refer to license documentation for details on the limit of managed servers.

  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.

- A specific license is required to enable a cluster configuration for the Admin Server.

  Refer to "Appendix B Manager Cluster Operation Settings and Deletion" in the "ServerView Resource Coordinator VE Installation Guide" for details.

- Clustering software can be used on managed servers.

  Note, however, that Resource Coordinator VE does not support server switchover or server replacement based on backup and restore for cluster-enabled servers.

- Use of the Windows Server 2008 BitLocker drive encryption function (Windows BitLocker Drive Encryption) is not supported.

  If the admin or managed servers are running under Windows Server 2008, do not encrypt the system disk using the BitLocker drive encryption function.

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 networks devices.

admin server

A server used to operate the manager software of Resource Coordinator VE.

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 Coordinator VE that operates on managed servers.

Auto-Recovery

A function which continues operations by automatically switching over the system image of a failed server to a spare server and restarting it in the event of server failure.
This function can be used when managed servers are in a local boot configuration or a SAN boot configuration.
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 using a SAN boot configuration, the system is recovered by a spare server inheriting the system image of the failed server over the SAN.
Also, when a VLAN is set for the public LAN of a managed server, the VLAN settings of adjacent LAN switches are automatically switched to those of the spare server.

BACS (Broadcom Advanced Control Suite)

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

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.

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.

CA (Channel Adapter)

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

chassis

A chassis used to house server blades.
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 Coordinator VE automatically changes server-specific information to that of the target server.

environmental data

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

FC switch (Fibre Channel Switch)

A switch that connects Fibre Channel interfaces and storage devices.

fibre channel switch blade

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

GLS (Global Link Services)

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

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.

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.

image file

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

I/O virtualization option

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

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.

iRMC (integrated Remote Management Controller)

The name of Fujitsu's Remote Management Controller.

LAN switch blade

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

link aggregation

Function used to multiplex multiple ports and use them as a single virtual port.
With this function, if one of the multiplexed ports fails its load can be divided among the other ports, and the overall redundancy of ports improved.

logical volume

A logical disk that has been divided into multiple partitions.

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.

manager

The section (program) of Resource Coordinator VE that operates on admin servers.
It manages and controls resources registered with Resource Coordinator VE.

NAS (Network Attached Storage)

A collective term for storage that is directly connected to a LAN.

network map

A GUI function for graphically displaying the connection relationships of the servers and LAN switches that compose a network.

network view

A window that displays the connection relationships and status of the wiring of a network map.

NFS (Network File System)

A system that enables the sharing of files over a network in Linux environments.

NIC (Network Interface Card)

An interface used to connect a server to a network.

OS

The OS used by an operating server (a physical OS or VM guest).

PDU (Power Distribution Unit)

A device for distributing power (such as a power strip).
Resource Coordinator VE uses PDUs with current value display functions as Power monitoring devices.

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.

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 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 Coordinator VE 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 Coordinator VE can collect power consumption data.

pre-configuration

Performing environment configuration for Resource Coordinator VE on another separate system.

primary server

The physical server that is switched from when performing server switchover.

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.

RC console

The GUI that enables operation of all functions of Resource Coordinator VE.

Remote Management Controller

A unit used for managing servers.
Used for gathering server data, failure notification, power control, etc.
An iRMC2 in the case of Fujitsu PRIMERGY servers, an iLO2 (integrated Lights-Out) in the case of HP servers, and a BMC (Baseboard Management Controller) in the case of Dell/IBM servers.

resource

Collective term or concept that refers to the physical resources (hardware) and logical resources (software) from which a system is composed.

Resource Pool

On Citrix XenServer, it indicates a group of VM hosts.
For details, refer to the Citrix XenServer manual.

resource tree

A tree that displays the relationships between the hardware of a server and the OS operating on it using hierarchies.

SAN (Storage Area Network)

A specialized network for connecting servers and storage.

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.

ServerView Operations Manager

Software that monitors a server's (PRIMERGY) hardware state, and notifies of errors by way of the network.

ServerView RAID

One of the RAID management tools for PRIMERGY.

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.

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.

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 unit

Used to indicate the entire secondary storage as one product.

switchover state

The state in which switchover has been performed on a managed server, but neither failback nor continuation have been performed.

system disk

The disk on which the programs (such as 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.

tower server

A stand-alone server with a vertical chassis.

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 Coordinator VE 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.

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 Coordinator VE it is used to indicate HBA address rename.

Virtual Machine

A virtual computer that operates on a VM host.

virtual server

A virtual server that is operated on a VM host using a virtual machine.

virtual switch

A function provided by server virtualization software to manage networks of VM guests as virtual LAN switches.
The relationships between the virtual NICs of VM guests and the NICs of the physical servers used to operate VM hosts can be managed using operations similar to those of the wiring of normal LAN switches.

VLAN (Virtual LAN)

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

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

VM host

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

VM maintenance mode

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

VM management software

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

VMware

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

Web browser

A software application that is used to view Web pages.

WWN (World Wide Name)

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

WWNN (World Wide Node Name)

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

WWPN (World Wide Port Name)

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

WWPN zoning

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

Xen

A type of server virtualization software.

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.