

ServerView Resource Coordinator VE



Operation Guide

Windows/Linux

J2X1-7460-02ENZ0(00)
November 2009

Preface

Purpose

This manual explains how to operate ServerView Resource Coordinator VE (hereinafter Resource Coordinator VE).

Target Readers

This manual is written for people who will operate Resource Coordinator VE.

An overview of the functions provided in Resource Coordinator VE can be found in "Chapter 1 Overview" of the "ServerView Resource Coordinator VE Setup Guide". It is strongly recommended that you read through this chapter before using this manual.

Resource Coordinator VE allows administrators to choose between two different views according to their level of authority or the kinds of operations that need to be performed. For details, refer to "[Chapter 2 Switching between Views](#)".

Organization

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

Title	Description
Chapter 1 Starting and Stopping	Explains how to start and stop Resource Coordinator VE.
Chapter 2 Switching between Views	Provides an overview of the views available in Resource Coordinator VE (RC console and BladeViewer) and explains how to switch between them.
Chapter 3 BladeViewer	Provides an overview of BladeViewer and describes its features.
Chapter 4 User Accounts	Describes the user accounts used in Resource Coordinator VE.
Chapter 5 Monitoring	Explains how to monitor the configuration and status of managed resources.
Chapter 6 Power Control	Explains how to remotely control the power state of managed resources.
Chapter 7 Control of VM Environments	Describes the features specific to VM guests and VM hosts.
Chapter 8 Backup and Restore	Explains how to use the backup and restore functions provided in Resource Coordinator VE.
Chapter 9 Hardware Maintenance	Explains how to replace hardware and perform maintenance tasks using Resource Coordinator VE.
Chapter 10 Server Switchover	Explains how to use the server switchover function.
Chapter 11 Maintaining Software with Cloning [Windows/Linux]	Explains how to perform software maintenance using the cloning function.
Chapter 12 Network Map	Provides an overview of the Network Map and describes its features.
Chapter 13 Power Consumption Data	Describes the power consumption data collected from power monitoring targets and explains how to export it.
Chapter 14 Customizing the RC Console	Explains how to customize the RC console.
Chapter 15 Troubleshooting	Explains how to solve problems and gather troubleshooting data for a technical investigation.
Appendix A Notes on Operating ServerView Resource Coordinator VE	Gives important reminders for the operation of Resource Coordinator VE.
Appendix B Admin Server Backup and Restore	Explains how to backup and restore the Admin Server.
Appendix C Event Handling Function	Explains how to connect events from monitored devices with external applications.
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
[Solaris]	Sections related to Solaris
[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/VMware]	Sections related to Linux and VMware
[Linux/Xen]	Sections related to Linux and Xen
[Linux/Solaris/VMware]	Sections related to Linux, Solaris, and VMware
[Linux/VMware/Xen]	Sections related to Linux, VMware, and Xen
[Linux/Solaris/VMware/Xen]	Sections related to Linux, Solaris, 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
Explains Resource Coordinator VE and its functions, as well as the settings and operations necessary for setup.

- ServerView Resource Coordinator VE Operation Guide (This manual)
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.

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

Abbreviation	Products
	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) 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
Solaris	Solaris(TM) 10 Operating System
VMware	VMware(R) Infrastructure 3 VMware vSphere(TM) 4
Xen	Citrix XenServer(TM) 5.5 Citrix Essentials(TM) for XenServer 5.5, Enterprise Edition Red Hat(R) Enterprise Linux(R) 5.3 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64) Linux Virtual Machine Function
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
VIOM	ServerView Virtual-IO Manager
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, Windows 7, Excel, and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.
- Openboot is a registered trademark of Japanese Sun Microsystems, Inc.

- 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.
- SPARC Enterprise is a trademark or registered trademark of SPARC International, Inc. in the United States and other countries and used under license.
- Sun, Sun Microsystems, the Sun logo, all trademarks and logos related to Solaris, are trademarks or registered trademarks of Sun Microsystems, Inc. or its subsidiaries 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.

November 2009, Second Edition

All Rights Reserved, Copyright(C) FUJITSU LIMITED 2007-2009

Contents

Chapter 1 Starting and Stopping.....	1
Chapter 2 Switching between Views.....	2
Chapter 3 BladeViewer.....	3
3.1 Overview.....	3
3.2 Login and Logout.....	4
3.3 BladeViewer Layout.....	5
3.4 Resource Status Monitoring.....	6
3.4.1 Status Panel.....	6
3.4.2 Chassis Panel.....	7
3.4.3 Blade Panel.....	8
3.4.3.1 Resource List.....	8
3.4.3.2 VM Guest List.....	11
3.4.4 Resource Details.....	13
3.5 Power Control.....	13
3.5.1 Server Blade.....	13
3.5.2 VM Guest.....	15
3.6 Status Panel Operations.....	16
3.6.1 Listing and Editing of Labels and Comments.....	17
3.6.2 Editing Contacts.....	18
3.6.3 Change of Password.....	18
Chapter 4 User Accounts.....	19
4.1 Overview.....	19
4.2 Managing User Accounts.....	19
Chapter 5 Monitoring.....	21
5.1 Overview.....	21
5.2 Resource Status.....	22
5.3 Addressing Resource Failures.....	24
Chapter 6 Power Control.....	26
6.1 Server Power Control.....	26
6.2 Chassis Power Control.....	27
Chapter 7 Control of VM Environments.....	28
7.1 Migration of VM Guests between Servers.....	28
7.2 VM Maintenance Mode of VM Hosts.....	29
Chapter 8 Backup and Restore.....	30
8.1 Overview.....	30
8.2 Backing Up System Images.....	31
8.3 Restoring System Images.....	33
8.4 Viewing System Images.....	34
8.5 Deleting a System Image.....	34
Chapter 9 Hardware Maintenance.....	36
9.1 Overview.....	36
9.2 Maintenance LEDs.....	37
9.3 Re-configuring Hardware Properties.....	38
9.4 Replacing Servers.....	39
9.5 Replacing Server Components.....	43
9.6 Replacing Non-server Hardware.....	44
Chapter 10 Server Switchover.....	46
10.1 Overview.....	46

10.2 Switchover.....	46
10.3 Post-Switchover Operations.....	47
Chapter 11 Maintaining Software with Cloning [Windows/Linux].....	50
11.1 Overview.....	50
11.2 Software Maintenance Procedure.....	50
Chapter 12 Network Map.....	52
12.1 Overview.....	52
12.2 Preparations.....	53
12.3 Screen Layout.....	53
12.3.1 Network Map Layout.....	54
12.3.2 Map Types.....	54
12.4 Resource Icons.....	55
12.4.1 Resource Statuses.....	55
12.4.2 VLAN Display.....	59
12.4.3 Other Icons.....	60
12.5 Network Links.....	60
12.5.1 Link Display.....	60
12.5.2 Link Statuses.....	61
12.5.3 Aggregate Display of Network Links.....	61
12.6 Display Filters.....	62
Chapter 13 Power Consumption Data.....	64
13.1 Overview.....	64
13.2 Exporting Power Consumption Data.....	64
13.3 Power Consumption Data File (CSV Format).....	66
Chapter 14 Customizing the RC Console.....	68
14.1 Event Log.....	68
14.2 Dialogs.....	68
14.3 External Software.....	68
Chapter 15 Troubleshooting.....	70
15.1 Types of Troubleshooting Data.....	70
15.1.1 Collecting Initial Troubleshooting Data.....	70
15.1.2 Collecting Exhaustive Troubleshooting Data.....	73
15.2 OS Startup Issues (with I/O Virtualization).....	74
15.3 "unknown" Server Status.....	75
15.4 Image Operation Issues [Windows/Linux][Hyper-V].....	77
15.5 Public LAN Communication Issues.....	78
15.6 Multipath Configuration Issues.....	78
15.7 Cloning Issues Following Manager Re-installation.....	78
15.8 Server Switchover and Failback Issues.....	81
15.9 HBA Address Rename is Set by Mistake.....	82
15.10 Boot Issues (Boot Order Related).....	82
15.11 Boot Issues (Endless Reboot Cycle).....	82
Appendix A Notes on Operating ServerView Resource Coordinator VE.....	83
Appendix B Admin Server Backup and Restore.....	84
B.1 Overview.....	84
B.2 Backup.....	84
B.3 Restore.....	86
Appendix C Event Handling Function.....	89
Glossary.....	93

Chapter 1 Starting and Stopping

This chapter explains how to start and stop Resource Coordinator VE.

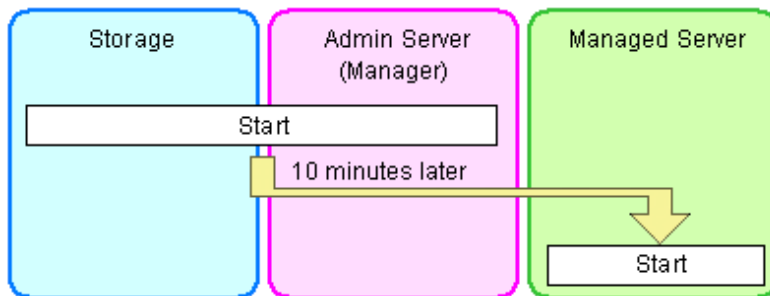
To use Resource Coordinator VE, first open the RC console or BladeViewer from an Admin Client. Refer to "5.3 RC Console" of the "ServerView Resource Coordinator VE Setup Guide" for details on opening and closing the RC console. For details on opening and closing BladeViewer, refer to "3.2 Login and Logout".

To use Resource Coordinator VE, both the Manager and Agents must be running. The Manager and Agents services are configured to start automatically upon startup of their respective servers (Admin Server, managed server). Normally, there should be no need to manually start or stop either the Manager or Agents. To start or stop the manager or an agent intentionally, refer to "5.1 Manager" and "5.2 Agent" of the "ServerView Resource Coordinator VE Setup Guide".

Note

When using the HBA address rename function, ensure that the Manager is started before starting any managed servers. The power on procedure should be managed as follows: first start the Admin Server together with the storage devices, and start the managed servers 10 minutes later.

Managed servers will not boot up properly if they are started before the Admin Server. Make sure that the Manager is running before starting managed servers.



Additionally, when using the HBA address rename function, the HBA address rename setup service should be started on a dedicated server (HBA address rename server) and left running continuously. For details on starting, stopping, and confirming the state of the HBA address rename setup service, refer to "6.2.2.1 Settings for the HBA address rename setup service" in the "ServerView Resource Coordinator VE Setup Guide".

Chapter 2 Switching between Views

This chapter provides an overview of the two views available in Resource Coordinator VE and explains how to switch between them.

Resource Coordinator VE allows administrators to choose between the following two views: the RC console and BladeViewer. Choosing an appropriate view depends on the administrator's authority level, or the kind of operations to be performed.

The RC console gives access to all of Resource Coordinator VE functions.

BladeViewer offers a simplified, lifelike representation of servers and their statuses. While this enables intuitive operation, it doesn't include the tree-based navigation and detailed menus available in the RC console. BladeViewer makes it easier to monitor blade servers, visualize their hosted applications or perform power operations.

This makes BladeViewer suitable for administrators who only need to monitor blades and perform basic operations.

To switch from the RC console to BladeViewer, click the <BladeViewer> button. To switch from BladeViewer to the RC console, click the <Advanced> button.



Information

- For details on the RC console, refer to "Chapter 2 User Interface" in the "ServerView Resource Coordinator VE Setup Guide".
- For details on BladeViewer, refer to "[Chapter 3 BladeViewer](#)". This explains the BladeViewer screen and the functions that it provides.
- 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.

Chapter 3 BladeViewer

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

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

Note

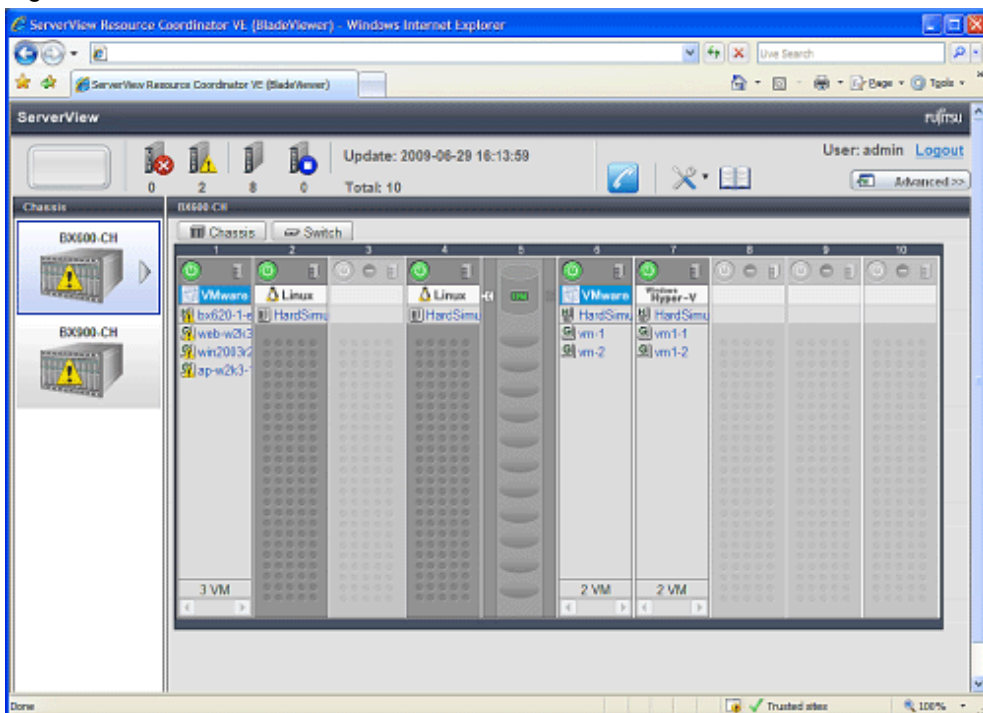
- When accessing the RC console from Internet Explorer 8, be sure to enable the Compatibility View in Internet Explorer.
- BladeViewer uses the standard Web browser font, and is optimized for a window size of 1024 by 768 pixels. Resizing the Web browser window to a very large extent may cause display to collapse.
- BladeViewer uses JavaScript, Cookies, and IFRAME. Therefore, those features should be enabled beforehand in the Web browser settings.
- BladeViewer communicates with the Admin Server using the XMLHttpRequest object. In Internet Explorer 6, XMLHttpRequest is an ActiveX object available by default in the system.
If BladeViewer is used from Internet Explorer 6, the following settings must be enabled.
 - Run ActiveX controls and plugins
 - Script ActiveX controls marked safe for scripting

3.1 Overview

This section provides a functional overview of BladeViewer.

BladeViewer provides a lifelike representation of blade servers and their statuses. It makes it easier to monitor resource states or perform basic operations on blade servers.

Figure 3.1 BladeViewer



BladeViewer allows the following operations.

- Monitoring of resource statuses

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

When using virtual servers, BladeViewer shows a list of VM guests for each VM host. This helps keeping track of relationships between VM guests and VM hosts.

BladeViewer also makes it easy to confirm which operating systems (physical OS and guest OS) are affected by a hardware failure.

- Display and control of power states

The power states of each server blade, storage blade, and VM guest is represented by an intuitive power button.

Clicking on this button provides quick access to power control operations (for both server blades and VM guests).

- Display of custom labels and comments

BladeViewer allows users to define custom labels and comments for each physical OS, VM host, and VM guest.

Once defined, labels are shown on top of each displayed physical OS, VM host, and VM guest. Using labels to display application contents makes it easy to visualize what applications are running on each blade and identify the applications affected by a server failure.

Clicking on a label will display the comment defined for the related resource. For example, registering troubleshooting and recovery procedures beforehand can speed up the recovery of affected applications when a problem occurs.

- Display of contact information

In a similar way, BladeViewer allows users to define technical (support) contact information for their entire IT system. This contact information can be shown by clicking on the Contact icon.

Registering contact details of technical support staff beforehand can help streamline recovery procedures when problems occur.

3.2 Login and Logout

This section explains how to log in and out of BladeViewer.

Log in

To log into BladeViewer, open a Web browser from an Admin Client and enter the RC console URL in the address bar. If the port number was changed, replace the port in the example below with the adequate port.

```
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.

If you are already logged in on a separate Web browser instance, login may be performed automatically without the login screen being displayed.



Note

- If the login screen is not displayed, confirm the following.
 - The correct URL was entered
 - The proxy settings of the Web browser are correct
 - The firewall settings on the Admin Server are correct
- 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 a unique, self-signed certificate for each Admin Server during Manager installation.

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. 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" of the "ServerView Resource Coordinator VE Setup Guide" for details.
- If already logged in from another Web browser window, login may be performed automatically (without displaying the login screen).

After accessing the Admin Server IP address from a browser, the login screen is displayed. Enter the following items in the login screen and click the <Login> button.

If the login is successful, either BladeViewer or RC console is displayed.

- User name
- Password

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

To log in as a different user, open a separate Web browser window from the Windows start menu.

Information

- Enter the user account name and password set during Manager installation, as 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.
- Clicking the <BladeViewer>>> button from the RC console will switch over to the BladeViewer view.

Log out

To log out of BladeViewer, click the "Logout" button text link displayed on the top right of the BladeViewer screen.

Note

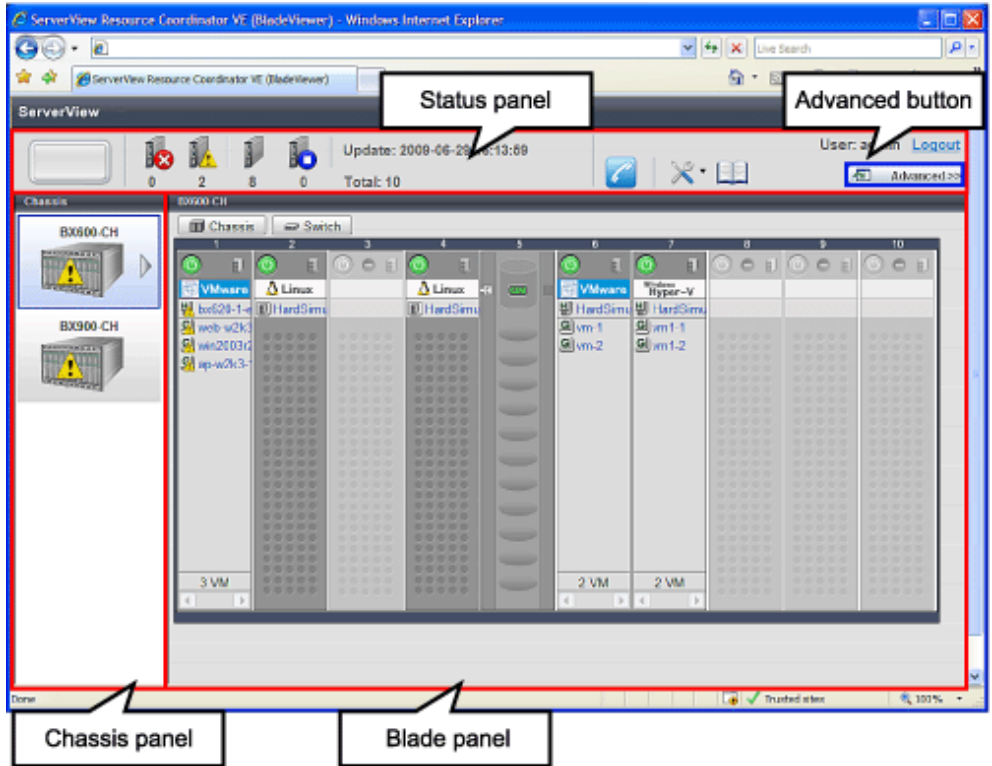
- If the Web browser is closed without logging out first, user authentication may be skipped the next time Resource Coordinator VE is accessed. In that case, users will be automatically logged in using the previously used session. To avoid such cases, please log out correctly before closing the Web browser.
- If multiple RC consoles or BladeViewer views are opened from multiple browsers, login sessions may be abruptly closed.

3.3 BladeViewer Layout

This section explains how the BladeViewer screen is organized.

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

Figure 3.2 BladeViewer screen layout



Status panel

This panel displays a summary of resources statuses.

Chassis panel

This panel displays the statuses of each registered chassis.

Blade panel

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

 **Information**

To switch from BladeViewer to the RC console, click the <Advanced>>> button displayed in the top right of the BladeViewer screen. Switch to the RC console when necessary, for example to register servers and change Resource Coordinator VE settings. The next time Resource Coordinator VE is accessed, the last used view (either RC console or BladeViewer) is displayed.

3.4 Resource Status Monitoring

This section explains how to monitor resource statuses using BladeViewer.

3.4.1 Status Panel

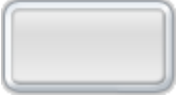


The status panel displays a summary of resources statuses (including resources other than PRIMERGY BX servers).

When a problem occurs in the system, a red or yellow light icon starts blinking on the left side of the status panel.

Clicking the light icon changes its color back to gray.

The table below shows the status and meaning associated with each light icon.

Table 3.1 Light icons

Icon	Color	Status	Meaning
	Gray (no light)	Normal	No errors or warnings have been detected in the system.
	Yellow (blinking)	Warning	A warning has been detected in the system.
	Red (blinking)	Error	An error has been detected in the system.


 Information

When the light icon blinks, it means that a warning or an error has been detected. Check the location of the problem from the chassis or blade panel.

If BladeViewer shows no resources with a warning or error status in either the chassis panel or blade panel, switch to the RC console and check the event log to identify the cause of the problem.




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

Table 3.2 Displaying the server icon and the number of units

Icon and number of units	Meaning
 N(*1)	Server and number of units

*1: N is the number of servers.


Table 3.3 Status icons

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

3.4.2 Chassis Panel

The chassis panel displays the statuses of each registered chassis.

Table 3.4 Chassis icon (in chassis panel)

Icon	Meaning
	Chassis

See

For details on the different chassis statuses, refer to "[Table 3.3 Status icons](#)" of "3.4.1 Status Panel".

If a chassis icon shows a warning or error status, it means that a problem occurred in a resource that is contained in the chassis.
For details on how to identify faulty resources, refer to "[3.4.3 Blade Panel](#)".

Information

Selecting a chassis icon from the chassis panel displays the contents of that chassis in the blade panel.
For details, refer to "[3.4.3 Blade Panel](#)".

3.4.3 Blade Panel

The blade panel displays the statuses of all the resources inserted into the selected chassis. Those resources are shown in a format representative of their physical configuration (shape and position).

To display the contents of a specific chassis in the blade panel, click on its icon in the chassis panel.

In the blade panel, the selected chassis and its LAN switches are represented by the following icons. Those icons are displayed in the top part of the blade panel.

Table 3.5 Chassis icon (in blade panel)



Icon	Meaning
	Chassis

Table 3.6 LAN switch icon

Icon	Meaning
	LAN switch

See

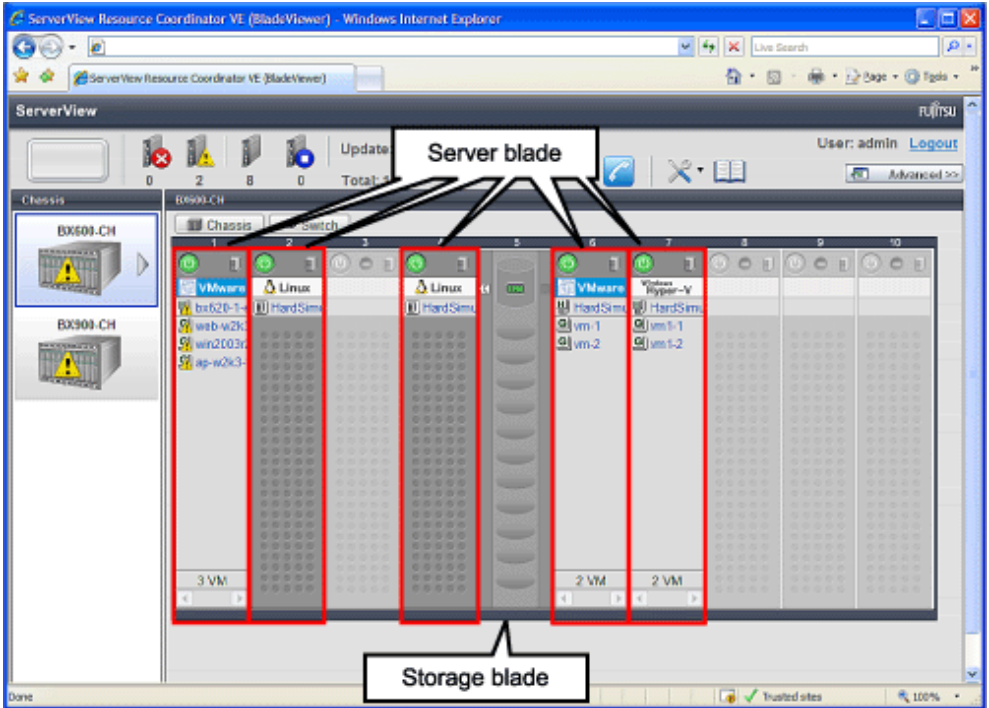
For details on the status icons that are displayed for the chassis and its LAN switches, refer to "[Table 3.3 Status icons](#)" of "3.4.1 Status Panel".

3.4.3.1 Resource List

The blade panel graphically displays each slot within a chassis. Each server or storage blade is displayed according to their actual position (slot) within the chassis.

Note that an unregistered server is shown in light gray while an empty slot is shown in white.

Figure 3.3 Blade Panel Resource List



Server blade

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

Table 3.7 Server blade power buttons




Power button	Color	Status	Meaning
	Green (is lit)	Power ON	Power ON status.
	Gray (no light)	Power OFF	Power OFF status.
	Green (blinking)	Power ON in progress	Power ON or reboot control in progress.
	Orange (blinking)	Power OFF in progress	Power OFF control in progress.

Information

The power status of a server blade can be easily controlled by clicking on its power button. For details, refer to "3.5.1 Server Blade".

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

Table 3.8 Physical server icons

Icon	Meaning
	Server
	Spare server
	Unregistered server




See

For details on the different physical server statuses, refer to "Table 3.3 Status icons" of "3.4.1 Status Panel".

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






Table 3.9 Admin Server icon

Icon	Status	Meaning
	Admin Server	Used as the Admin Server.

An OS icon is displayed below the physical server icon.

The table below shows the meaning of each OS icon.

Table 3.10 OS icons

Icon	Meaning
	Windows OS
	Linux OS
	VMware host OS
	Hyper-V host OS
	Xen host OS



Information

Clicking on a VM host OS icon displays a detailed list of the VM guests operating on the selected VM host.



For details, refer to "3.4.3.2 VM Guest List".


A user-defined label is displayed with a resource icon below the OS icon. If no label was defined yet for a server blade, its OS name is displayed instead.

If the OS name cannot be acquired (because the OS has not been installed or for other reasons), the server name (physical server name, or VM guest name) is displayed.

The table below shows the meaning associated with each resource icon.

Table 3.11 Resource icons

Icon	Meaning
	Physical OS
	VM host

Icon	Meaning
	VM guest

 See

For details on the resource status, refer to "Table 3.3 Status icons" of "3.4.1 Status Panel".

 Information

If a comment has been defined for a server, clicking on its label displays the [Server Properties] dialog.

The [Server Properties] dialog displays the comment and label set for the selected server, as well as its OS name, server name (for a physical OS, the physical server name, for a VM guest, the VM guest name), and IP address. This information can be used to easily identify a server.



For details on defining comments, refer to "3.6.1 Listing and Editing of Labels and Comments".

Storage blade

A power lamp is displayed in the top part of each storage blade.

The table below shows the status and meaning associated with each power lamp.

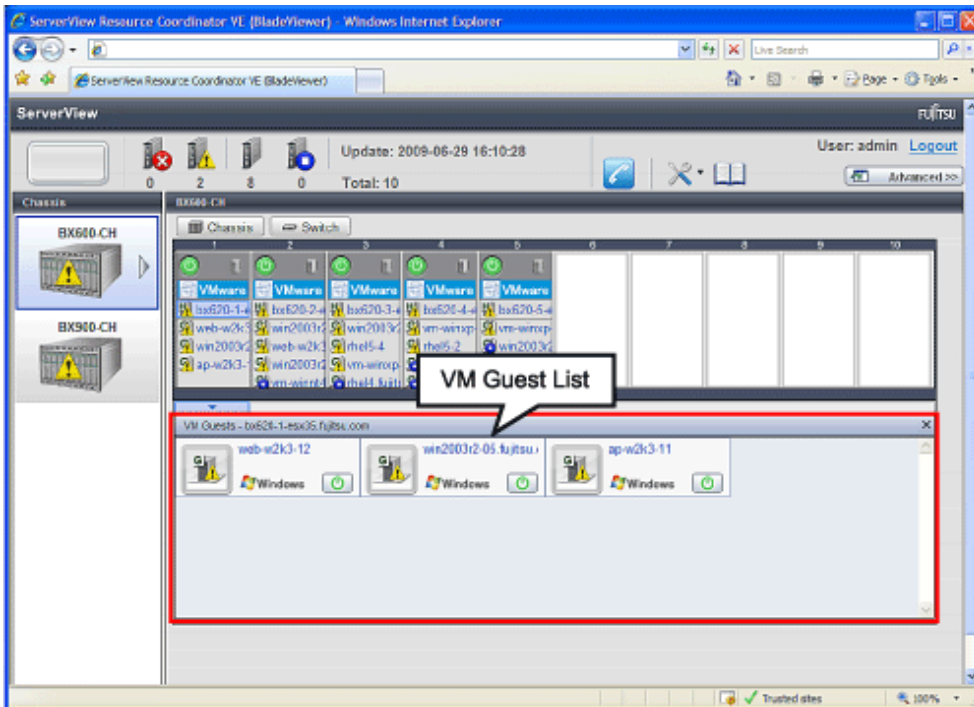
Table 3.12 Storage blade power lamps

Power lamp	Color	Status	Meaning
	Green (is lit)	Power ON	Power ON status.
	Gray (no light)	Power OFF	Power OFF status.

3.4.3.2 VM Guest List


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

Figure 3.4 Blade Panel: VM Guest List



A VM guest icon is shown on the left side of each VM guest displayed in the VM guest list.

Table 3.13 VM guest icon

Icon	Meaning
	VM guest



See

For details on the different VM guest statuses, refer to "Table 3.3 Status icons" of "3.4.1 Status Panel".

A user-defined label is displayed on the upper-right side of the VM guest icon. If no label was defined yet for a VM guest, its OS name is displayed instead.

If the OS name cannot be acquired (because the OS has not been installed or for other reasons), the VM guest name is displayed.





An OS icon is displayed below the label.

For details on the different OS icons, refer to "Table 3.10 OS icons" of "3.4.3.1 Resource List".

A power button is displayed on the bottom-right side of each VM guest.

This power button is used to represent the power status of each VM guest, as shown below.

Table 3.14 VM guest power buttons

Power button	Color	Status	Meaning
	Green (is lit)	Power ON	Power ON status.
	Gray (no light)	Power OFF	Power OFF status.
	Green (blinking)	Power ON in progress	Power ON or reboot control in progress.
	Orange (blinking)	Power OFF in progress	Power OFF control in progress.

Information

The power status of a VM guest can be easily controlled by clicking on its power button.
Refer to "[3.5.2 VM Guest](#)" for details.

3.4.4 Resource Details

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

- Chassis

Clicking the chassis icon (from the blade panel) opens up its management blade's Web interface in a new window.
This Web interface provides more details on the chassis' status and contents.
For details on the chassis icon, refer to "[3.4.3 Blade Panel](#)".

- LAN switch

Clicking on a LAN switch icon opens up its LAN switch details screen.
This screen provides more details on the LAN switch's status and configuration.
For details on the LAN switch icon, refer to "[3.4.3 Blade Panel](#)".

- Physical server

Clicking on a physical server icon opens it up in ServerView Operation Manager's Web interface.
This interface provides more details on the physical server's status and its inner components.
For details on the physical server icon, refer to "[Table 3.8 Physical server icons](#)" in "[3.4.3.1 Resource List](#)".



3.5 Power Control

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

3.5.1 Server Blade

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

Table 3.15 Actions of server blade power buttons

Power button	Color	Current Status	Action
	Gray (no light)	Power OFF	Powers on a server blade.
	Green (is lit)	Power ON	Shuts down or reboots a server blade.

Power On

Clicking on a power button that shows a "Power OFF" state will power on the target server blade. A confirmation dialog is displayed first.

Clicking the <OK> button in the confirmation dialog powers on the server and starts its OS.

At this time, the power button changes to an intermediate "Power ON in progress" state (green - blinking). The power button finally displays a "Power ON" state after confirming that the OS has correctly started up on the target server.

Power Off and Reboot

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

Figure 3.5 Power Operation dialog



- Shutdown action

Selecting "Shutdown" will shut down the target server blade. A confirmation dialog is displayed first.

Clicking the <OK> button in the confirmation dialog shuts down the OS and powers off the server.

At this time, the power button changes to an intermediate "Power OFF in progress" state (orange - blinking). The power button finally displays a "Power OFF" state after confirming that the target server has been correctly shut down.

- Reboot action

Selecting "Reboot" will reboot the target server blade. A confirmation dialog is displayed first.

Clicking the <OK> button in the confirmation dialog shuts down the OS and restarts the server.

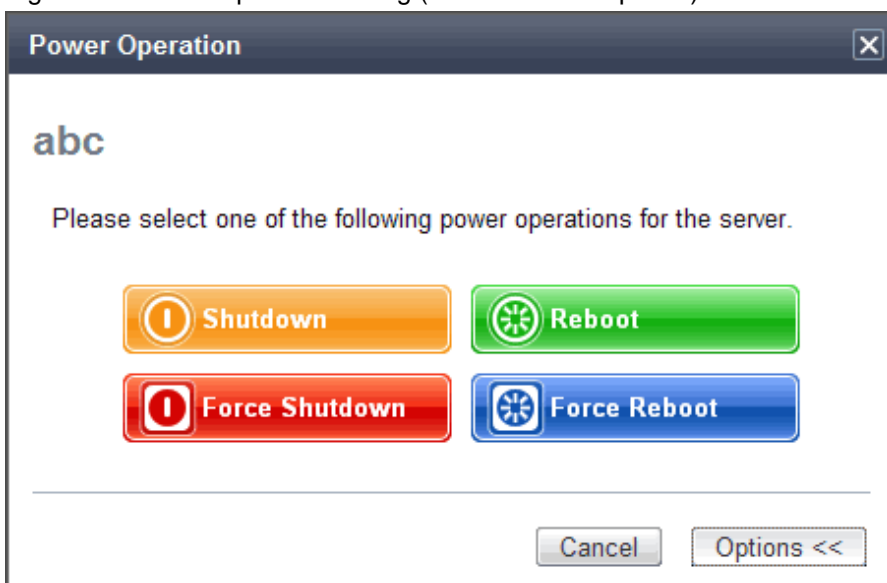
At this time, the power button changes to an intermediate "Power ON in progress" state (green - blinking). The power button finally displays a "Power ON" state after confirming that the OS has correctly started up on the target server.

Forced Power Off and Reboot

Clicking on a power button that shows a "Power ON" state, and selecting <Options >>> in the displayed [Power Operation] dialog enable selection of the "Force Shutdown" and "Force Reboot" actions.

A forced shutdown (or reboot) will forcibly power off (or reboot) the managed server blade without waiting for its OS to cleanly shut down.

Figure 3.6 Power Operation dialog (with additional options)



- "Force Shutdown" action

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

- "Force Reboot" action

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

Note

Take care of the following points when powering-off or rebooting a VM host.



- When using a server virtualization software's high-availability feature, confirm that the server is set to VM maintenance mode within that virtualization software. This can be confirmed from the virtualization software client.
- Perform a power operation only after setting VM maintenance mode (either from the VM management software client or using the resource control command). Refer to the server virtualization software manual, or to "3.2 rcxadm server" in the "ServerView Resource Coordinator VE Command Reference" for details. Depending on the server virtualization product used, some restrictions may apply to the use of VM maintenance mode settings. Refer to "A.3 Functional Differences between Products" in the "ServerView Resource Coordinator VE Setup Guide" for details about such restrictions.

3.5.2 VM Guest

The power state of a VM guest can be controlled by clicking the OS icon of its VM host and then clicking its power button in the list of VM guests that is displayed.

Clicking on that power button provides power controls similar to those provided for server blades.

Table 3.16 Actions of VM guest power buttons

Power Button	Color	Current Status	Action
	Gray (no light)	Power OFF	Powers on a VM guest.
	Green (is lit)	Power ON	Shuts down or reboots a VM guest.

Note

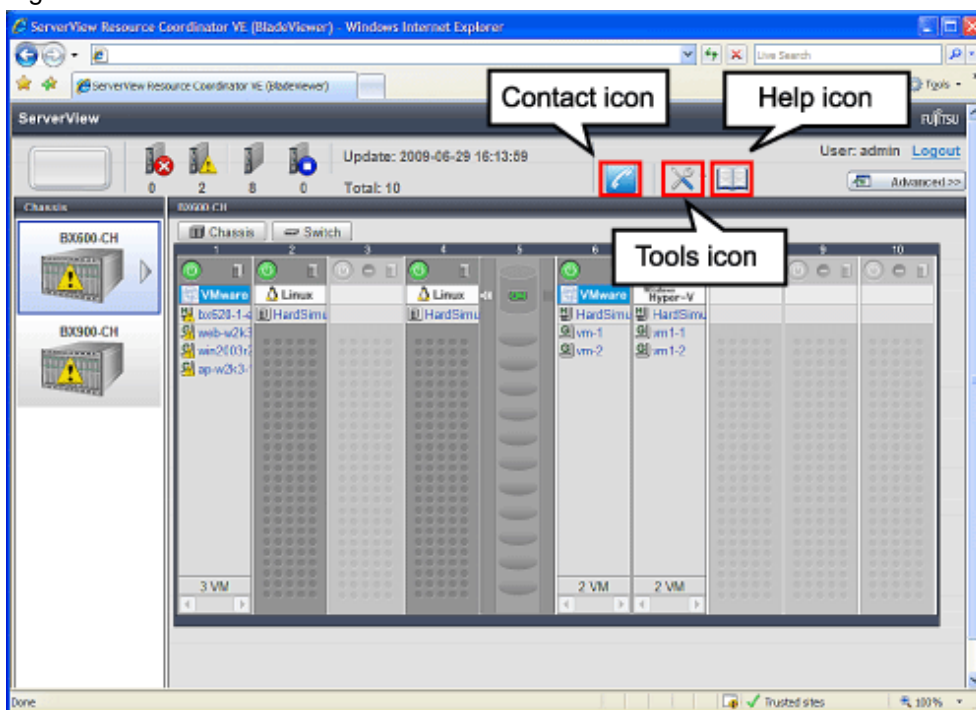
- VM guests should be properly configured in order to use the shut down or reboot buttons. Attempting to shut down or reboot a VM guest that wasn't properly configured will result in an error. Refer to "A.2 Configuration Requirements" of the "ServerView Resource Coordinator VE Setup Guide" for details.
- Depending on the server virtualization environment, a VM guest may automatically migrate to another VM host when being shut down. This may cause power control operations to fail and return an error when used on VM guests. Refer to "A.3 Functional Differences between Products" of the "ServerView Resource Coordinator VE Setup Guide" for details.
- A VM guest can be configured to automatically start or stop whenever its VM host starts up or shuts down. This can be achieved by setting up the VM guest's startup and shutdown options in the virtualization software used. Refer to the virtualization software manual for details.

- Take care of the following points when shutting down or rebooting a server running a Windows Operating System.
 - If Windows is not configured to shut down when the computer's power button is pressed, the power operations in Resource Coordinator VE may not function properly.
To check this option, open [Control Panel]-[Power Options]. In the [Power Options Properties] dialog, click the [Advanced] tab, and check the action that is set to be performed when the computer's power button is pressed.
 - If a file is being edited by a logged-in user, a dialog prompting the user to save the file is displayed, and the system may not shut down immediately.
In such cases, shutdown does not take place until the user takes the appropriate action or a specified time (approximately five minutes) has elapsed.

3.6 Status Panel Operations

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

Figure 3.7 BladeViewer tool icons



Contact icon

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

Tools icon

Displays the following menu options.

Label List

Displays the [Label List] dialog.

Displays a list of labels. This list also allows modification of labels and comments.

For details on editing labels and comments, refer to "[3.6.1 Listing and Editing of Labels and Comments](#)".

Set Contact Information

Displays the [Set Contact Information] dialog.

For details on modifying contact information, refer to "[3.6.2 Editing Contacts](#)".

Change Password

Displays the [Change Password] dialog.

For details on changing passwords, refer to "[3.6.3 Change of Password](#)".

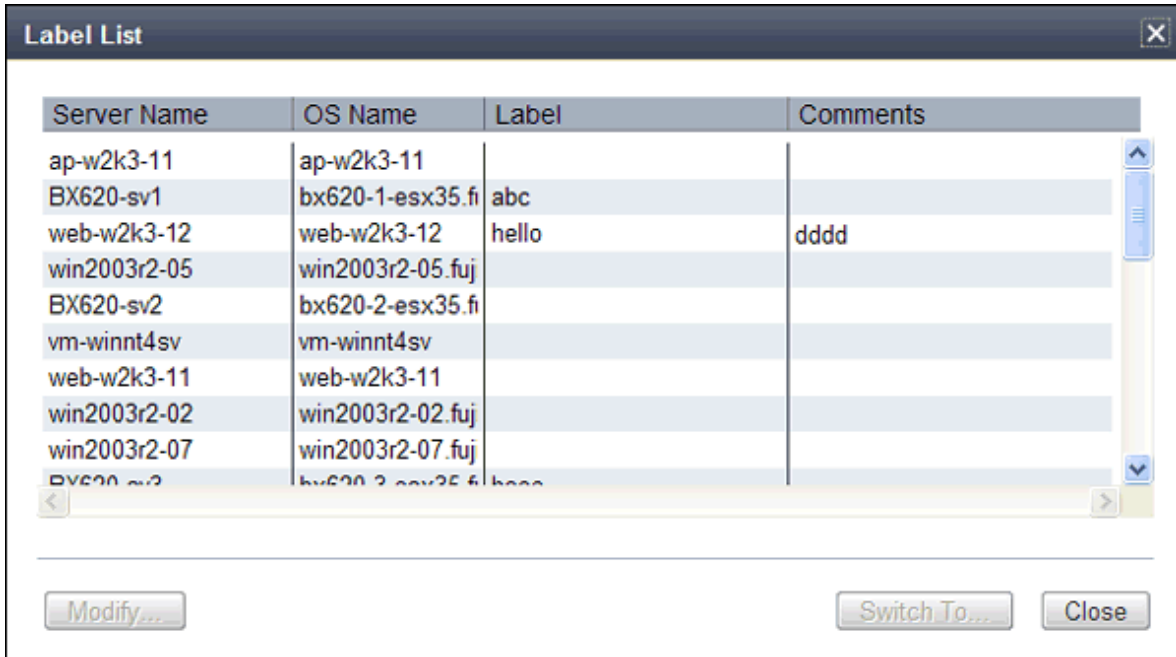
Help icon

The Help is displayed.

3.6.1 Listing and Editing of Labels and Comments

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

Figure 3.8 Label List



Server Name	OS Name	Label	Comments
ap-w2k3-11	ap-w2k3-11		
BX620-sv1	bx620-1-esx35.f	abc	
web-w2k3-12	web-w2k3-12	hello	dddd
win2003r2-05	win2003r2-05.fuj		
BX620-sv2	bx620-2-esx35.f		
vm-winnt4sv	vm-winnt4sv		
web-w2k3-11	web-w2k3-11		
win2003r2-02	win2003r2-02.fuj		
win2003r2-07	win2003r2-07.fuj		
BX620-sv2	bx620-2-esx35.f	hello	

Contents of the label list

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

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

Editing labels and comments

This function is only available to privileged users.

General users are only able to consult labels and comments.

- Privileged user

In the [Label List] dialog, select a server and click on the <Modify> button.

The [Modify Server Properties] dialog is displayed.

The label and comment of the selected server can be edited directly from the [Modify Server Properties] dialog.

Enter the following items:

Label

Enter a maximum of 32 characters.

Comments

Enter a maximum of 256 characters.

 **Note**

New lines are counted as 2 characters.

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

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

- General user

If logged in as a general user, a <Show> button is displayed in place of the <Modify> button in the [Label List] dialog.

Clicking on the <Show> button displays the [Server Properties] dialog, but does not allow editing of labels or comments.

3.6.2 Editing Contacts

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

Enter the following item.

Contact

The currently defined contact information is displayed.

Enter a maximum of 256 characters.

 **Note**

New lines are counted as 2 characters.

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

3.6.3 Change of Password

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

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

- Privileged user

New Password (Confirm Password)

Enter a maximum of 16 characters that consists of alphanumeric characters and symbols.

- General user

Current Password

Enter the password that is currently set.

Enter a maximum of 16 characters that consists of alphanumeric characters and symbols.

New Password (Confirm Password)

Enter a maximum of 16 characters that consists of alphanumeric characters and symbols.

Chapter 4 User Accounts

This chapter describes the user accounts used in Resource Coordinator VE.

4.1 Overview

Managing user accounts in Resource Coordinator VE prevents unsafe operations from unauthorized users, resulting in safer system administration.

User accounts are divided into the following user types.

Table 4.1 User Types

User types	Authority level	Description
Privileged user	Manage	Can perform all operations on resources
General user	Monitor	Can perform only resource monitoring

It is required to create at least one privileged user. The creation of general users is optional and depends on your own administration policy.

User accounts consist of the following:

- User name
- Password
- Authority level ("Manage" or "Monitor")

These Resource Coordinator VE user accounts differ from the operating system user accounts on the Admin Server.

Refer to "2.2.1 List of Menus" in the "ServerView Resource Coordinator VE Setup Guide" for information on the functions that these user accounts can execute.

4.2 Managing User Accounts

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

Add User Account

Only privileged users can perform this operation.

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

The [User Accounts] dialog is displayed.

2. In the [User Accounts] dialog, click the <Add> button.

The [Add User Account] dialog is displayed.

3. In the [Add User Account] dialog, set the following:

User name

Enter a string of no more than 16 characters, where the first character must be a letter and the remaining characters can include alphanumeric characters, underscores ("_"), hyphens ("-") and periods (".").

Please note that user names are case-sensitive.

Password (Password confirmation)

Enter a string using no more than 16 alphanumeric characters or symbols.

Authority level

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

4. Click the <OK> button.

The user account is created.

Change User Account Settings

Both privileged users and general users can perform this operation.

Privileged users can modify any account information. General users can only modify their own password.

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

The [User Accounts] dialog is displayed.

2. In the [User Accounts] dialog, select the user account to modify, and click the <Change> button.

The [Change User Account] dialog is displayed.

3. In the [Change User Account] dialog, set the following:

Password

No change/Change

Select the appropriate action.

By default the "No change" option is selected.

Current password

Enter a string using no more than 16 alphanumeric characters or symbols.

This is displayed when general users modify their own passwords.

New password (Password confirmation)

Enter a string using no more than 16 alphanumeric characters or symbols.

Authority level

No change/Change

Select the appropriate action.

By default the "No change" option is selected.

Authority level

Select either "Manage" or "Monitor".

By default, the current authority level is selected.

4. Click the <OK> button.

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

Delete User Account

Only privileged users can perform this operation.

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

The [User Accounts] dialog is displayed.

2. In the [User Accounts] dialog, select the user account to delete, and click the <Delete> button.

The [Delete User Account] dialog is displayed.

3. In the [Delete User Account] dialog, click the <OK> button.

The selected user account is deleted.

Chapter 5 Monitoring

This chapter explains how to monitor the configuration and status of managed resources.

5.1 Overview

Resource Coordinator VE can centrally monitor the configuration and status of servers or other managed resources directly from the RC console. This enables the identification of resources experiencing problems, which reduces time spent on system maintenance. Moreover, Resource Coordinator VE can easily launch external management software to precisely locate faulty parts within a managed resource.

Monitoring is based on the following three components:

- Resources

The resource tree displays chassis, servers, LAN switches, physical OS's, VM hosts, VM guests, power monitoring device relationships or statuses (either PDU or UPS). When a hardware problem occurs on a server, affected guest operating systems can easily be detected.

 **Note**

Power monitoring devices are not subject to monitoring.

- Events

Resource Coordinator VE displays events such as hardware failures, server switchovers triggered by hardware failures, and the results of every performed operation.

- Recent Operations

Resource Coordinator VE displays the progress status of the various operations performed on resources.

The following table shows the level of monitoring performed for each resource monitored in Resource Coordinator VE.

Table 5.1 Monitoring level for each resource type

Resource	Status monitoring	Event monitoring
Chassis	Yes	Yes
Server	Yes	Yes
Physical OS	Yes	No
VM host	Yes	No
VM guest	Yes	No
VM management software	Yes	No
LAN switch	Yes	Yes
Power monitoring device	No	No

Yes: Supported

No: Not supported

Regular update of resource data

The Resource Coordinator VE Manager regularly updates resource data with information gathered from the following resources.

Table 5.2 List of regularly updated resources and their related resources

Resources subject to regular update	Related resources	Data source
Chassis	Chassis	Server Management Unit

Resources subject to regular update	Related resources	Data source
Server	Server Physical OS VM host (*1) VM guest (*1)	ServerView Agent (*2) Server Management Unit Server Virtualization Software
LAN switch	LAN switch	LAN switch Server Management Unit (*3)
VM management software	VM management software VM host (*1) VM guest (*1)	VM management software

*1: When no VM management software is registered, the status of VM hosts and VM guests is updated during a regular update of their physical server. When a VM management software is registered, their status is updated during a regular update of the VM management software.

*2: only for PRIMERGY servers.

*3: only for LAN switch blades mounted in a PRIMERGY BX chassis.

The time required to update all resources depends on the number of registered resources. For one chassis that contains 10 servers and 4 LAN switches, the update takes about 2 minutes. For 5 chassis that have identical configurations, the update should take about 10 minutes.

VM management software updates are independent from other resource updates, and takes approximately 2 minutes.

In the following cases, resource data is refreshed without waiting for the regular update.

- When a resource's state is changed as the result of an operation performed by Resource Coordinator VE
- When a failure-triggered SNMP Trap is received from a resource

If a resource was operated externally to Resource Coordinator VE, there may be a slight delay before its state is updated in the RC console. To force an update of a resource's data, right-click the resource and select [Update] from the displayed menu. The time required to update resource data depends on the device. Generally, update should take no more than 40 seconds.

In order to restrain device and network load, resource data is not refreshed for 7 seconds following the last update time. However, when a failure-triggered SNMP Trap is received, resource data is refreshed unconditionally. When manually updating a resource from the menu right after performing an operation on that resource, if its data is not refreshed within 40 seconds, try updating it from the menu again.

5.2 Resource Status

Resources are monitored in the [Status] tab of the RC console.

The [Status] tab shows the number of servers listed under the statuses "warning", "unknown", "error" or "fatal".

Servers whose status is "warning" or "unknown" are counted under "Warning", and servers whose status is "fatal" or "error" are counted under "Error".

Clicking on "Error" or "Warning", displays the resources under the corresponding status in the [Resource List] tab.




The status of resources can also be monitored from both the resource tree and the [Resource List] tab. When an error occurs, a status icon is added to the icon of the resource concerned.








Double-clicking on a resource icon displays the [Resource Details] tab, which provides detailed information about the corresponding resource.

Icons displayed in the RC console

The following table shows the resource icons used in the RC console and their associated meaning.

Table 5.3 Resource icons




Icon	Meaning
	Server resource
	Chassis
	Server

Icon	Meaning
	Physical OS
	VM host
	VM guest
	LAN switch
	Power monitoring device (*1)
	PDU (*1)
	UPS (*1)

*1: Power monitoring devices (PDU or UPS) are not subject to monitoring.

The following table shows the status icons used in Resource Coordinator VE and their associated meaning. It also shows which status icons require corrective actions.

Table 5.4 Status icons

Icon	Status	Meaning	Corrective Action
None	normal	Normal	No action is necessary
	warning	Warning An error occurred but the resource can still be used. (*1)	Action must be taken
	unknown	Unknown The status of the resource cannot be obtained. (*2, *3)	Action must be taken
	stop	Stop The resource has stopped and cannot be used.	No action is necessary
	error	Error An error whose cause is unknown has occurred and the resource cannot be used.	Action must be taken
	fatal	Fault A fault has occurred in the resource and the resource cannot be used.	Action must be taken

*1: When a LAN switch is in a "warning" status, it means that the LAN switch may have been replaced with another model.

To use the LAN switch as it is, first delete the registered LAN switch, and then register it again.






*2: When a VM guest is in "unknown" status, check the operation status of the VM host on which the VM guest is running.

*3: When a LAN switch is in "unknown" status, check the physical connection between the LAN switch and Admin LAN as well as whether or not the LAN switch is responding to commands.

Note

For other servers, hardware statuses can not be obtained from server management software (ServerView). Therefore, only "normal", "stop" or "unknown" statuses are shown, while "warning", "error" and "fatal" statuses can not be detected.

Table 5.5 OS icons

Icon	Meaning
	Windows OS
	Linux OS
	Solaris OS
	VMware host OS
	Hyper-V host OS

Icon	Meaning
Xen	Xen host OS

Information

- For server virtualization software, the following information is also displayed.
 - VM management software

The status of a VM management software is displayed in the "VM management software Settings" dialog. Only "normal" and "unknown" statuses are displayed. If an "unknown" is shown, check whether the VM management software is operating properly.
 - VM host

The status of a VM host is displayed in the same way as for a physical OS.
 - VM guest

Errors detected from server virtualization software are reflected in VM guest statuses. VM guest statuses can be either one of the following: "normal", "warning", "error", "unknown" and "stop". Refer to "A.3 Functional Differences between Products" of the "ServerView Resource Coordinator VE Setup Guide".
- For LAN switches, "error" and "fatal" are not displayed. Only "warning", "normal", and "unknown" are displayed.

5.3 Addressing Resource Failures

This section explains how to address problems like hardware failures occurring in a system.

Basic Procedure

The following procedure is used to confirm and resolve problems using the RC console.

1. Confirm the existence of a problem

Use the RC console to confirm that a problem has occurred on a resource.
Refer to the following for details on checking resource statuses.

- For PRIMERGY servers

Refer to "[5.2 Resource Status](#)" in this chapter and "2.3 Status Panel" of the "ServerView Resource Coordinator VE Setup Guide".

- For servers other than PRIMERGY servers

Refer to "2.3 Status Panel" of the "ServerView Resource Coordinator VE Setup Guide".

2. Check the event log

Use the event log to check the device where the error occurred and the content of the event.

In some cases a single problem can cause a series of events to occur, so search back through past events to find events with dates that are close together.

3. Check the status of resources

From the resource tree, open the resource where the problem occurred and look for any affected chassis, physical server, LAN switch, physical OS, VM host and VM guests.

If Auto-Recovery has been enabled for a physical OS or VM host, it will be automatically switched over with a spare server. If Auto-Recovery has not been enabled, server switchover can still be performed manually as long as a spare server has been designated.

For more information regarding server switchover, refer to "[10.2 Switchover](#)".

4. Perform detailed investigation and recovery

From the [Resource Details] tab of the failed resource, launch the external management software to investigate the precise cause of the problem.

When no management software is available, confirm with the maintenance staff of the failed resource to investigate the problem. Once this is done, perform the necessary maintenance work on any faulty hardware identified. If a server hardware failure requires replacing a managed server, carry out the replacement operation as described in "[9.4 Replacing Servers](#)".

5. Perform post-recovery verification

Following recovery, confirm that there are no more icons indicating problems on the RC console.

Chapter 6 Power Control

This chapter explains how to remotely control the power state of managed resources.

6.1 Server Power Control

This section explains how to remotely control the power states of physical servers, VM hosts and VM guests.

1. In the RC console resource tree, right-click the desired server (or the physical OS or VM host running on the server) or VM guest, select [Power] from the popup menu, and select one of the following options:

ON

This option powers on a halted resource and starts its operating system.

OFF

This option powers off an active resource after shutting down its operating system.

OFF (Forced)

This option forcibly powers off an active resource without first shutting down its operating system.

Reboot

This option restarts an active resource after shutting down its operating system.

Reboot (Forced)

This option forcibly restarts an active resource without first shutting down its operating system.

2. Click the <OK> button in the confirmation dialog displayed.
The specified power control operation is executed.
3. The progress of the specified operation is displayed in the Recent Operations area. Check that the operation status is shown as "completed", and that the resource in the resource tree or [Resource List] tab has changed to the expected power state.

Information

A reboot or forced reboot of a physical server or VM host is done by shutting down the server once, and powering on again (instead of a system reset).

Note

- VM guests should be properly configured in order to use the power off or reboot options. Attempting to power off or reboot a VM guest that wasn't properly configured will result in an error. Refer to "A.2 Configuration Requirements" of the "ServerView Resource Coordinator VE Setup Guide" for details.
- Depending on the server virtualization environment, a VM guest may automatically migrate to another VM host when being shut down. This may cause power control operations to fail and return an error when used on VM guests. Refer to "A.3 Functional Differences between Products" of the "ServerView Resource Coordinator VE Setup Guide" for details.
- A VM guest can be configured to automatically start or stop whenever its VM host starts up or shuts down. This can be achieved by setting up the VM guest's startup and shutdown options in the server virtualization software used. Refer to the virtualization software manual for details.
- Take care of the following points when shutting down or rebooting a server running a Windows operating system.
 - If Windows is not configured to shut down when the computer's power button is pressed, the power operations in Resource Coordinator VE may not function properly.
To check this option, open [Control Panel]-[Power Options]. In the [Power Options Properties] dialog, click the [Advanced] tab, and check the action that is set to be performed when the computer's power button is pressed.

- If a file is being edited by a logged-in user, a dialog prompting the user to save the file is displayed, and the system may not shut down immediately.
In such cases, shutdown does not take place until the user takes the appropriate action or a specified time (approximately five minutes) has elapsed.
 - Take care of the following points when powering-off or rebooting a VM host.
 - When using a server virtualization software's high-availability feature, confirm that the server is set to VM maintenance mode within that virtualization software. This can be confirmed from the virtualization software client.
 - Perform a power operation only after setting VM maintenance mode (either from the VM management software client or using the resource control command).
Refer to the server virtualization software manual, or to "3.2 rcxadm server" in the "ServerView Resource Coordinator VE Command Reference" for details.
Depending on the software virtualization product used, some restrictions may apply to the use of VM maintenance mode settings. Refer to "A.3 Functional Differences between Products" in the "ServerView Resource Coordinator VE Setup Guide" for details about such restrictions.
-

6.2 Chassis Power Control

This section explains how to remotely control the power state of a blade server chassis.

The power state of a blade chassis can be controlled using the "rcxadm chassis" command. Refer to "3.1 rcxadm chassis" in the "ServerView Resource Coordinator VE Command Reference" for details.

Chapter 7 Control of VM Environments

This chapter describes the Resource Coordinator VE functions that are specific to VM guests and VM hosts.

Some functions may or may not be available depending on the server virtualization software used. Refer to "A.1 Supported Functions" in the "ServerView Resource Coordinator VE Setup Guide" for details.

Other functions are similar in use to those available for regular physical OS's (without server virtualization software).

7.1 Migration of VM Guests between Servers

This section explains how to migrate a VM guest to a VM host on a different physical server.

Two types (methods) of VM guest migration are available in Resource Coordinator VE. Although such types are named differently depending on the virtualization software used, Resource Coordinator VE makes use of the following naming convention.

For details on migration pre-requisites and terminology, refer to "A.3 Functional Differences between Products" in the "ServerView Resource Coordinator VE Setup Guide".

- Live migration: migration of a VM guest without shutting down its VM host.
- Cold migration: migration of a VM guest while its VM host is shut down. The resulting power state of a migrated VM guest is the same as it was before migration.

Availability of those migration types depends on the power state of VM guests, as described below.

Table 7.1 Migration Types Available for Each Power State

VM Guest Power State	Migration Type	
	Cold Migration	Live Migration
ON	Available	Default
OFF	Default	N/A

Default: available and selected by default.

Available: available.

N/A: not available.

A VM guest after migration is set to the same power state as it was before the migration. For example, performing a cold migration on an operating VM guest will temporarily shut it down during migration, before starting it up again after completion of the migration process. It is therefore recommended to set the target VM guest in the desired post-migration state before starting a migration.

Use the following procedure to migrate a VM guest.

1. In the RC console resource tree, right-click on the VM guest to migrate and select "Migrate" from the popup menu.

The [VM Guest Migration] dialog is displayed.

2. In the [VM Guest Migration] dialog, set the following items.

Destination

Select a destination VM host.

Migration Type

Select the desired migration type.

3. Click the <OK> button

The selected VM guest is migrated to its new host.

VM guests can be migrated from the command-line, using the "rcxadm server migrate" command. Refer to "3.2 rcxadm server" in the "ServerView Resource Coordinator VE Command Reference" for details.

7.2 VM Maintenance Mode of VM Hosts

This section explains how to set and release VM maintenance mode on VM hosts.

For details on VM maintenance modes, refer to "A.3 Functional Differences between Products" in the "ServerView Resource Coordinator VE Setup Guide".

VM maintenance mode can also be set or released from the command-line, using the "rcxadm server set" command. For details, refer to "3.2 rcxadm server" in the "ServerView Resource Coordinator VE Command Reference".

Chapter 8 Backup and Restore

This chapter explains how to use the backup and restore functions provided in Resource Coordinator VE.

8.1 Overview

The backup and restore functions allow the backup and restore of system images from physical OS's or VM hosts.

The system images are backed up over the network and stored to a disk on the Admin Server.

A system image backup can be used for the following purposes:

- Software maintenance

A system image backup can be created as a precautionary measure before performing maintenance tasks such as applying patches, installing, or modifying installed software.

- Hardware maintenance

A system image backup can be used to guard against hardware problems such as disk failures.



Note

- This function is disabled if ServerView Deployment Manager is used on the Admin LAN. Use the backup and restore functions available in ServerView Deployment Manager instead. For more details, please refer to "Appendix H Co-Existence with ServerView Deployment Manager" of the "ServerView Resource Coordinator VE Setup Guide".
- Only the contents of the first disk (boot disk) that were recognized by the managed server's BIOS can be backed up and restored. The contents of other disks (data disks) cannot be backed up and restored. To properly back up and restore such data disks, it is recommended to use dedicated backup software, or the copy function available in storage devices. When the first disk contains multiple partitions (Windows drive, Linux/VMware partition), all partitions are backed up.

Table 8.1 Examples of system image backup and restore targets

Disk	Windows drive name	Is this a target of backup and restore?
First	C:	Yes
	E:	Yes
Second	D:	No
	F:	No

- As the managed server is restarted during backup and restore operations, its applications should be stopped beforehand.
- The first partition must be the boot partition.
- Backup and restore of VM hosts differ depending on the server virtualization software used. For an explanation of the behavior differences that occur when VM guests are included in the VM host's boot disk, refer to "A.3 Functional Differences between Products" in the "ServerView Resource Coordinator VE Setup Guide". If VM guests on the boot disk are not to be backed up (and restored), VM guest files should be moved to another disk.
- To preserve the configuration of the server virtualization software used, VM guests should also be backed up at the time of the VM host's backup. During backup, because the target VM host will be automatically set to VM maintenance mode, the VM host should be in a state that allows for VM maintenance mode to be set.

If the target VM host is in high-availability configuration, all VM guests stored on shared disks should be migrated to another VM host beforehand.

After backing up the VM host, migrate back the VM guests to their original VM host.

Refer to the server virtualization software manual and "A.3 Functional Differences between Products" in the "ServerView Resource Coordinator VE Setup Guide" for information on how to back up and migrate VM guests, or details about the VM maintenance mode.

- To preserve the configuration of the server virtualization software used, the VM guests backed up at the time of the VM host's backup should be restored when restoring a VM host. Note that this is not required if no changes likely to alter the virtualization software configuration were made (e.g. changes such as addition or deletion of a VM guest, or changing the placeholder for VM guest definition files).

During restore, because the target VM host will be automatically set to VM maintenance mode, the VM host should be in a state that allows for VM maintenance mode to be set.

If the target VM host is in a high-availability configuration, all VM guests stored on shared disks should be migrated to another VM host beforehand.

After restoring the VM host, migrate back the VM guests to their original VM host.

Refer to the server virtualization software manual and "A.3 Functional Differences between Products" in the "ServerView Resource Coordinator VE Setup Guide" for information on how to restore and migrate VM guests, or details about the VM maintenance mode.

- Deleting a managed server will delete its backed up system images at the same time.
- It is not possible to backup, restore, or delete a system image from a managed server for which a system image (including different versions) is already being backed up, restored, or deleted.
- When restoring a system image on a server whose name was changed after the deployment of a cloning image, check that the "*Server name*" displayed on the resource tree and the System Image List match the new server name before restoring the system image.
- For servers on which the Watchdog function is enabled, backup or restore operations on that server may be aborted by an automatic restart or shutdown. The Watchdog is a function which automatically restarts or shuts down non-responsive servers when their operating system does not respond for a given period of time.
It is therefore highly recommended to disable the Watchdog function before a backup or restore operation.
Refer to the server manual for details on the Watchdog function.
- If the disk size of the source (backed up) server differs from that of the destination (restored) server, restore is possible only in the case where the disk size on the destination server is larger than that of the source server.

In that case, an unused disk space will remain on the destination server. To use this unused disk space, a partition should first be created from it.

Restoring a system image to a server on which the disk size is smaller than that of the source (backed up) server is not possible. This also applies to server switchover and failback operations that are based on backup and restore, as well as cloning operations.

Therefore, it is also necessary to ensure that spare servers of cloning destination servers have a large enough disk.

8.2 Backing Up System Images

This section explains how to collect a system image backup.

System images can only be backed up from managed servers that are not in "stop" status.

System images can also be backed up using commands.

Refer to "Chapter 4 Image Operations" in the "ServerView Resource Coordinator VE Command Reference" for details.

Backing up a System Image

Use the following procedure to back up a system image from a managed server.

1. Put the target server into maintenance mode and stop all of its applications.
 - a. In the RC console resource tree, right-click the target server (or its physical OS or VM host) and select [Maintenance Mode]-[Set] from the popup menu.
The [Set Maintenance Mode] dialog is displayed.
Because the target server is restarted during backup, all of its applications should be stopped beforehand. When backing up a VM host, all of its VM guests should also be stopped.
 - b. In the confirmation dialog, click the <OK> button.
The target server is put into maintenance mode.

2. Back up a system image from the target server.
 - a. In the RC console resource tree, right-click the target physical OS or VM host and select [Backup/Restore]-[Backup] from the popup menu.

The [Backup] dialog is displayed.
 - b. In the [Backup] dialog, specify the following information.

Comment

Enter a comment to identify the system image.
A comment can be of no more than 128 characters. Percents ("%"), backslashes ("\"), double quotes ("), and linefeed characters are not allowed.

 **Note**

A list of resources that will be powered off during backup is displayed in the [Backup] dialog. Confirm that it is safe to shutdown those resources before continuing with the backup operation.
When backing up a VM host, all of its VM guests will also be stopped.

- c. Click the <OK> button.

The system image is backed up.

After backing up a VM host, stop and back up all of its VM guests.
For details on VM guest backup, refer to the server virtualization software manual.

3. Release the target server from maintenance mode before resuming its applications.
 - a. In the RC console resource tree, right-click the target server (or its physical OS or VM host) and select [Maintenance Mode]-[Release] from the popup menu.

The [Release Maintenance Mode] dialog is displayed.
 - b. Click the <OK> button.

The target server is released from maintenance mode.

 **Note**

- The number of system image versions that can be kept for a managed server is limited.
If a new system image backup is collected while this limit has already been reached, the oldest version will be deleted.
By default, the maximum number of system images is 3.
This limit can be changed by following the instructions given in "6.3.1.3 Changing the Maximum Number of System Image Versions" in the "ServerView Resource Coordinator VE Setup Guide".
- When backing up a new system image, its version number will be increased by one. The version number of the first backed up system image of a managed server will always be 1.
- When backing up a VM host in a high-availability configuration, all VM guests stored on shared disks should be migrated to another VM host beforehand.
During backup, because the target VM host will be automatically set to VM maintenance mode, the VM host should be in a state that allows for VM maintenance mode to be set.
After backing up the VM host, migrate back the VM guests to their original VM host.
Refer to the server virtualization software manual and "A.3 Functional Differences between Products" in the "ServerView Resource Coordinator VE Setup Guide" for information on how to migrate VM guests, or details about the VM maintenance mode.
- When using PRIMERGY GLS for Admin LAN redundancy, a system image backup may fail if the following message is displayed in the event log.

```
FJSVrcx:WARNING:41306:server.NIC takeover on Admin LAN was detected
```

In that case, wait for the following message to show in the event log before performing backup again.

8.3 Restoring System Images

This section explains how to restore a system image backup.

System images can also be restored using commands.

Refer to "Chapter 4 Image Operations" in the "ServerView Resource Coordinator VE Command Reference" for details.

Restoring a System Image

Use the following procedure to restore a system image to a managed server.

1. Put the target server into maintenance mode.
 - a. In the RC console resource tree, right-click the target server (physical server, physical OS or VM host) and select [Maintenance Mode]-[Set] from the popup menu.

The [Set Maintenance Mode] dialog is displayed.

As the target server is restarted during restoration, all of its applications should be stopped beforehand. When restoring a VM host, all of its VM guests should also be stopped.
 - b. Click the <OK> button.

The target server is set to maintenance mode.
2. Restore a system image.
 - To restore the system image from the resource tree:
 - a. In the RC console resource tree, right-click the target server (physical server, physical OS or VM host) and select [Backup/Restore]-[Restore] from the popup menu.

The [Restore] dialog is displayed.
 - b. In the [Restore] dialog, select the system image to restore and click the <OK> button.

The system image is restored.
 - To restore a system image from the [Image List] tab:
 - a. In the RC console, click the [Image List] tab.

The System Image List is displayed.
 - b. In the System Image List right-click the system image to be restored and select [Restore] from the popup menu.

The [Restore] dialog is displayed.
 - c. Click the <OK> button.

The system image is restored.

When restoring a VM host, be sure to also restore the VM guest backups that correspond to the restored VM host backup version.

For details on restoring VM guests, refer to the server virtualization software manual.
3. Release the target server from maintenance mode before resuming its applications.
 - a. In the RC console resource tree, right-click the target server (physical server, physical OS or VM host), and select [Maintenance Mode]-[Release] from the popup menu.

The [Release Maintenance Mode] dialog will be displayed.
 - b. Click the <OK> button.

The target server is released from maintenance mode.

Note

When restoring a VM host in a high-availability configuration (within its virtualization software), all VM guests stored on shared disks should be migrated to another VM host beforehand. The VM host should also be set to maintenance mode within the server virtualization software used before restore.

During restore, because the target VM host will be automatically set to VM maintenance mode, the VM host should be in a state that allows for VM maintenance mode to be set.

After restoring the VM host, migrate back the VM guests to their original VM host.

Refer to the server virtualization software manual and "A.3 Functional Differences between Products" in the "ServerView Resource Coordinator VE Setup Guide" for information on how to migrate VM guests, or details about the VM maintenance mode.

8.4 Viewing System Images

This section explains how to browse and view existing system image backups.

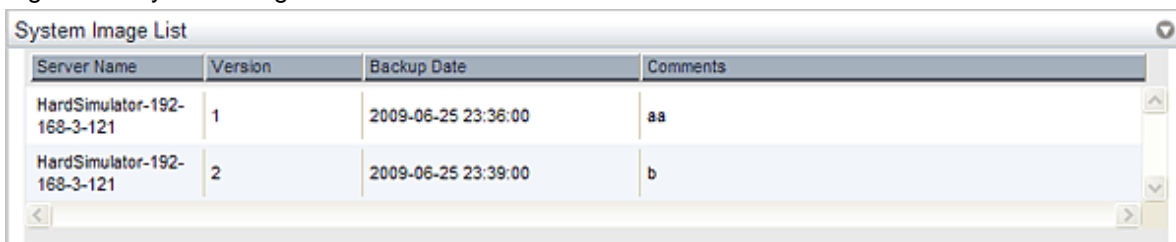
System images can also be listed using commands.

Refer to "Chapter 4 Image Operations" in the "ServerView Resource Coordinator VE Command Reference" for details.

In the RC console, select the [Image List] tab.

The System Image List is displayed.

Figure 8.1 System Image List



Server Name	Version	Backup Date	Comments
HardSimulator-192-168-3-121	1	2009-06-25 23:36:00	aa
HardSimulator-192-168-3-121	2	2009-06-25 23:39:00	b

Refer to "2.5.4 [Image List] tab" in the "ServerView Resource Coordinator VE Setup Guide" for details on the System Image List.

To view the most recent system image backup of a managed server, select a server OS from the resource tree and click the [Resource Details] tab.

The latest system image backup taken from the selected server is displayed under "Latest System Image".

Refer to "2.5.2 [Resource Details] tab" in the "ServerView Resource Coordinator VE Setup Guide" for details.

8.5 Deleting a System Image

This section explains how to delete system image backups.

System images can also be deleted using commands.

Refer to "Chapter 4 Image Operations" in the "ServerView Resource Coordinator VE Command Reference" for details.

Deleting System Images

Use the following procedure to delete a system image.

1. In the RC console, select the [Image List] tab.

The System Image List is displayed.

2. In the System Image List, right-click the system image to delete and select [Delete] from the popup menu.

The confirm dialog is displayed.

3. Click the <OK> button.

The selected system image is deleted.

 Note

.....
A system image cannot be recovered once it has been deleted.
.....

Chapter 9 Hardware Maintenance

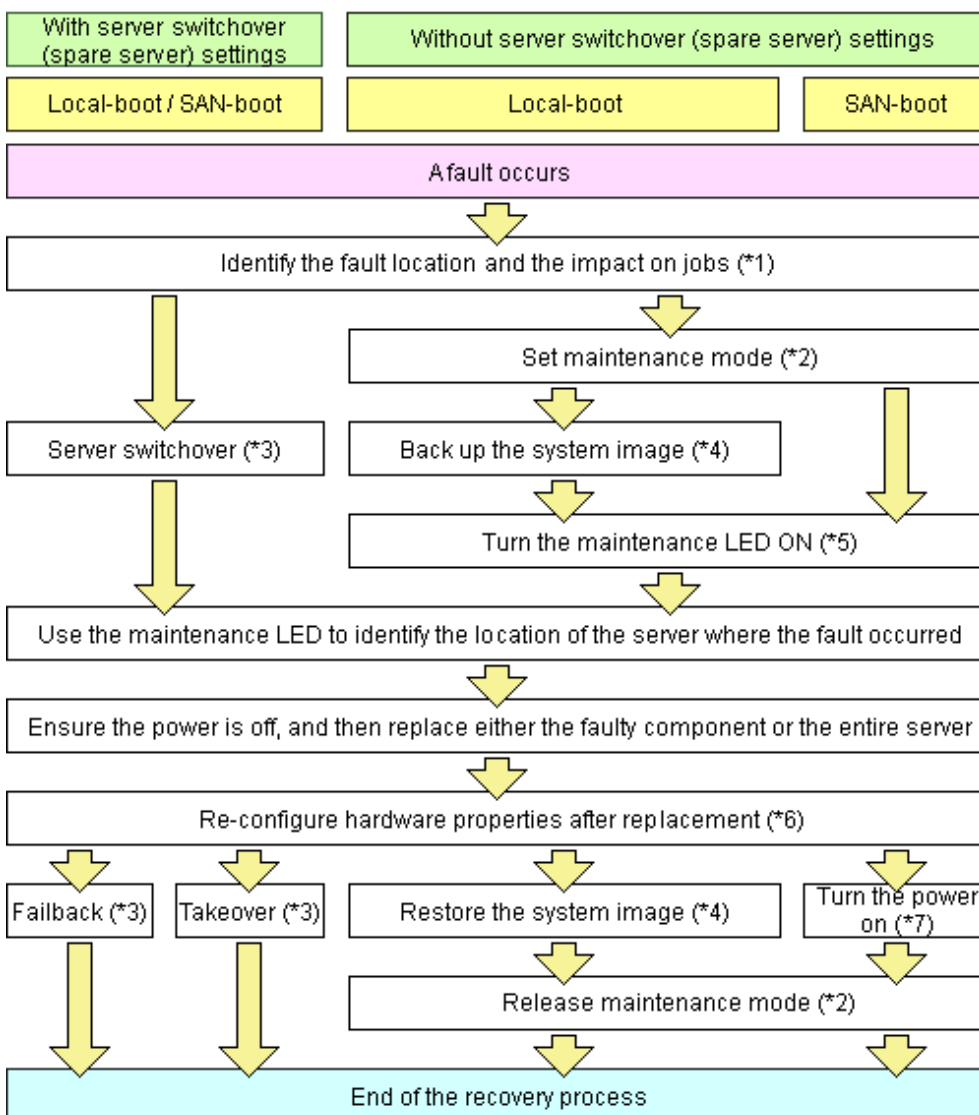
This chapter explains how to perform hardware maintenance.

9.1 Overview

This section explains how to perform maintenance on the hardware devices managed by Resource Coordinator VE.

The following flowchart shows the procedure for maintaining hardware when failures occur on registered servers.

Figure 9.1 Hardware maintenance flow



*1: Refer to "5.3 Addressing Resource Failures" for details on how to identify failures.

*2: Refer to "Appendix F Maintenance Mode" of the "ServerView Resource Coordinator VE Setup Guide" for details on how to set and release maintenance mode settings.

*3: Refer to "Chapter 10 Server Switchover" for details on server switchover, failback or takeover.

*4: Refer to "Chapter 8 Backup and Restore" for details on backing up and restoring system images.

*5: Refer to "9.2 Maintenance LEDs" for details on maintenance LED operations. However, maintenance LED operations are only supported for PRIMERGY BX servers.

*6: Refer to "9.3 Re-configuring Hardware Properties" for details on re-configuring hardware properties.

*7: Refer to "Chapter 6 Power Control" for details on power control.

The following hardware replacements can be performed:

- Replacing servers

Replace a server that has been registered in Resource Coordinator VE.
For details on replacing servers, refer to "9.4 Replacing Servers".

- Replacing server components

Replace hardware parts (such as an NIC, HBA or the hard disk) of a registered server.
For details on replacing server parts, refer to "9.5 Replacing Server Components".

- Replacing non-server hardware

Replace registered chassis, management blades or any other hardware components external to servers.
For details on replacing non-server hardware, refer to "9.6 Replacing Non-server Hardware".

9.2 Maintenance LEDs

This section explains how to operate maintenance LEDs.

Activating a server blade's maintenance LED make it easy to identify a server from others. When replacing servers, it is recommended to use this function to identify which server should be replaced.

To activate the maintenance LED of a managed server running either a physical OS or a VM host, the server should be put into maintenance mode first.

Refer to "Appendix F Maintenance Mode" of the "ServerView Resource Coordinator VE Setup Guide" for information on maintenance mode.

Note

- Maintenance LED control is only available for PRIMERGY BX servers. The actual LED used as an identification LED differs between server models.
 - For PRIMERGY BX600 servers, the power LED is used (blinks when activated).
 - For PRIMERGY BX900 servers, the ID indicator is used (lighted when activated).
- If SNMP agent settings within the management blade configuration are incorrect, maintenance LED operations in Resource Coordinator VE will end successfully, but the state of the identification LED will not change. SNMP agent settings should be set according to the instructions given in to "3.5 Configuring the Server Environment" in the "ServerView Resource Coordinator VE Setup Guide".

Activate a maintenance LED

Use the following procedure to activate a server blade's maintenance LED.

1. In the RC console resource tree, right-click the target server, and from the popup menu select [LED]-[ON].

The [Turning on maintenance LED] dialog is displayed.

2. Click the <OK> button.

Selecting the "Automatically turn off" checkbox will automatically shut down the server after activating its maintenance LED.

Note

Once the maintenance LED of a server blade is activated, new errors detected in that server cannot be checked from its LED anymore. Check the server status directly from the RC console.

Deactivate a maintenance LED

Use the following procedure to deactivate a server blade's maintenance LED.

1. In the RC console resource tree, right-click the target server, and from the popup menu, select [LED]-[OFF].

A confirmation dialog is displayed.

2. In the confirmation dialog, click the <OK> button.

The maintenance LED is turned off.

9.3 Re-configuring Hardware Properties

This section explains how to re-configure hardware properties from replaced hardware.

After hardware replacement, it is necessary to re-configure Resource Coordinator VE with the new hardware properties.



- Ensure this operation is performed only after the replacement of one of the following: the server itself, the NIC used either for the admin or public LAN, or the HBA.
If not, there is a possibility that operations on the server will not run correctly.
- After replacing the hardware, the server status becomes "unknown". The appropriate status can be restored by re-configuring the hardware properties from the server.

Preconditions

The following preconditions must be satisfied before this operation can be performed:

- Both the replaced server and replacement server must be the same model.
A warning message is shown if the model of the replacement server differs from that of the replaced server.
- When replacing a PRIMERGY BX server, the replacement server must be inserted into the same slot as the server that is being replaced.
Hardware properties cannot be re-configured from a server inserted in a different slot. An error occurs if no server is inserted in the slot occupied by the previous server.

To move a server to a different slot within the chassis, that server must be deleted first, then registered again after being inserted in its new slot.

Re-configuring Hardware Properties following a Server Replacement

- For PRIMERGY BX servers

Use the following procedure to re-configure properties from replaced hardware.

1. After hardware replacement, insert the server and check that the following message is displayed in the event log.

Server blade added

2. After approximately 30 seconds, right-click the target server in the RC console resource tree, and select [Hardware Maintenance]-[Re-configure] from the popup menu.

The [Re-configure Hardware Properties] dialog is displayed.

3. Click the <OK> button.

The original hardware properties of the selected managed server are updated with new hardware properties obtained from the replacement server. If the maintenance LED is on it will be turned off automatically.

- For rack-mount or tower servers

Use the following procedure to re-configure properties from replaced hardware.

1. If an Agent was already registered, power on the server.
2. In the RC console resource tree, right-click the target server and select [Hardware Maintenance]-[Re-configure] from the popup menu.

The [Re-configure Hardware Properties] dialog is displayed.

3. Enter MAC addresses for the network interfaces used on the Admin LAN.

This step can be skipped if no network interface was replaced.

- MAC address (NIC1) under Admin LAN

This item is not required if an Agent was already registered.

- MAC address (NIC2) under SAN Boot/Admin LAN Redundancy

This item is only required for the following cases.

- When using the HBA address rename setup service.
- When using GLS for Admin LAN redundancy on the target server.
- For the spare server of a server using Admin LAN redundancy.

4. Click the <OK> button.

The original hardware properties of the selected managed server are updated with new hardware properties obtained from the replacement server.

9.4 Replacing Servers

This section details the procedure to follow when replacing servers.



Follow the same procedure when replacing servers where VM hosts are running.

For PRIMERGY BX servers

- Replacing a server assigned with spare servers

Use the following procedure to switch applications over to a spare server and replace a server with minimal interruption.

1. Perform server switchover

Switch over the server to replace with its spare server.

Refer to "[Chapter 10 Server Switchover](#)" for details on the switchover function.

After the server has been switched over, its maintenance LED is automatically activated, and the server is powered down.

2. Replace the server

Replace the server whose maintenance LED is activated.

Change the BIOS settings of the replacement server to match the operating environment.

Refer to "3.5 Configuring the Server Environment" of the "ServerView Resource Coordinator VE Setup Guide" for details on BIOS settings.

Shut down the server after completing BIOS settings.

3. Re-configure hardware properties following replacement

After replacing the server, re-configure Resource Coordinator VE with the latest hardware properties.

Refer to "[9.3 Re-configuring Hardware Properties](#)" for details on how to re-configure hardware properties.

After hardware properties have been re-configured, the maintenance LED is automatically turned off in the RC console.

4. Perform post-switchover operations

Refer to "[10.3 Post-Switchover Operations](#)" and carry out the operations that must be performed after a server switchover.

• Replacing a server with no spare server assigned

Use the following procedure to smoothly replace a server and resume its applications.

1. Put the target server into maintenance mode

Put the primary server to replace into maintenance mode.

Refer to "Appendix F Maintenance Mode" of the "ServerView Resource Coordinator VE Setup Guide" for details on the maintenance mode.

2. Collect a system image backup

For local boot servers, collect a system image backup when possible.

Refer to "[Chapter 8 Backup and Restore](#)" for details and conditions of system image backups.

In a SAN boot environment, the boot disk can be restored without having to back up and restore a system image.

3. Activate the maintenance LED

Activate the maintenance LED on the server that is to be replaced before shutting it down.

Refer to "[9.2 Maintenance LEDs](#)" for details on how to activate maintenance LEDs.

4. Replace the server

Replace the server whose maintenance LED is activated.

Change the BIOS settings of the replacement server to match the operating environment.

Refer to "3.5 Configuring the Server Environment" of the "ServerView Resource Coordinator VE Setup Guide" for details on BIOS settings.

Shut down the server after completing BIOS settings.

5. Re-configure hardware properties following replacement

After replacing the server, update Resource Coordinator VE with the latest hardware properties.

Refer to "[9.3 Re-configuring Hardware Properties](#)" for details on how to re-configure hardware properties.

After hardware properties have been re-configured, the maintenance LED is automatically turned off in the RC console.

6. Restore the boot disk

- Local boot

There is no need to restore the boot disk if the original disk is installed on the replaced server. Simply power on the replacement server.

Otherwise, if a system image backup was taken, restore that backup.

Refer to "[8.3 Restoring System Images](#)" for details on how to restore a system image. After the system image is restored, the server will be automatically powered on.

If a backup of the system image does not exist, run the installation program again.

- SAN boot

The replaced server can be easily configured to access the original boot disk using I/O virtualization. Therefore, there is no need to restore the boot disk. Simply power on the replacement server.

7. Release maintenance mode

Release the replaced server from maintenance mode.

Refer to "Appendix F Maintenance Mode" of the "ServerView Resource Coordinator VE Setup Guide" for details on maintenance mode.

- Servers with no Agent registered

Use the following procedure to replace servers on which the Resource Coordinator VE Agent was not registered.

1. Activate the maintenance LED

Activate the maintenance LED on the server that is to be replaced. Shut down the server if it is still powered on.
Refer to "[9.2 Maintenance LEDs](#)" for details on how to activate maintenance LEDs.

2. Replace the server

Replace the server whose maintenance LED is activated.

Change the BIOS settings of the replacement server to match the operating environment.

Refer to "3.5 Configuring the Server Environment" of the "ServerView Resource Coordinator VE Setup Guide" for details on BIOS settings.

Shut down the server after completing BIOS settings.

3. Re-configure hardware properties following replacement

After replacing the server, update Resource Coordinator VE with the latest hardware properties.

Refer to "[9.3 Re-configuring Hardware Properties](#)" for details on how to re-configure hardware properties.

After hardware properties have been re-configured, the maintenance LED is automatically turned off in the RC console.

For Rack-Mount and Tower Servers

- Replacing a server assigned with spare servers

Use the following procedure to switch applications over to a spare server and replace a server with minimal interruption.

1. Perform server switchover

Switch over the server to replace with its spare server.

Refer to "[Chapter 10 Server Switchover](#)" for details on the switchover function.

The server to replace is automatically powered off after switchover.

2. Replace the server

Replace the target server.

Change the BIOS settings of the replacement server to match the operating environment.

Refer to "3.5 Configuring the Server Environment" of the "ServerView Resource Coordinator VE Setup Guide" for details on BIOS settings.

Shut down the server after completing BIOS settings.

Configure the remote management controller of the replacement server with the same IP address, user name, password and SNMP trap destination as those set on the original server.

3. Re-configure hardware properties following replacement

After replacing the server, re-configure Resource Coordinator VE with the latest hardware properties.

Refer to "[9.3 Re-configuring Hardware Properties](#)" for details on how to re-configure hardware properties.

4. Perform post-switchover operations

Refer to "[10.3 Post-Switchover Operations](#)" and carry out the operations that must be performed after a server switchover.

- Replacing a server with no spare server assigned

Use the following procedure to smoothly replace a server and resume its applications.

1. Put the target server into maintenance mode

Put the primary server to replace into maintenance mode.

Refer to "Appendix F Maintenance Mode" of the "ServerView Resource Coordinator VE Setup Guide" for details on maintenance mode.

2. Create a system image backup

For local boot servers, create a system image backup when possible.

Refer to "[Chapter 8 Backup and Restore](#)" for details and conditions of system image backups.

In a SAN boot environment, the boot disk can be restored without having to back up and restore a system image.

3. Shut down the server

Shut down the server to replace if it is still powered on.

Refer to "[Chapter 6 Power Control](#)" for details on shutting down servers.

4. Replace the server

Replace the target server.

Change the BIOS settings of the replacement server to match the operating environment.

Refer to "3.5 Configuring the Server Environment" of the "ServerView Resource Coordinator VE Setup Guide" for details on BIOS settings.

Shut down the server after completing BIOS settings.

Configure the remote management controller of the replacement server with the same IP address, user name, password and SNMP trap destination as those set on the original server.

5. Re-configure hardware properties following replacement

After replacing the server, update Resource Coordinator VE with the latest hardware properties.

Refer to "[9.3 Re-configuring Hardware Properties](#)" for details on how to re-configure hardware properties.

6. Restore the boot disk

- Local boot

There is no need to restore the boot disk if the original disk is installed on the replaced server. Simply power on the replacement server.

Otherwise, if a system image backup was taken, restore that backup.

Refer to "[8.3 Restoring System Images](#)" for details on how to restore a system image. After the system image is restored, the server will be automatically powered on.

If a backup of the system image does not exist, run the installation program again.

- SAN boot

The replaced server can be easily configured to access the original boot disk using HBA address rename. Therefore, there is no need to restore the boot disk. Simply power on the replacement server.

7. Release maintenance mode

Release the replaced server from maintenance mode.

Refer to "Appendix F Maintenance Mode" of the "ServerView Resource Coordinator VE Setup Guide" for details on maintenance mode.

• Servers with no Agent registered

Use the following procedure to replace servers on which the Resource Coordinator VE Agent was not registered.

1. Shut down the server

Shut down the server to replace if it is still powered on.

Refer to "[Chapter 6 Power Control](#)" for details on shutting down servers.

2. Replace the server

Replace the target server.

Change the BIOS settings of the replacement server to match the operating environment.

Refer to "3.5 Configuring the Server Environment" of the "ServerView Resource Coordinator VE Setup Guide" for details on BIOS settings.

Shut down the server after completing BIOS settings.

Configure the remote management controller of the replacement server with the same IP address, user name, password and SNMP trap destination as those set on the original server.

3. Re-configure hardware properties following replacement

After replacing the server, update Resource Coordinator VE with the latest hardware properties.

Refer to "[9.3 Re-configuring Hardware Properties](#)" for details on how to re-configure hardware properties.

For SPARC Enterprise Servers

No specific action is required in Resource Coordinator VE.

9.5 Replacing Server Components

This section explains how to replace server components.

• Replacing a network interface

The procedure used to replace a network interface is the same as that described in "9.4 Replacing Servers".

Refer to "9.4 Replacing Servers" for details.

If the target server is running Red Hat Enterprise Linux 5 or Citrix XenServer, log in with administrative privileges on the server and run the following command (this should be performed after completing the steps described in "[9.4 Replacing Servers](#)").

```
# /usr/local/sbin/macbindconfig update <RETURN>
```

[Xen]

When using Citrix XenServer, login from the console and run the following command. After running the command, reinstall XenServer referring to the manual for Citrix XenServer.

```
# /usr/local/sbin/macbindconfig update <RETURN>
```

When using Red Hat Enterprise Linux 5 Virtualization (Xen-Based), perform the following procedure.

1. Execute the following command to temporarily disable automatic startup of the xend daemon then restart the managed server.

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

2. Once the server has restarted, execute the following commands to update MAC address bindings, re-enable automatic startup of the xend daemon, and restart the xend daemon itself.

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

• Replacing an HBA

The procedure used to replace an HBA is the same as that described in "9.4 Replacing Servers".

Refer to "[9.4 Replacing Servers](#)" for details.

When using I/O virtualization, the replacement HBA will automatically inherit the WWN originally set on the replaced HBA. Therefore, there is no need to re-configure access paths on the storage side.

• Replacing a boot disk (in local-boot environments)

Use the following procedure to replace a boot disk.

1. Replace the faulty boot disk with a new one.
2. If a backup of the original boot disk was taken, restore it to the new replacement disk.



The backup and restore functions available in Resource Coordinator VE can be used to restore the boot disk contents.

Refer to "[Chapter 8 Backup and Restore](#)" for details.

- **Replacing other server components**

No specific action is required in Resource Coordinator VE when replacing onboard server components like memory modules or other parts.

9.6 Replacing Non-server Hardware

This section explains how to replace hardware external to servers.

- **Replacing a chassis**

No specific action is required in Resource Coordinator VE.

- **Replacing a management blade**

No specific action is required in Resource Coordinator VE.

- **Replacing a LAN switch blade**

No specific action is required for PRIMERGY BX900 LAN switch blades.

For other PRIMERGY BX models, replacing a LAN switch blade requires restoring the VLAN settings that were previously applied to it via Resource Coordinator VE.

Use the following procedure to replace a LAN switch blade.

1. Replace the faulty LAN switch blade.
2. Restore the LAN switch blade configuration backup (which includes various settings) to the new LAN switch blade.

If the LAN switch blade configuration has not been backed up yet, it has to be restored by configuring each setting (except VLAN settings) to the same values as those set during the initial installation.

Refer to the manual of the LAN switch blade used for details on how to back up and restore LAN switch blade configurations.

3. Update the new LAN switch blade with the latest VLAN settings configured in Resource Coordinator VE.
 - a. In the RC console resource tree, right-click the target LAN switch blade, and from the popup menu, select [Restore].
The [Restore LAN switch] dialog is displayed.
 - b. Click the <OK> button.
VLAN settings are applied to the specified LAN switch blade.



Note

To replace LAN switch blades with different models, first delete the LAN switch blade that is registered, and then register the replacement LAN switch blade.

After the LAN switch blade is registered, the VLAN settings must be configured for the internal and external ports.

For details on the VLAN settings, refer to "6.2.1 Configuring VLANs on LAN Switches" in the "ServerView Resource Coordinator VE Setup Guide".

For PRIMERGY BX900 LAN switch blades, changing the operating mode (switch mode or IBP mode) doesn't require any specific action in Resource Coordinator VE.

- **Replacing a Fibre Channel switch blade**

No specific action is required in Resource Coordinator VE.

- **Replacing a power monitoring device (PDU or UPS)**

After replacing a power monitoring device, re-configure the power monitoring device's (PDU or UPS) hardware properties.

Use the following procedure to replace a power monitoring device.

1. Replace the faulty power monitoring device.
2. Set the Admin LAN IP address and SNMP community on the replacement device to the same values as those that were set on the faulty device.

3. Re-configure the power monitoring device's hardware properties.

- a. In the RC console resource tree right-click the target power monitoring device (PDU or UPS), and from the popup menu, select [Hardware Maintenance]-[Re-configure].

The [Re-configure Hardware Properties] dialog is displayed.

- b. Click the <OK> button.

The target power monitoring device's hardware properties are re-configured.

• **Replacing a storage blade**

No specific action is required in Resource Coordinator VE when replacing a storage blade that does not contain the boot disk of a server blade.

Use the following procedure to replace a storage blade that contains the boot disk of a server blade.

1. Replace the storage blade.
2. Insert the server blade's boot disk in the new storage blade.
3. If the boot disk's content was backed up, restore it.

 **Information**

.....
The backup and restore functions provided by Resource Coordinator VE can be used to restore the boot disk's content.

Refer to "[Chapter 8 Backup and Restore](#)" for details.
.....

• **Replacing a LAN switch**

No specific action is required in Resource Coordinator VE when replacing a LAN switch.

Chapter 10 Server Switchover

This chapter explains how to use the server switchover function.

10.1 Overview

Server switchover is a function that enables applications to be switched over to and restarted on a pre-assigned spare server when a primary server fails or needs to be shut down for maintenance.

Server switchover is the basis for the Auto-Recovery function, which is able to automatically switch over applications to a spare server upon failure.

Server switchover settings should be configured before using the server switchover function.

Refer to "Chapter 9 Server Switchover Settings" of the "ServerView Resource Coordinator VE Setup Guide" for details on server switchover settings and an overview of the server switchover function.



- If ServerView Deployment Manager is used on the Admin LAN, server switchover is not available for local-boot servers or SAN-boot servers without a VIOM profile. For more details, please refer to "Appendix H Co-Existence with ServerView Deployment Manager" of the "ServerView Resource Coordinator VE Setup Guide".
- **When the switchover method is backup and restore**
When backing up or restoring system images, or collecting or deploying cloning images, no more than four processes can be executed simultaneously. If four processes are already executing, any system image restore triggered by a switchover or failback operation will enter a wait state. Any process put under wait state will be resumed after one of the already running processes completes.

10.2 Switchover

A server switchover can be triggered either manually from the user, or automatically with the Auto-Recovery function.

Regardless of what action triggered a switchover, the user must decide whether to switch back applications to their original server (failback), or let the spare server indefinitely take over those applications (takeover). Choosing takeover will result in the spare server becoming the new active server.

Refer to "[10.3 Post-Switchover Operations](#)" for details.

Different switchover methods are available according to each server's hardware configuration. Refer to the "Note" in "1.2 Hardware Environment" of the "ServerView Resource Coordinator VE Installation Guide" for details.



- During switchover, server restarts and configuration changes may trigger SNMP Traps (which are shown in the Event Log). For details, refer to "Chapter 1 Resource Coordinator VE Messages" of the "ServerView Resource Coordinator VE Messages".
- When using the backup and restore switchover method, do not start up the original primary server during or after the switchover operation.
The primary server and spare server both run the same system image. Having the two servers running together will cause conflicts of IP addresses and other information. This can adversely affect the applications recovered on the spare server.
If it becomes necessary to start the primary server, for maintenance or other tasks, ensure that it does not start up from the same system image as that of the spare server. This can be done by turning off the spare server first, or by stopping the primary server at its BIOS screen (before startup of the OS).
- When using PRIMERGY BX servers, the maintenance LED of a switched over server is automatically activated.

Auto-Recovery

By enabling Auto-Recovery in the spare server settings of a server, it will be automatically switched over to a spare server when its status changes to either "error" or "fatal", and no response is obtained from its OS.

Manual Switchover

Use the following procedure to manually switch over applications from a primary server to a spare server.

Manual switchover can be either performed at will when necessary, or to verify that the switchover process operates properly.

Refer to "Conditions for Server Switchover" in "9.3 Server Switchover Conditions" of the "ServerView Resource Coordinator VE Setup Guide" for details on the conditions for a server switchover.

1. In the RC console's resource tree, right-click the physical OS or VM host to be switched, and from the popup menu select [Spare Server]-[Switchover].

The [Execute Switchover Operation] dialog is displayed.

2. Select the switchover destination server.

If "Automatic allocation" is selected, the switchover destination server is automatically selected.

3. Click the <OK> button.

The primary server stops, and the physical OS or VM host starts on the spare server.



Information

Manual switchover can be performed regardless of the status of the primary server.

10.3 Post-Switchover Operations

After a switchover was performed (either manually or automatically), perform either one of the following post-switchover recovery procedures.

Refer to "[Chapter 9 Hardware Maintenance](#)" for details on how to replace hardware.

- Server failback procedure
 1. Replace failed server hardware
 2. Perform a "Failback" operation to return to a pre-switchover configuration.

- Server takeover procedure

Perform the following two operations.

- Replace failed server hardware
- Perform a "Takeover" operation to keep the configuration created by a server switchover.



Information

For a server takeover procedure, server hardware can be replaced either before or after the "Takeover" operation.

Failback

Use the following procedure to return to a pre-switchover configuration.

Refer to "Conditions for Server Failback" in "9.3 Server Switchover Conditions" of the "ServerView Resource Coordinator VE Setup Guide" for details on the conditions for a server failback.

1. In the RC console's resource tree, right-click the physical OS or VM host that was switched over to the spare server, and from the popup menu select [Spare Server]-[Failback].

The [Server recovery Failback] dialog is displayed.

2. Click the <OK> button.

The spare server is stopped and the server OS is switched back to the primary server. The primary server finally starts up and resumes its applications.

Note

- When using the backup and restore switchover method, do not start up the original spare server during or after the failback operation.
The primary server and spare server both run the same system image. Having the two servers running together will cause conflicts of IP addresses and other information. This can adversely affect the applications switched back to the spare server.
If it becomes necessary to start the spare server, for maintenance or other tasks, ensure that it does not start up from the same system image as that of the primary server. This can be done by turning off the primary server first, or by stopping the spare server at its BIOS screen (before startup of the OS).
- When using the backup and restore switchover method, and newly generated data on the spare server needs to be transferred to the primary server, back up the spare server before performing the failback.
Refer to "[Backing up a System Image](#)" in "8.2 Backing Up System Images" and apply the backup instructions to the spare server.
Unless there is a need to keep the data that was generated on the spare server while active, backup of the spare server can be skipped. In that case, a system image backed up prior to failure will be restored to the primary server.
- When using PRIMERGY BX servers, the maintenance LED of a primary server is automatically deactivated after a server failback.

Takeover

Use the following procedure to keep the configuration created by a server switchover:

1. In the RC console's resource tree, right-click the physical OS or VM host that was switched over to the spare server, and from the popup menu select [Spare Server]-[Takeover].

The [Takeover] dialog is displayed.

2. Click the <OK> button.

The spare server continues operating as the primary server and the server that functioned as the primary server before switchover becomes a spare server.

If the spare server was originally shared by multiple primary servers, all those servers will now use the original primary server as their spare server.



Example

1. Status before switchover

Application 1: Server A (active) - Server B (spare)

Application 2: Server C (active) - Server B (spare)

2. Status after a fault in Server A triggered a switchover of Application 1

Application 1: Server A (fault) - Server B (active)

Application 2: Server C (active) - Server B (*1)

3. Status after replacing server A and letting Server B take over Application 1

Application 1: Server B (active) - Server A (spare)

Application 2: Server C (active) - Server A (spare)

*1: At this point, manual switchover or automatic recovery from server C to server B becomes impossible.

 Note

Once server switchover has taken place, Auto-Recovery and manual server switchover cannot be performed until either failback or takeover has been executed.

Perform either failback or takeover to enable switchover to be performed again.

Chapter 11 Maintaining Software with Cloning [Windows/Linux]

This chapter explains how to perform software maintenance using server cloning.

11.1 Overview

Cloning servers allows users to apply patches, install or modify installed software on a managed server before propagating those changes to other servers.

After performing necessary maintenance tasks on one managed server, a cloning image can be collected from that server and deployed to other servers. This minimizes the time required for the software maintenance of multiple managed servers while preventing operation mistakes.

Using the network parameter auto-configuration function also enables automatic configuration of Public LAN settings for each cloned server. This is done by actually re-configuring the network interfaces used for the Public LAN following deployment of a cloning image.

Refer to "Chapter 8 Cloning [Windows/Linux]" of the "ServerView Resource Coordinator VE Setup Guide" for details on the cloning function.



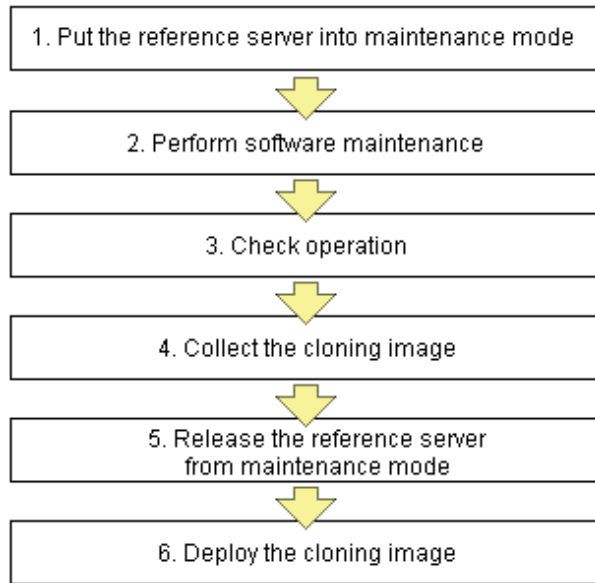
- This function is disabled if ServerView Deployment Manager is used on the Admin LAN. Use the cloning function available in ServerView Deployment Manager instead. For more details, please refer to "Appendix H Co-Existence with ServerView Deployment Manager" of the "ServerView Resource Coordinator VE Setup Guide".
 - Software maintenance tasks performed using the cloning function only apply to servers that share the same hardware and software configuration.
 - Deployment of a cloning image will reset the VLAN settings used for the public LAN of each target server. Those settings should be restored either manually or automatically using the network parameter auto-setup function.
 - The following data will also be reset on the servers to which a cloning image is deployed. If necessary, this data should be manually backed up (copied) before deployment, and restore once complete.
 - OS system logs
 - Application settings and logs
 - This function is not available for servers running a SUSE Linux Enterprise Server operating system.
-

11.2 Software Maintenance Procedure

This section describes how to perform maintenance operations on managed servers.

Maintenance operations should be performed first on one reference server before propagating changes to the remaining target servers.

Figure 11.1 Software maintenance procedure using cloning



Each of these steps is explained below.

1. Put the reference server into maintenance mode

Be sure to stop all applications on the target server before continuing.

In the RC console resource tree, right-click the target server (or physical OS or VM host) to put into maintenance mode, and select [Maintenance Mode]-[Set] from the popup menu.

Refer to "Appendix F Maintenance Mode" in the "ServerView Resource Coordinator VE Setup Guide" for details on maintenance mode.

2. Perform software maintenance

Perform the necessary software maintenance tasks (patch application, software addition or modification) on the reference server.

3. Check operation

After completion of maintenance tasks, confirm that the OS and applications still operate properly to validate the changes made during maintenance.

4. Collect the cloning image

Once all changes have been validated, collect a cloning image from the reference server.

Refer to "8.2 Collecting a Cloning Image" in the "ServerView Resource Coordinator VE Setup Guide" for details on how to collect cloning images.

5. Release the reference server from maintenance mode

In the RC console resource tree, right-click the server (or physical OS or VM host on the server) to be released from maintenance mode, and from the popup menu, select [Maintenance Mode]-[Release].

Refer to "Appendix F Maintenance Mode" in the "ServerView Resource Coordinator VE Setup Guide" for details on the maintenance mode.

6. Deploy the cloning image

Propagate the changes made during maintenance by deploying the cloning image collected in step 4. to the remaining target servers.

Refer to "8.3 Deploying a Cloning Image" in the "ServerView Resource Coordinator VE Setup Guide" for details on how to deploy cloning images.

Chapter 12 Network Map

This chapter provides an overview of the Network Map and describes its features.

12.1 Overview

The Network Map displays the following information for resources managed in Resource Coordinator VE.

- Network configuration of physical and virtual servers (including virtual switches and VM guests)
- Statuses of network links between all resources
- VLAN configuration affecting each physical and virtual server

Two different maps (listed below) are available within the Network Map. Switch between those maps as necessary.

- Overall map

Displays chassis, servers and their connections (network links) with adjacent LAN switches.

- Local map

Shows a more detailed map focused on the selected resource (chassis or server). This map displays resources contained in the selected resource (e.g. server blades, switch blades, VM hosts, VM guests, virtual switches), and their connections (links) with adjacent LAN switches or chassis. Up to two chassis can be displayed at a time.

In the Network Map, resource icons are used to represent the status of each resource. Moreover, different colors are used to represent different link statuses.



See

For details on resource icons, refer to "[12.4 Resource Icons](#)".

For details on link statuses, refer to "[12.5 Network Links](#)".



Note

While the Network Map can display the connections between virtual servers and virtual switches in a virtualization host, it can not show the bridge connections made to directly link virtual servers with external networks.

The following actions are available in the Network Map.

- Switch between map types
- Screen scrolling
 - Scroll button
 - Map drag and drop
 - Navigation map drag and drop
- Maximize or minimize the display area
- Hide the navigation map
- Hide display filter options
- Show or hide the following information
 - Resource descriptions
 - Network links
 - VLANs

- Reset to initial display
- Highlight a selected resource
- Show or hide details for the following resources
 - Servers (including VM hosts)
 - LAN switches
 - VM guests
 - Virtual switches

12.2 Preparations

The following preparations are required to add display content into the Network Map.

1. Register LAN switches (switch blades included in a chassis or external switches)

Refer to "6.1.4 Registering LAN Switches" in the "ServerView Resource Coordinator VE Setup Guide".
The following LAN switches are supported by the Network Map.

- BX600 GbE Switch Blade 30/12
 - PY CB Eth Switch/IBP 1Gb 36/12
 - PY CB Eth Switch/IBP 1Gb 36/8+2
 - Cisco Catalyst 2950 series
 - Cisco Catalyst 2960 series
 - Cisco Catalyst 3560 series
 - Cisco Catalyst 3750 series
2. Detect physical network links
 - a. From the RC console's menu, select [Tools]-[Topology]-[Detect physical links].
 - b. Click the <OK> button in the [Detect Physical Links] dialog.

Note

- If no switch blade is registered yet, only network links between external LAN switches will be displayed. If only one external switch is registered, no links will be displayed at all.
- If a non-supported LAN switch is registered, links may not be properly displayed for that switch.
- The Network Map cannot display links between the following switch models: BX600 GbE Switch Blade 30/12 and PY CB Eth Switch/IBP 1Gb (PY CB Eth Switch/IBP 1Gb 36/12 or PY CB Eth Switch/IBP 1Gb 36/8+2).
- Links between two supported LAN switches may not display properly if an un-registered or un-supported LAN switch was placed between them.

Example

In such a case, the following inconsistencies may be displayed. A LAN switch port maybe seen as being connected to multiple switches (multiple links are shown attached to that switch port).

12.3 Screen Layout

This section describes the Network Map's layout.

The main part of the Network Map is the network view.

12.3.1 Network Map Layout

Network view

Shows the statuses of registered resources and the network links between them.

Map selection area

Provides buttons to select which map to display (overall map or local map).

Scroll button

Scrolls the network view into the selected direction (up, down, left or right).

Reset button

Resets the network view to its initial display.

Magnification slider

Maximizes or minimizes the network view.

Display filter area

Provides checkboxes to select what information to display in the network view.

Map navigation area

Shows a zoomed-out version of the selected map (including items which are too far away to be displayed in the network view).

VLAN display area

Displays the VLAN ID selected in the VLAN tree.

12.3.2 Map Types

This sections details the different types of map available.

Overall map

The overall map displays links between chassis, servers and adjacent LAN switches for all the resources managed in Resource Coordinator VE.

Local map button

Selecting a resource icon in the network view will show a button on the upper-right side of this icon. Clicking this button will show the local map.



.....
The local map and overall map buttons in the map selection area (located on the upper side of the screen) are initially disabled. Selecting a chassis in the network view will enable them.
.....

Local map

The local map displays all resources contained in the selected resource, as well as their connections (network links) with other resources.



-
- Up to two chassis can be expanded in the local map.
 - When two chassis are already expanded, expanding a new one will close the chassis that was expanded first.
-

Selecting a chassis will show all server blades, VM hosts, VM guests, virtual switches and LAN switch blades contained in that chassis, as well as the external LAN switches connected to its switch blades, and the chassis that are in turn connected to those external switches. All links between such resources are also included in the display.

Selecting a server will show all its network interfaces, as well as (for VM hosts) all VM guests, virtual switches and ports contained in that server. Network links are also included in the display.

Selecting a LAN switch blade will show all its ports. For PRIMERGY BX900 LAN switch blades operating in IBP mode, a list of port group is displayed. Selecting a port group from the list will highlight (in blue color) the ports belonging to the selected port group. Moreover, selecting a port from a switch in IBP mode will show a list of port groups to which the selected port belongs. If the selected port belongs to more than one port group, all port groups are shown in the displayed list.

Expand button

Selecting a server blade, switch blade, VM server, VM guest, virtual switch or LAN switch will show a button on the upper-right side of its icon. Clicking this button will expand the resource contents.

Close button

Clicking this button will close the expanded chassis contents, replacing it by a chassis icon.



Clicking the close button will close the detailed content (server blades, LAN switch blades) that was shown for the selected chassis.

12.4 Resource Icons

This section describes the icons used to represent resource statuses.

12.4.1 Resource Statuses

The following table details the resource statuses associated with each icon.

Table 12.1 Chassis icons

Icon	Status	Meaning
	normal	No errors or warning were detected from the chassis.
	warning	A warning was detected from the chassis.
	unknown	The chassis status could not be obtained.
	error	An error was detected from the chassis.
	fatal	A fatal error was detected from the chassis, which is now unusable.
	stop	The chassis was detected to have been powered off.

Table 12.2 Server icons













Icon	Status	Meaning
	normal	No errors or warning were detected from the server.
	warning	A warning was detected from the server.
	unknown	The server status could not be obtained.
	error	An error was detected from the server.
	fatal	A fatal error was detected from the server, which is now unusable.
	stop	The server was detected to have been powered off.

Table 12.3 LAN switch blade icons

Icon		Status	Meaning
	 (*1)	normal	No errors or warning were detected from the LAN switch blade.
	 (*1)	warning	A warning was detected from the LAN switch blade.
		unknown	The LAN switch blade status could not be obtained.
	 (*1)	error	An error was detected from the LAN switch blade.
		fatal	A fatal error was detected from the LAN switch blade, which is now unusable.
	 (*1)	stop	The LAN switch blade was detected to have been powered off.

*1: When operating in IBP mode

Table 12.4 VM host icons





Icon	Status	Meaning
	normal	No errors or warning were detected from the VM host.
	warning	A warning was detected from the VM host.
	unknown	The VM host status could not be obtained.
	error	An error was detected from the VM host.
	fatal	A fatal error was detected from the VM host, which is now unusable.
	stop	The VM host was detected to have been powered off.

Table 12.5 VM guest icons





Icon	Status	Meaning
	normal	No errors or warning were detected from the VM guest.
	warning	A warning was detected from the VM guest.
	unknown	The VM guest status could not be obtained.
	error	An error was detected from the VM guest.
	fatal	A fatal error was detected from the VM guest, which is now unusable.
	stop	The VM guest was detected to have been powered off.

Table 12.6 Virtual switch icons





Icon	Status	Meaning
	normal	No errors or warning were detected from the virtual switch.
	warning	A warning was detected from the virtual switch.
	unknown	The virtual switch status could not be obtained.
	error	An error was detected from the virtual switch.
	fatal	A fatal error was detected from the virtual switch, which is now unusable.
	stop	The virtual switch was detected to have been powered off.

Table 12.7 LAN switch icons

Icon	Status	Meaning
	normal	No errors or warning were detected from the LAN switch.
	warning	A warning was detected from the LAN switch.
	unknown	The LAN switch status could not be obtained.
	error	An error was detected from the LAN switch.
	fatal	A fatal error was detected from the LAN switch, which is now unusable.
	stop	The LAN switch was detected to have been powered off.

Table 12.8 Port icons

Icon	Status	Meaning
	(*1)	normal
		No errors or warnings were detected from the port.

Icon		Status	Meaning
	 (*1)	error	An error was detected from the port (e.g. its opposite port or NIC was disabled, or the cable between this link and its opposite port or NIC was disconnected).
	 (*1)	disabled	The port was detected to have been disabled (offline).








*1: This icon is displayed for the following ports.



- The currently selected port.
- The port opposite to the selected port.
- In IBP mode, all ports that belong to the a selected port group
- In IBP mode, all ports that belong to the same port group as the selected port.

12.4.2 VLAN Display

The following resource icons are used when displaying VLANs in the Network Map.

Table 12.9 Resource icons for VLAN display

Icon		Meaning
		Chassis
		Server
	 (*1)	LAN switch blade
		VM host
		VM guest
		Virtual switch

Icon	Meaning
	LAN switch
	Port

*1: When operating in IBP mode

Information

If a problem occurs on a resource, a status icon indicating the problem is shown on top of the resource's own icon.

Refer to "[12.4.1 Resource Statuses](#)" for details on status icons.

12.4.3 Other Icons

The following table details other icons displayed in the Network Map.

Table 12.10 Admin Server icon








Icon	Status	Meaning
	Admin Server	Indicates a server used as the Admin Server.

Table 12.11 Icons for map navigation

Icon	Meaning
	Chassis
	Server
	VM host
	VM guest
	Switch
	Virtual switch


12.5 Network Links




This section details the network links displayed in the Network Map.

12.5.1 Link Display

The following table details the physical and virtual links displayed between resources.

Table 12.12 Links

Link	Meaning
	Represents a physical or virtual link.



Link	Meaning
	Represents a VLAN link.
	Represents a VLAN link related to the selected resource.
	Represents a disabled port.

12.5.2 Link Statuses

Link statuses are shown by adding colored outlines to displayed links (described in "[12.5.1 Link Display](#)").

The following table shows display examples of abnormal link statuses.

Table 12.13 Statuses of physical or virtual links

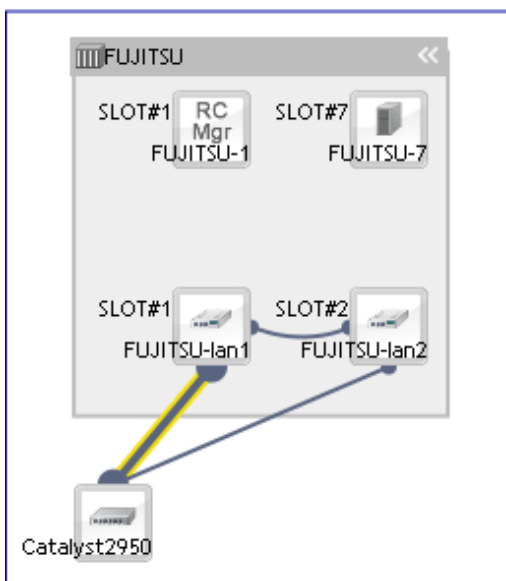
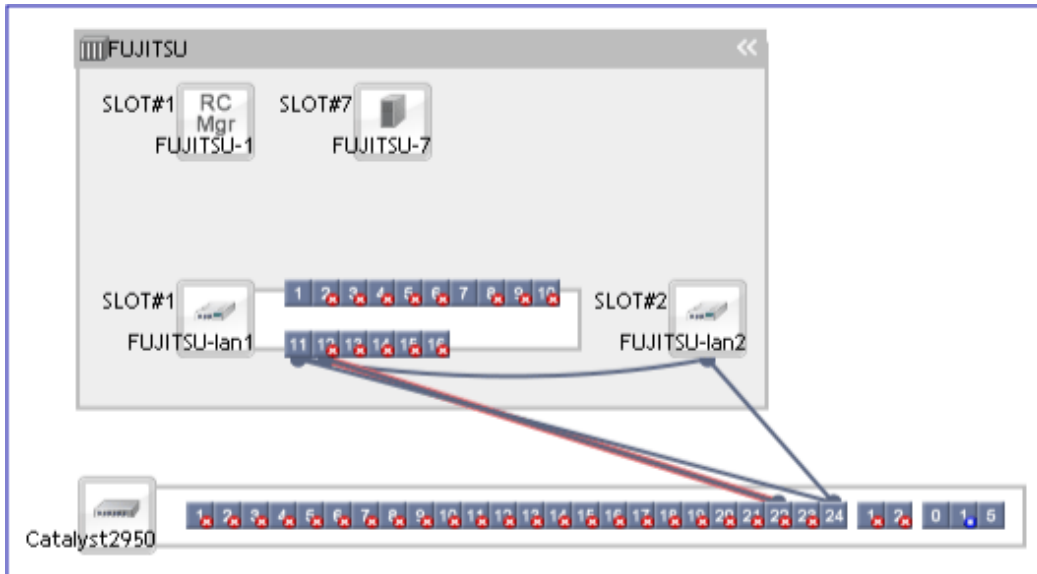
Link	Meaning
	Represents a link with an error status (e.g. its opposite port or NIC was disabled, or the cable between this link and its opposite port or NIC was disconnected).
	Represents a link with a warning status. For example, an aggregated link (as described in " 12.5.3 Aggregate Display of Network Links ") will show a warning status if only a subset of its links have an error status.

12.5.3 Aggregate Display of Network Links

When two resources are linked by two or more links, those links are represented as one aggregated link (please note that this appellation is not related with the Link Aggregation Protocol, but only refers to the display representation of multiple links as one entity).

Aggregated links are shown as thick lines in the Network Map. The following diagram shows an example of aggregate display.

Example



Note

Selecting a displayed resource will focus display on that resource. In such a focus mode, all links that are not directly related to the selected resource will be shown in lighter colors.

12.6 Display Filters

This section explains how to use display filters.

The display filter area includes the following filters (checkboxes). Selecting or unselecting a filter's checkbox will either show or hide the content associated with that filter.

Display filters and their associated content are detailed below.

Resource descriptions

Enabling this filter will show name identifiers on top of each resources. Disabling it will hide those identifiers.

This filter is enabled by default.

Physical links

Enabling this filter will show all physical links between resources. Disabling it will hide those links.

This filter is enabled by default.

VLANs

Enabling this filter will show the VLAN selected in the VLAN tree. Disabling it will hide this VLAN.

This filter is enabled by default.

Chapter 13 Power Consumption Data

This chapter explains how to export the power consumption data that was collected from registered power monitoring targets, and describes the exported data's format.

13.1 Overview

This section details the power consumption data that is collected from registered power monitoring targets.

Resource Coordinator VE calculates the power (in Watts) and energy (Watt-hours) consumed by a power monitoring target by multiplying its collected electrical current (Amperes) by its registered voltage value (Volts). This data can then be exported to a file in CSV format. This data can then be summarized or visualized as a graph using an external tool such as Excel to obtain a graphical representation of the power consumed by each power monitoring target.

Information

In Resource Coordinator VE, power consumption is calculated as the product of electrical current (A) multiplied by voltage (V). Normally, power consumption is the product of an electrical current multiplied by a voltage and an additional phase factor (if the phase difference between the current and voltage is defined as " θ ", this factor is expressed as " $\cos \theta$ ").

Note

This data should only be used as a reference to evaluate the power consumption status. It should not be used as an exact power consumption measurement for billing purposes.

13.2 Exporting Power Consumption Data

This section explains how to export power consumption data.

Power consumption data can be exported in CSV format for each power monitoring target that is registered in the power monitoring environment.

The exported data can be selected by specifying the desired data types (power and energy), time spans, and sampling rate.

Use the following procedure to export power consumption data.

1. In the RC console resource tree, right-click a power monitoring target, and select [Export]-[Environmental Data] from the popup menu.

The [Export Environmental Data (*target_type*)] dialog is displayed.

- In the [Export Environmental Data (*target_type*)] dialog, set the following items.

Figure 13.1 [Export Environmental Data (*target_type*)] dialog

Choose the type and period of environmental data that will be exported.

Target Resources

Select	Device Name	Comments
<input checked="" type="checkbox"/>	ups	

Data Type

Select	Data Type	Unit	Description
<input checked="" type="checkbox"/>	Power	W	Instantaneous power consumption
<input type="checkbox"/>	Average power	W	Average power consumption during the selected time span
<input type="checkbox"/>	Energy	Wh	Total energy consumption during the selected time span

Output time span: Last hour

Rate: Finest sampling

Format: CSV

OK Cancel Help

Target Resources

Specify the power monitoring target for which to export power consumption data. Select the checkboxes of each desired target. More than one target can be selected.

Data Type

Specify the type of the data to export. Select the checkbox of each desired data type. More than one data type can be selected.

Output time span

Select the time span for which to export data from the drop-down menu. Select one of the following options: "Last hour", "Last day", "Last week", "Last month", "Last year", or "Custom". When "Custom" is selected, the "Start Date", "Start Time", "End Date", and "End Time" fields must all be specified.

Rate

Select the data sampling rate to export from the drop-down menu. Select one of the following options: "Finest sampling", "Hourly", "Daily", "Monthly", or "Annual".

- Click the <OK> button.

In the download dialog that is displayed, specify the name of the file to be downloaded. The data will be exported to the specified file.

Note

Exporting large amounts of data will take time, and may fail if processing exceeds five minutes. In that case, wait for a while before retrying as server-side processing (on the Manager) may not be finished yet.

To avoid such problems, try reducing the amount of exported data by selecting fewer resources and a shorter output time span (respectively in the "Target resources" and "Output time span" options).

Table 13.1 Recommended settings

Rate	Output time span	Target resources
Finest sampling	Last day	12
Hourly	Last month	30
Daily	Last year	30
Monthly	select "Custom" and specify 5 years	60
Annual	select "Custom" and specify 5 years	60

13.3 Power Consumption Data File (CSV Format)

This section explains the power consumption data file format (CSV format).

Each defined item of the exported power consumption data is separated by a comma (",").

Each line is exported in the following format.

- Data format

Data is exported using the following format:

```
Time,target_name(data_type)[,target_name(data_type)]...  
time1,data1[,data1]...  
time2,data2[,data2]...
```

- Header line

The header line contains column titles identifying the data (from line 2 and later) that is displayed under each column. Each column title is set according to the data types that have been selected in the [Export Environmental Data (*target_type*)] dialog.

- Time

This column displays the date and time at which each data sample was collected.

Within data lines, the entry corresponding to this column is displayed in the following format: "YYYY-MM-DD hh:mm:ss" ("YYYY": Year, "MM": Month, "DD": Date, "hh:mm:ss": Hours:Minutes:Seconds). The time is displayed according to the time zone set in the Admin Server operating system.

- *target_name(data_type)*

This column title defines the device and data type of the value displayed in the data lines under each column.

The *target_name* part displays the name of the selected target.

The *data_type* part displays the selected data type. Power (W) is shown as "power", Average Power (W) as "power-average", and Energy (Wh) as "energy".

- Data lines

Each data line contains data values corresponding to each of the column titles shown in the header line.

A hyphen ("-") is displayed for any data that could not be collected.

Note

- Regardless of the specified power monitoring target, the data held within Resource Coordinator VE that fits the conditions given for the selected time span and rate will be exported.

- Depending on the status(es) of specified power monitoring target(s), the data corresponding to the specified time span and rate may not have been collected.
In this case, a hyphen ("-") will be displayed for any data that could not be collected.
Hyphens can be displayed when data was collected from another power monitoring target (including a deleted one) at the same collection time, and data was not collected from the specified power monitoring target.
No data is collected from servers on which ServerView Agent is not running. In this case, missing data is shown using hyphens ("-").
 - When exporting power consumption data, data collection itself may still be in-progress. In this case, a hyphen ("-") will be displayed for any data that hasn't been collected yet.
 - If the "Finest sampling" rate is selected in the [Export Environmental Data (*target_type*)] dialog, the power and average power values will be equal for each data sample.
 - If a rate other than "Finest sampling" has been selected in the [Export Environmental Data (*target_type*)] dialog, values for each sample are displayed as follows. If data was collected at the displayed sample time, that value is displayed. If no data was collected at the displayed sample time, the data that was last collected in the time interval between that sample and the previous sample will be displayed.
 - The energy (Wh) value of a finest sample is calculated under the assumption that the power value (W) collected for the sample stayed at the same value until the next sampling (in other words it is assumed that power values (W) do not vary during the duration of the polling interval).
 - Only daily average data can be collected from blade chassis.
 - Data collected from servers do not include power consumed by storage blades.
 - For rates other than "Finest sampling", the energy value is calculated as the sum of energy samples. The energy value of samples for which no data could be collected will be deemed to be 0.
 - The average power (W) of each sample is calculated from the energy value (Wh) of that sample and its corresponding time interval.
-

Chapter 14 Customizing the RC Console

This chapter explains how to customize the RC console.

14.1 Event Log

This section explains how to change the number of events that can be displayed in the event log of the RC console. Change the number of displayed events if the default settings do not allow enough events to be displayed. This may happen when a large number of resources are being used.

Use the following procedure to change the number of displayed events:

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

The [Options] dialog is displayed.

2. In the [Options] dialog, click the "Event Log" category title, and then change the following item in the area that is displayed.

Event Displayed

Enter the number of events to be displayed in the event log.

Enter a value between 10 and 1000.

3. Click the <Apply> button.

The new values are applied.



Information

Clicking the <Default> button resets this to the default value of 1000.

14.2 Dialogs

This section explains how to enable or disable display of some of the confirmation (or warning) dialogs used by the RC console.

Use the following procedure to change dialog display settings.

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

The [Options] dialog is displayed.

2. In the [Options] dialog, click the "Dialog" category title, and change the following settings in the displayed area.

Dialog display options (checkboxes)

To disable further display of a confirmation or warning dialog, select its corresponding checkbox.

To restore display of a disabled dialog, deselect its corresponding checkbox.

<Select All> button

Selects all dialog checkboxes.

<Deselect All> button

Deselects all dialog checkboxes.

3. Click the <Apply> button.

The new settings are applied.

14.3 External Software

This section explains how to configure the settings required by Resource Coordinator VE to interact with third party software.

VM management console

To launch an external VM management console (provided by the virtualization software used) from the RC console, users must be granted the permission to launch this management console in the Java Plug-in policy settings. Refer to "A.2 Configuration Requirements" in the "ServerView Resource Coordinator VE Setup Guide" for details on the VM management consoles that can be started from the RC console.

Use the following procedure to enable launch of the VM management console.

1. In the RC console resource tree, right-click the target VM host or VM guest, and select [VM Management Console] in the menu that is displayed.
2. The [Launch VM Management Console] dialog is displayed.
3. Click the <OK> button.
4. If launch of the VM management console from the RC console was not enabled yet, a [Download] dialog for the Java policy setup script is displayed.
5. Click the <OK> button.

Clicking the <OK> button will download the Java policy setup script. Save this script to an arbitrary location.

6. Execute the saved Java policy setup script. This will configure java policy settings and allow launch of the VM management console.
7. Close all Web browsers.

After closing all opened Web browsers, start a new Web browser and re-log into the RC console. The VM management console can now be launched from the RC console.

Information

Depending on script-related settings, the command prompt opened by the Java policy setup script may close right after finishing its execution, making it impossible to confirm whether or not the script ended successfully.

In this case, use the Windows start menu to select [Start]-[Run], and execute the following command.

```
wscript "full path name of the Java policy setup script"
```

Chapter 15 Troubleshooting

This chapter explains how to address problems that occur, and how to collect data in order to request investigation of problems.

15.1 Types of Troubleshooting Data

If a problem occurs on a system using Resource Coordinator VE, use the following procedures to collect troubleshooting data so that Fujitsu technical staff can investigate the problem.

Two kinds of troubleshooting data can be collected. Collect the data which is relevant to one of the situations described below:

1. Collect initial troubleshooting data

To identify the cause of a problem, collect the data required to perform an initial diagnostic of the problem and contact Fujitsu technical staff.

The amount of data collected is small enough to be sent by e-mail.

Refer to "[15.1.1 Collecting Initial Troubleshooting Data](#)" for more information.

2. Collect exhaustive troubleshooting data

In some cases, the cause of a problem can be identified from the initial troubleshooting data alone, but in other cases additional information is required.

In such cases, a large volume of data is required to perform a more exhaustive investigation and identify the cause of a problem. As a result, exhaustive troubleshooting data is significantly larger in size than initial troubleshooting data.

Collect and send exhaustive troubleshooting data if requested to do so by Fujitsu technical staff.

Refer to "[15.1.2 Collecting Exhaustive Troubleshooting Data](#)" for more information.



Note

Once a problem occurs, troubleshooting data should be collected promptly. Otherwise data necessary for a problem investigation may be overridden.

15.1.1 Collecting Initial Troubleshooting Data

This section explains how to collect the data required to diagnose a problem's cause.

Collection Methods

The initial troubleshooting data can be collected using the following methods.

Based on each collection method's characteristics, choose the appropriate one according to the environment and system state for which the problem occurred.

- **Collecting data from the Admin Server**

This method involves executing a troubleshooting data collection command (`rcxadm mgrctl snap -all`) on the Admin Server.

This method allows data from each managed server to be collected all at once via the network. This is easier than executing a command individually on each managed server.

Refer to "[Collecting Data from the Admin Server \(rcxadm mgrctl snap -all\)](#)" to collect the data.

Executing the `rcxadm mgrctl snap -all` command requires approximately the free space determined by the following formula:

number of registered servers * 30 MB + 65 MB

- **Collecting data separately from each server**

This method involves executing a data collection command (`rcxadm mgrctl snap` or `rcxadm agtctl snap`) on each server.

Refer to "[Collecting Data separately from each Server \(rcxadm mgrctl snap, rcxadm agtctl snap\)](#)" to collect the data.

About 65 MB of free space is required to execute the `rcxadm mgrctl snap` command, and about 30 MB of free space is required to execute the `rcxadm agtctl snap` command.

- **Collecting HBA address rename setup service environment data**

This method involves collecting data that is required for identifying the cause of a problem that occurs on the HBA address rename setup service.

Refer to "[Collecting HBA Address Rename Setup Service Environment Data](#)" to collect the data.

About 8 MB of free space is required to collect troubleshooting data for the HBA address rename server.

Note

[VMware]

For VMware ESX 4, please also collect and send the following data to Fujitsu technical staff.

- Use the copy command to collect and send the following files.

`/var/log/vmware/hostd-*.log.gz`

`/var/log/vmware/hostd-*.log`

`/var/log/vmware/hostd-*.log.gz`

- Collect and send the result (output) of the following command.

`/usr/sbin/esxcfg-firewall -q`

Collecting Data from the Admin Server (rcxadm mgrctl snap -all)

Troubleshooting data from every managed server can be collected all at once by executing the command for collecting troubleshooting data, `rcxadm mgrctl snap -all`, on an Admin Server.

The following method is used to collect data with the data collection command, `rcxadm mgrctl snap -all`.

Collection Method

Perform the following procedure on the Admin Server to collect investigation data:

1. Log on to the Admin Server with OS administrative privileges.
OS administrative privileges are required to collect troubleshooting data.
2. Execute the `rcxadm mgrctl snap` command with the `-all` option specified.

[Windows]

```
>"Installation_Folder\Manager\bin\rcxadm" mgrctl snap [-dir dir] -all <RETURN>
```

[Linux]

```
# /opt/FJSVrcvmr/bin/rcxadm mgrctl snap [-dir dir] -all <RETURN>
```

3. Send the collected troubleshooting data to Fujitsu technical staff.

Note

- The Manager must be running on the Admin Server in order to collect data from the Admin Server. If the Manager cannot run, collect data from each server.
- When collecting data via the Admin Server, data cannot be collected from a managed server in the following cases.
 - Communication cannot be established with that server
 - The server is stopped

Even in such cases, however, data will continue to be collected from other managed servers.
Use the command execution logs to check the execution results.

Refer to "5.6 rcxadm mgrctl" of the "ServerView Resource Coordinator VE Command Reference" for details.
For managed servers where data collection has failed, collect data by either executing the rcxadm mgrctl snap -all command on the Admin Server again, or by executing the rcxadm agtctl snap command on the managed server where data collection failed.

Collecting Data separately from each Server (rcxadm mgrctl snap, rcxadm agtctl snap)

In addition to the rcxadm mgrctl snap -all command, which can collect troubleshooting data from all the managed servers at once, the commands rcxadm mgrctl snap and rcxadm agtctl snap are also provided. These collect data from only the server on which they are executed.

Use the following procedure to collect data with the rcxadm mgrctl snap command or the rcxadm agtctl snap command.

Collection Method

Perform the following procedure on the server from which data is to be collected:

1. Log on to the server with OS administrative privileges.
OS administrative privileges are required to collect troubleshooting data.
2. Execute the rcxadm mgrctl snap command or the rcxadm agtctl snap command.

Note that the command differs depending on the server from which data is collected.

- Admin Servers

[Windows]

```
>"Installation_folder\Manager\bin\rcxadm" mgrctl snap [-dir dir] <RETURN>
```

[Linux]

```
# /opt/FJSVrcvmr/bin/rcxadm mgrctl snap [-dir dir] <RETURN>
```

- Managed servers

[Windows]

```
>"Installation_folder\Agent\bin\rcxadm" agtctl snap [-dir dir] <RETURN>
```

[Linux/VMware]

```
# /opt/FJSVrcxat/bin/rcxadm agtctl snap [-dir dir] <RETURN>
```

[Solaris]

```
# /opt/FJSVrcxat/bin/rcxadm agtctl snap [-dir dir] <RETURN>
```

3. Send the collected information to Fujitsu technical staff.

Refer to "5.1 rcxadm agtctl" or "5.6 rcxadm mgrctl" of the "ServerView Resource Coordinator VE Command Reference" for details.

Collecting HBA Address Rename Setup Service Environment Data

The following method is used to collect the troubleshooting data necessary to investigate problems that occur on an HBA address rename setup service.

Collection Method

Perform the following procedure on the HBA address rename server to collect troubleshooting data.

1. Collect files from the HBA address rename server.

[Windows]

the data under the following folder: *installation_folder*\WWN Recovery.

[Windows]

From the HBA address rename server, collect the log file *installation_folder*\WWN Recovery\rcxinstaller.log, and all files and folders under the following folder: *installation_folder*\WWN Recovery\var.

[Linux]

Collect the log file /var/tmp/rcxinstaller.log, and all files and folders under the following folder: /var/opt/FJSVrcvhb.

2. Take a screenshot of the window displayed when the problem occurred.

Perform the following operation on the server for HBA address rename setup service from which the data is to be collected in order to take a screenshot of the window:

Press the Print Screen key to copy image data onto the Clipboard, and then paste the image data into an image editing tool and save it as a bitmap file.

3. Obtain system version information.

[Windows]

From Windows explorer, right-click the "My Computer" icon, and from the popup menu select "Properties".

In the [System Properties] dialog click the [General] tab and use the procedure explained in step 2 to obtain information such as the OS type, version and level, and service pack number.

[Linux]

Execute and collect the results of the following commands.

cat /etc/redhat-release <RETURN>
cat /proc/version <RETURN>
cat /proc/meminfo <RETURN>
cat /proc/cpuinfo <RETURN>
rpm -qa <RETURN>

4. Send the collected information to Fujitsu technical staff.

15.1.2 Collecting Exhaustive Troubleshooting Data

This section explains how to collect exhaustive troubleshooting data.

When the cause of a problem cannot be determined from the initial troubleshooting data, exhaustive troubleshooting data becomes necessary.

About Collection Methods

The troubleshooting data used to identify the causes of problems is collected by executing troubleshooting data collection commands (rcxadm mgrctl snap -full or rcxadm agtctl snap -full) on each server.

About 80 MB of free space is required to use this function.

Collection Method

Perform the following procedures on the server from which data is to be collected:

1. Log on to the server with OS administrator privileges.

OS administrative privileges are required for collecting investigation data.

2. Execute the `rcxadm mgrctl snap -full` command or the `rcxadm agtctl snap -full` command.

Note that the command differs depending on the server from which data is collected.

- Admin Server

[Windows]

```
>"Installation_folder\Manager\bin\rcxadm" mgrctl snap -full [-dir dir] <RETURN>
```

[Linux]

```
# /opt/FJSVrcvnr/bin/rcxadm mgrctl snap -full [-dir dir] <RETURN>
```

- Managed servers

[Windows]

```
>"Installation_folder\Agent\bin\rcxadm" agtctl snap -full [-dir dir] <RETURN>
```

[Linux/VMware]

```
# /opt/FJSVrcxat/bin/rcxadm agtctl snap -full [-dir dir] <RETURN>
```

[Solaris]

```
# /opt/FJSVrcxat/bin/rcxadm agtctl snap -full [-dir dir] <RETURN>
```

3. Send the collected information to Fujitsu technical staff.

Refer to "5.1 rcxadm agtctl" or "5.6 rcxadm mgrctl" of the "ServerView Resource Coordinator VE Command Reference" for details.



Note

[Hyper-V]

The following files should also be collected manually and sent to Fujitsu technical staff.

OS system log

All files under the following folder: `windows_folder\system32\wbem\logs`

15.2 OS Startup Issues (with I/O Virtualization)

This section explains the troubleshooting operations to perform when a managed server that uses I/O virtualization fails to boot.

- When using HBA address rename

When using HBA address rename, the WWN that was set for the server's HBA is set from the Manager when the power to the server is turned on again.

When errors occur within the Admin Server, the HBA address rename setup service sets the WWN for the server's HBA.

Use the following procedure to confirm and correct the problem.

1. If the server had been replaced immediately beforehand, check the following:

Confirm that hardware information was successfully re-configured following server replacement.

For details, refer to "[9.3 Re-configuring Hardware Properties](#)".

2. Check the storage environment.

Check that the WWN set for the server's HBA have access to the appropriate storage device and logical volume. Set a proper access path if none was configured yet.

For details, refer to "3.7 Configuring the Storage Environment" of the "ServerView Resource Coordinator VE Setup Guide".

3. Check the Manager's startup status.

Refer to "5.1 Manager" of the "ServerView Resource Coordinator VE Setup Guide" for details on how to check the startup status of the Manager.

4. Perform either one of the following based on the Manager's startup status.

- If the Manager is not running

Start the Manager.

If the Manager cannot start because of a server fault, for example, recover the server after completing step 5.

- If the Manager is already running

Occasionally the timing of the Manager startup can prevent it from controlling a managed server. If this is the case, restart the managed server.

Even if the Manager is running, if communication problems happen on the Admin LAN (due to network interface, cabling or LAN switch issues), the managed server will not start. After performing step 5, the LAN configuration must be repaired.

5. Check the running state of the HBA address rename setup service.

Check the running state of this service in the server for HBA address rename setup service.

Start the server where this service has been set up if it is not running yet, then start the managed server.

The WWN for the server's HBA will then be set up using the most recent state synchronized with the Admin Server.

6. Check the managed server console.

Check the managed server console to confirm that it has successfully started up.

If an error message is output, take action according to the corresponding message ID in "Messages".

7. For servers other than PRIMERGY BX servers, check that the MAC address entered at registration is correct. If incorrect, re-configure the server's hardware properties.

The registered MAC address can be confirmed in the [Resource Details] tab for the corresponding physical server.

Refer to "2.5.2 [Resource Details] tab" in the "ServerView Resource Coordinator VE Setup Guide" for details.

8. Check the network environment.

- Make sure that the managed server is able to communicate with the Admin Server.
- Make sure that there are no DHCP or PXE servers running on the subnet used by managed servers.

• When using VIOM

1. Check the WWN that was set for the server's HBA in VIOM

Open the VIOM client and confirm that the WWN value set for the server is correct.

2. Check the storage environment

Check that the WWN set for the server's HBA (confirmed in the above step) has access to the appropriate storage device and logical volume. Set a proper access path if none was configured yet.

For details, refer to "3.7 Configuring the Storage Environment" of the "ServerView Resource Coordinator VE Setup Guide".

15.3 "unknown" Server Status

This section explains how to troubleshoot a registered managed server whose status is "unknown" even though the managed server is still running.

When errors or warning messages are displayed in the event log, take the appropriate action by referring to the "ServerView Resource Coordinator VE Messages". Check the following points and correct the cause of any problems:

- Communication between the Admin Server and the server management device is not possible.

Check if it is possible to connect to either the Web or telnet interface of the server management device (management blade or remote management controller).

- Communication between the Admin Server and the managed server is not possible.

Check LAN switch blade configurations to confirm that the same VLAN ID or the same port group (for switch blades operating in IBP mode) is set for the ports used by the managed server and the Admin Server on the Admin LAN.

When using PRIMERGY BX servers and changing the VLAN ID used for Admin LAN, proceed as follows to preserve communication from the Admin Server to the LAN switch blade. First, change the VLAN ID set for the Admin LAN port (on the LAN switch blade) connected to the Admin Server, as well as the VLAN ID set for the switch blade's own network interface. Then, change the VLAN ID for the Admin LAN port connected to the managed server.

Refer to "3.2.1 Network Configuration" and "6.3.2.8 Changing the VLAN Settings of a LAN Switch" of the "ServerView Resource Coordinator VE Setup Guide" for the overview and the setup of VLAN for the managed server.

- Communication is not allowed for the ports used by Resource Coordinator VE

Allow communication for the ports described in "Appendix C Port List" of the "ServerView Resource Coordinator VE Setup Guide".

- The Resource Coordinator VE Agent is not running

Make sure that the Agent is running on the managed server.

- The ServerView Agent is not running.

For PRIMERGY servers, check whether the ServerView Agent is running properly on the managed server.

[Windows/Hyper-V]

From the Windows Control Panel, open "Administrative Tools" and then open the [Services] window. Check that the status of the Server Control Service and SNMP Service is shown as "started".

[Linux/VMware/Xen]

Execute the following commands to check if the ServerView Agent service is running.

```
# /etc/init.d/srvmagt status <RETURN>
# /etc/init.d/eecd status <RETURN>
# /etc/init.d/snmpd status <RETURN>
```

The above commands are not available if the ServerView Agent is not installed. In this case install the ServerView Agent on the managed server.

If the above commands indicate that the ServerView Agent is not running, refer to the ServerView Agent manual to start the ServerView Agent.

- SNMP community settings are incorrect

Make sure that the SNMP community settings on the management blade and managed server match those set in Resource Coordinator VE during chassis and server registration.

- Hardware properties were not re-configured after replacing the server.

Identify the MAC address of the replacement server, and check if it is the same address as that set for the Admin LAN (MAC address) in the [Resource Details] tab of the RC console.

If the MAC address is different, re-configure the hardware properties from the RC console.

- No information could be obtained from the virtualization software running on the managed server.

In environments where no VM management software was registered, or for VM hosts that are not managed by a VM management software, the status of a VM guest is displayed as "unknown" if its information could not be obtained from the server virtualization software used to run that VM guest. Check whether the virtualization software is operating correctly.

If it is operating correctly, its account information (user account name and password) may have changed. As a result, the settings no longer correspond to those registered in Resource Coordinator VE. In that case, change the virtualization software's account settings registered in Resource Coordinator VE.

Refer to "6.3.2.7 Changing VM Host Login Account Information" of the "ServerView Resource Coordinator VE Setup Guide" for details.

- No information could be obtained from VM management software

In environments where a VM management software was registered, the status of a VM guest (on a VM host managed by this VM management software) is displayed as "unknown" if its information could not be obtained from the VM management software. Check whether the VM management software is operating correctly.

If it is operating correctly, its account information (user account name and password) may have changed. As a result, the settings no longer correspond to those registered in Resource Coordinator VE. In that case, change the VM management software's account settings registered in Resource Coordinator VE.

Refer to "6.3.6 Changing VM Management Software Settings" of the "ServerView Resource Coordinator VE Setup Guide" for details.

- The remote management controller's IP address, user name, or password was changed after server registration

Change the IP address, user name and password settings registered for this remote management controller in Resource Coordinator VE.

Refer to "6.3.2.5 Changing Remote Management Controller Settings" in the "ServerView Resource Coordinator VE Setup Guide" for details.

- High load on the Admin Server, server management unit or managed server

Resource statuses may be temporarily shown as "unknown".

15.4 Image Operation Issues [Windows/Linux][Hyper-V]

If the Admin Server IP address that was set up in the "Register Admin Server Information" dialog described in "2.2.2 Installation [Windows/Hyper-V]", or step 5. of "2.2.3 Installation [Linux/VMware/Xen]" of the "ServerView Resource Coordinator VE Installation Guide" is incorrect, the following message is displayed when collecting or deploying cloning images, or when backing up or restoring system images.

FJSVrcx:ERROR:68295:deployment engine error:
no response from the managed server node. invalid BIOS setting found *detail*

detail

The information describing error details is displayed.

Use the following procedure to confirm and correct the problem.

[Windows/Hyper-V]

1. On the managed server, select [Start]-[Run], and then execute the following command.

Installation folder\Agent\scw\config.bat

The IP address of the Admin Server that has been set up and the port settings are displayed.



Note

Note the "Development Server" referred to in this section actually refers to the Admin Server.

2. In the Development Server field, check that either the Admin Server IP address or the server name is correctly set up.

If the settings are incorrect, change the value displayed and click the <OK> button.



Note

When entering the server name, check that the IP address on the managed server side of the Admin Server can be resolved from the server name.

3. In the confirmation dialog asking to restart the client agent, click the <Yes> button.

[Linux]

1. Open the `/etc/scwagent.conf` file on the managed server.

Confirm the Admin Server IP address and the settings of the port currently being used.

2. In the `server_ip` field, check that either the Admin Server IP address or the server name is correctly set up.

If the settings are incorrect, edit `scwagent.conf` directly, and then restart the managed server.

After fixing the cause of the error, execute the operation again as described in step 4. of "Message number 68295" of the "ServerView Resource Coordinator VE Messages".

If the settings are found to be satisfactory, take action described in "Message number 68295" of the "ServerView Resource Coordinator VE Messages".

15.5 Public LAN Communication Issues

This section explains how to troubleshoot communication issues for managed servers on the public LAN.

Use the following procedure to confirm and correct any problem.

- VLAN is not correctly set up

LAN switch blade internal ports must be set to the same VLAN ID(s) as external public LAN ports.

- Port groups are not correctly set up

For LAN switch blades operating in IBP mode, internal ports and external ports should belong to the same port group.

- Public LAN IP address is not correctly set up

Check that the public LAN IP address is correctly set on the managed server.

- The subnet mask must be correct
- There should be no IP address conflicts

- Routing information is not correctly set up

Verify that the routing settings for the server allow for communication to an address on a different subnet.

15.6 Multipath Configuration Issues

This section explains how to troubleshoot startup issues on managed servers set with a multi-path configuration.

When using HBA address rename, the server will start in a single path configuration if the selected number of HBA ports was set to "1" in the "HBA Address Rename Settings" dialog. For a multi-path configuration, the number of HBA ports should be set to "2".

Refer to "6.2.2 Configuring HBA address rename" of the "ServerView Resource Coordinator VE Setup Guide" for details on how to re-configure this setting.

15.7 Cloning Issues Following Manager Re-installation

This section explains how to troubleshoot cloning issues that occur after re-installing the Manager.

When performing a cloning image operation (collection or deployment) on a managed server that was already registered on the Manager before re-installation, the following problem may occur. The Manager and Agent certificates may not match, resulting in the Admin Server being unable to communicate with its managed server. In such a case, trying to deploy or collect an image to or from the managed server will fail. This problem occurs when the following conditions are met.

- The Manager was re-installed, but its certificate store was not properly backed up, as described in "3.1.2 Uninstallation [Windows]" or "3.1.3 Uninstallation [Linux]" of the "ServerView Resource Coordinator VE Installation Guide"
- Both the Manager and Agent were re-installed (and their certificates renewed), but a cloning image that was collected before the re-installation is deployed, thus restoring an outdated Agent certificate on the managed server

Use the following procedure to correct the problem.

After correcting problem, it is also recommended to update any cloning image that contains an outdated Agent certificate in order to avoid further certificate problems.

Checking the Certificates

How to check certificates

1. Stop the Manager and then display SSL certificate data by executing the following commands on the Admin Server.

[Windows]

```
>"Installation_folder\Manager\bin\rxadm" mgrctl stop <RETURN>
>"Installation_folder\Manager\bin\rxadm" certctl list <RETURN>
```

[Linux]

```
# /opt/FJSVrcvmr/bin/rxadm mgrctl stop <RETURN>
# /opt/FJSVrcvmr/bin/rxadm certctl list <RETURN>
```

Refer to "5.2 rxadm certctl" and "5.6 rxadm mgrctl" of the "ServerView Resource Coordinator VE Command Reference" for information on these commands.

Example Results

```
Truststore:
-----

Key store type: jks
Key store provider: SUN

The key store includes four entries.

client2, May, 10, 2007, trustedCertEntry,
Certificate fingerprint (MD5): 0F:4E:1C:DB:19:AE:3B:82:9D:74:93:6C:46:D8:7C:D2
client1, May, 10, 2007, trustedCertEntry,
Certificate fingerprint (MD5): 9D:99:ED:88:C0:8F:32:26:60:FA:4C:96:A2:34:5A:45
server4, May, 11, 2007, trustedCertEntry,
Certificate fingerprint (MD5): DC:E3:19:59:08:6D:C4:AD:B4:C7:F6:5C:E1:52:0A:1A (*1)
server3, May, 11, 2007, trustedCertEntry,
Certificate fingerprint (MD5): 9B:EB:94:58:90:E8:09:BE:BD:FA:14:83:9D:87:3A:E4
...

Keystore:
-----

Keystore type: jks
Keystore provider: SUN

2 entries are contained in the keystore.

client, 2007/05/11, keyEntry,
Certificate fingerprint (MD5):
AA:55:85:54:6B:57:80:4F:8C:6E:2E:AA:7C:77:DB:F6 (*2)
server, 2007/05/11, keyEntry,
Certificate fingerprint (MD5):
14:48:31:68:C9:CA:66:E1:E0:34:8A:FC:1C:17:19:EF
```


2. Stop the Agent and display SSL certificate data by executing the following commands on the managed server where the error occurred.

[Windows]

```
>"Installation_folder\Agent\bin\rxadm" agtctl stop <RETURN>  
>"Installation_folder\Agent\bin\rxadm" certctl list <RETURN>
```

[Linux]

```
# /opt/FJSVrcxat/bin/rxadm agtctl stop <RETURN>  
# /opt/FJSVrcxat/bin/rxadm certctl list <RETURN>
```

[Solaris]

```
# /opt/FJSVrcxat/bin/rxadm agtctl stop <RETURN>  
# /opt/FJSVrcxat/bin/rxadm certctl list <RETURN>
```

Refer to "5.1 rxadm agtctl" and "5.2 rxadm certctl" of the "ServerView Resource Coordinator VE Command Reference" for information on these commands.

Example Results

```
Truststore:  
-----  
  
Keystore type: jks  
Keystore provider: SUN  
  
1 entry is contained in the keystore.  
  
client1, 2007/05/11, trustedCertEntry,  
Certificate fingerprint (MD5):  
AA:55:85:54:6B:57:80:4F:8C:6E:2E:AA:7C:77:DB:F6 (*2)  
...  
  
Keystore:  
-----  
  
Key store type: jks  
Key store provider: SUN  
  
The key store includes one entry.  
  
server, May, 11, 2007, keyEntry,  
Certificate fingerprint (MD5): DC:E3:19:59:08:6D:C4:AD:B4:C7:F6:5C:E1:52:0A:1A (*1)
```

3. Check the fingerprint that is contained in the Agent Keystore.
As shown in the example in (*1), check that the fingerprint that is contained in the Agent Keystore is also contained in the Manager Truststore that is shown in "Example Results" of step 1.
If it is not, refer to "Corrective Action" to take proper corrective action.
4. Check the fingerprint that is contained in the Agent Truststore.
As shown in the example in (*2), check that the fingerprint that is contained in the Agent Truststore is also contained in the Manager Keystore that is shown in "Example Results" of step 1.
If it is not, refer to "Corrective Action" to take proper corrective action.

Corrective Action

1. Execute the following commands on the server for which the problem occurred to re-initialize its SSL certificate, and restart its Agent.

[Windows]

```
>"Installation_folder\Agent\bin\rxadm" certctl init <RETURN>  
>"Installation_folder\Agent\bin\rxadm" agtctl start <RETURN>
```

[Linux]

```
# /opt/FJSVrcxat/bin/rxadm certctl init <RETURN>  
# /opt/FJSVrcxat/bin/rxadm agtctl start <RETURN>
```

[Solaris]

```
# /opt/FJSVrcxat/bin/rxadm certctl init <RETURN>  
# /opt/FJSVrcxat/bin/rxadm agtctl start <RETURN>
```

2. Execute the following command on the admin server to start the Manager.

[Windows]

```
>"Installation_folder\Manager\bin\rxadm" mgrctl start <RETURN>
```

[Linux]

```
# /opt/FJSVrcvnr/bin/rxadm mgrctl start <RETURN>
```

15.8 Server Switchover and Failback Issues

This section explains the troubleshooting steps to be performed when the server switchover or server failback process fails.

If server switchover or server failback is performed without all the conditions specified in "9.3 Server Switchover Conditions" of the "ServerView Resource Coordinator VE Setup Guide" being satisfied, one of the following error messages may be output:

Switchover:

```
FJSVrcx:ERROR:61143:switchover:failed  
FJSVrcx:ERROR:69122:timeout occurred while executing power control modules
```

Failback:

```
FJSVrcx:ERROR:61143:failback:failed  
FJSVrcx:ERROR:69122:timeout occurred while executing power control modules
```

Use the following procedure to check and correct the problem:

1. Recheck the spare server conditions with reference to "9.3 Server Switchover Conditions" of the "ServerView Resource Coordinator VE Setup Guide".
If any conditions are not satisfied, change the configuration to ensure that all conditions are met.
2. If HBA address rename is being used and the following error message is output to the managed server console, the WWN may have failed to be set for the server HBA. Take the action specified for "Message number 61308" of the "ServerView Resource Coordinator VE Messages". Note that in this case there is no need to set the WWN again.

```
FJSVrcx:ERROR:61308:WWN setting failed. code=%1,%2
```

An internal error code is displayed in %1.

Either one of the following message is displayed in %2.

- a. HBA adapter not found

- b. command error
 - c. TFTP error
3. Perform the switchover or failback operation again.

15.9 HBA Address Rename is Set by Mistake

This section explains the troubleshooting steps to perform when HBA address rename is mistakenly set for a managed server that does not need it (such as when the managed server is made up of internal disks only).

If HBA address rename is set for a server that does not have an HBA, the following message will be output to the managed server console when the managed server is restarted:

```
FJSVrcx:ERROR:61308:WWN setting failed. code=%1,%2
```

An internal error code is displayed in %1.

Either one of the following message is displayed in %2.

- a. HBA adapter not found
- b. command error
- c. TFTP error

To prevent HBA address rename from being used, delete and then re-register the managed server.

15.10 Boot Issues (Boot Order Related)

This section explains the action to take when the managed server cannot be booted from the CD-ROM, or the system disk (local disk or SAN storage) cannot be recognized even though the managed server can be booted from the CD-ROM.

If this trouble occurs, it may mean that the priority boot order of the system BIOS is incorrect.

Refer to "BIOS Settings for Managed Servers" in "3.5 Configuring the Server Environment" of the "ServerView Resource Coordinator VE Setup Guide", and check that the priority boot order of the system BIOS is correct.

15.11 Boot Issues (Endless Reboot Cycle)

This section explains how to troubleshoot a server stuck in an endless reboot cycle, when that server is using HBA address rename.

Confirm the following points to identify and fix the cause of this issue.

- Make sure that BIOS settings were properly configured. Refer to "BIOS Settings for Managed Servers" in "3.5 Configuring the Server Environment" of the "ServerView Resource Coordinator VE Setup Guide" for instructions on BIOS settings.
- Make sure that the network environment was properly configured. Refer to "Required Network Configuration when Using HBA Address Rename" in "3.2.1 Network Configuration" of the "ServerView Resource Coordinator VE Setup Guide" for instructions on the network configuration.
- Make sure that all Manager services are started. Refer to "5.1 Manager" in the "ServerView Resource Coordinator VE Setup Guide" for details on Manager services.

Appendix A Notes on Operating ServerView Resource Coordinator VE

This appendix provides important reminders for the operation of Resource Coordinator VE.

Server Switchover

- Servers can be set up as spare servers even if it may not be possible to switch over with them.
Ensure that server switchover is possible after setting up spare servers.
For details on server switchover conditions, refer to "9.3 Server Switchover Conditions" of the "ServerView Resource Coordinator VE Setup Guide".
- Auto-Recovery cannot be performed if maintenance mode has not been released.
Ensure maintenance mode is released once maintenance operations are complete.
- Note the following points regarding the occurrence of a fault in the switchover destination spare server during server switchover.
 - The server switchover state returns to pre-switchover state. Additionally, maintenance mode is set for the switchover source server, and server switchover processing ends. If the switchover source server is stopped, the switchover source server does not start.
 - Even when more than one spare server is set for the primary server, there is no automatic switch to another spare server. Specify the other spare server, then perform server switchover manually.
 - To perform operations on the switchover source server, start the server and then release the maintenance mode. When Auto-Recovery is enabled and the switchover source server is faulty, however, Auto-Recovery occurs when the maintenance mode is released. Restore the switchover source server to its pre-fault status and then release the maintenance mode.

Redundant Configurations for the Admin LAN

If communication issues happen on the Admin LAN, or one of the network interfaces (NIC1 or NIC2) used by a managed server on the Admin LAN fails, the following operations may result in errors. In such cases, restore the Admin LAN network as quickly as possible.

- Backup and restore operations
- Collection and deployment of cloning images
- Server switchover and failback

HBA Address Rename

- With Resource Coordinator VE, the factory-set WWN of a managed server's HBA is overridden when the HBA address rename function is used. The WWN is reset to its factory-set value when the server is deleted from Resource Coordinator VE.
Before using HBAs in an environment that is not managed by Resource Coordinator VE, first delete the server in which it is mounted using the RC console.
Refer to "6.4.2 Deleting Managed Servers" of the "ServerView Resource Coordinator VE Setup Guide" for information on deleting servers.
- The WWN of a managed server is set up during startup, using a network book session to connect to the Admin Server. Once set up with a proper WWN, the managed server reboots into its own Operating System. Therefore, a managed server may reboot during its startup.

Changing the Manager's System Time

- When the Admin Server system time is reset to a time in the past, the resource monitoring by the Manager stops for this period. To reset the system time to more than just a few minutes in the past, return the time and then restart the Manager.
To restart the Manager, refer to "5.1 Manager" in the "ServerView Resource Coordinator VE Setup Guide".

Appendix B Admin Server Backup and Restore

This section explains how to back up and restore the Admin Server.

B.1 Overview

The Admin Server can be recovered even when resources on the server are damaged by operator error, provided that the resources managed by Resource Coordinator VE were backed up beforehand.

It is recommended that you create a backup once a system has been set up under Resource Coordinator VE, or after the registration, modification or deletion of resources.

The resource files managed by Resource Coordinator VE are:

- Resource Coordinator's environment definition files (files under the installation folder)
- System and cloning images (files under the image file storage folder)

Back up Resource Coordinator VE resources on the Admin Server using the following procedure:

1. Back up authentication resources
2. Back up system and cloning images
3. Export the system configuration file

Restore Resource Coordinator VE resources to the Admin Server using the following procedure:

1. Reinstall the Manager and restore authentication resources
2. Restore system and cloning images
3. Import the system configuration file

Information

Recovery can also be performed by first backing up the entire Admin Server disk, then restoring it.

In a clustered Manager configuration, the disk shared between cluster nodes should also be backed up and restored.

However, take note of the following:

- Do not perform a backup or restore of the Admin Server while server switchover or failback is taking place, or while a system image is being backed up or restored.
- After a backup, restore is only possible if the configuration of the following hardware devices has not changed.
 - Replacement of a chassis, LAN switch, managed server, power monitoring device hardware
 - Replacement of a managed server NIC
 - LAN connection between managed servers and LAN switches
 - Server switchback, takeover (*1)

*1: If in switchback status after server switchover, restore can be performed.

In addition, when backing up Resource Coordinator VE resources on the Admin Server after backing up the entire Admin Server disk, first restore the entire Admin Server disk, then restore those resources and import the system configuration file by following the instructions given in steps 2 and 3 of "[B.3 Restore](#)".

B.2 Backup

This section explains how to back up the Admin Server.

Note

- When using server switchover settings, backup cannot be performed after switchover to a spare server has been performed, so backup must be performed following a recovery procedure. For information on the recovery method, refer to "[10.3 Post-Switchover Operations](#)".
- If a second or subsequent backup is performed, earlier backups of folders and system configuration files can be deleted after the latest backup is complete. Delete earlier backups when disk space constraints make it advisable to do so.
- Do not perform backup during server switchover, failback, while a system image is being backed up or restored, or while a cloning image is being obtained or deployed.
- In a clustered Manager configuration, because files are actually stored on the shared disk, the files and folders to be copied in this procedure are those stored on the shared disk. Refer to "B.3 Configuration" in the "ServerView Resource Coordinator VE Installation Guide" for details on where files and folders should be backed up from.

1. Back up authentication resources

Authentication resources include agent certificates and an encryption key used by the Manager to authenticate users.

Back up the folder in which agent certificates are stored.

Refer to "3.1.2 Uninstallation [Windows]" of the "ServerView Resource Coordinator VE Installation Guide" for information on the folder in which certificates are stored.

Backup of the session encryption key is only required if passwords were saved using the -save option of the rcxlogin command. This step is not required if no password was saved, or if passwords are to be saved again after re-installation. For details on the rcxlogin command, refer to "2.1 rcxlogin" of the "ServerView Resource Coordinator VE Command Reference".

When backing up the session encryption key, back up the following file:

[Windows]

Installation folder\Manager\Rails\config\rcx_secret.key

[Linux]

/etc/opt/FJSVrcvmt/rails/config/rcx_secret.key

Because saved passwords are stored in the home directory of the OS user account for which the password was saved, it is also recommended to back up of the contents of the home directory.

Note

This step should be performed only once (after installing the Manager).

2. Backing up system and cloning images

Copy the folder containing the system and cloning images to a backup folder.

Example

Default value after installation:

[Windows]

Installation_folder\ScwPro\depot

[Linux]

/var/opt/FJSVscw-deploysv/depot

Check available disk space before backing up a system or cloning image.

For information about the disk space requirements for cloning images and system images, refer to "1.1.2.5 Dynamic Disk Space" of the "ServerView Resource Coordinator VE Installation Guide".

This step is not required if deployment services have not been installed.

Note

Perform this step again after either of the following operations has been performed:

- Backing up a system image
Refer to "[8.2 Backing Up System Images](#)" for details on backing up system images.
- Collecting a cloning image
Refer to "8.2 Collecting a Cloning Image" of the "ServerView Resource Coordinator VE Setup Guide" for details on collecting cloning images.

3. Export the system configuration file

Export the system configuration file according to the instructions given in "7.3 Exporting the System Configuration File" of the "ServerView Resource Coordinator VE Setup Guide".

Note

To restore a system, it is necessary for all the certificates, system images, cloning images and system configuration files to have been backed up at the same time. It is recommended that you store all of the backed up data together in a folder whose name clearly indicates the date and time of the backup.

The following settings and data will not be automatically preserved after backup and restore of the Admin Server. Follow the following instructions to manually restore them.

- Maintenance mode
Maintenance mode is released after restore is performed. If performing backup while maintenance mode is set, record the maintenance mode state for each managed server at backup time.
- Power consumption data for power monitoring devices
Power consumption data for power monitoring devices cannot be restored. Before reinstalling the Manager, exporting of power consumption data is recommended. For the operation method, refer to "[13.2 Exporting Power Consumption Data](#)".

4. Confirm image settings

Confirm the following image settings.

- Maximum number of system image versions
- Maximum number of cloning image versions
- Image files folder

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

This step is not required if deployment services have not been installed.

B.3 Restore

This section explains how to restore the Admin Server.

Note

In a clustered Manager configuration, restore backed up contents to the cluster-shared disk. Refer to "B.3 Configuration" in the "ServerView Resource Coordinator VE Installation Guide" for details on where files and folders should be restored to.

1. Reinstall the Manager and restore authentication resources

If the Manager does not run correctly because of damaged files, uninstall and re-install the Manager before restoring agent certificates and the session encryption key.

When re-installing the Manager, use the path confirmed during backup for the image files folder.

Refer to "2.1 Manager Installation" and "3.1 Manager Uninstallation" of the "ServerView Resource Coordinator VE Installation Guide" for details on restoring certificates.

Restore of the session encryption key is only required if passwords were saved using the -save option of the rcxlogin command. This step is not required if no password was saved, or if passwords are to be saved again after re-installation. For details on the rcxlogin command, refer to "2.1 rcxlogin" of the "ServerView Resource Coordinator VE Command Reference".

To restore the session encryption key, restore the following file from the backup folder to the following destination.

[Windows]

Installation folder\Manager\Rails\config\rcx_secret.key

[Linux]

/opt/FJSVrcvnr/rails/config/rcx_secret.key

Because saved passwords are stored in the home directory of the OS user account for which the password was saved, authentication may fail if the home directory contents were damaged. In that case, either restore the home directory contents or save the password again using the rcxlogin command.

2. Restore the system and cloning images

Use the following procedure to restore system and cloning images.

This step is not required if deployment services have not been installed.

a. Stop the Manager.

Refer to "5.1 Manager" of the "ServerView Resource Coordinator VE Setup Guide" for details on how to stop the Manager.

b. Restore the backup folder that was copied in "2. Backing up system and cloning images" of "B.2 Backup" to the folder that was specified at installation time.

 Example

Default value after installation:

[Windows]

Installation_folder\ScwPro\depot

[Linux]

/var/opt/FJSVscw-deploysv/depot

c. Restart the Manager.

Refer to "5.1 Manager" of the "ServerView Resource Coordinator VE Setup Guide" for details on how to restart the Manager.

3. Import the system configuration file

Import the system configuration file that was exported in "3. Export the system configuration file" of "B.2 Backup".

Refer to "7.2 Importing the System Configuration File" of the "ServerView Resource Coordinator VE Setup Guide" for details.

4. Restore image settings

Restore the following image settings if those had been modified at the time of backup.

- Maximum number of system image versions
- Maximum number of cloning image versions

For details on the maximum number of system image versions, refer to "6.3.1.3 Changing the Maximum Number of System Image Versions" in the "ServerView Resource Coordinator VE Setup Guide".

For details on the maximum number of cloning image versions, refer to "6.3.1.4 Changing the Maximum Number of Cloning Image Versions" in the "ServerView Resource Coordinator VE Setup Guide".

This step is not required if deployment services have not been installed.

Note

- When the system configuration file is exported, in all sections, "operation" will become a hyphen ("-"). Therefore, do not import the system configuration file until after correcting "operation" to "new". For details on the system configuration file, refer to "Appendix D Format of CSV System Configuration Files" of the "ServerView Resource Coordinator VE Setup Guide".
- If you are importing the system configuration file when the OS of the managed server is not started, registration of the Agent will fail. Therefore, start the OS before performing import.
- If you are setting a VM host as a spare server, leave "operation" as a hyphen ("-") in the "SpareServer" section of the corresponding physical server. After import is completed, set the spare server of the corresponding physical server from the RC console.
- Do not perform restore during server switchover, failback, while a system image is being backed up or restored, or while a cloning image is being collected or deployed.
- Restore only certificates, system images, cloning images and system configuration files that were backed up at the same time.
- Restore can only be executed if none of the settings or hardware configuration changes described below have been made since backing up the Admin Server:
 - Replacement of a chassis, LAN switch blade, managed server or power monitoring device hardware
 - Replacement of a managed server NIC
 - LAN connections between managed servers and LAN switch blades
 - server switchover or takeover (*1)
- *1: If in switchback status after server switchover, restore can be performed.
- A managed server using HBA address rename must be restarted after being restored.
- Maintenance mode settings cannot be recovered after restore. Set the maintenance mode in accordance with the information recorded at backup time.
- If the managed server's Agent was registered, perform either one of the following after restoring the Admin Server to enable subsequent system image backup or cloning image collection operations.
 - Restart the managed server.
 - Restart the service described in "Deployment service" in "5.2 Agent" of the "ServerView Resource Coordinator VE Setup Guide".
- LAN switches and physical link data (used by the Network Map) are not subject to backup.
LAN switches and physical link data should be manually restored following the instructions given in "[12.2 Preparations](#)".

Appendix C Event Handling Function

This appendix explains the event handling function.

This function allows execution of a pre-defined file whenever the Admin Server receives SNMP Traps (events) from a registered device. This function works with the following devices.

- Chassis (Management Blade)
- Managed Server (ServerView)
- LAN switch

The following file is executed each time an event occurs.

[Windows]

Installation folder\Manager\etc\trapop.bat Argument 1 Argument 2 Argument 3 Argument 4 Argument 5 Argument 6

[Linux]

/etc/opt/FJSVrcvmr/trapop.sh Argument 1 Argument 2 Argument 3 Argument 4 Argument 5 Argument 6

The default-installed file will log each event, but will not trigger any action based on those events.

However, it is possible to trigger operations such as email notifications or calls to external management software (command calls or event notifications) by providing a custom-script to use in place of the default script.

- The following information is passed as arguments:
 - Argument 1
Message describing the event
 - Argument 2
IP address of the device in which the event occurred
 - Argument 3
Host name (FQDN) inferred from the IP address received in Argument 2 (when the name cannot be inferred, this is set to the device's IP address)
 - Argument 4
Number of milliseconds counted from 01/01/1970 00:00:00 GMT until the current time
 - Argument 5
Event level ("INFO", "WARNING" or "ERROR")
 - Argument 6
Name of the device in which the event occurred

For the following events, however, only the event log is displayed. The file is not executed.

- Events logged during RC console operations, command execution, or automatic server switchovers (Auto-Recovery)
 - Start of processing, in-progress status, end of processing
 - Changes in resource status during a running process
 - Errors that occur within Resource Coordinator VE
- Errors detected from regular monitoring (when no SNMP Trap is sent, or when SNMP traps do not reach the Manager because of communication errors or an abnormally high load on the system)



Note

In a clustered Manager configuration, it is necessary to store the same file on both the primary and secondary nodes for this function to work properly.

E-Mail Notification Sample

Below is a sample program that will send e-mail notifications for each event received.

To customize e-mail contents and adapt the program to your practical configuration, it is recommended to create your own version using this sample as a reference.

[Windows]

Set the following addresses (in the "E-Mail Notification Sample") to match actual environment values.

- Mail server address
- Sender address
- Destination address

E-Mail Notification Sample (*Installation folder\Manager\etc\trapop.bat*)

```
@echo off

rem set MAIL_SERVER_ADDRESS=server.address          <- mail server address
rem set MAIL_FROM=from_your@e-mail.address         <- sender address
rem set MAIL_TO=to_your@e-mail.address             <- destination address

rem set MAIL_SUBJECT="Resource Coordinator VE (%COMPUTERNAME%) event mail"

rem set SENDMAIL_VBS=sendmail.vbs

rem set MAILCMD=cscript"%~dp0%SENDMAIL_VBS%" %MAIL_FROM% %MAIL_TO%
%MAIL_SUBJECT% %MAIL_SERVER_ADDRESS% %1 %2 %3 %4 %5 %6 //nologo
rem %MAILCMD%
```

When actually using this script, remove all comments and enter appropriate addresses.

```
@echo off

set MAIL_SERVER_ADDRESS=server.address          <- mail server address
set MAIL_FROM=from_your@e-mail.address         <- sender address
set MAIL_TO=to_your@e-mail.address             <- destination address

set MAIL_SUBJECT="Resource Coordinator VE (%COMPUTERNAME%) event mail"

set SENDMAIL_VBS=sendmail.vbs

set MAILCMD=cscript"%~dp0%SENDMAIL_VBS%" %MAIL_FROM% %MAIL_TO% %MAIL_SUBJECT%
%MAIL_SERVER_ADDRESS% %1 %2 %3 %4 %5 %6 //nologo
%MAILCMD%
```

Information

The sample sendmail.vbs file (stored in the same folder as trapopt.bat) is making use of Windows CDO (Microsoft Collaboration Data Objects) to connect to an external SMTP server and send e-mail notifications.

For details on VBScript and CDO, refer to the technical reference provided by Microsoft.

[Linux]

Set the following addresses (in the "E-Mail Notification Sample") to match actual environment values.

- Sender address
- Destination address

E-Mail Notification Sample (/etc/opt/FJSVrcvmr/trapop.sh)

```
#!/bin/sh

# MAIL_FROM=from_your@e-mail.address  <- sender address
# MAIL_TO=to_your@e-mail.address      <- destination address

# HOSTNAME=`/bin/uname -n`
# MAILCMD="/usr/sbin/sendmail -t"

# $MAILCMD <<ENDMAIL
# From: $MAIL_FROM
# To: $MAIL_TO
# Subject: Resource Coordinator VE($HOSTNAME) event mail

# -----
# Resource Coordinator VE: event mail
# -----
# $1

# ENDMAIL
```

When actually using this script, remove all comments and enter appropriate addresses.

```
#!/bin/sh

MAIL_FROM=from_your@e-mail.address  <- sender address
MAIL_TO=to_your@e-mail.address      <- destination address

HOSTNAME=`/bin/uname -n`
MAILCMD="/usr/sbin/sendmail -t"

$MAILCMD <<ENDMAIL
From: $MAIL_FROM
To: $MAIL_TO
Subject: Resource Coordinator VE($HOSTNAME) event mail

-----
Resource Coordinator VE: event mail
-----
$1

ENDMAIL
```

 **Information**

.....

The above sample assumes that the sendmail command is available on the Admin Server. Adapt the path to the sendmail command to your own environment if required. The outgoing SMTP server can be defined by changing the sendmail command's configuration files.

.....

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 and MAC 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 the Remote Management Controller for Fujitsu's PRIMERGY servers.

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 backup

A function for LAN switches which is also referred to as backup port.

port VLAN

A VLAN in which the ports of a LAN switch are grouped, and each LAN group is treated as a separate LAN.

port zoning

The division of ports of fibre channel switches into zones, and setting of access restrictions between different zones.

power monitoring devices

Devices used by Resource 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.

- For Fujitsu PRIMERGY servers
 - iRMC2
- For SPARC Enterprise
 - XSCF
- For HP servers
 - iLO2 (integrated Lights-Out)
- For Dell/IBM servers
 - BMC (Baseboard Management Controller)

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 Deployment Manager

Software used to collect and deploy server resources over a network.

ServerView Operations Manager

Software that monitors a server's (PRIMERGY) hardware state, and notifies of errors by way of the network.

ServerView 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.

VIOM (ServerView Virtual-IO Manager)

The name of both the I/O virtualization technology used to change the WWNs of HBAs and the MAC addresses of NICs and the software that performs the virtualization.

Changes to values of WWNs and MAC addresses can be performed by creating a logical definition of a server, called a server profile, and assigning it to a server.

Virtual 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 and ServerView Virtual-IO Manager (VIOM).

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.

XSCF (eXtended System Control Facility)

The name of the Remote Management Controller for SPARC Enterprise.

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.