FUJITSU Software
ServerView Resource Orchestrator V3.4.0

Automatic Quarantining Function User's Guide

Windows

Preface

Purpose of This Document

This manual explains the automatic quarantining function (hereafter, this function) of FUJITSU Software ServerView Resource Orchestrator (hereafter, Resource Orchestrator).

Intended Readers

This manual is written for people who will install, operate, and maintain systems using Resource Orchestrator.

Structure of This Document

This manual is composed as follows:

Chapter 1 Automatic Quarantining Function Overview

Provides an overview of this function.

Chapter 2 Implementing the Automatic Quarantining Function

Explains installation of this function.

Chapter 3 Operation Using the Automatic Quarantining Function

Explains operation when using this function.

Chapter 4 Reference

Explains the commands for this function.

Chapter 5 Messages

Explains the messages that may be output when using this function.

Chapter 6 Advisory Notes

Explains advisory notes regarding use of this function.

Appendix A Customization of Definition Files

Explains how to customize definition files.

Appendix B Corrective Actions for Errors

Explains the corrective actions to take when errors occur when linking configured virtual PCs with L-Servers.

Appendix C Stopping Use

Explains how to stop using this function.

Appendix D Preparations for Automatic Configuration and Operation of Network Devices

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

Web Site URLs

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

Document Conventions

The notation in this manual conforms to the following conventions.

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

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

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

[Windows Manager]

Sections related to Windows manager

[Linux Manager]

Sections related to Linux manager

[Windows]

Sections related to Windows

[Linux]

Sections related to Linux

[Red Hat Enterprise Linux]

Sections related to Red Hat Enterprise Linux

[Solaris]

Sections related to Solaris

[VMware]

Sections related to VMware

[Horizon View]

Sections related to VMware Horizon View

[Hyper-V]

Sections related to Hyper-V

[Xen]

Sections related to RHEL5-Xen

[KVM]

Sections related to RHEL-KVM

[Solaris Zones]

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

[Solaris Zones (Solaris 10)]

Sections related to Solaris Zones with Solaris 10 VM hosts

[Solaris Zones (Solaris 11)]

Sections related to Solaris Zones with Solaris 11 VM hosts

[OVM for x86]

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

[OVM for x86 2.2]

Sections related to Oracle VM Server for x86 2.2

[OVM for x86 3.x]

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

[OVM for SPARC]

Sections related to Oracle VM Server for SPARC

[Citrix Xen]

Sections related to Citrix XenServer

[Physical Servers]

Sections related to physical servers

[Trend Micro OfficeScan]

Sections related to Trend Micro OfficeScan

[Symantec]

Sections related to Symantec Endpoint Protection

[McAfee]

Sections related to McAfee ePolicy Orchestrator

- Unless specified otherwise, the blade servers mentioned in this manual refer to PRIMERGY BX servers.

- Oracle Solaris may also be indicated as Solaris, Solaris Operating System, or Solaris OS.

- Oracle Solaris Zones may also be indicated as Solaris Containers or Solaris Container.

- Oracle VM Server for x86 may also be indicated as Oracle VM.

- In Resource Orchestrator, the following servers are referred to as SPARC Enterprise.

  - SPARC Enterprise M3000/M4000/M5000/M8000/M9000

  - SPARC Enterprise T5120/T5140/T5220/T5240/T5440

- In Resource Orchestrator, the following servers are referred to as SPARC M12.

  - SPARC M12-1/M12-2/M12-2S

- In Resource Orchestrator, the following servers are referred to as SPARC M10.

  - SPARC M10-1/M10-4/M10-4S

- Fujitsu SPARC M12 is the product name used for SPARC M12 when they are sold outside Japan.

- Fujitsu M10 is the product name used for SPARC M10 when they are sold outside Japan.

- In this manual, Fujitsu SPARC M12 is referred to as SPARC M12.

- In this manual, Fujitsu M10 is referred to as SPARC M10.

- In this manual, Fujitsu SPARC M12 and Fujitsu M10 are collectively referred to as SPARC M10/M12.

- In Resource Orchestrator, the following software is referred to as GLS.

  - PRIMECLUSTER GLS 4.4 or earlier

- In Resource Orchestrator, the following software is referred to as GDS.

  - PRIMECLUSTER GDS 4.4 or earlier

- References and character strings or values requiring emphasis are indicated using double quotes (").

- GUI items are shown enclosed by brackets ([ ]).

- The order of selecting menus is indicated using [ ]-[ ].

- Text to be entered by the user is indicated using bold text.

- Variables are indicated using italic text and underscores.

- The ellipses ("...") in menu names, indicating settings and operation window startup, are not shown.

- The ">" used in Windows is included in usage examples. When using Linux, read ">" as meaning "#".

- When using Resource Orchestrator on Windows 8 and Windows Server 2012, please note the following. When OS operations are explained in this manual, the examples assume OSs up to Windows 7 and Windows Server 2008. When using Resource Orchestrator on Windows 8 or Windows Server 2012, take explanations regarding the [Start] menu as indicating the [Apps] screen. The [Apps] screen can be displayed by right-clicking on the [Start] screen and then right-clicking [All apps].

- When using Resource Orchestrator on Windows 8.1 and Windows Server 2012 R2, please note the following. When OS operations are explained in this manual, the examples assume OSs up to Windows 7 and Windows Server 2008. When using Resource Orchestrator on Windows 8.1 or Windows Server 2012 R2, take explanations regarding the [Start] menu as indicating the [Apps] screen. The [Apps] screen can be displayed by swiping the [Start] screen from bottom to top, or clicking the downward facing arrow on the lower-left of the [Start] screen.

Menus in the ROR console

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

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

Regarding Installation Folder Paths

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

Replace it as shown below.

[Virtual Edition]

- When using Windows 64-bit (x64)

   C:\Program Files (x86)\Resource Orchestrator

- When using Windows 32-bit (x86)

   C:\Program Files\Resource Orchestrator

[Cloud Edition]

C:\Program Files (x86)\Resource Orchestrator

Command Examples

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

Abbreviations

The following abbreviations are use in this manual.

Category

Abbreviation

- Products

Windows

Windows

- Microsoft(R) Windows Server(R) 2012 Standard

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

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

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

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

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

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

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

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

- Windows(R) 7 Professional

- Windows(R) 7 Ultimate

- Windows(R) 8.1 Pro

- Windows(R) 8.1 Enterprise

- Windows(R) 10 Pro

- Windows(R) 10 Enterprise

Windows Server 2012

- Microsoft(R) Windows Server(R) 2012 Standard

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

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

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

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

Windows Server 2016

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

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

Windows Server 2019

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

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

Windows PE

- Microsoft(R) Windows(R) Preinstallation Environment

Windows 7

- Windows(R) 7 Professional

- Windows(R) 7 Ultimate

Windows 8.1

- Windows(R) 8.1 Pro

- Windows(R) 8.1 Enterprise

Windows 10

- Windows(R) 10 Pro

- Windows(R) 10 Enterprise

DOS

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

MSFC

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

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

SCVMM

- Microsoft(R) System Center 2012 Virtual Machine Manager

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

- Microsoft(R) System Center 2016 Virtual Machine Manager

Linux

Linux

- Red Hat(R) Enterprise Linux(R) 6.0 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.0 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.1 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.1 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.2 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.3 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.3 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.4 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.4 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.5 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.5 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.6 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.6 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.7 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.7 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.8 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.8 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.9 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.9 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.10 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.10 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 7.0 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 7.1 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 7.2 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 7.4 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 7.5 (for Intel64)

- SUSE(R) Linux Enterprise Server 10 Service Pack 2 for x86

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

- SUSE(R) Linux Enterprise Server 10 Service Pack 3 for x86

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

- SUSE(R) Linux Enterprise Server 11 for x86

- SUSE(R) Linux Enterprise Server 11 for AMD64 & Intel64

- SUSE(R) Linux Enterprise Server 11 Service Pack 1 for x86

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

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

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

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

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

Red Hat Enterprise Linux

- Red Hat(R) Enterprise Linux(R) 6.0 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.0 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.1 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.1 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.2 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.3 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.3 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.4 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.4 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.5 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.5 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.6 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.6 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.7 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.7 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.8 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.8 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.9 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.9 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.10 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.10 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 7.0 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 7.1 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 7.2 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 7.4 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 7.5 (for Intel64)

Red Hat Enterprise Linux 6

- Red Hat(R) Enterprise Linux(R) 6.0 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.0 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.1 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.1 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.2 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.3 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.3 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.4 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.4 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.5 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.5 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.6 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.6 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.7 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.7 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.8 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.8 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.9 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.9 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.10 (for x86)

- Red Hat(R) Enterprise Linux(R) 6.10 (for Intel64)

Red Hat Enterprise Linux 7

- Red Hat(R) Enterprise Linux(R) 7.0 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 7.1 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 7.2 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 7.4 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 7.5 (for Intel64)

SUSE Linux Enterprise Server

- SUSE(R) Linux Enterprise Server 10 Service Pack 2 for x86

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

- SUSE(R) Linux Enterprise Server 10 Service Pack 3 for x86

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

- SUSE(R) Linux Enterprise Server 11 for x86

- SUSE(R) Linux Enterprise Server 11 for AMD64 & Intel64

- SUSE(R) Linux Enterprise Server 11 Service Pack 1 for x86

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

Oracle Enterprise Linux

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

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

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

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

KVM

RHEL-KVM

- Red Hat(R) Enterprise Linux(R) 6.1 (for x86) Virtual Machine Function

- Red Hat(R) Enterprise Linux(R) 6.1 (for Intel64) Virtual Machine Function

- Red Hat(R) Enterprise Linux(R) 6.2 (for x86) Virtual Machine Function

- Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64) Virtual Machine Function

- Red Hat(R) Enterprise Linux(R) 6.3 (for x86) Virtual Machine Function

- Red Hat(R) Enterprise Linux(R) 6.3 (for Intel64) Virtual Machine Function

- Red Hat(R) Enterprise Linux(R) 6.4 (for x86) Virtual Machine Function

- Red Hat(R) Enterprise Linux(R) 6.4 (for Intel64) Virtual Machine Function

- Red Hat(R) Enterprise Linux(R) 6.5 (for x86) Virtual Machine Function

- Red Hat(R) Enterprise Linux(R) 6.5 (for Intel64) Virtual Machine Function

- Red Hat(R) Enterprise Linux(R) 6.6 (for x86) Virtual Machine Function

- Red Hat(R) Enterprise Linux(R) 6.6 (for Intel64) Virtual Machine Function

- Red Hat(R) Enterprise Linux(R) 6.7 (for x86) Virtual Machine Function

- Red Hat(R) Enterprise Linux(R) 6.7 (for Intel64) Virtual Machine Function

- Red Hat(R) Enterprise Linux(R) 6.8 (for x86) Virtual Machine Function

- Red Hat(R) Enterprise Linux(R) 6.8 (for Intel64) Virtual Machine Function

Xen

Xen

- Citrix XenServer(R) 5.5

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

- Citrix XenServer(R) 6.0

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

Citrix

Citrix XenServer

- Citrix XenServer(R) 6.0

- Citrix XenServer(R) 6.0.2

- Citrix XenServer(R) 6.1.0

- Citrix XenServer(R) 6.2.0

- Citrix XenServer(R) 7.1 LTSR

- Citrix XenServer(R) 7.2

- Citrix Hypervisor(R)

XenServer 6

- Citrix XenServer(R) 6.0

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

Citrix XenApp

- Citrix XenApp(R)

- Citrix Virtual Apps(R)

Citrix XenDesktop

- Citrix XenDesktop(R)

- Citrix Virtual Apps and Desktops(R)

Oracle Solaris

Solaris

- Oracle Solaris 10 05/09 (Update7)

- Oracle Solaris 11 11/11

- Oracle Solaris 11.1

- Oracle Solaris 11.2

- Oracle Solaris 11.3

Oracle VM

OVM for x86 2.2

- Oracle(R) VM Server for x86 2.2

OVM for x86 3.x

OVM for x86 3.2

- Oracle VM Server for x86 v3.2.x

OVM for x86 3.3

- Oracle VM Server for x86 v3.3.x

OVM for SPARC

- Oracle(R) VM Server for SPARC

Oracle VM Manager

- Oracle(R) VM Manager

EMC

Navisphere

- EMC Navisphere Manager

Solutions Enabler

- EMC Solutions Enabler

VMware

VMware vSphere or vSphere

- VMware vSphere(R) 4

- VMware vSphere(R) 4.1

- VMware vSphere(R) 5

- VMware vSphere(R) 5.1

- VMware vSphere(R) 5.5

- VMware vSphere(R) 6

- VMware vSphere(R) 6.5

- VMware vSphere(R) 6.7

VMware ESX

- VMware(R) ESX(R)

VMware ESX 4

- VMware(R) ESX(R) 4

VMware ESXi

- VMware(R) ESXi(TM)

VMware ESXi 5.0

- VMware(R) ESXi(TM) 5.0

VMware ESXi 5.1

- VMware(R) ESXi(TM) 5.1

VMware ESXi 5.5

- VMware(R) ESXi(TM) 5.5

VMware ESXi 6.0

- VMware(R) ESXi(TM) 6.0

VMware ESXi 6.5

- VMware(R) ESXi(TM) 6.5

VMware ESXi 6.7

- VMware(R) ESXi(TM) 6.7

VMware Infrastructure Client

- VMware(R) Infrastructure Client

VMware Tools

- VMware(R) Tools

VMware vSphere 4.0 or vSphere 4.0

- VMware vSphere(R) 4.0

VMware vSphere 4.1 or vSphere 4.1

- VMware vSphere(R) 4.1

VMware vSphere 5 or vSphere 5

- VMware vSphere(R) 5

VMware vSphere 5.1 or vSphere 5.1

- VMware vSphere(R) 5.1

VMware vSphere 5.5 or vSphere 5.5

- VMware vSphere(R) 5.5

VMware vSphere 6.0 or vSphere 6.0

- VMware vSphere(R) 6.0

VMware vSphere 6.5 or vSphere 6.5

- VMware vSphere(R) 6.5

VMware vSphere 6.7 or vSphere 6.7

- VMware vSphere(R) 6.7

VMware vSphere Client or vSphere Client

- VMware vSphere(R) Client

VMware vCenter Server or vCenter Server

- VMware(R) vCenter(TM) Server

VMware vCenter Server Appliance or vCenter Server Appliance

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

VMware vClient

- VMware(R) vClient(TM)

VMware FT

- VMware(R) Fault Tolerance

VMware DRS

- VMware(R) Distributed Resource Scheduler

VMware DPM

- VMware(R) Distributed Power Management

VMware Storage VMotion

- VMware(R) Storage VMotion

VMware vDS

- VMware(R) vNetwork Distributed Switch

VMware Horizon View

- VMware Horizon View 5.2.x

- VMware Horizon View 5.3.x

- VMware Horizon 6.0 (with View)

VMware VSAN or VSAN

- VMware(R) Virtual SAN(TM)

VMware vSphere Web Client or vSphere Web Client

- VMware vSphere(R) Web Client

VMware NSX

- VMware NSX(R)

- VMware NSX(R) for vSphere(R)

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

VMware NSX Controller or NSX Controller

- VMware NSX(R) Controller(TM)

VMware NSX Edge or NSX Edge

- VMware NSX(R) Edge(TM)

VMware NSX Manager or NSX Manager

- VMware NSX(R) Manager(TM)

Excel

Excel

- Microsoft(R) Office Excel(R) 2007

- Microsoft(R) Office Excel(R) 2010

- Microsoft(R) Office Excel(R) 2013

Excel 2007

- Microsoft(R) Office Excel(R) 2007

Excel 2010

- Microsoft(R) Office Excel(R) 2010

Excel 2013

- Microsoft(R) Office Excel(R) 2013

Browsers

Internet Explorer

- Windows(R) Internet Explorer(R) 9

- Internet Explorer(R) 10

- Internet Explorer(R) 11

Firefox

- Firefox(R)

Antivirus Software

OfficeScan

- Trend Micro OfficeScan

McAfee ePolicy Orchestrator

- McAfee(R) ePolicy Orchestrator(R)

McAfee ePO

- McAfee(R) ePolicy Orchestrator(R)

McAfee Agent

- McAfee(R) Agent

McAfee Endpoint Security

- McAfee(R) Endpoint Security

Symantec Endpoint Protection

- Symantec(TM) Endpoint Protection

Symantec Endpoint Protection Manager

- Symantec(TM) Endpoint Protection Manager

BMC

BladeLogic

- BMC BladeLogic Server Automation

ETERNUS

ESC

- ETERNUS SF Storage Cruiser

ServerView

ServerView Agent

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

- ServerView Agents Linux

- ServerView Agents VMware for VMware ESX Server

VIOM

- ServerView Virtual-IO Manager

ISM

- ServerView Infrastructure Manager

- Infrastructure Manager

SVOM

- ServerView Operations Manager

SVFAB

- ServerView Fabric Manager

RCVE

- ServerView Resource Coordinator VE

ROR

- FUJITSU Software ServerView Resource Orchestrator

ROR VE

- FUJITSU Software ServerView Resource Orchestrator Virtual Edition

ROR CE

- FUJITSU Software ServerView Resource Orchestrator Cloud Edition

Resource Coordinator

- Systemwalker Resource Coordinator

- Systemwalker Resource Coordinator Virtual server Edition

Resource Coordinator VE

- ServerView Resource Coordinator VE

- Systemwalker Resource Coordinator Virtual server Edition

Resource Orchestrator

- FUJITSU Software ServerView Resource Orchestrator

Export Administration Regulation Declaration

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

Trademark Information

- BMC, BMC Software, and the BMC Software logo are the exclusive properties of BMC Software, Inc., are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries.

- Citrix, Citrix Virtual Apps and Desktops, Citrix Virtual Apps, Citrix Hypervisor, XenApp, XenDesktop, XenServer, Citrix Essentials are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

- EMC, EMC2, CLARiiON, VNX, Symmetrix, and Navisphere are trademarks or registered trademarks of EMC Corporation.

- HP is a registered trademark of Hewlett-Packard Company.

- Linux(R) is a trademark or registered trademark of Linus Torvalds in the United States and other countries.

- McAfee and the McAfee logo, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the United States and other countries.

- Microsoft, Windows, MS-DOS, Windows Server, Windows Vista, Excel, Active Directory, and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

- Firefox is a trademark or registered trademark of the Mozilla Foundation in the United States and other countries.

- NetApp is a registered trademark of Network Appliance, Inc. in the US and other countries. Data ONTAP, Network Appliance, and Snapshot are trademarks of Network Appliance, Inc. in the US and other countries.

- Oracle and Java are registered trademarks of Oracle and/or its affiliates.

- Red Hat, RPM and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries.

- "SUSE" and the SUSE logo are trademarks of SUSE LLC or its subsidiaries or affiliates.

- Symantec and the Symantec logo are trademarks or registered trademarks of the Symantec Corporation or its subsidiaries in the United States and other countries.

- TREND MICRO and OfficeScan are registered trademarks of Trend Micro, Inc.

- VMware, the VMware "boxes" logo and design, Virtual SMP, and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.

- ServerView and Systemwalker are registered trademarks of FUJITSU LIMITED.

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

Notices

- The contents of this manual shall not be reproduced without express written permission from FUJITSU LIMITED.

- The contents of this manual are subject to change without notice.

Revision History

Month/Year Issued, Edition	Manual Code
February 2017, Edition 1.0	J2X1-8079-01ENZ0(00)
April 2017, Edition 2.0	J2X1-8079-02ENZ0(00)
May 2017, Edition 2.1	J2X1-8079-02ENZ0(01)
August 2017, Edition 2.2	J2X1-8079-02ENZ0(02)
September 2017, Edition 2.3	J2X1-8079-02ENZ0(03)
December 2017, Edition 2.4	J2X1-8079-02ENZ0(04)
February 2018, Edition 2.5	J2X1-8079-02ENZ0(05)
March 2018, Edition 2.6	J2X1-8079-02ENZ0(06)
October 2018, Edition 3.0	J2X1-8079-03ENZ0(00)
December 2018, Edition 3.1	J2X1-8079-03ENZ0(01)
December 2018, Edition 3.2	J2X1-8079-03ENZ0(02)
October 2020, Edition 3.3	J2X1-8079-03ENZ0(03)

Copyright Notice

Contents

Chapter 1 Automatic Quarantining Function Overview

This chapter explains the required configuration and other prerequisites for using the automatic quarantining function.

In addition to automatic quarantining or restarting of all affected servers when an infection is detected, it is also possible for an administrator to use their discretion and perform quarantining or restarting with a single click.

1.1 What Is the Automatic Quarantining Function?

In environments in which virtual PCs are used (hereafter, virtual PC environments) and environments in which Server Based Computing is used (hereafter, SBC environments), using the automatic quarantining function of Resource Orchestrator enables security risks to be handled more quickly than in environments in which the function is not used.

Virtual PC environments and SBC environment servers are managed by Resource Orchestrator as L-Servers.

- Virtual PC environments and SBC environment servers operating on VM hosts are managed as virtual L-Servers.

- SBC environment servers operating on physical servers are managed as physical L-Servers.

- Virtual L-Servers and physical L-Servers are collectively referred to as "L-Servers".

The automatic quarantining function provides the following functionality so that corrective action is taken quickly when security risks are detected on L-Servers managed using Resource Orchestrator.

- Action targeting security risks detected on L-Servers can be performed automatically, or manually at the discretion of an administrator.

- The following actions can be performed in response to security risks. Which action is performed can either be selected (hereafter, "action selection") during system preparations.

  Automatically performed actions

   - Transfer from the operation network to the quarantine network

   - Reboot

   - Reboot after transferring from the operation network to the quarantine network

  Actions performed at the discretion of an administrator

   - Sending of mail notifications to the administrator. The administrator can choose whether to perform the same operation as would be performed automatically, according to the content of the email notification which will change based on the situation.

- After transfer to the quarantine network, once security risks have been resolved, the L-Server is recovered from the quarantine network to the operation network.

- When actions are performed automatically when security risks are detected, an email notification is sent to the administrator so that quarantining of the L-Servers on which security risks are detected can begin immediately.

- Message notifications are sent to users to inform them of the reason why they can no longer use virtual PCs when security risks are detected.

* The types of security risks which can cause an L-Server to be quarantined are "viruses" and "malware".

This function does not handle "spyware", "grayware", or "C&C callbacks".

This function does not handle "outbreaks" (occurrences of mass infections or mass failures).

Figure 1.1 Automatic Quarantining Function
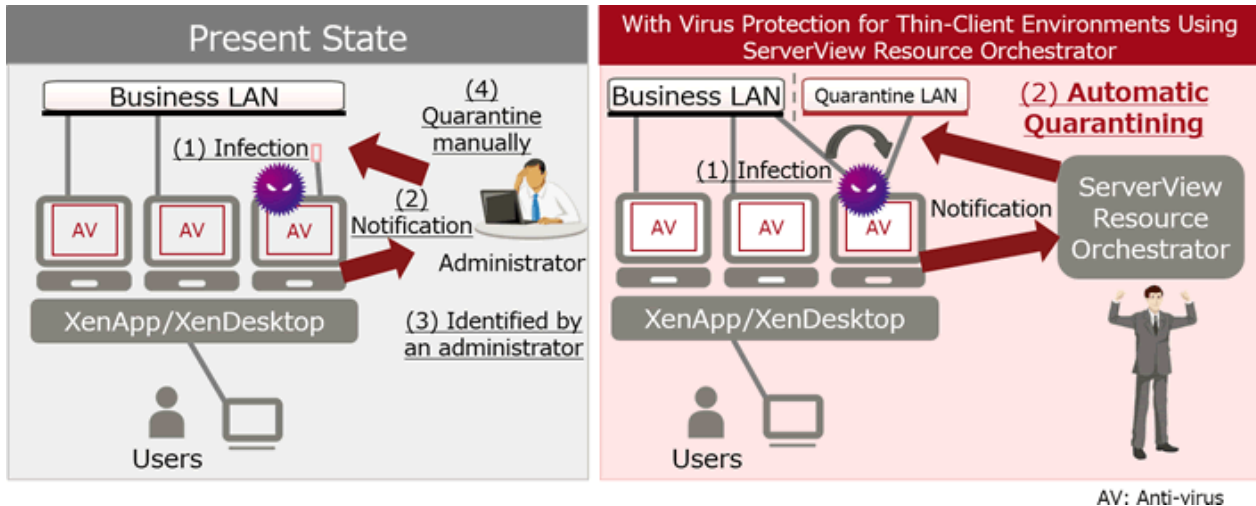
1.2 System Configuration in which the Automatic Quarantining Function Is Used

The automatic quarantining function provides security measures as a solution for environments in which Citrix XenDesktop, Citrix XenApp, other virtualization software, or antivirus software has been installed.

Therefore, it is assumed that the following components in the example configuration have been configured.

- A server operated using something other than Resource Orchestrator

- Management terminals

- Networks (business network, quarantine network, and management network)

Note
....
Connect only the Resource Orchestrator manager to the management network.
....

- SBC environments deployed on physical servers using Citrix XenApp

[VMware]

- Virtual PC environments deployed on VMware vSphere (VMware ESXi) using Citrix XenDesktop

- SBC environments deployed on VMware vSphere (VMware ESXi) using Citrix XenApp

[Hyper-V]

- Virtual PC environments deployed on Hyper-V on Windows Server 2016 using Citrix XenDesktop

- SBC environments deployed on Hyper-V on Windows Server 2016 using Citrix XenApp

[Citrix Xen]

- Virtual PC environments deployed on Citrix XenServer using Citrix XenDesktop

- SBC environments deployed on Citrix XenServer using Citrix XenApp

Virtual PC

In this manual, "virtual PCs" collectively refers to the following:

[VMware]

- Virtual machines deployed on VMware vSphere (VMware ESXi) using Citrix XenDesktop

- SBC environment servers deployed on VMware vSphere (VMware ESXi) using Citrix XenApp

[Hyper-V]

- Virtual machines deployed on Hyper-V on Windows Server 2016 using Citrix XenDesktop

- SBC environment servers deployed on Hyper-V on Windows Server 2016 using Citrix XenApp

[Citrix Xen]

- Virtual machines deployed on Citrix XenServer using Citrix XenDesktop

- SBC environment servers deployed on Citrix XenServer using Citrix XenApp

SBC Servers

In this manual, "SBC servers" refers to the following servers.

- SBC environment servers deployed on physical servers using Citrix XenApp

Operation Network

In this manual, "operation network" collectively refers to the following networks:

For Virtual PCs

[VMware]

- Business networks of virtual PCs deployed on VMware vSphere (VMware ESXi) using Citrix XenDesktop

[Hyper-V]

- Business networks of virtual PCs deployed on Hyper-V on Windows Server 2016 using Citrix XenDesktop

[Citrix Xen]

- Business networks of virtual PCs deployed on Citrix XenServer using Citrix XenDesktop

For SBC servers

- Business networks of SBC servers deployed on physical servers using Citrix XenApp

- Management networks of SBC servers deployed on physical servers using Citrix XenApp

When receiving email notification when a security risk is detected on an L-Server and then performing corrective action, it is possible to set a different administrator to be notified for each group of L-Servers. It is possible to manage a group of L-Servers with the same administrator using a unit referred to as a tenant.

The pools in which resources are managed are each created using a combination of a tenant and a resource type. On the manager, create a pool for resources which are related to L-Servers that do not belong to a tenant.

However, when using this function in large-scale environments where there are large numbers of L-Servers to be managed, refer to "1.3 Configuration for Managing Large-scale Environments".

📙 Note
. . . .

When using this function, use Virtual Edition. When using a platform provision service other than this function, use Cloud Edition.

- This function does not support environments in which tenants are used or in which multiple L-Servers are configured with the same IP address.

- This function supports environments that use folders, but does not support environments containing L-Servers with the same name under different folders.

- This function cannot be used for L-Servers under L-Platforms.

- Configured physical servers with UMC enabled cannot be correctly linked with L-Servers. Disable UMC before performing server registration.

- This function does not support environments in which multiple virtual PCs configured with the same name are deployed on different VM hosts.

[VMware]

- When using a VDS (distributed virtual switch) in a network configuration with virtual PCs, the following definition procedure must be performed in advance.

    - "E.1.4 Network Preparations" in the "Design Guide CE"

        - When Using Distributed Virtual Switch (VMware vDS)

When two networks with the same name exist on both a standard switch and a virtual switch, if that network name is specified as the target network for server switchover, then the switchover will be performed targeting the network on the standard switch.

To perform switchover to a network on a VDS, ensure that the network has a unique name in the system.

1.2.1 [VMware] Example Configuration of an Environment in which the Automatic Quarantining Function Is Implemented

An example configuration is shown below.

Figure 1.2 [VMware] [Trend Micro OfficeScan] Example Configuration of an Environment in which the Automatic Quarantining Function Is Implemented
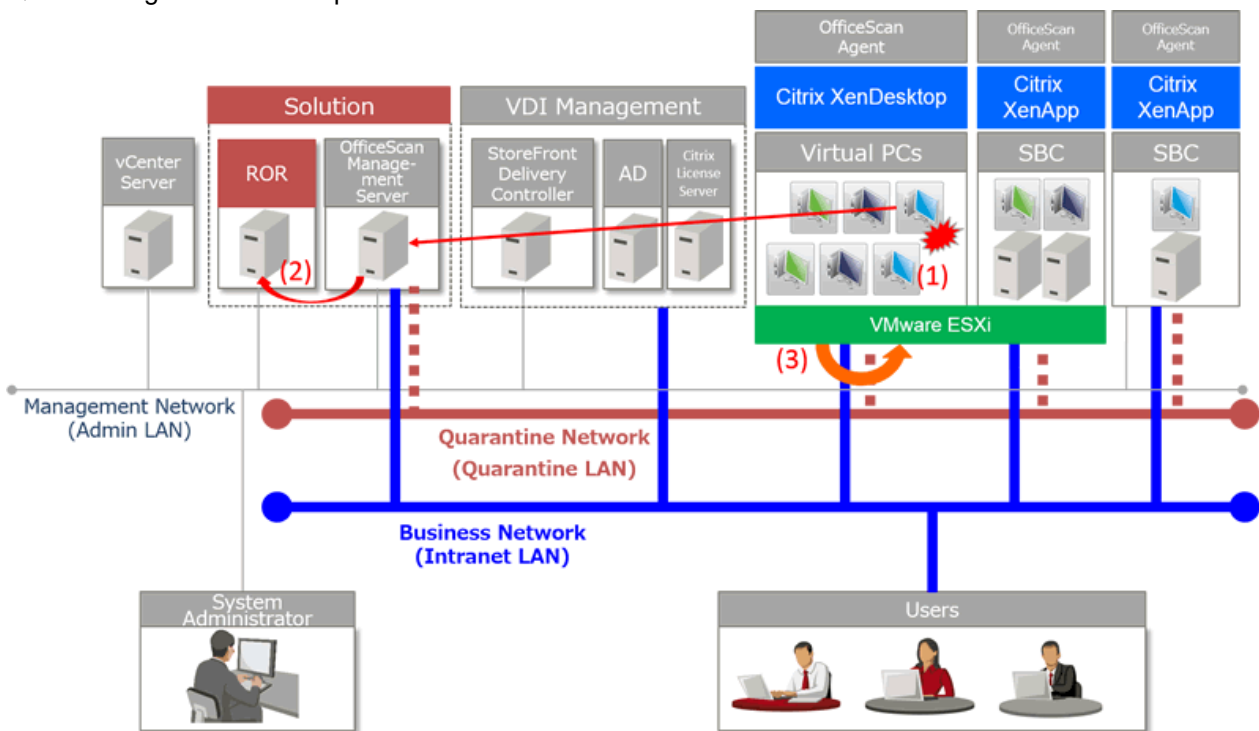
(1) Notification of virus detection

(2) When a virus is detected, Resource Orchestrator is notified using an SNMP trap

(3) When a virus is detected, the relevant virtual PC or SBC server is automatically quarantined by Resource Orchestrator

Figure 1.3 [VMware] [Symantec] Example Configuration of an Environment in which the Automatic Quarantining Function Is Implemented

SEP: Symantec Endpoint Protection Manager

(1) Notification of virus detection

(2-1) When a virus is detected, the Symantec coordination batch file provided by Resource Orchestrator is executed by Symantec Endpoint Protection Manager

(2-2) After being executed, the Symantec coordination batch file uses a REST-API to notify Resource Orchestrator

(3) When a virus is detected, the relevant virtual PC or SBC server is automatically quarantined by Resource Orchestrator

Figure 1.4 [VMware] [McAfee] Example Configuration of an Environment in which the Automatic Quarantining Function Is Implemented
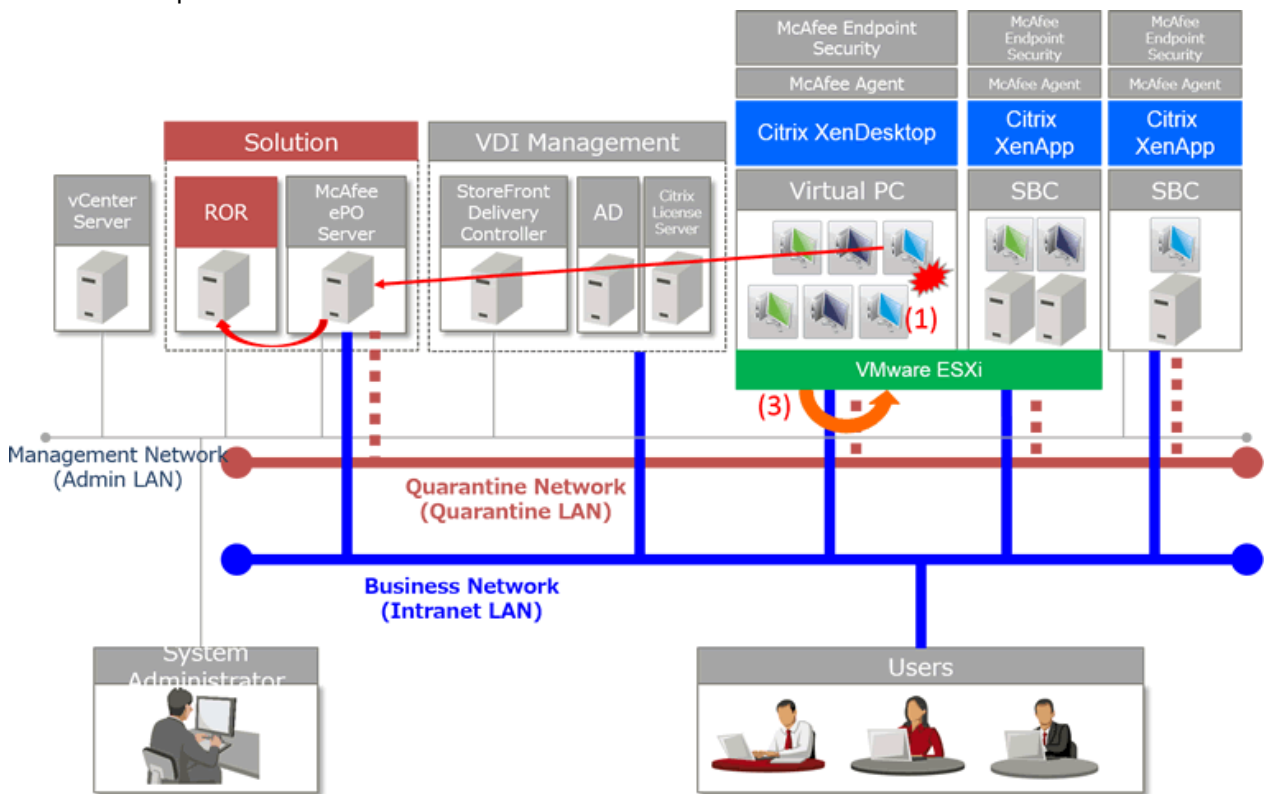
(1) Notification of virus detection

(2) When a virus is detected, Resource Orchestrator is notified using an SNMP trap

(3) When a virus is detected, the relevant virtual PC or SBC server is automatically quarantined by Resource Orchestrator

1.2.2 [Hyper-V] Example Configuration of an Environment in which the Automatic Quarantining Function Is Implemented

An example configuration is shown below.

Figure 1.5 [Hyper-V] [Trend Micro OfficeScan] Example Configuration of an Environment in which the Automatic Quarantining Function Is Implemented
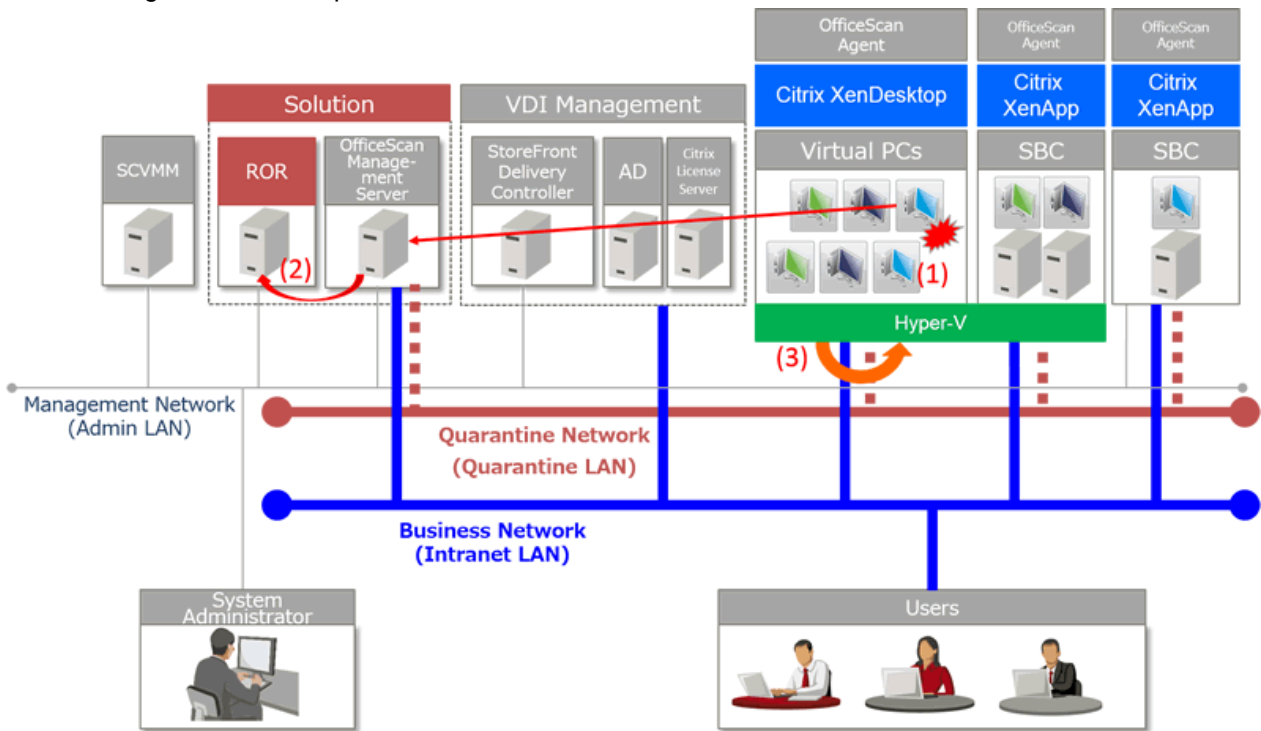
(1) Notification of virus detection

(2) When a virus is detected, Resource Orchestrator is notified using an SNMP trap

(3) When a virus is detected, the relevant virtual PC or SBC server is automatically quarantined by Resource Orchestrator

Figure 1.6 [Hyper-V] [Symantec] Example Configuration of an Environment in which the Automatic Quarantining Function Is Implemented

SEP: Symantec Endpoint Protection Manager

(1) Notification of virus detection

(2-1) When a virus is detected, the Symantec coordination batch file provided by Resource Orchestrator is executed by Symantec Endpoint Protection Manager

(2-2) After being executed, the Symantec coordination batch file uses a REST-API to notify Resource Orchestrator

(3) When a virus is detected, the relevant virtual PC or SBC server is automatically quarantined by Resource Orchestrator

Figure 1.7 [Hyper-V] [McAfee] Example Configuration of an Environment in which the Automatic Quarantining Function Is Implemented
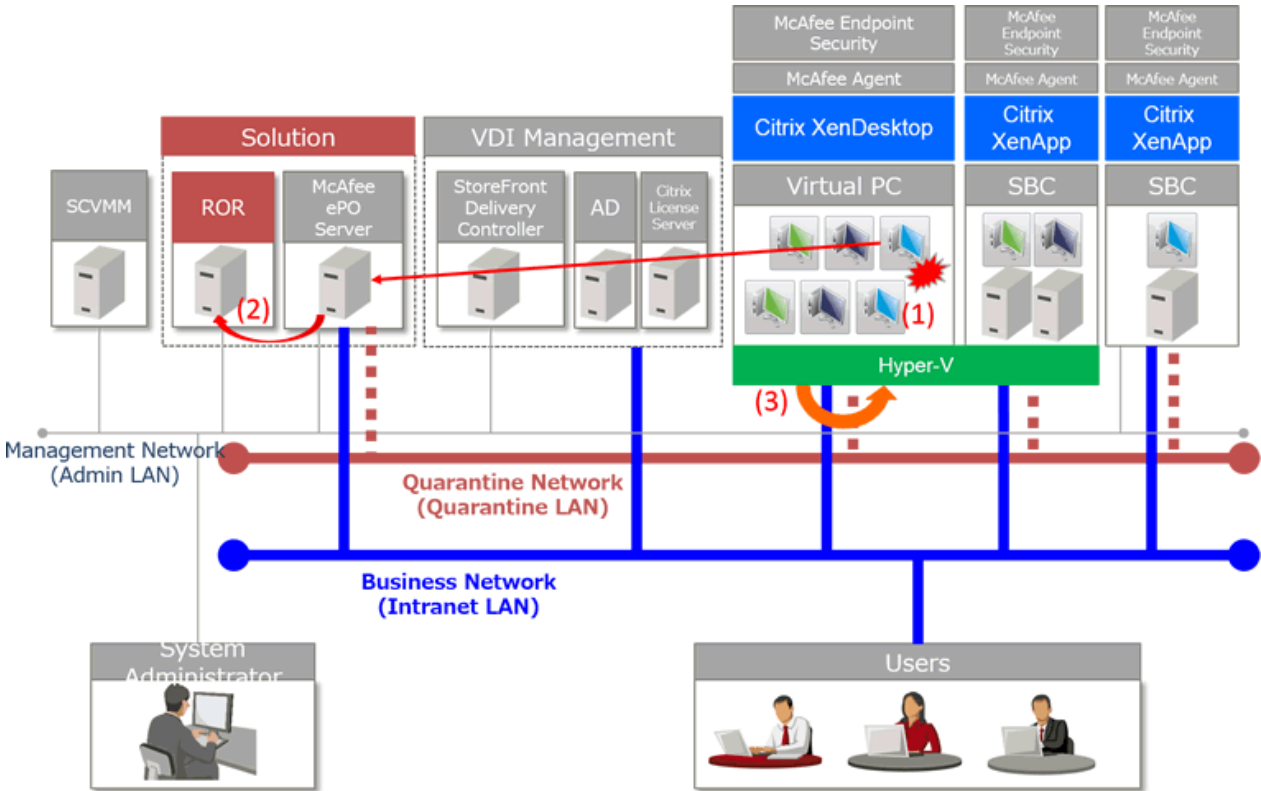
(1) Notification of virus detection

(2) When a virus is detected, Resource Orchestrator is notified using an SNMP trap

(3) When a virus is detected, the relevant virtual PC or SBC server is automatically quarantined by Resource Orchestrator

1.2.3 [Citrix Xen] Example Configuration of an Environment in which the Automatic Quarantining Function Is Implemented

An example configuration is shown below.

Figure 1.8 [Citrix Xen] [Trend Micro OfficeScan] Example Configuration of an Environment in which the Automatic Quarantining Function Is Implemented
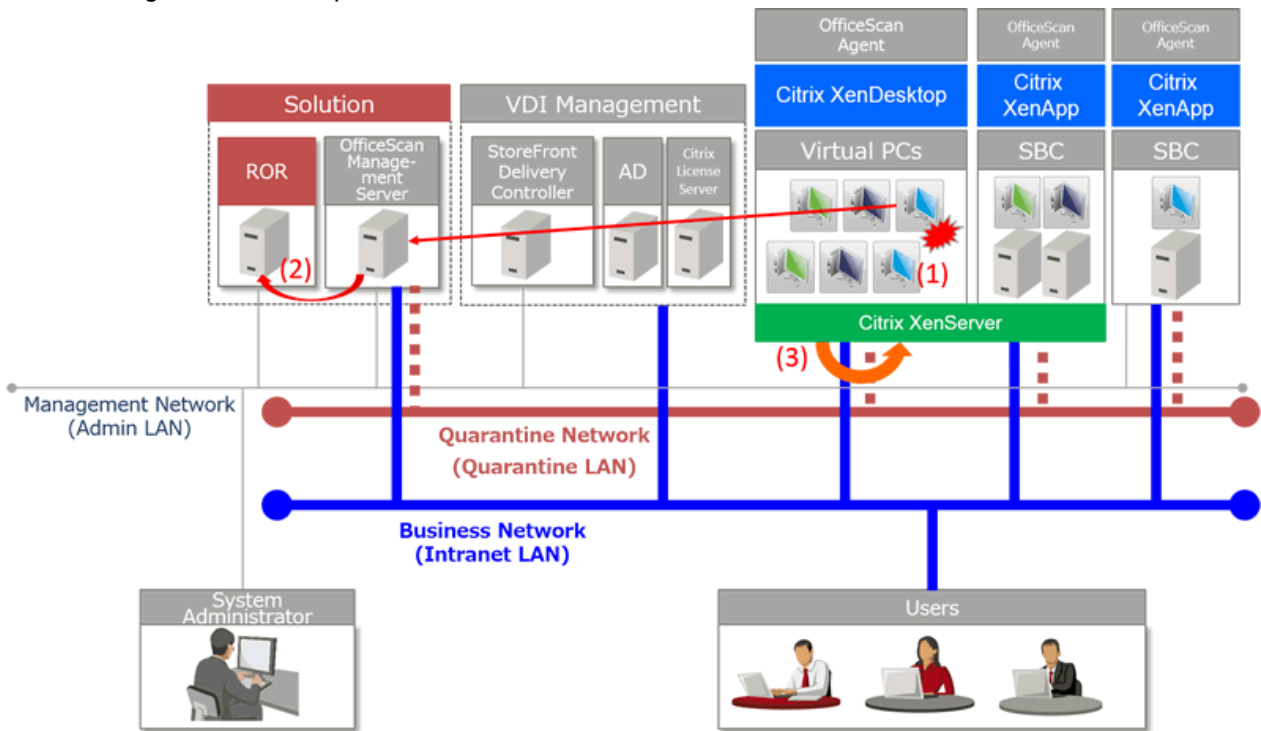
(1) Notification of virus detection

(2) When a virus is detected, Resource Orchestrator is notified using an SNMP trap

(3) When a virus is detected, the relevant virtual PC or SBC server is automatically quarantined by Resource Orchestrator

Figure 1.9 [Citrix Xen] [Symantec] Example Configuration of an Environment in which the Automatic Quarantining Function Is Implemented

SEP: Symantec Endpoint Protection Manager

(1) Notification of virus detection

(2-1) When a virus is detected, the Symantec coordination batch file provided by Resource Orchestrator is executed by Symantec Endpoint Protection Manager

(2-2) After being executed, the Symantec coordination batch file uses a REST-API to notify Resource Orchestrator

(3) When a virus is detected, the relevant virtual PC or SBC server is automatically quarantined by Resource Orchestrator

Figure 1.10 [Citrix Xen] [McAfee] Example Configuration of an Environment in which the Automatic Quarantining Function Is Implemented
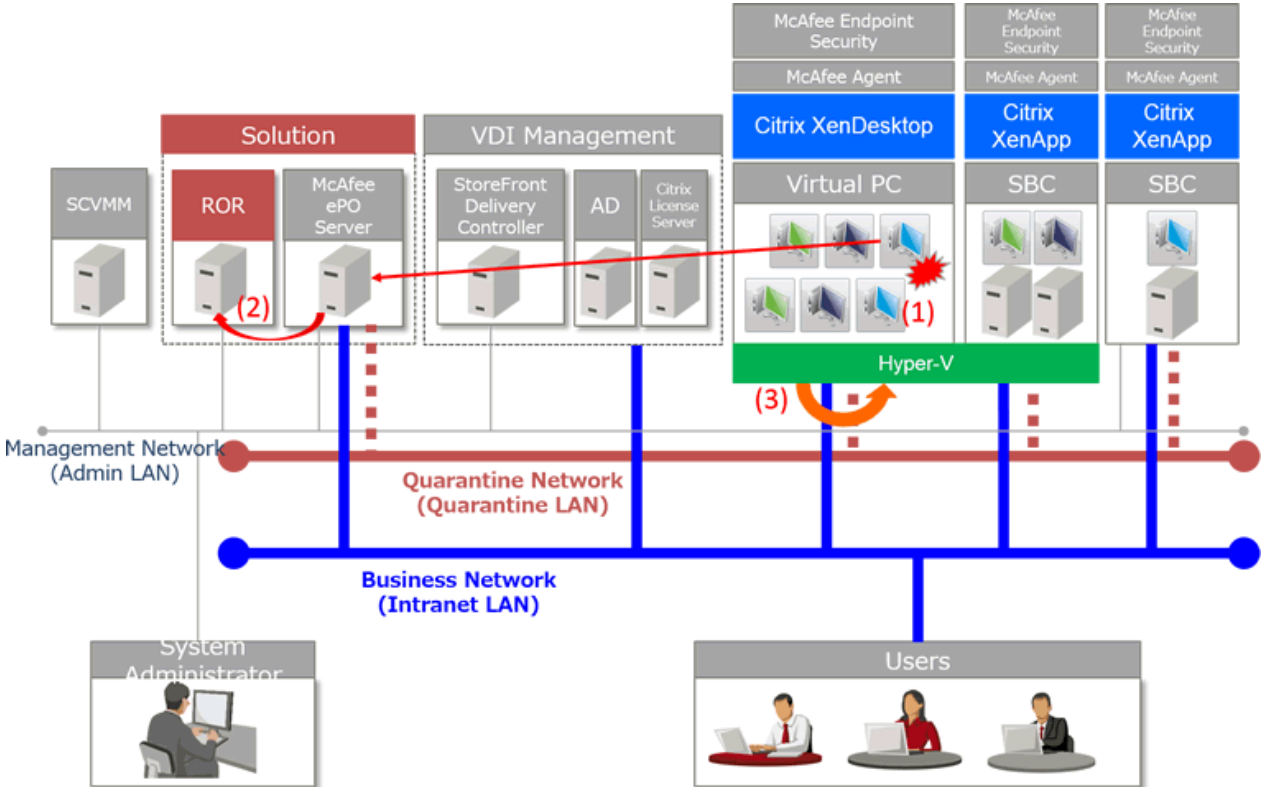
(1) Notification of virus detection

(2) When a virus is detected, Resource Orchestrator is notified using an SNMP trap

(3) When a virus is detected, the relevant virtual PC or SBC server is automatically quarantined by Resource Orchestrator

1.3 Configuration for Managing Large-scale Environments

The number of VMs that a single Resource Orchestrator manager can manage is limited as shown below. To manage more VMs than the limit it is necessary to use multiple managers.

When using this function

When operating in a VMware environment using Virtual Edition	2,500 VMs
In all other cases	1500 VMs

Therefore, in configurations where there are multiple Resource Orchestrator managers, the first manager of Resource Orchestrator sends notifications/requests to the other managers (hereafter, sub managers) if necessary, and the automatic quarantining function operates in coordination.

An example of automatic quarantining from a sub manager is shown in Figure 1.11 Example of a Configuration with Multiple Managers.

Figure 1.11 Example of a Configuration with Multiple Managers
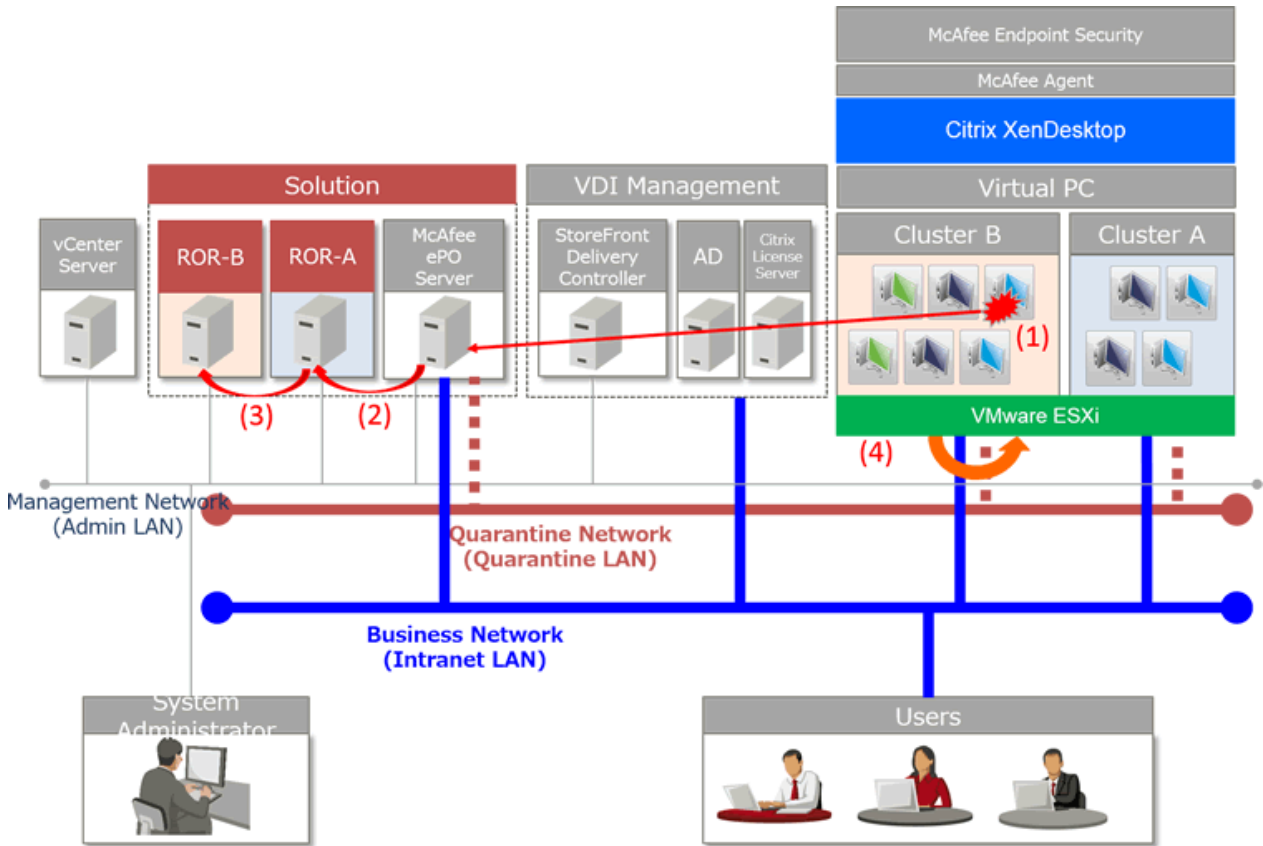
(1) Notification of virus detection

(2) When a virus is detected, the first Resource Orchestrator (hereafter, the first manager) is notified using an SNMP trap

(3) As the relevant L-Server is managed by a sub manager, the relevant sub manager is notified

(4) When a virus is detected, the relevant virtual PC or SBC server is automatically quarantined by the sub manager

📝 **Note**

....

- In configurations where there are multiple Resource Orchestrator managers, perform configuration so virtual machines belonging to the same cluster are managed by the same Resource Orchestrator manager. In addition, perform configuration so L-Servers that are moved between servers using HA, etc. are still managed by the same manager.

- As with a cluster, perform configuration so that tenants are also managed by the same Resource Orchestrator manager.

....

1.4 Prerequisites for Using the Automatic Quarantining Function

In addition to Resource Orchestrator, the following software is required to use the automatic quarantining function. When using a configuration in which there are multiple managers, ensure that the environment of each manager is the same as the manager environment described below.

This tool can be used in the following environments.

Version of Resource Orchestrator

FUJITSU Software ServerView Resource Orchestrator V3.4.0

Resource Orchestrator Manager

- Windows manager

For details, refer to the following.

[Virtual Edition]

"Table 6.2 [Windows Manager]" in "6.1.1.1 Required Basic Software" in the "Overview"

[Cloud Edition]

"Table 6.47 [Windows Manager]" in "6.1.1.1 Required Basic Software" in the "Overview"

Required software for the Resource Orchestrator manager

- Windows PowerShell 3.0 or later

[Trend Micro OfficeScan]

- SNMP Trap Service (Standard OS service) (*1, *2)

*1: Ensure that community names conform to the community name set for the OfficeScan 11.0 server or the OfficeScan XG server.

*2: The following port is used when using this function.

Sender		Receiver				Protocol
Server	Port	Server	Service	Port	Modification	
OfficeScan 11.0 server or OfficeScan XG server	Indefinite	Admin server	snmptrap	162	Not possible	udp

[McAfee]

- SNMP Trap Service (Standard OS service) (*1, *2)

*1: Ensure that community names conform to the community name set for the McAfee ePolicy Orchestrator v5.9 server.

*2: The following port is used when using this function.

Sender		Receiver				Protocol
Server	Port	Server	Service	Port	Modification	
McAfee ePolicy Orchestrator v5.9 server	Indefinite	Admin server	snmptrap	162	Not possible	udp

[Symantec]

There is no required software.

The following port is used when using this function.

Sender		Receiver				Protocol
Server	Port	Server	Service	Port	Modification	
Symantec Endpoint Protection management server	Indefinite	Admin server	rcxweb	23461	Not possible	tcp

[VMware]

- VMware vCenter Server 6.0

- VMware vCenter Server 6.5

- VMware vCenter Server 6.7

It can be placed on the admin server with the manager, or on any other server.

- VMware vSphere PowerCLI 6.0 or later

> 📄 **Note**
> ....
> - When using VMware vSphere 6.7, install VMware PowerCLI 10.1.0 or later.
>
> - When using VMware PowerCLI 6.5.1 or later, it is necessary to execute VMware PowerCLI from Windows PowerShell (x86).

Perform installation so the VMware PowerCLI module is located on the following path.

```
C:\Program Files (x86)\WindowsPowerShell\Modules
```

- After installing VMware PowerCLI, start the Windows PowerShell console using administrator privileges, and execute the following.

    1. Change the Windows PowerShell execution policies.

    ```
    > Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
    ```

    2. Change the settings for security warnings of VMware PowerCLI. (VMware PowerCLI 10.0.0 or later)

    ```
    > Set-PowerCLIConfiguration -InvalidCertificateAction Warn -Scope AllUsers
    ```

[Hyper-V]

- Microsoft(R) System Center 2016 Virtual Machine Manager

It can be placed on the admin server with the manager, or on any other server.

[Citrix Xen]

- None.

Antivirus Software

[Trend Micro OfficeScan]

- OfficeScan 11.0 server or OfficeScan XG server

Notifies Resource Orchestrator of security risks detected on VM guests and physical L-Servers.

It can be placed on the admin server with the manager, on the VM management software, or on any other server.

Multiple OfficeScan 11.0 servers or OfficeScan XG servers can be registered as antivirus software.

[Symantec]

- Symantec Endpoint Protection Manager 14.0

Notifies Resource Orchestrator of security risks detected on VM guests and physical L-Servers.

It can be placed on the admin server with the manager, on the VM management software, or on any other server.

It is not possible to register multiple Symantec Endpoint Protection Manager servers in Resource Orchestrator.

- Windows PowerShell 3.0 or later

This must be installed on the Symantec Endpoint Protection Manager server as the execution environment for the script used to notify the Resource Orchestrator manager of security risks.

[McAfee]

- McAfee ePolicy Orchestrator v5.9

Notifies Resource Orchestrator of security risks detected on VM guests and physical L-Servers.

It can be placed on the admin server with the manager, on the VM management software, or on any other server.

Multiple McAfee ePolicy Orchestrator servers can be registered as antivirus software.

For details on required software other than the above, refer to the following.

[Virtual Edition]

"6.1.1.4 Required Software" in the "Overview"

[Cloud Edition]

"6.1.2.4 Required Software" in the "Overview"

Required hardware for the Resource Orchestrator manager

For details, refer to "Table 2.1 Admin Server Hardware Specifications".

Basic software for Resource Orchestrator agents

For VM hosts

[VMware]

- VMware vSphere 6.0

- VMware vSphere 6.5

- VMware vSphere 6.7

[Hyper-V]

- Windows Server 2016

[Citrix Xen]

- Citrix XenServer 7.1 LTSR or Citrix XenServer 7.2

For SBC servers operating on physical servers

- Windows

For details, refer to the following.

[Virtual Edition]

"Table 6.4 Agent [Windows]" in "6.1.1.1 Required Basic Software" in the "Overview"

[Cloud Edition]

"Table 6.49 Agent [Windows]" in "6.1.1.1 Required Basic Software" in the "Overview"

Required software for Resource Orchestrator agents

For VM hosts

[Hyper-V]

- ServerView Agents for Windows

For details, refer to the following.

[Virtual Edition]

"Table 6.35 Agent [Windows] [Hyper-V]" in "6.1.1.4 Required Software" in the "Overview"

[Cloud Edition]

"Table 6.85 Agent [Windows]" in "6.1.2.4 Required Software" in the "Overview"

- Resource Orchestrator agent

For SBC servers operating on physical servers

- ServerView Agents for Windows

For details, refer to the following.

[Virtual Edition]

"Table 6.35 Agent [Windows] [Hyper-V]" in "6.1.1.4 Required Software" in the "Overview"

[Cloud Edition]

"Table 6.85 Agent [Windows]" in "6.1.2.4 Required Software" in the "Overview"

- Resource Orchestrator agent

Required patches for Resource Orchestrator agents

For VM hosts

[Hyper-V]

- Use Microsoft Update, etc. to apply the latest updates to Windows Server 2016 and Windows guest OSs.

- For Windows guest OSs, update KB3063109 is required. Apply KB3063109 using Microsoft Update, etc.

- It is necessary to install the latest available integration services on each VM guest OS.

Required hardware for Resource Orchestrator agents

For Virtual PCs

[VMware]

Operates on the following servers

- VMware vSphere 6.0

- VMware vSphere 6.5

- VMware vSphere 6.7

For details, refer to the vSphere column in "Table 6.110 Required Hardware Conditions for Agents" in "6.2.1 All Editions" in the "Overview".

[Hyper-V]

- A Fujitsu server on which Hyper-V on Windows Server 2016 will operate

For details, refer to the Hyper-V column in "Table 6.110 Required Hardware Conditions for Agents" in "6.2.1 All Editions" in the "Overview".

[Citrix Xen]

- A server on which Citrix XenServer 7.1 LTSR or Citrix XenServer 7.2 will operate

For SBC servers operating on physical servers

- PRIMERGY RX servers

Basic software for thin clients

- Necessary when using virtual PCs.

  - Citrix XenDesktop (R)

  - Citrix Virtual Apps and Desktops(R) 7 1808

- In the above versions, it is possible to enable notification of quarantining.

  - Citrix Virtual Apps and Desktops(R) 7 1808

  - Citrix XenDesktop(R) 7 - 7.18

- Necessary when using either of the following environments:

  - Citrix XenApp (R)

  - Citrix Virtual Apps(R) 7 1808

    #### SBC servers deployed on VM hosts

    ##### [VMware]

    SBC servers deployed on VMware vSphere (VMware ESXi)

    ##### [Hyper-V]

    SBC servers deployed on Hyper-V on Windows Server 2016

    ##### [Citrix Xen]

    SBC servers deployed on Citrix XenServer

SBC servers deployed on physical servers

In the above versions, it is possible to enable notification of quarantining.

- Citrix Virtual Apps(R) 7 1808

- Citrix XenApp(R) 7.5 - 7.18

[VMware] Virtual NICs for VM guests

The following virtual NICs are supported:

- E1000e

- E1000

- VMXNET3

Basic software for VM guests and physical L-Servers

[Trend Micro OfficeScan]

- OSs supported by OfficeScan 11.0 agents or OfficeScan XG agents

[McAfee]

- OSs supported by McAfee Agent and McAfee Endpoint Security

[Symantec]

- OSs supported by Symantec Endpoint Protection agents

P Point

. . . .

To perform the quarantining process, the infrastructure administrator needs to know the user ID and password for the OS administrator of each VM guest and physical L-Server.

. . . .

Required software for VM guests and physical L-Servers

[Trend Micro OfficeScan]

- OfficeScan 11.0 agents or OfficeScan XG agents

[McAfee]

- McAfee Agent and McAfee Endpoint Security

[Symantec]

- Symantec Endpoint Protection Agents

Required hardware for physical L-Servers

- L2 switches

For details, refer to the following in the "Overview".

[Virtual Edition]

"Table 6.111 Supported Network Devices" in "6.2.2 Virtual Edition"

[Cloud Edition]

"Table 6.114 Supported Network Devices" in "6.2.3 Cloud Edition"

Chapter 2 Implementing the Automatic Quarantining Function

This chapter explains the procedure for implementing the automatic quarantining function. When multiple managers are configured, perform the following procedure for each of them. Do the same when adding sub managers after operations have commenced.

2.1 Preparations for Using the Automatic Quarantining Function

This section explains the preparations for using the automatic quarantining function.

The following settings are required as preparation.

In configurations where there are multiple Resource Orchestrator managers, only one Resource Orchestrator manager (hereafter, the first manager) can be specified from the antivirus software.

Perform the settings below for the first manager.

Antivirus Software

[Trend Micro OfficeScan]

OfficeScan 11.0 Server or OfficeScan XG Server

- Check "Enable notification via SNMP trap" in the Virus/Malware sections of the SNMP trap notification settings of Administrator Notification Settings, and define the message to be sent as follows.

```
virus_name:%v,ip_address:%i,file:%p,datetime:%y,result:%a
```

- If it is necessary for email notifications to be sent to the administrator, configure the email notification settings for the administrator so that an email is sent to the email address of the administrator when a virus or malware is detected.

- Specify the IP address of the Resource Orchestrator manager in the SNMP trap notification settings of the General Notification Settings.

For details, refer to the manuals of OfficeScan 11.0 server or OfficeScan XG server.

[McAfee]

- Register the SNMP server of Resource Orchestrator in the McAfee ePolicy Orchestrator server

Open "Registered Servers" in the McAfee ePolicy Orchestrator Web console, then click "New Server", and register the SNMP server of Resource Orchestrator.

Ensure the following items are entered as follows:

Address

Select "IPv4" for the type of the server address, and configure the IP address of the Resource Orchestrator manager.

SNMP server version

For the SNMP server version, select "SNMPv1", and specify the community string under "Security".

- For details on this operation, refer to "Register SNMP servers" in the product guide of McAfee ePolicy Orchestrator.

The above guide contains the procedure for sending test traps, but as Resource Orchestrator does not support test traps it is not necessary to perform this procedure.

- Configure notification settings by adding an automatic response rule for the McAfee ePolicy Orchestrator server

On the McAfee ePolicy Orchestrator server Web console, select "Automatic Responses" > "New Response" and add automatic response rules to enable notification of security risks to the Resource Orchestrator manager using SNMP traps and notification of the administrator using e-mail.

Ensure the following items are entered as follows:

Description

Select "Enable" for "Status".

Filters

Select "Threat Category", and configure "Malware" for the "Belongs to" setting.

Actions

- Notification of security risks using SNMP traps

Select "Send SNMP Trap".

Specify the SNMP server registered in "Registered Servers".

Define the values to be sent in SNMP traps by selecting "Value" for "Available Types" and then adding all values using the [>>] button.

- Notification of security risks using email

Select "Send Email".

Click "..." next to "Recipients" and select the recipients for messages.

Specify the subject and the body of the email.

- For details, refer to "Setting up automatic responses" in the product guide of McAfee ePolicy Orchestrator.

- Install McAfee Agent and deploy McAfee Endpoint Security on virtual PCs and physical servers

Refer to the following in the product guide of McAfee ePolicy Orchestrator:

- "Installing the McAfee Agent and licensed software" in "Setting up your McAfee ePO server"

- "Deploying products" in "Advanced configuration"

[Symantec]

1. Place the Symantec coordination batch file and script files

The compressed file (SEPMfile.zip) containing the Symantec coordination batch file and script files is stored in the following folder on the Resource Orchestrator manager.

```
Installation_folder\SVROR\Manager\opt\FJSVrcxmr\sys\SEPM
```

Store SEPMfile.zip in the following folder on the Symantec Endpoint Protection Manager server, and extract its content there.

```
drive\Symantec\Symantec Endpoint Protection Manager\bin
```

The descriptions, file names, and storage locations of the Symantec coordination batch file and each script file that are extracted are given below. Confirm that all of the files were successfully extracted.

If extraction was successful, delete SEPMfile.zip.

Symantec coordination batch file

The batch file that is run when the SEP Manager notifies Resource Orchestrator that a virus has been detected.

- File name

```
rcx_quarantine_lserver.bat
```

- File extraction location

```
drive\Symantec\Symantec Endpoint Protection Manager\bin
```

Symantec coordination script file

The PowerShell script file called by rcx_quarantine_lserver.bat.

- File name

```
rcx_quarantine_lserver.ps1
```

- File extraction location

```
drive\Symantec\Symantec Endpoint Protection Manager\bin\ResourceOrchestrator\bin
```

Script file for registering Resource Orchestrator user information

The script file for registering Resource Orchestrator user information with the Symantec Endpoint Protection Manager.

- File name

```
rcx_register_ror.ps1
```

- File extraction location

```
drive\Symantec\Symantec Endpoint Protection Manager\bin\ResourceOrchestrator\cmd
```

2. Execute the script file for registering Resource Orchestrator user information

   a. Change the PowerShell execution policy

   On the Symantec Endpoint Protection Manager server, change the PowerShell execution policy to "RemoteSigned".

   Start the PowerShell console using administrator privileges and execute the following command.

```
PS > Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
```

   b. Execute the following command to change the current directory.

```
PS > Set-Location -Path 'drive\Symantec\Symantec Endpoint Protection Manager\bin
\ResourceOrchestrator\cmd'
```

   c. Execute the following command to register Resource Orchestrator user information.

   For the Resource Orchestrator user ID, specify the user account name for logging in as the privileged user that was created during installation of Resource Orchestrator.

```
PS > ./rcx_register_ror.ps1 create -host
IP_address_or_host_name_(FQDN)_of_the_Resource_Orchestrator_manager -user
Resource_Orchestrator_user_account_name -password password
```

   If information is already registered, the following message will be output.

   If you wish to overwrite the information, enter "y".

```
INFO:230:Information already exists. Overwrite it? [y/n]
```

   d. Confirm that the Resource Orchestrator user information has been registered. Execute the following command.

```
PS > ./rcx_register_ror.ps1 show
```

   📊 Example
   ●

```
PS > ./rcx_register_ror.ps1 show
HOST:192.168.10.40
PORT:23461
USER:manage
PASSWORD:*******
```
   ●

   For the script file for registering Resource Orchestrator user information, refer to "5.6 [Symantec] Messages Output during Execution of the rcx_register_ror.ps1 Command".

3. Configure the settings for notifying Resource Orchestrator when a security risk is detected

   Enable the Symantec Endpoint Protection Manager to notify the Resource Orchestrator manager when it detects a security risk.

   To configure the settings, perform the following procedure from the Symantec Endpoint Protection Manager Web console:

   a. Open the [Monitors] > [Notifications] tab on the left pane and click [Notification Conditions] on the lower right.

   b. Click [Add] on the top left and select "Single risk event".

   c. On the window for editing notification conditions, check "Run the batch or executable file:".

    d. Enter the name of the Symantec coordination batch file (rcx_quarantine_lserver.bat) and click "OK".

For details on this operation, refer to "Setting up administrator notifications" in the "Symantec Endpoint Protection 14 Installation and Administration Guide".

  4. Configure settings for calling the Symantec coordination batch file

In order to enable calling of the Symantec coordination batch file, edit the following configuration file.

```
drive\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\semlaunchsrv.properties
```

Add the following line to the end of the file.

```
sem.launchsrv.authorized.userdefined.tasks=bin\\notification.bat|bin\
\rcx_quarantine_lserver.bat
```

After editing the configuration file, rebooting the following server enables calling of the Symantec coordination batch file.

- Symantec Embedded Database

- Symantec Endpoint Protection Manager

- Symantec Endpoint Protection Launcher

- Symantec Endpoint Protection Manager Web Server

  5. Configure email notification settings for the administrator

Configure the email notification settings for the administrator so email is sent to the email address of the administrator whenever a virus or malware is detected.

Note that this email is sent from Symantec Endpoint Protection Manager.

It is different from the email set in "2.7 Procedure for Configuring Email Notification to the Administrator".

Virtual PCs

Perform one of the following.

[Trend Micro OfficeScan]

- Install the OfficeScan 11.0 agent, and perform configuration so the agent is managed by the OfficeScan 11.0 server.

For details, refer to the manuals of OfficeScan 11.0.

- Install the OfficeScan XG agent, and perform configuration so the agent is managed by the OfficeScan XG server.

For details, refer to the manuals of OfficeScan XG.

[Symantec]

- Install the Symantec Endpoint Protection agent, and perform configuration so the agent is managed by Symantec Endpoint Protection Manager.

For details, refer to the manuals of Symantec Endpoint Protection.

SBC Servers

Perform one of the following.

[Trend Micro OfficeScan]

- Install the OfficeScan 11.0 agent, and perform configuration so the agent is managed by the OfficeScan 11.0 server.

For details, refer to the manuals of OfficeScan 11.0.

- Install the OfficeScan XG agent, and perform configuration so the agent is managed by the OfficeScan XG server.

For details, refer to the manuals of OfficeScan XG.

[McAfee]

- Install McAfee Agent and perform configuration so the agent is managed from the McAfee ePolicy Orchestrator server, and then deploy McAfee Endpoint Security.

Refer to the following in the product guide of McAfee ePolicy Orchestrator:

- "Installing the McAfee Agent and licensed software" in "Setting up your McAfee ePO server"

- "Deploying products" in "Advanced configuration"

[Symantec]

- Install the Symantec Endpoint Protection agent, and perform configuration so the agent is managed by Symantec Endpoint Protection Manager.

For details, refer to the manuals of Symantec Endpoint Protection.

Resource Orchestrator Manager

[VMware]

Install VMware vSphere PowerCLI 6.0 or later, and confirm that VMware PowerCLI is running.

For details, refer to the manuals of VMware vSphere PowerCLI.

Note

. . . .

- If PowerCLI is installed after the Resource Orchestrator manager, Resource Orchestrator may not be able to properly operate the functions of PowerCLI.

In such cases, reboot the Resource Orchestrator manager.

For details on how to stop and restart the manager, refer to the following.

[Virtual Edition]

"2.1 Starting and Stopping Managers" in the "Operation Guide VE"

[Cloud Edition]

"2.1 Starting and Stopping Managers" in the "Operation Guide CE"

- If the admin server is not connected to the Internet, Power CLI Snap-ins will take longer to load, which will interfere with network switchover.

Therefore, please connect the admin server to the Internet.

If it is not possible to connect to the Internet, perform corrective actions by disabling the "Microsoft Root Certificate Program" and disabling the settings related to checking for certificate revocation of publishers.

Perform the following two procedures on the admin server:

- Disable the "Microsoft Trusted Root Certificate Program"

1. Open the Local Group Policy Editor.

2. Select [Computer Configuration]-[Windows Settings]-[Security Settings]-[Public Key Policies].

3. Double-click [Certificate Path Validation Settings].

4. Click the [Network Retrieval] tab.

5. Check the [Define these policy settings] checkbox.

6. Clear the [Automatically update certificates in the Microsoft Root Certificate Program] checkbox.

Information

. . . .

Leave the [Allow issuer certificate (AIA) retrieval during path validation] checkbox checked. This item affects how certificate chains are validated.

Validation of certificate chains

If necessary, download CA certificates other than the root certificate (intermediate certificates) based on the path described for authority information access (AIA) of certificates. Construct a certificate chain to the root CA certificate using these intermediate certificates.

. . . .

7. Click [OK].

8. Reboot the OS.

- Disable the setting for checking certificate revocation

    1. Open the Registry Editor.

    2. Open the following registry key.

       ```
       HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers
       \Software Publishing
       ```

    3. Modify the value of [State (REG_DWORD)] as follows.

Before modification	0x00023c00: Enabled
After modification	0x00023e00: Disabled

2.2 Configuring the Resource Orchestrator Admin Server and Installing the Manager

This section explains the procedures for configuring the Resource Orchestrator admin server and installing the manager.

2.2.1 Signing In to the Resource Orchestrator Admin Server

Sign in to the Resource Orchestrator admin server as the Windows administrator.

2.2.2 Configuring the Host Name (FQDN) in the hosts File

This section explains the procedure for editing the hosts file.

For the admin server to operate normally, it is necessary to set the host name (FQDN) in the hosts file.

Note

This operation is necessary even if DNS name resolution is possible for the admin server.

Procedure

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

Configuration Method

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

Note the following when configuring the hosts file.

  - Do not specify a host name (FQDN) or computer name for "127.0.0.1".

  - Confirm that the "localhost" is configured using IPv4 (127.0.0.1).

    Do not configure it using IPv6.

Example

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

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

2.2.3 Configuring the Windows Firewall

This section explains the procedure for configuring the Windows firewall.

Procedure

[Virtual Edition]

Configure the Windows firewall.

```
>  netsh  advfirewall  firewall  add  rule  name="ServerView  Resource  Orchestrator(TCP)"  dir=in  protocol=tcp
localport=162,14974-14989,23461 action=allow

>  netsh  advfirewall  firewall  add  rule  name="ServerView  Resource  Orchestrator(UDP)"  dir=in  protocol=udp
localport=67,69,162,4011,4972,14974-14989 action=allow
```

When using the email notification function, perform the following settings.

```
> netsh advfirewall firewall add rule name="ServerView Resource Orchestrator(SMTP)" dir=out protocol=tcp localport=25
action=allow
```

[Cloud Edition]

For the settings to use when using ROR CE, refer to "Appendix A Port List" in the "Design Guide CE", and perform the same procedure as for ROR VE.

Confirmation of Results

Confirm that the above settings are configured in the [Inbound Rules].

```
>netsh advfirewall firewall show rule name="ServerView Resource Orchestrator(TCP)"

>netsh advfirewall firewall show rule name="ServerView Resource Orchestrator(UDP)"
```

When using the function for sending email notifications, the following will also be configured in the [Inbound Rules].

```
>netsh advfirewall firewall show rule name="ServerView Resource Orchestrator(SMTP)"
```

2.2.4 Tuning the System Parameters of the Admin Server

This section explains the procedure for tuning the system parameters of the admin server.

It is necessary to tune the system parameters of the admin server before installing the Resource Orchestrator manager.

The system parameter to tune and the value to specify are as follows.

- Desktop heap

  Check the value of the desktop heap. If the value is less than 3328, change it to 3328.

Procedure

Perform the following procedure in Windows to change the value of the desktop heap.

1. Open the Registry Editor.

   Click [Start]-[Run]. Enter "regedit", and then click the [OK] button.

2. Move to the [SubSystems] key.

   Move to the following key on the [HKEY_LOCAL_MACHINE] tree.

   ```
   \SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems
   ```

3. Select [Windows].

4. Open the [Edit] menu and select [Modify].

5. Change the value for [SharedSection] to increase the size of the desktop heap.

    If the value of the third value (zzzz) is less than "3328", change it to "3328". The unit of the third value (zzzz) is KB.

    ```
    SharedSection=xxxx,yyyy,zzzz
    ```

    * Note: It is not necessary to change the first value (*xxxx*) or the second value (*yyyy*) in order to operate Resource Orchestrator.

6. Restart the system.

Note

Improper modification of the registry using the Registry Editor could cause serious problems. In the worst-case scenario, it could be necessary to reinstall the OS in order to resolve such problems.

Before modifying the registry, be sure to take the proper precautions, such as backing up the system in advance.

2.2.5 Executing the Environment Setup Conditions Check Tool

This section explains how to use the "environment setup conditions check tool".

Before installing the Resource Orchestrator manager, execute the environment setup conditions check tool to check whether the admin server satisfies the configuration requirements for the manager.

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

Procedure

1. Log in as the administrator.

2. Confirm that a single folder path is set for the TEMP environment variable.

3. Start the installer.

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

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

    In cases where the check results specify which edition can be installed, confirm that the edition to install is specified.

Confirmation of Results

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

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

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

2. Confirm that "Warning" or "NG" is not included in the check results. If there are check items that were determined as "Warning" or "NG", resolve the cause of the problem based on the output message.

3. In addition to the items checked by the "environment setup conditions check tool", confirm that the server satisfies the following requirements:

    1. The hardware specifications of the admin server must satisfy or exceed the values shown below

Table 2.1 Admin Server Hardware Specifications

Item		Value
Memory capacity		**[Virtual Edition]** 8 GB **[Cloud Edition]** 20 GB
CPU count	Number of virtual sockets	4
	Number of cores per socket	1
Disk capacity		200 GB
[VMware] Network adapter type		VMXNET 3

2. The following four PMS and SVIM programs must not be installed

  - Fujitsu ServerView Profile Manager Service

  - Fujitsu ServerView Installation Manager PXE Server

  - Fujitsu ServerView Installation Manager Data Packages

  - Fujitsu ServerView Installation Manager

  If any of these programs are installed, uninstall them in the same order as above.

2.2.6 Installing the Resource Orchestrator Manager

This section explains the procedure for installing the Resource Orchestrator manager.

Procedure

Install the Resource Orchestrator manager using the following procedure:

1. Log on to the system as the administrator.

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

2. Set the first Resource Orchestrator DVD-ROM.

  The installer starts automatically.

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

3. Select the edition to install.

4. Click [Manager installation].

5. Install the manager interactively, following the instructions provided by the installer.

  [Virtual Edition]

Item No.	Window	Entry	Description

1	Installation Folder Selection	Installation Folder	This is the folder where Resource Orchestrator is installed.
			
			  - For Windows 64-bit (x64)
			
			  Initial value: *System_drive*\Program Files (x86)\Resource Orchestrator
			
			  - For Windows 32-bit (x86)

Item No.	Window	Entry	Description
			Initial value: *System_drive*\Program Files\Resource Orchestrator
			The installation folder path can contain 45 characters or less including the drive letter and "\".
			A path starting with "\\" or a relative path cannot be specified.
			Alphanumeric characters, blank spaces (" "), and parentheses ("()") can be used.
			The following folder cannot be specified for the installation folder.
			- For Windows 64-bit (x64)
			- *System_drive*\
			- *System_drive*\Program Files(x86)
			- For Windows 32-bit (x86)
			- *System_drive*\
			- *System_drive*\Program Files
			The following folder and its subfolders cannot be specified for the installation folder.
			- For Windows 64-bit (x64)
			- *System_drive*\Windows
			- *System_drive*\Program Files
			- For Windows 32-bit (x86)
			- *System_drive*\Windows
			Specify an NTFS disk.
2	Admin LAN Selection	Network to use for the admin LAN	This is the network to be used as the admin LAN. Select it from the list.
			The maximum value for the subnet mask is 255.255.255.255 (32-bit mask). The minimum value is 255.255.0.0 (16-bit mask). However, 255.255.255.254 cannot be specified.
3	Authentication Method Selection	Authentication Method	Select "Internal Authentication".
4	Privileged User Creation	User Account	This is the user account name to be used for logging in to Resource Orchestrator as a privileged user.
			The name must start with an alphabetic character and can be up to 16 alphanumeric characters long, including underscores ("_"), hyphens ("-"), and periods ("."). Input is case-sensitive.
		Password	The password of the privileged user.
		Retype password	The string must be composed of alphanumeric characters and symbols (excluding blank spaces), and can be up to 16 characters long.

[Cloud Edition]

Item No.	Window	Entry	Description
1	Installation Folder Selection	Installation Folder	This is the folder where Resource Orchestrator is installed.
			Initial value: *System_drive*\Program Files (x86)\Resource Orchestrator
			The installation folder path can contain 45 characters or less including the drive letter and "\".

Item No.	Window	Entry	Description
			A path starting with "\\" or a relative path cannot be specified.
			Alphanumeric characters, blank spaces (" "), and parentheses ("()") can be used.
			The following folder cannot be specified for the installation folder.
			System_drive\
			System_drive\Program Files(x86)
			The following folder and its subfolders cannot be specified for the installation folder.
			System_drive\Windows
			System_drive\Program Files
			Specify an NTFS disk.
2	Admin LAN Selection	Network to use for the admin LAN	This is the network to be used as the admin LAN. Select it from the list.
			The maximum value for the subnet mask is 255.255.255.255 (32-bit mask). The minimum value is 255.255.0.0 (16-bit mask). However, 255.255.255.254 cannot be specified.
3	Authentication Method Selection	Authentication Method	Select "Internal Authentication".
4	Privileged User Creation	User Account	This is the user account name to be used for logging in to Resource Orchestrator as a privileged user.
			The name must start with an alphabetic character and can be up to 16 alphanumeric characters long, including underscores ("_"), hyphens ("-"), and periods ("."). Input is case-sensitive.
		Password	The password of the privileged user.
		Retype password	The string must be composed of alphanumeric characters and symbols (excluding blank spaces), and can be 8 - 16 characters long.

6. When prompted to change disks, set the second Resource Orchestrator DVD-ROM, and then continue installation.

2.3 Post-Installation Configuration of the Resource Orchestrator Manager

This section explains the procedure for configuring the Resource Orchestrator manager after installation is complete.

2.3.1 Configuring Environment Variables

This section explains the procedure for configuring environment variables.

Procedure

Use the following procedure to configure the environmental variables on the admin server.

1. Press the [Windows key].

2. Enter the following in [Search].

```
taskmgr
```

For Windows Server versions other than 2016 or later, enter the following in [Search programs and files].

For Windows Server 2016, enter the following in [Search].

3. Right-click taskmgr.exe, then click [Run as administrator].

The [Windows Task Manager] is displayed.

4. Click [File]-[New Task (Run)].

   The [Create New Task] dialog is displayed.

5. Enter the following.

   ```
   rundll32.exe sysdm.cpl,EditEnvironmentVariables
   ```

6. Select the [Create this task with administrative privileges.] checkbox.

7. Click the [OK] button.

   The [Environment Variables] dialog is displayed.

8. In the [System variables] area, click the [New] button.

   The [New System Variable] dialog is displayed.

9. Enter the following.

   Variable name: ROR_MGR

   Variable value: *Installation_folder*\SVROR\Manager

10. Click the [OK] button.

11. In the [Variable] column in the [System variables] area, select [Path].

12. In the [System variables] area, click the [Edit] button.

    For Windows Server 2016, the [Edit System Variable] dialog is displayed.

    For Windows Server versions other than 2016 or later, the [Edit System Variable] dialog is displayed.

13. For Windows Server 2016, add the following to the end of the value for [Variable value].

    For Windows Server versions other than 2016 or later, add the following to the end of the value for [Variable value].

    ```
    ;%ROR_MGR%\bin
    ```

14. Click the [OK] button.

15. Restart the admin server.

Confirmation of Results

Execute the rcxlogin command, and confirm that you can log in to Resource Orchestrator.

1. Start the command prompt as an administrator.

   The command prompt is displayed.

2. Execute the following command.

   ```
   > rcxlogin user_name
   ```

3. Enter the appropriate password.

   A new command prompt is displayed.

2.3.2 Signing In to the Resource Orchestrator Admin Server

Sign in to the Resource Orchestrator admin server as the Windows administrator.

2.3.3 Registering the Licenses for Managed Servers

This section explains the procedure for registering the licenses for the following types of managed servers:

- VM hosts

- Physical servers on which SBC servers operate

When using the automatic quarantining function, it is necessary to register the licenses for managed servers in Resource Orchestrator.

2.3.3.1 Registering Licenses Using the GUI (ROR Console)

This section explains the procedure for registering licenses using the GUI (ROR console).

Use the GUI (ROR console) to register the licenses for managed servers in Resource Orchestrator.

Items to Confirm Beforehand

P Point

. . . .

It is necessary to prepare the number of licenses necessary for the installed version, in advance.

. . . .

Procedure

Register the licenses for the installed version using the following procedure.

1. Log in to the GUI (ROR console).

   Click [ROR Console] on the [Apps] screen, or access the following address using IE.

   ```
   https://FQDN_of_the_admin_server:23461/
   ```

2. Select [Tools]-[Licenses] from the GUI (ROR console) menu, and then click the [Add] button in the displayed dialog.

   The [Register License] dialog is displayed.

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

4. Click the [OK] button.

   The license will be registered.

5. Create rorsetup.conf. [Virtual Edition]

   Location of the File

   [Windows Manager]

   Installation_folder\SVROR\Manager\etc\conf

   Name of the File

   rorsetup.conf

   File Format

   Empty file

6. After registering the licenses for the installed version, reboot the Resource Orchestrator manager.

   Execute the following commands.

   ```
   > rcxadm mgrctl stop
   > rcxadm mgrctl start
   ```

Confirmation of Results

Confirm that the number of licenses necessary for the installed version have been registered.

Confirm using the following procedure:

1. Log in to the GUI (ROR console).

2. Select [Tools]-[Licenses] from the GUI (ROR console) menu, and then click the name of the license in the displayed dialog.

3. The [Licenses] dialog is displayed.

4. [Virtual Edition] Confirm that "Orchestration Tree" is displayed in the "Tree" on the GUI (ROR console).

2.3.4 Creating Certificates for Use during HTTPS Communication

This section explains the procedure for creating the certificates that are used during HTTPS communication performed by Resource Orchestrator.

Procedure

1. Execute the following commands to back up the existing certificates.

```
> cd "C:\Program Files (x86)\Resource Orchestrator\SVROR\Manager\sys\apache\conf"
> ..\..\..\bin\rcxadm mgrctl stop
> copy ssl.crt\server.crt ssl.crt\server.crt.org
> copy ssl.key\server.key ssl.key\server.key.org
```

2. Execute the following command to create the new certificates.

```
> ..\bin\openssl.exe req -new -x509 -nodes -sha256 -newkey rsa:2048 -out ssl.crt\server.crt -
keyout ssl.key\server.key -days 5479 -config openssl.cnf
```

3. Press the [Enter] key when prompted to do so.

💾 **Example**

● ●

```
> cd "C:\Fujitsu\ROR\SVROR\Manager\sys\apache\conf"
> ..\..\..\bin\rcxadm mgrctl stop
> copy ssl.crt\server.crt ssl.crt\server.crt.org
> copy ssl.key\server.key ssl.key\server.key.org
> ..\bin\openssl.exe req -new -x509 -nodes -sha256 -newkey rsa:2048 -out ssl.crt\server.crt -
keyout ssl.key\server.key -days 5479 -config openssl.cnf
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
................+++++
..............................+++++
writing new private key to 'ssl.key\server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) [localhost]: IP_address or Host_name (*)
Email Address []:
> ..\..\..\bin\rcxadm mgrctl start
```

* Note: Enter the IP address or host name (FQDN) to be entered in the Web browser.

● ●

2.3.5 Disabling Internet Explorer Enhanced Security Configuration (IE ESC)

This section explains the procedure for disabling Internet Explorer Enhanced Security Configuration (IE ESC).

For the GUI (ROR console) to operate correctly, it is necessary to disable Internet Explorer Enhanced Security Configuration (IE ESC).

Procedure

Perform the following procedure:

1. Record the list of IE trusted sites.

   a. Press the Windows key, and select the [Control Panel] from the Start menu.

   b. Click [Network and Internet].

   c. Select [Internet Options] in the Network and Internet menu.

   d. Open the [Security] tab and select [Trusted sites], then click the [Sites] button.

2. Disable Internet Explorer Enhanced Security Configuration (IE ESC).

   a. Launch the [Server Manager] from the Taskbar.

   b. Click [Local Server], and then click [On] next to [IE Enhanced Security Configuration].

   c. Change the setting for [Administrators] to [Off], and then click [OK].

   d. Close the [Server Manager].

3. Reconfigure the IE trusted sites.

   a. Press the Windows key, and select [Control Panel] from the Start menu.

   b. Click [Network and Internet].

   c. Select [Internet Options] in the Network and Internet menu.

   d. Open the [Security] tab and select [Trusted sites], then click the [Sites] button.

   e. Under [Add this website to the zone:], enter the website information recorded in step 1.

   Ensure that [Require server verification (https:) for all sites in this zone] is unchecked, and then click the [add] button.

   f. Confirm that the entered value has been added to the [Websites] field, and then click the [Close] button.

   g. In the [Internet Options] window, click [OK].

2.3.6 Importing Certificates to a Browser

This section explains the procedure for importing certificates to a browser.

To use the [Resources] tab of the GUI (ROR console), it is necessary to install certificates in Internet Explorer.

2.3.6.1 Importing Certificates to the [Resource] Tab of the GUI (ROR Console)

To use the [Resource] tab of the GUI (ROR console), install certificates in Internet Explorer.

Procedure

Use the following procedure to install certificates in Internet Explorer:

1. Log in to the GUI (ROR console).

   Click [ROR Console] on the [Apps] screen, or access the following address using IE.

   ```
   https://FQDN_of_the_admin_server:23461/
   ```

2. If the message "Protected mode is turned off for the Local intranet zone." is displayed, click [Turn on Protected mode].

3. In the IE menu bar, click [Tools]-[Pop-up Blocker]-[Turn off Pop-up Blocker].

4. Select [Continue to this website (not recommended)].

5. If a security alert is displayed, click the [OK] button.

6. Enter the user name and password of a privileged user of Resource Orchestrator, and then click the [Login] button.

7. Click [Certificate Error]-[View certificates].

8. Click [Install Certificate].

9. Select [Current User], and then click the [Next] button.

10. Select the [Place all certificates in the following store] option button, and then click [Browse].

11. Select [Trusted Root Certification Authorities], and then click the [OK] button.

12. Confirm that the selected certification authority is displayed, and then click the [Next] button.

13. Click [Finish].

14. In the security alert dialog, click the [Yes] button.

15. In the Certificate Import Wizard dialog, click the [OK] button.

16. In the Certificate dialog, click the [OK] button.

17. Log out and close all open browser windows.

Confirmation of Results

Confirm that the certificates have been imported using the following procedure:

1. Click [ROR Console] on the [Apps] screen.

2. Enter the user name and password of a privileged user of Resource Orchestrator, and then click the [Login] button.

3. Confirm that [Certificate Error] is not displayed on the screen after logging in.

2.4 Installing the Resource Orchestrator Agent

This section explains the procedure for installing the Resource Orchestrator agent.

It is necessary to install agents on managed servers when using Hyper-V on Windows Server 2016 or SBC servers.

Prerequisites

It is necessary to install ServerView Agents for Windows before installing the Resource Orchestrator agent.

Procedure

Install the Resource Orchestrator agent using the following procedure:

1. Log on to the system as the administrator.

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

2. Set the first Resource Orchestrator DVD-ROM.

   The installer starts automatically.

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

3. Select the edition to install.

4. Click [Agent installation].

5. The Resource Orchestrator setup window is displayed.

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

6. Install the manager interactively, following the instructions provided by the installer.

Window	Entry	Description
Installation Folder Selection	Installation Folder	This is the folder where Resource Orchestrator is installed. When changing the installation folder, refer to the "Note" below.
Admin Server Registration	Admin LAN IP Address of the Admin Server	When the admin server has multiple IP addresses, specify the IP address used for communication with managed servers.

Window	Entry	Description
License Authentication	License Authentication Information for the Windows Volume License	- When not using cloning Click [Next>] without selecting [Using the cloning feature of this product]. - When using cloning Select [Using the cloning feature of this product]. - [Virtual Edition] For details, refer to "2.2.2 Installation [Windows] [Hyper-V]" in the "Setup Guide VE". - [Cloud Edition] For details, refer to "2.2.2 Installation [Windows] [Hyper-V]" in the "Setup Guide CE".

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

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

   Copying of files will start.

   To change the content, click [<Back].

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

   When setup is complete, the setup completion window will be displayed.

   Click [Finish] and close the window.

🈁 Note

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

- Do not specify the installation folder of the system (such as C:\).

- Enter the location using 100 characters or less. Do not use double-byte characters or the following symbols in the folder name.

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

- When using a 64-bit Windows Server OS, the following folder name cannot be specified for the installation folder.

  - "%SystemRoot%\System32\"

- When using cloning, installation on the OS system drive is advised, because Sysprep initializes the drive letter during deployment of cloning images.

2.5 Creating Definition Files

This section explains how to create definition files and rulesets (scripts).

It is necessary to create definition files and rulesets (scripts) before using the automatic quarantining function.

Definition Files

Create the following definition files and place them in the designated folder of the Resource Orchestrator manager.

The necessary definition files vary depending on the type of the managed servers.

Virtual PCs

- Definition file for the quarantine policy for security risks

- Definition file for selecting action settings

- System configuration file

- Definition file for enabling notification

- Definition file for loading IP addresses of virtual PCs to virtual L-Servers

- Definition file for configuring the business and quarantine networks

- Definition files for registering VM hosts as managed servers

- Definition file for connection to the virtual network that was created in advance

SBC servers

- Definition file for the quarantine policy for security risks

- Definition file for selecting action settings

- System configuration file

- Definition file for enabling notification

- Rulesets (scripts) for L2 switches

Note that the definition file of the quarantine policy for security risks is predefined with the recommended values.

2.5.1 Definition File of the Quarantine Policy for Security Risks

Set whether to transfer all of the L-Servers corresponding to any security risks for which notification is sent from one of the following servers to the Resource Orchestrator manager to the quarantine network.

[Trend Micro OfficeScan]

- OfficeScan 11.0 server

- OfficeScan XG server

Under the default and recommended settings for all security risks, the corresponding L-Servers are transferred to the quarantine network.

When changing the settings, refer to "A.1 Definition File of the Quarantine Policy for Security Risks".

2.5.2 Definition File Setting Action Selection

Sets the action to take when a malware infection is detected.

For details on configuration, refer to "A.1 Definition File of the Quarantine Policy for Security Risks".

2.5.3 System configuration file

Register the managed servers.

Point

For details on the format of the system configuration file, refer to the following.

[Virtual Edition]

"B.2 File Format" in the "User's Guide VE"

[Cloud Edition]

"B.2 File Format" in the "User's Guide for Infrastructure Administrators (Resource Management) CE"

Purpose

This definition file is necessary when registering managed servers.

2.5.3.1 Obtaining the System Configuration File

The system configuration file can be obtained from the ROR console.

Obtain it using the following procedure.

Procedure

1. Log in to the ROR console.

2. From the ROR console menu, select [File]-[System Configuration File]-[Download Template].

   The [File Download] window is displayed.

3. Click the [Save] button.

4. Specify the storage directory and the file name.

5. Click the [Save] button.

2.5.3.2 Format of the System Configuration File

The items defined in the system configuration file are delimited using commas (",").

P Point

. . . .

For details on the format of the system configuration file, refer to the following.

[Virtual Edition]

   "B.2 File Format" in the "User's Guide VE"

[Cloud Edition]

   "B.2 File Format" in the "User's Guide for Infrastructure Administrators (Resource Management) CE"

. . . .

Format of the System Configuration File (Excerpt)

Edit the contents of the system configuration file shown below in underlined text.

```
RCXCSV
V3.5
#     ServerView Resource Orchestrator
#     System configuration file

[Server]
operation,chassis_name,slot_no,server_name,ip_address,mac_address,second_mac_address,snmp_communi
ty_name,ipmi_ip_address,ipmi_user_name,ipmi_passwd,ipmi_passwd_enc
new,,,server_name1,ip_address1,mac_address1,,,,,,
new,,,server_name2,ip_address2,mac_address2,,snmp_community_name2,ipmi_ip_address2,ipmi_user_name
2,ipmi_passwd2,ipmi_passwd_enc2
new,,,server_name3,ip_address3,mac_address3,,,,,,
new,,,server_name4,ip_address4,mac_address4,,snmp_community_name4,ipmi_ip_address4,ipmi_user_name
4,ipmi_passwd4,ipmi_passwd_enc4




[VMManager]
operation,name,ip_address,product,login_name,login_passwd,passwd_enc
new,vCenterServer,mgr_ip_address1,vmware-vc,login_name1,login_passwd1,passwd_enc1
new,SCVMM,mgr_ip_address2,ms-scvmm,login_name2,login_passwd2,passwd_enc2




[ServerVMHost]
```

```
operation,server_name,vm_login_name,vm_login_passwd,vm_passwd_enc
new,server_name1,vm_login_name1,vm_login_passwd1,vm_passwd_enc1
new,server_name2,vm_login_name2,vm_login_passwd2,vm_passwd_enc2
new,server_name3,vm_login_name3,vm_login_passwd3,vm_passwd_enc3


[ServerAgent]
operation,server_name
new,server_name2
new,server_name4
```

🅿 Point

- It is necessary to create as many definitions as the number of managed servers.

- The items to edit vary depending on the type of the target managed server.

  - Virtual PCs

    [VMware]

      Edit the items shown for *server_name1* in "Format of the System Configuration File (Excerpt)".

      - Server management information

      - VM management software information

      - VM host management information

    [Hyper-V]

      Edit the items shown for *server_name2* in "Format of the System Configuration File (Excerpt)".

      - Server management information

      - VM management software information

      - VM host management information

      - Server agent management information

    [Citrix Xen]

      Edit the items shown for *server_name3* in "Format of the System Configuration File (Excerpt)".

      - Server management information

      - VM host management information

  - SBC servers

    Edit the items shown for *server_name4* in "Format of the System Configuration File (Excerpt)".

    - Server management information

    - Server agent management information

Server Management Information

- **Section Name**

  Enter "[Server]".

- **Section Header**

  operation

    Enter the desired operation for the server. Enter a hyphen ("-") to skip this line.

server_name

Enter the name that will be used to identify the server. Enter a character string beginning with an alphabetical character and containing up to 15 alphanumeric characters and hyphens ("-").

📖 **Note**

Names must be unique among all resources of the same type. Names are not case-sensitive.

ip_address

Enter the same IP address as the one configured for the server.

Enter a character string consisting of numbers (0 to 255) and periods (".").

📖 **Note**

IP addresses must be unique among all resources.

mac_address

Enter the MAC address used by the server on the admin LAN.

Enter a string delimited by hyphens ("-") or colons (":") ("xx-xx-xx-xx-xx-xx" or "xx:xx:xx:xx:xx:xx").

snmp_community_name

Enter the name of the SNMP community name (read permission) set for the server.

A string composed of up to 32 alphanumeric characters, underscores, ("_"), and hyphens ("-").

ipmi_ip_address

Enter the IP address of the server's Remote Management Controller.

Enter a character string consisting of numbers (0 to 255) and periods (".").

📖 **Note**

IP addresses must be unique among all resources.

ipmi_user_name

Enter the name of a user account with Administrator/OEM privileges on the Remote Management Controller used to manage the server.

Enter up to 16 characters, including alphanumeric characters and symbols (ASCII characters 0x20 to 0x7e).

📖 **Note**

If a 17-character or longer string is already set for the relevant user name on the Remote Management Controller, either add a new user, or change the relevant user name so that it is 16 characters or less.

ipmi_passwd

Enter the password of the above user account on the server's remote management controller.

Enter up to 16 characters, including alphanumeric characters and symbols (ASCII characters 0x20 to 0x7e).

This field can be omitted if no password has been set for this user account.

ipmi_passwd_enc

Enter either of the following:

- If ipmi_passwd is plain text

  "plain"

- If the password is encrypted

  "encrypted"

VM Management Software Information

- **Section Name**

  Enter "[VMManager]".

- **Section Header**

  operation

  Enter the desired operation for the server. Enter a hyphen ("-") to skip this line.

  name

  Enter the name that will be used to identify the VM management software.

  [VMware]

  - When using VMware vCenter Server as VM management software

    "vCenterServer"

  [Hyper-V]

  - When using Microsoft(R) System Center 2016 Virtual Machine Manager as VM management software

    "SCVMM"

  ip_address

  Enter the IP address of the VM management software or a hyphen ("-").

  Enter a character string consisting of numbers (0 to 255) and periods (".").

  When a hyphen ("-") is specified, the location is set to "Admin Server".

  product

  Enter the name of the VM management software.

  [VMware]

  - When using VMware vCenter Server as VM management software

    "vmware-vc"

  [Hyper-V]

  - When using Microsoft(R) System Center 2016 Virtual Machine Manager as VM management software

    "ms-scvmm"

  login_name

  Enter the name of the user account set for the VM management software.

  Enter up to 84 characters, including alphanumeric characters and symbols (ASCII characters 0x21 to 0x7e). When specifying a domain name, use the format "*domain_name|user_name*".

login_passwd

Enter the password set for the VM management software.

Enter up to 128 characters, including alphanumeric characters and symbols (ASCII characters 0x21 to 0x7e).

passwd_enc

Enter either of the following:

- If login_passwd is plain text

  "plain"

- If the password is encrypted

  "encrypted"

VM Host Management Information

- **Section Name**

  Enter "[ServerVMHost]".

  This section name is necessary for batch registration of the agents of managed servers of the VM host.

- **Section Header**

  operation

  Enter the desired operation for the server. Enter a hyphen ("-") to skip this line.

  server_name

  Enter the name of the VM host to define (the value of "server_name" in the [Server] section).

  vm_login_name

  Enter the name of the user account used to remotely log in to the VM host.

  vm_login_passwd

  Enter the password of the above user account (for remote login).

  vm_passwd_enc

  Enter either of the following:

  - If the password is plain text

    "plain"

  - If the password is encrypted

    "encrypted"

Server Agent Management Information

- **Section Name**

  Enter "[ServerAgent]".

  This section name is necessary for batch registration of the agents of Windows managed servers.

- **Section Header**

  operation

  Enter the desired operation for the server. Enter a hyphen ("-") to skip this line.

  "change" cannot be used.

  server_name

  Enter the name of the server to define (the value of "server_name" in the [Server] section).

Example

```
RCXCSV    V3.5

#    ServerView Resource Orchestrator
#    System configuration file
[Server]
operation,chassis_name,slot_no,server_name,ip_address,mac_address,second_mac_address,snmp_community_
name,ipmi_ip_address,ipmi_user_name,ipmi_passwd,ipmi_passwd_enc
new,,,esxi000,192.168.10.13,90:E5:35:0C:34:AD,90:E5:35:0C:34:AE,,,,,
new,,,xenapp000,192.168.10.14,90:E5:35:0C:34:AC,,public,192.168.10.201,admin,admin,plain

[VMManager]
operation,name,ip_address,product,login_name,login_passwd,passwd_enc
new,vCenterserver,192.168.10.50,vmware-vc,administrator,vCenter_server_password,plain

[ServerVMHost]
operation,server_name,vm_login_name,vm_login_passwd,vm_passwd_enc
new,esxi000,root,esxi000_password,passwd_enc

[ServerAgent]
operation,server_name
new,xenapp000
```

2.5.4 Definition File for Enabling Notification

This section explains the definition file for enabling notification of switchover to the quarantine network.

This definition is only enabled when message notifications are enabled using the msgnotice command.

For details on the msgnotice command, refer to "4.9 msgnotice".

Purpose

Regarding the notification when actions are executed after infection with malware is detected, define the message content in this definition file. When notification has been enabled, the notification displayed on the user window will use the messages defined in this definition file.

If this definition file does not exist, then the default message will be sent. In addition, if definition is not performed for each action, then the default message will be sent.

However, it not necessary to restart the services of the Resource Orchestrator manager after editing this type of definition file.

Format of the Definition File

Location of the Definition File

[Windows Manager]

Installation_folder\SVROR\Manager\etc\customize_data

Name of the Definition File

avmgr_msgnotice.rcxprop

Character Code

[Windows Manager]

UTF-8

Line Break Code

[Windows Manager]

CR/LF

Format of the Definition File

In the definition file, specify each line in the following format:

```
Key = Value
```

Definition File Items

The items to specify in the definition file are given below.

Item	Key	Value
Default Title	message_title	A string of 1 to 32 characters (Both double-byte and single-byte characters can be used)
Default Body	message_text	A string of 1 to 256 characters (Both double-byte and single-byte characters can be used)
Title Displayed when Quarantining	message_title_quarantine	A string of 1 to 32 characters (Both double-byte and single-byte characters can be used)
Body Displayed when Quarantining	message_text_quarantine	A string of 1 to 256 characters (Both double-byte and single-byte characters can be used)
Title Displayed when Rebooting	message_title_reboot	A string of 1 to 32 characters (Both double-byte and single-byte characters can be used)
Body Displayed when Rebooting	message_text_reboot	A string of 1 to 256 characters (Both double-byte and single-byte characters can be used)
Title Displayed when Quarantining and Rebooting	message_title_quarantine_reboot	A string of 1 to 32 characters (Both double-byte and single-byte characters can be used)
Body Displayed when Quarantining and Rebooting	message_text_quarantine_reboot	A string of 1 to 256 characters (Both double-byte and single-byte characters can be used)

The default values for the message title and body are as follows.

Item	Value
Title	Warning!
Body	Security threat detected. This virtual application/desktop will be disconnected for safety reasons.

Example Definition File

An example definition of user-defined messages is given below.

```
message_title=Warning!
message_text=A threat to security has been detected.
```

```
message_title_quarantine=Quarantine!
message_text_quarantine=A threat to security has been detected.\ r\nThe virtual application/
desktop is being disconnected to ensure safety.
```

```
message_title_reboot=Reboot!
message_text_reboot=A threat to security has been detected.\ r\nThe machine will be restarted to
ensure safety.
```

Note

. . . .

- If the notification received for a message that has been set using multibyte character is displayed as garbled characters, it is recommended to change the content of the message to single-byte characters.

- If there are multiple lines of message text in the definition, only the first line is used.

- It is possible to specify a line break in the body of the message by inserting the line break character string "\r\n". Line break character strings are treated as being two characters in length. Depending on the OS of the terminal being used, line breaks in the title may not be displayed correctly.

- If a character string that is longer than the maximum allowed length for the message text character string is specified, the message up to the maximum allowed character string length will be sent. If the character string is empty, or the key has been omitted, the default message will be sent.

2.5.5 Definition File for Loading IP Addresses of Virtual PCs to Virtual L-Servers

This section explains the definition file for loading the IP addresses of virtual PCs to virtual L-Servers. This definition file is used when linking virtual PCs with virtual L-Servers.

Purpose

To modify a network in which virtual L-Servers operate, it is necessary that the L-Server information includes IP address information.

After creating this definition file, when linking virtual PCs with virtual L-Servers, the IP addresses assigned to the virtual PCs are automatically loaded to the virtual L-Servers.

Format of the Definition File

The format of the definition file is given below.

It is not necessary to restart the services of the Resource Orchestrator manager after editing this type of definition file.

Location of the Definition File

[Windows Manager]

Installation_folder\SVROR\Manager\etc\customize_data

Name of the Definition File

l_server.rcxprop

Character Code

[Windows Manager]

UTF-8

Line Break Code

[Windows Manager]

CR/LF

Format of the Definition File

Describe the file using the following format. If the definition file already exists, add to it using the following format.

```
reserve_ip_address=true
```

2.5.6 Definition File for Configuring the Business and Quarantine Networks

This section explains the definition file for configuring the business and quarantine networks.

Purpose

This file defines the contents of the XML files for changing the network that are created using the convertVMtoLServer -file and convertVMtoLServer -createxml commands.

Format of the Definition File

Location of the Definition File

[Windows Manager]

Installation_folder\SVROR\Manager\etc\customize_data

Name of the Definition File

avmgr_network.rcxprop

Character Code

[Windows Manager]

UTF-8

Line Break Code

[Windows Manager]

CR/LF

Format of the Definition File

Describe the file using the following format.

For each network resource name, enter a string beginning with an alphanumeric character, and containing up to 32 alphanumeric characters, underscores ("_"), periods ("."), and hyphens ("-"). Both upper and lower case letters can be used.

The network name must be the same as the one specified in "Table A.1 Excerpt from Definition Information for Virtual L-Servers (XML)".

When the names of multiple network resources are specified as the quarantine network for a single operation network, only the last line of specification is used.

```
Resource_name_of_business_network_1=Resource_name_of_quarantine_network_1
Resource_name_of_business_network_2=Resource_name_of_quarantine_network_2
Resource_name_of_business_network_3=Resource_name_of_quarantine_network_3
```

2.5.7 Definition Files for Registering VM Hosts as Managed Servers

This section explains the definition files for registering the following VM hosts as managed servers.

- VMware ESXi

- Citrix XenServer

Create the following two definition files:

- 2.5.7.1 server_control.rcxprop

- 2.5.7.2 register_ipmiless

2.5.7.1 server_control.rcxprop

Purpose

This definition file is necessary for Resource Orchestrator to manage VM hosts without installing Resource Orchestrator agents on them.

In VM hosts registered using these definitions, obtain the server status or hardware configuration information (CPU core count, CPU clock speed, memory capacity, etc.) from VM software.

When the definition file is changed after registration, the modification is not valid.

Format of the Definition File

Format of the Definition File

Location of the Definition File

[Windows Manager]

Installation_folder\SVROR\Manager\etc\customize_data

P Point
. . . .

In the storage location above, the sample definition file (server_control.sample.rcxprop) is stored. When using the sample as the definition file, place the file after deleting the ".sample" included in the file name.
. . . .

Name of the Definition File

server_control.rcxprop

Character Code

[Windows Manager]

UTF-8

Line Break Code

[Windows Manager]

CR/LF

Format of the Definition File

- The following line must be entered in the first line of definition files.

```
ServerControl,V1.1
```

- In the definition file, the name of each server is described on an individual line.

When defining two or more servers, use line breaks.

Each line is entered in the following format.

```
physical_server, ipmi
```

Even if the same physical server name is entered on multiple lines, no errors occur.

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

Definition File Items

physical_server

Enter the same physical server name as the one entered when registering a managed server.

Enter a character string beginning with an alphabetical character and containing up to 15 alphanumeric characters and hyphens ("-").

ipmi

Specify "false".

Example
. . . .

An example definition file is indicated below.

```
ServerControl,V1.1
########################################################################
# server_control.rcxprop
#
#All Rights Reserved, Copyright(C) FUJITSU LIMITED 2011
########################################################################
#
# physical_server, ipmi
#
```

```
server1, false
server2, false
```

2.5.7.2 register_ipmiless

Purpose

The file used to register physical servers which cannot perform IPMI communication with Resource Orchestrator.

Format of the Definition File

Create an empty file with the name shown below.

Location of the Definition File

[Windows Manager]

Installation_folder\SVROR\Manager\etc\vm

Name of the Definition File

register_ipmiless

2.5.8 Definition File for Connection to the Virtual Network that Was Created in Advance

This section explains how to create a definition file for connecting to an existing virtual network.

Explanations are provided for the following environments:

- Hyper-V

- Citrix Xen

2.5.8.1 Definition File for Connection to the Virtual Network that Was Created in Advance [Hyper-V]

For Hyper-V environments, when not configuring network redundancy for L-Servers on blade servers, or when using servers other than blade servers, the functionality for VM guests to connect to a virtual network that has been created in advance is only provided if the NICs of those VM guests are configured with IP addresses and VLAN IDs for that virtual network.

When manually configuring a virtual network in advance while also using server virtualization software other than Hyper-V with the same manager, configure names for the virtual switch, virtual network, and virtual bridge of Hyper-V that are different from those configured on the other server virtualization software.

Preparations

1. Create the virtual network

   Create a virtual network with the same name (including the use of uppercase and lowercase) on all VM hosts in the cluster.

   This virtual network enables VM guests to migrate between VM hosts. When using System Center 2012 Virtual Machine Manager or later versions as VM management software, only "External" can be used for the type of virtual network which is the connection destination for the VM guest.

   For details on creating external virtual networks, refer to the System Center Virtual Machine Manager help.

2. Configure the virtual network communication settings

   Perform configuration of the LAN switch blade so that virtual networks with the same name can communicate with each other using tagged VLAN communication.

   a. In the server resource tree of the ROR console, right-click the relevant LAN switch blade, and then select [Modify]-[Network Settings] in the displayed menu.

b. The [VLAN Settings] dialog is displayed.

c. Configure the VLAN settings.

Definitions of Correspondences Between Virtual Networks and VLAN IDs

The following Resource Orchestrator definition file contains correspondences between virtual networks and VLAN IDs.

Format of the Definition File

Location of the Definition File

[Windows Manager]

Installation_folder\SVROR\Manager\etc\customize_data

Name of the Definition File

vnetwork_hyperv.rcxprop

Character Code

[Windows Manager]

UTF-8

Line Break Code

[Windows Manager]

CR/LF

Format of the Definition File

Define each line of the definition file as follows.

```
"Name_of_the_virtual_network_created_on_the_VM_host"=VLAN ID[,VLAN ID...]
```

Specify a value between 1 and 4094 for each VLAN ID. When specifying a sequence of numbers, include a hyphen ("-"), as in "1-4094".

Example
. . . .
"Network A"=10

"Network B"=21,22,23

"Network C"=100-200,300-400,500
. . . .

Any spaces before or after an equal sign ("=") or a comma (",") will be ignored.

Ensure that you specify the name of the virtual network using exactly the same notation as on the VM host, including the use of uppercase and lowercase.

Save the file in the UTF-8 character code.

When there are multiple lines with the same virtual network name, all of the lines are valid.

When there are multiple lines with the same VLAN ID but different virtual network names, the line closest to the top of the file is treated as valid, and all lower lines are ignored.

Example
. . . .
"Network D"=11

"Network D"=12 (*1)

"Network E"=11,15 (*2)

*1: These two lines could also be written as one line, as in '"Network D"=11,12'.

*2: "11" is ignored.

. . . .

2.5.8.2 Definition File for Connection to the Network that Was Created in Advance [Citrix Xen]

Functionality is provided for connecting networks created on XenServer to virtual NICs.

Manually configure the networks on XenServer in advance. To connect networks created on XenServer to

virtual NICs, use a different VLAN ID for each XenServer network.

Preparations

1. Create XenServer networks

    It is necessary to create networks on VM hosts for L-Servers to connect to.

    Create a network with the same name (including the use of uppercase and lowercase) on all VM hosts in the cluster.

    This virtual network enables VM guests to migrate between VM hosts.

    When configuring a XenServer network while also using server virtualization software other than XenServer with the same manager, configure names for the virtual switch, virtual network, and virtual bridge of XenServer that are different from those configured on the other server virtualization software.

    For how to create networks on XenServer, refer to the manuals for Citrix XenServer.

2. Configure the XenServer network communication settings

    Perform configuration of the LAN switch blade so that networks created in XenServer with the same name can communicate with each other using tagged VLAN communication.

    a. In the server resource tree of the ROR console, right-click the relevant LAN switch blade, and then select [Modify]-[Network Settings] in the displayed menu.

    b. The [VLAN Settings] dialog is displayed.

    c. Configure the VLAN settings.

Definitions of Correspondences Between Networks Created on XenServer and VLAN IDs

The following Resource Orchestrator definition file contains correspondences between networks created on XenServer and VLAN IDs.

Format of the Definition File

Location of the Definition File

[Windows Manager]

Installation_folder\SVROR\Manager\etc\customize_data

Name of the Definition File

vnetwork_citrixxen.rcxprop

Character Code

[Windows Manager]

UTF-8

Line Break Code

[Windows Manager]

CR/LF

Format of the Definition File

Define each line of the network definition file as follows.

```
"Name_of_the_network_created_on_XenServer"=VLAN ID[,VLAN ID...]
```

Specify a value between 1 and 4094 for each VLAN ID. When specifying a sequence of numbers, include a hyphen ("-"), as in "1-4094".

📝 Example
. . . .

"Network A"=10

"Network B"=21,22,23

"Network C"=100-200,300-400,500

. . . .

Any spaces before or after an equal sign ("=") or a comma (",") will be ignored.

Ensure that you specify the name of the network using exactly the same notation as on the VM host, including the use of uppercase and lowercase.

Save the file in the UTF-8 character code.

When there are multiple lines with the same network name, all of the lines are valid.

When there are multiple lines with the same VLAN ID but different network names, the line closest to the top of the file is treated as valid, and all lower lines are ignored.

📝 Example
. . . .

"Network D"=11

"Network D"=12 (*1)

"Network E"=11,15 (*2)

*1: These two lines could also be written as one line, as in '"Network D"=11,12'.

*2: "11" is ignored.

. . . .

2.5.9 Rulesets (scripts) for L2 switches

This section explains rulesets (scripts) for L2 switches.

Purpose

When using SBC servers, it is necessary to register rulesets (scripts) for L2 switches in folders of Resource Orchestrator.

Preparations

The following operations are necessary to automatically configure and operate network devices using user customization mode.

- Creating Model Definitions for Network Devices

  For supported models, it is not necessary to create model definitions for the network devices.

- Create network device automatic configuration and operation definition files

- Creating a Folder for Registering Rulesets

- Create rulesets for automatic configuration and operations

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

For details on preparations, refer to "Appendix D Preparations for Automatic Configuration and Operation of Network Devices".

2.6 Procedure for Enabling Notification of Switchover to the Quarantine Network

This section explains the procedure for enabling notification of switchover to the quarantine network.

Performing the following procedure will cause a pop-up message to be displayed on the desktop of a virtual PC or SBC server when it has been quarantined.

If notification of users fails, a warning message will be output in the GUI (ROR console), and the quarantining will proceed.

Procedure

1. Register the connection information of the VDI management server.

   Execute the following command using the Resource Orchestrator manager.

   ```
   > msgnotice register -name VDI_management_server_name -ip
   IP_address_for_connecting_to_the_VDI_management_server -user_name
   Administrator_user_ID_for_the_VDI_management_server -passwd
   Administrator_password_for_the_VDI_management_server
   ```

2. Enable notification of quarantining.

   Execute the following command.

   ```
   > msgnotice enable
   ```

3. Authorize remote management.

   a. Execute the following command, and record the content displayed in TrustedHosts.

   ```
   > winrm get winrm/config/client
   ```

   Record the content displayed in TrustedHosts.

   If the displayed content is a single asterisk ("*"), or the "*IP_address_for_connecting_to_the_VDI_management_server*" configured in step 1, it is not necessary to perform steps b and c below.

   ### 📝 Example
   ....
   Results Displayed when Multiple Servers Are Registered

   ```
   192.168.1.100, 192.168.1.101
   ```
   ....

   b. Execute the following command. When entering the command, enter the results of step a in "*Content_recorded_in_step_a*".

   ```
   > winrm set winrm/config/client @{TrustedHosts="Content_recorded_in_step_a,
   IP_address_for_connecting_to_the_VDI_management_server"}
   ```

   ### 📝 Example
   ....
   Command when Multiple VDI Management Servers Are Registered

   ```
   > winrm set winrm/config/client @{TrustedHosts="192.168.1.100, 192.168.1.101,
   IP_address_for_connecting_to_the_VDI_management_server"}
   ```
   ....

   c. Execute the following command, and confirm the content in TrustedHosts.

   ```
   > winrm get winrm/config/client
   ```

   If the address of the VDI management server you entered in "*Content_recorded_in_step_a*" has been added, then there are no problems.

4. Configure the VDI management server to allow access from Windows Remote Management.

   Log in to the VDI management server as a user with administrator privileges, and execute the following command from the command prompt. When the prompt is displayed, enter "y".

   ```
   > winrm quickconfig
   ```

5. Change the PowerShell execution policies.

   On both the machine to be set up as the admin server of Resource Orchestrator and the VDI management server, change the PowerShell execution policy to "RemoteSigned".

   Start the PowerShell console using administrator privileges and execute the following command.

   ```
   > Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
   ```

Confirmation of Results

Execute the following command, and confirm that notification has been enabled.

```
> msgnotice info
```

See

For details on the msgnotice command, refer to "4.9 msgnotice".

Point

The default message is shown below.

```
Warning!
Security threat detected.
This virtual application/desktop will be disconnected for safety reasons.
```

When changing the content of the message, configure it in the definition file.

For details on the definition results file, refer to "2.5.4 Definition File for Enabling Notification".

Note

- When notification is enabled, there will be a delay of up to 10 seconds before automatic quarantining is performed.

- In order to use this function, it is necessary to configure Citrix Studio on the same server as Citrix Delivery Controller, which is on the VDI management server.

2.7 Procedure for Configuring Email Notification to the Administrator

This section explains the procedure for configuring email notification to the administrator.

When a malware infection is detected, it is possible to notify the tenant administrator of the relevant machine, after executing a pre-defined action.

In addition, when "none" is set for the action, a link for performing actions will be included in the body of the notification email. By clicking the link it is possible to select actions such as quarantine, reboot, quarantine and reboot. After the action is executed, another email notifying the administrator of the results will be sent.

However, this function is disabled by default. When using this function, enable it using the following procedure.

Procedure

Perform the following procedure on the Resource Orchestrator manager.

1. Register the connection information for the SMTP server.

   Execute the following command using the Resource Orchestrator manager.

   ```
   > mailnotice register -name name -ip ipaddress -from from_address [-port port]
   ```

2. Enable the email notification function.

   Execute the following command.

   ```
   > mailnotice enable
   ```

3. Set the email address of the tenant administrator.

   For a new tenant

   [Virtual Edition]

   1. Create an XML definition file containing the information of the email address of the administrator.

   2. Execute the following command, and create the tenant.

      ```
      > rcxadm tenant create -file file.xml [-nowait]
      ```

   [Cloud Edition]

   Refer to "11.3 Creating a Tenant" in the "User's Guide for Infrastructure Administrators".

   For an existing tenant

   [Virtual Edition]

   Execute the following command, and add the email address of the administrator to the tenant information.

   ```
   > rcxadm tenant modify -name name -mail mail_address
   ```

   [Cloud Edition]

   Refer to "11.4 Modifying a Tenant" in the "User's Guide for Infrastructure Administrators".

4. Check that the email notification function has been enabled. Check that "Notice: enable" is contained in the output results for the command.

   ```
   > mailnotice info
   ```

   Output Example

   ```
   > Notice: enable
   > Name: smtpsv
   > IP address: 192.168.100.21
   > Port: 25
   > From address: alert@ror.com
   ```

 See
. . . .

For details on the commands, refer to "4.10 mailnotice" and "4.4 rcxadm tenant".

The number of times email notification is sent when each action is selected is as shown below.

Actions	Number of Times Notification is Sent Before the Action	Number of Times Notification is Sent After the Action	Total
quarantine	No notification	1 time	1 time
reboot	No notification	1 time	1 time

quarantine_reboot (*1)	No notification	2 times	2 times
none (*2)	quarantine	1 time	1 time	2 times
	reboot	1 time	1 time	2 times
	quarantine_reboot (*1)	1 time	2 times	3 times
	none	1 time	No notification	1 time

*1: When the action is "quarantine_reboot", email notification will be given two times, "quarantine_reboot (quarantine)" and "quarantine_reboot (reboot)".

*2: When the action is "none", the administrator will select the response pattern.

· ·

Note

· ·

The Email Notification function cannot be used for virtual PCs that do not belong to tenants.

If "none" is specified for the action to execute when a malware infection is detected, as email notification will not be sent, it will be necessary to perform corrective action manually.

Use this function after assigning the virtual PCs for which "none" will be set as the action to a tenant.

· ·

2.8 Registering Sub Manager Information

This section explains the procedure for registering information of sub managers, in configurations where there are multiple Resource Orchestrator managers.

Procedure

· Register sub manager information.

Execute the following command on the first manager of Resource Orchestrator.

```
> rcxadm submgr create -host IP_address_or_FQDN_of_the_sub_manager -port
Port_number_used_for_the_rcxweb_service -user
User_name_of_the_user_with_administrator_privileges_for_the_OS_of_the_sub_manager -password
Password_of_the_user_with_administrator_privileges_for_the_OS_of_the_sub_manager -ror_user
User_name_of_the_privileged_user_of_the_sub_manager -ror_password
Password_of_the_privileged_user_of_the_sub_manager
```

When using multiple sub managers, register all of the sub manager.

Confirmation of Results

Execute the following command, and confirm that the information of the sub manager has been registered.

```
> rcxadm submgr list
```

See

· ·

For details on the rcxadm submgr command, refer to "4.7 rcxadm submgr".

· ·

[Trend Micro OfficeScan] [McAfee]

1. Authorize remote management.

   a. Execute the following command on the first manager, and record the content displayed in TrustedHosts.

   ```
   > winrm get winrm/config/client
   ```

Record the content displayed in TrustedHosts. If the displayed content is a single asterisk ("*"), or the manually configured "*IP_address_or_FQDN_of_the_sub_manager*", it is not necessary to perform steps b and c below.

Example

. . . .

Results Displayed when Multiple Servers Are Registered

```
192.168.1.100, 192.168.1.101
```

. . . .

b. Execute the following command on the first manager of Resource Orchestrator. When entering the command, enter the results of step a in the "*Content_recorded_in_step_a*" below.

```
> winrm set winrm/config/client @{TrustedHosts="Content_recorded_in_step_a,
IP_address_or_FQDN_of_the_sub_manager"}
```

Example

. . . .

Command for when Multiple Sub Managers Are Registered

```
> winrm set winrm/config/client @{TrustedHosts="192.168.1.100,
192.168.1.101,IP_address_or_FQDN_of_the_sub_manager_1,
IP_address_or_FQDN_of_the_sub_manager_2"}
```

. . . .

Note

. . . .

The same value must be set for the value set using the "rcxadm submgr" command and the value set using the winrm command.

When set using the IP address, set the IP address, and when set using the FQDN, set the FQDN.

. . . .

c. Execute the following command on the first manager, and check the content of TrustedHosts.

```
> winrm get winrm/config/client
```

If the address of the sub manager you entered in "*Content_recorded_in_step_a*" has been added, then there are no problems.

2. Configure the sub manager to allow access from Windows Remote Management.

Log in to the sub manager as a user with administrator privileges, and execute the following command from the command prompt. When the prompt is displayed, enter "y".

```
> winrm quickconfig
```

3. Change the PowerShell execution policies.

On the first manager and the sub managers, change the PowerShell execution policy to "RemoteSigned".

Start the PowerShell console using administrator privileges and execute the following command.

```
> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
```

2.9 Registering Resource Orchestrator Resources

This section explains the procedure for registering the resources of Resource Orchestrator.

2.9.1 Importing the System Configuration File

This section explains the procedure for importing a CSV format "2.5.2 Definition File Setting Action Selection" using the GUI (ROR console).

Procedure

Use the following procedure to import a system configuration file.

1. Start the GUI (ROR console) and log in.

2. In the GUI (ROR console), select [File]-[System Configuration File]-[Import].

   The [Import System Configuration File] dialog is displayed.

3. Specify the system configuration file prepared in "2.5.2 Definition File Setting Action Selection".

4. Click the [OK] button.

   The import process starts. The system configuration file is verified first, and then resources are imported one by one, following the order defined in the system configuration file.

5. The processing of resource registration or change is executed after verification.

   The process status can be checked in the Recent Operations area of the GUI (ROR console).

   Clicking [Cancel] in the Recent Operations area displays a confirmation dialog and stops the import process. Cancelling interrupts the import process after the current process is complete. Note that the processing performed up to the point of cancellation is reflected on the system.

Confirmation of Results

When import is completed successfully, a message is displayed in the Recent Operations area.

2.10 Registering Resources in Resource Pools

This section explains the procedure for registering resources in resource pools.

The resources which must be registered vary depending on the types of the managed servers.

Virtual PC

- Registering VM hosts in VM pools

- Register network resources

   The following networks must be registered as network resources:

   - Business Network

   - Quarantine Network

SBC Servers

- Register physical servers in server pools

- Register network devices (adjacent switches)

- Register network resources

   The following networks must be registered as network resources:

   - Management Network

   - Business Network

   - Quarantine Network

2.10.1 Registering VM hosts in VM pools

This section explains the procedure for registering VM hosts in VM pools.

Necessary when using virtual PCs.

2.10.1.1 Registering VM Hosts in VM Pools Using the GUI (ROR Console)

This section explains the procedure for registering VM hosts in VM pools using the GUI (ROR console).

Procedure

Perform the following procedure:

1. In the orchestration tree of the GUI (ROR console), right-click the target VM pool and select [Register Resources] from the popup menu.

2. The [Register Resources] dialog is displayed.

3. Select the VM hosts to register.

   The list of the VM hosts that can be registered is displayed in the resource list. Select the [Select] checkboxes for the VM hosts to register, or click the [Select all] button to select all of the VM hosts displayed in the list of resources.

4. Click the [OK] button.

   The VM host resources are registered.

Confirmation of Results

In the [Resource List] tab, confirm that the VM host resources have been registered in the target VM pool.

2.10.2 Registering Physical Servers in Server Pools

This section explains the procedure for registering physical servers in server pools.

This procedure is necessary when using SBC servers.

2.10.2.1 Registering Physical Servers in Server Pools Using the GUI (ROR Console)

This section explains the procedure for registering physical servers in server pools using the GUI (ROR console).

Procedure

Perform the following procedure:

1. In the ROR console orchestration tree, right-click the target server pool, and select [Register Resources] from the popup menu.

   The [Register Resources] dialog is displayed.

   Select the [Display servers with OS installed] checkbox.

2. Select the physical servers to register.

   The list of the physical servers that can be registered is displayed in the resource list. Select the [Select] checkboxes for the physical servers to register, or click the [Select all] button to select all of the physical servers displayed in the list of resources.

3. Click the [OK] button.

   The physical servers are registered.

2.10.3 Registering Network Devices (Adjacent Switches)

This section explains the procedure for registering network devices (adjacent switches).

2.10.3.1 Registering Network Devices (Adjacent Switches) Using the CLI

This section explains the procedure for registering network devices (adjacent switches) using the CLI.

Purpose

When enabling the automatic quarantining of physical servers, it is necessary to register switches adjacent to the physical servers as network devices in Resource Orchestrator.

Preparations

To enable the VLAN settings of network devices to be modified during automatic quarantining, it is necessary to register scripts in advance which will automatically configure and operate network devices.

For details, refer to the following.

- Appendix D Preparations for Automatic Configuration and Operation of Network Devices

Procedure

Perform the following procedure:

1. To register adjacent network switches, create the network configuration information XML file.

   For details, refer to "XML definitions for batch creation of multiple network devices" in "A.6 Network Configuration Information XML File".

2. Import the network configuration information XML file. Execute the following command.

   ```
   > rcxadm netconfig import -file file.xml
   ```

Confirmation Procedure

Confirm that the network configuration information has been successfully registered. Execute the following command.

```
> rcxadm netdevice show -name network_device_name
```

📘 Information

. . . .

When Creating Network Devices Individually

Perform the following procedure:

1. Create the network configuration information XML file.

   For details, refer to "XML definitions for creation of individual network devices" in "A.6 Network Configuration Information XML File".

2. Create the network device. Execute the following command. For *file.xml*, specify the network configuration XML file created in step 1.

   ```
   > rcxadm netdevice create -file file.xml
   ```

. . . .

2.10.4 Registering Network Resources

This section explains the procedure for registering network resources.

Network resources are registered as operation and quarantine networks.

📘 Point

. . . .

For SBC Servers

- When registering an SBC server, it is necessary to create the following three network resources:

    - Management Network (The network resource of the admin LAN directly connected to the manager)

    - Business Network

    - Quarantine Network

- For both the business network and the quarantine network, select [public LAN] for the type. For the management network, select [admin LAN] for the type.

- A management network resource with the name "AdminLan", and the VLAN ID "1" is automatically created during installation of Resource Orchestrator.

- After deleting "AdminLan", create network resources following "2.10.4.2 Registering Management Network Resources Using the GUI (ROR Console)".

. . . .

P Point

. . . .

For Virtual PCs

- When registering a virtual PC, it is necessary to create network resources for the business network and the quarantine network.

- For both the business network and the quarantine network, select [public LAN] for the type.

- For the network resource names of the business network, specify the resource names of the business network specified in "2.5.6 Definition File for Configuring the Business and Quarantine Networks".

- For the network resource names of the quarantine network, specify the resource names of the quarantine network specified in "2.5.6 Definition File for Configuring the Business and Quarantine Networks".

. . . .

Prerequisites (SBC Servers)

It is necessary to register rulesets (scripts) for the L2 switches corresponding to network resources in folders of Resource Orchestrator.

For details on the ruleset (script), refer to "Appendix D Preparations for Automatic Configuration and Operation of Network Devices".

Prerequisites (Virtual PCs)

The prerequisites for registering network resources are as follows.

For the prerequisites for loading an IP address assigned to a virtual PC to an L-Server, refer to the prerequisites of "2.12 Linking Virtual L-Servers with Configured Virtual PCs".

1. The network resources satisfy all of the following conditions:

   - The network resources are registered in resource pools that users can access

   - The IP address assigned to the virtual machine is within the range of IP addresses configured for the network resources

   - The VLAN ID of the virtual machine matches that of the L-Server

   - There are not multiple network resources registered with different VLAN IDs and the same subnet address

   - In environments in which the VLAN ID cannot be obtained from the virtual machine, there is only a single network resource that is included in the range of the IP addresses assigned to the virtual PC registered in an accessible resource pool

     In the above situation, ensure that there are not multiple network resources configured with overlapping IP address ranges.

2. The network information of the VM hosts is up to date

   Perform the following for each VM host.

   [For VMware vSphere 6.0]

   To update the network information, perform the following procedure using the virtualization software (vSphere Web Client).

   a. From the Inventory, move to [Hosts and Clusters].

   b. Select the VM host to update the information for.

   c. Click the [Configuration] tab.

   d. Under [Hardware], click [Networking].

   e. Click [Refresh], and then wait for the updating of network information to complete.

[VMware vSphere 6.5 or later]

To update the network information, perform the following procedure using vSphere Web Client:

a. From the Inventory, move to [Hosts and Clusters].

b. Select the VM host to update the information for.

c. Click the [Configure] tab.

d. Click [Networking]-[Virtual switches].

e. Click the [Refresh the host's network system] icon, and then wait for the update of network information to complete.

[For Hyper-V]

To update the network information, perform the following procedure using the virtualization software (VMM console):

a. Open the [VMs and Services] work space.

b. From [All Hosts], select the VM host to update the information of.

c. Select [Refresh] from the pop-up menu.

d. Wait for the "Refresh host cluster" job to complete.

e. In [VMs], select all virtual machines and then right-click.

f. Select [Refresh] from the pop-up menu.

g. Wait for the "Refresh virtual machine" job to complete.

3. The most recent information of the VM management software is reflected on the configuration definition information of Resource Orchestrator

Execute the following command on the admin server.

[Windows Manager]

```
> rcxadm vmmgr refresh
```

2.10.4.1 Registering Business Network Resources Using the GUI (ROR Console)

This section explains the procedure for registering business network resources using the GUI (ROR console).

Procedure

Perform the following procedure:

1. In the orchestration tree of the GUI (ROR console), right-click the target network pool, and select [Create Network Resource]-[New] from the displayed menu.

The [Create a network resource] dialog is displayed.

2. Configure the following items:

Network resource name

Enter a name for the network resource.

- If a type other than [Admin LAN] is selected

Enter up to 32 characters beginning with an alphanumeric character (upper or lower case), and including alphanumeric characters (upper or lower case), underscores ("_"), periods ("."), or hyphens ("-").

Category

Set the network resources type to create using the following option button.

- Public LAN

When creating the public LAN, a network resource name and a VLAN ID must be entered.

Detail configuration

Configure as follows.

- Use configured virtual switches

Select this checkbox to use a virtual switch that was set up beforehand.

VLAN ID/Uplink port settings

Perform the settings for VLAN IDs and uplink ports.

VLAN ID

Specify the VLAN ID to allocate to the LAN switch blade and virtual switch. Select a VLAN ID allocated to the uplink port of the LAN switch blade, or enter a number. Specify a pre-designed VLAN ID.

Enter an integer between "1" and "4094".

- For internal networks or external networks with rack mount servers only

Enter a VLAN ID.

Specifying VLAN IDs and clicking [Setting] displays the [Define VLAN ID/Uplink port settings] dialog.

Uplink port settings (Chassis/LAN Switch/Position/Port/LAG Name) (Optional)

Do not specify for internal networks or external networks with rack mount servers only.

Subnet settings

Enter this item to automatically set a network and IP address for the NIC connected to the network resource when deploying an image on an L-Server.

IP addresses included in subnet addresses are allocated to L-Servers, but it is possible to specify a range of addresses to exclude. Clicking the [Add] button will display the [Define start and end IP addresses] dialog, specify the range of IP addresses to exclude, and click the [Add] button. To reactivate excluded IP addresses, check the appropriate checkboxes on the list, and click the [Delete] button. Clicking the [OK] button displays the original dialog with the entered settings.

Network addresses and broadcast addresses are automatically excluded.

Information

If a subnet address has been set for the network resource, the IP address can be automatically set when deploying an image to an L-Server.

Subnet address/mask

Enter the subnet address and subnet mask to set using the "*xxx.xxx.xxx.xxx*" format.

The maximum value for a subnet mask is 255.255.255.255 (32-bit mask) and the minimum value is 255.255.0.0 (16-bit mask). However, 255.255.255.254 cannot be specified.

Note

Specifying the same subnet between network resources for an admin LAN is not possible.

For details, refer to the following.

[Virtual Edition]

"Chapter 7 Defining and Configuring the Network Environment" in the "Design Guide VE"

[Cloud Edition]

"Chapter 9 Defining and Configuring the Network Environment" in the "Design Guide CE"

Default gateway (Optional)

This setting can be omitted if something other than [Admin LAN] is selected.

Enter the IP address for the default gateway to use when communicating externally of the subnet.

Exclusion IP range (Optional)

IP addresses that you do not want to automatically allocate to an L-Server (because they are being used or are planned to be used for other devices) can be specified.

Information
. . . .
The IP addresses that are being used by configured physical servers, virtual PCs, and other devices must be specified for this item to prevent them from being used for L-Servers.
. . . .

Note
. . . .
Of the IP addresses specified for the Subnet address/mask, the following addresses are automatically excluded from the target of allocation. They cannot be specified for Exclusion IP range.

- Admin server

- Network address and broadcast address
. . . .

Ruleset (Optional)

When using SBC servers, select a ruleset to use from the rulesets available for network resources.

Register the ruleset to use in the common folder on the network device for the network resource. For the folders to register the rulesets for network resources in, refer to "D.3.1 Folders for Network Resources".

Label (Optional)

A custom label can be defined for the network resource. User-defined labels make it easier to identify the resource.

Enter a string of up to 32 alphanumeric characters (Both double-byte and single-byte characters can be used).

Comment (Optional)

A custom comment can be defined for the network resource. For example, registering detailed work content, troubleshooting, and recovery procedures can speed up recovery.

Enter a string of up to 256 alphanumeric characters (Both double-byte and single-byte characters can be used).

3. Click the [OK] button.

The network resource is created and registered in a network pool.

Confirmation of Results

In the [Resource List] tab, confirm that the operation network resource has been registered in the target network pool.

2.10.4.2 Registering Management Network Resources Using the GUI (ROR Console)

This section explains the procedure for registering management network resources using the GUI (ROR console).

Registration of management network resources is necessary when using SBC servers.

Prerequisites

A management network resource with the name "AdminLan", and the VLAN ID "1" is automatically created during installation of Resource Orchestrator.

Delete "AdminLan" in advance.

Procedure

Use the following procedure to create a network resource using an admin LAN subnet, and register it in a network pool:

1. In the ROR console orchestration tree, right-click the target network pool, and select [Create Network Resource]-[Using existing admin subnet] from the popup menu.

   The [Create a network resource] dialog is displayed.

2. Enter the following items:

   Network resource name

   Clicking the [Select] button displays the [Select a subnet for the admin LAN] dialog.

   Select an already configured admin LAN subnet.

   When the selected admin LAN subnet has no name, enter the name of a network resource for "Network resource name".

   Enter up to 32 characters beginning with an alphanumeric character (upper or lower case), and including alphanumeric characters (upper or lower case), underscores ("_"), periods ("."), or hyphens ("-").

   Click the [OK] button.

   Type

   "Admin LAN" is displayed.

   VLAN ID/Uplink port settings

   Refer to "VLAN ID/Uplink port settings" of "2.10.4.1 Registering Business Network Resources Using the GUI (ROR Console)".

   Subnet settings

   Refer to "Subnet settings" in "2.10.4.1 Registering Business Network Resources Using the GUI (ROR Console)".

   Ruleset (Optional)

   Refer to "Ruleset (Optional)" in "2.10.4.1 Registering Business Network Resources Using the GUI (ROR Console)".

   Label (Optional)

   Refer to "Label (Optional)" in "2.10.4.1 Registering Business Network Resources Using the GUI (ROR Console)".

   Comment (Optional)

   Refer to "Comment (Optional)" in "2.10.4.1 Registering Business Network Resources Using the GUI (ROR Console)".

3. Click the [OK] button.

   The network resource is created and registered in a network pool.

   When the [Automatically configure VLANs for the uplink ports.] checkbox in the VLAN ID/Uplink port settings is checked, a tagged VLAN is automatically configured in the uplink port of LAN switch blade, when creating a network resource.

Confirmation of Results

In the [Resource List] tab, confirm that the management network resources have been registered in the target network pool.

2.10.4.3 Registering Quarantine Network Resources Using the GUI (ROR Console)

This section explains the procedure for registering quarantine network resources using the GUI (ROR console).

Procedure

For details, refer to "2.10.4.1 Registering Business Network Resources Using the GUI (ROR Console)".

Confirmation of Results

In the [Resource List] tab, confirm that the quarantine network resource has been registered in the target network pool.

2.11 Registering Antivirus Software

This section explains the procedure for registering antivirus software.

Registration of antivirus software is possible even when Resource Orchestrator is operating.

2.11.1 Registering Antivirus Software Using the CLI

This section explains the procedure for registering antivirus software using the CLI.

When coordinating either of the following antivirus software with the Automatic Quarantining Function, it is not necessary to register antivirus software using the CLI.

- Trend Micro Control Manager

- Symantec Endpoint Protection

In addition, in configurations where there are multiple Resource Orchestrator managers, it is not necessary to perform the registration procedure for antivirus software using the CLI on sub managers.

Items to Confirm Beforehand

1. Confirm the IP address of the SNMP trap agent of the antivirus software to be registered.

Note

. . . .

When there are multiple IP addresses, register antivirus software for each IP address.

. . . .

2. Confirm the registered antivirus software. Execute the following command.

```
> rcxadm avmgr list
```

For details, refer to "4.1 rcxadm avmgr".

Procedure

Register the antivirus software. Execute the following command.

For -ip, specify the IP address confirmed in step 1 above.

Specify one of the following:

[Trend Micro OfficeScan]

- The IP address of the SNMP trap agent of the OfficeScan 11.0 server

- The IP address of the SNMP trap agent of the OfficeScan XG server

```
> rcxadm avmgr create -name Resource_name_of_the_antivirus_software -mgmt_soft_name corp -ip
IP_address_of_the_SNMP_trap_agent_of_the_antivirus_software
```

[McAfee]

- The IP address of the SNMP trap agent of the McAfee ePolicy Orchestrator server

```
> rcxadm avmgr create -name Resource_name_of_the_antivirus_software -mgmt_soft_name epo -ip
IP_address_of_the_SNMP_trap_agent_of_the_antivirus_software
```

For details, refer to "4.1 rcxadm avmgr".

Note

. . . .

It is not possible to register antivirus software with the same name as any of the registered antivirus software confirmed in step 2 above.

In addition, it is not possible to register antivirus software with the same identifier and IP address as any of the registered antivirus software confirmed in step 2.

. . . .

Confirmation of Results

Confirm the registered antivirus software. Execute the following command.

```
> rcxadm avmgr list
```

For details, refer to "4.1 rcxadm avmgr".

2.12 Linking Virtual L-Servers with Configured Virtual PCs

This section explains how to link virtual L-Servers with configured virtual PCs.

Notification of security risks detected on virtual PCs by the following servers is sent to Resource Orchestrator using SNMP traps or a REST API.

[Trend Micro OfficeScan]

- OfficeScan 11.0 server

- OfficeScan XG server

[Symantec]

- Symantec Endpoint Protection Manager

[McAfee]

- McAfee ePolicy Orchestrator server

In response, the virtual PCs to be switched to the quarantine network are identified. This identification requires that there are L-Servers configured with the IP addresses of the virtual PCs to be quarantined.

In addition, the switchover to the quarantine network requires a virtual L-Server for network operation.

[VMware]

For the virtual L-Server for network operation, there are restrictions on the types of virtual NICs of virtual PCs to be linked with virtual L-Servers. The following virtual NICs are supported:

- E1000e

- E1000

- VMXNET3

Linking virtual PCs with virtual L-Servers enables the IP addresses assigned to the virtual PCs to be loaded to the virtual L-Servers.

Prerequisites

The prerequisites for loading an IP address of a virtual PC to an L-Server are as follows:

- The virtual PC is turned on
- Resource Orchestrator has detected the virtual PC

    Turn on the virtual PC, and then wait about six minutes.

[VMware]

- VMware Tools is operating on the virtual PC, and the virtualization software has detected the IP address

    Confirm this using the virtualization software (vSphere Client or vSphere Web Client). Confirm the following:

    - The [VMware Tools] label on the [Summary] tab for the virtual PC indicates that the software is running

    - The [IP Addresses] label on the [Summary] tab for the virtual PC shows the IP address assigned to the virtual PC

[Hyper-V]

- The virtualization software has detected the IP address

> 📝 **Note**

....

If a Hyper-V virtual PC is running Windows and update KB3063109 has not been applied, it may not be possible to load the IP address assigned to that virtual PC to an L-Server. Be sure to use Microsoft Update, etc. to apply the latest updates.

....

[Citrix Xen]

- XenServer Tools is operating on the virtual PC, and the virtualization software has detected the IP address

    Confirm this using the virtualization software (XenCenter). Confirm the following:

    - In [Virtualization state] on the [General] tab for the virtual machine, "Management Agent installed" is displayed

    - [IP Address] on the [Networking] tab for the virtual machine shows the IP address assigned to the virtual machine

- Home Server is set on the virtual machine.

2.12.1 Batch Loading Virtual PCs Using the convertVMtoLServer Command

This section explains the procedure for using the convertVMtoLServer command to batch load virtual PCs to virtual L-Servers.

Purpose

Execute this command to perform batch linking of virtual PCs with virtual L-Servers and batch creation of XML files for changing the network of virtual L-Servers.

Procedure

1. Execute the convertVMtoLServer command to create the CSV configuration file.

    Execute the following command.

    ```
    > convertVMtoLServer -exportfile Storage_folder_of_the_CSV_configuration_file
    ```

    The CSV configuration file is created with the following name in the *storage_folder_of_the_CSV_configuration_file*.

    convertVMtoLserver_*yyyymmddhhmmss*.csv

    yyyymmddhhmmss is the date and time when the CSV configuration file was created.

    When linking virtual PCs with each tenant, specify the -setfolder option. For details, refer to "4.2 convertVMtoLServer".

2. Link the virtual PCs with virtual L-Servers and perform batch creation of the XML files for changing the network of virtual L-Servers.

    Execute the following command. Specify the CSV configuration file created in step 1.

    ```
    > convertVMtoLServer -file Storage_folder_of_the_CSV_configuration_file
    \convertVMtoLserver_yyyymmddhhmmss.csv
    ```

> 📘 **Information**

....

- In the following cases, edit the CSV configuration file created in step 1 before performing step 2.

    - When you want to include comments or labels in the CSV configuration file

    - When you want to use a folder structure to organize the resources of L-Servers

- If the CSV configuration file created in step 1 contains the information of a virtual PC that you do not want to load, delete the line in the CSV file which corresponds to that virtual PC before performing step 2.

....

> 📚 **See**

....

For details on the convertVMtoLServer command, refer to "4.2 convertVMtoLServer".

....

Confirmation of Results

Confirm the following:

- View the CSV results file, and confirm that no error messages have been output.

  After executing the command, a CSV results file is generated under the *storage_folder_of_the_CSV_configuration_file*, and the execution results and any error messages are output to it.

  If there are any virtual PCs which could not be linked with L-Servers, refer to the information in the *Note* column to identify the cause of the error, and then perform the relevant "Appendix B Corrective Actions for Errors".

See

. . . .

For details on the CSV results file, refer to "CSV Results File".

. . . .

- Confirm that the network information of each linked virtual L-Server contains the IP address of the relevant virtual PC.

  Select the virtual L-Server from the GUI (ROR console), and then select [Resource Details]-[Network Information].

  Confirm that the relevant IP address and network resource name are shown in the corresponding columns in the displayed information.

  If values have not been acquired, refer to "B.2 When the IP Address of a Linked Virtual L-Server Is Not Displayed in the Network Information for the Virtual L-Server" and take corrective action.

- Confirm that the XML files for changing the network of the linked virtual L-Servers have been created.

  Storage Location of the XML Files for Changing the Network

  [Windows Manager]

  Installation_folder\SVROR\Manager\etc\files\avmgr

  Names of the XML Files for Changing the Network

  quarantine_*L-Server_name*.xml

  unquarantine_*L-Server_name*.xml

  If the XML files for changing the network have not been created, perform "B.3 When the XML Files for Changing the Network Have Not Been Created" and create them.

Note

. . . .

- Specify the CSV configuration file name using an absolute path.

- If this command is executed again with the same CSV configuration file specified, the CSV results file output during the previous execution will be overwritten. To prevent the file being overwritten, back up previously output CSV results files.

- Only virtual PCs that are powered on can be loaded to virtual L-Servers. If you attempt to load a virtual PC that is powered off to a virtual L-Server, the error message 69133 will be output. Power on the virtual PC, wait a couple of minutes, and then execute the command again.

- If the convertVMtoLServer -exportfile command is executed, even if the attempt to link the virtual PC with a virtual L-Server of Resource Orchestrator fails, the information of the target virtual PC will be still be output to the CSV configuration file. However, if the convertVMtoLServer -file command is executed, the attempt to link the target virtual PC to a virtual L-Server will result in an error, and error message 67154 will be output. For virtual PCs that could not be linked, perform "B.1 When Linking of Virtual PCs with Virtual L-Servers Fails".

- If there are multiple VM guests which have the same name operating on the VM hosts registered in a VM pool, execution of the convertVMtoLServer -exportfile command will not result in an error. Instead, the same line describing the duplicated VM guest name will be output on multiple lines in the CSV configuration file. If this CSV configuration file is specified during execution of the convertVMtoLServer -file command, the attempt to link any duplicate VM guests after the first one to a virtual L-Server will result in an error, and the error message 67280 will be output. Take corrective action according to the details of error message 67280.

- If the linking of a virtual PC with a virtual L-Server succeeds, but an error in the description of the definition file, etc. causes the creation of the XML files for changing the network to fail, resolve the cause of the error, and then use the convertVMtoLServer -createxml command to create the XML definition files for changing the network. For details, refer to "B.3 When the XML Files for Changing the Network Have Not Been Created".

- For virtual PCs that have multiple NICs, refer to "A.4 XML Files for Changing the Network", and create an XML file for changing the network that handles multiple NICs.

. . . .

2.13 Linking Physical L-Servers with Configured SBC Servers

This section explains how to link physical L-Servers with configured SBC servers.

Notification of security risks detected on physical servers by the following servers is sent to Resource Orchestrator using SNMP traps or a REST API.

[Trend Micro OfficeScan]

- OfficeScan 11.0 server

- OfficeScan XG server

[Symantec]

- Symantec Endpoint Protection Manager

[McAfee]

- McAfee ePolicy Orchestrator server

In response, the physical servers to be switched to the quarantine network are identified. This identification requires that there are L-Servers configured with the IP addresses of the physical servers to be quarantined.

Also, the switchover to the quarantine network requires a physical L-Server for network operation.

Linking physical servers with physical L-Servers enables the IP addresses assigned to the SBC servers to be loaded to the physical L-Servers.

2.13.1 Linking SBC Servers with Physical L-Servers Using the rcxadm lserver Command

This section explains the procedure for linking SBC servers with physical L-Servers using the rcxadm lserver command.

Purpose

Perform this procedure when linking SBC servers with physical L-Servers.

Prerequisites

For an SBC server to be linked, it is necessary for an agent to be installed on it, and for that agent to be registered in Resource Orchestrator.

Procedure

Link the physical server with a physical L-Server. Execute the following command.

```
> rcxadm lserver convert -with /Server_pool_name/Physical_server_name
```

For details on the rcxadm lserver command, refer to "4.3 rcxadm lserver".

Confirmation Procedure

Confirm that the linking with the physical L-Server has been completed successfully. Execute the following command.

```
> rcxadm lserver show -name Physical_L-Server_name -format xml
```

P **Point**
....
The name of the physical L-Server must be the same as that of the physical server.
....

2.13.2 Loading the IP Addresses of the Business Network Assigned to Physical Servers

When a physical server is linked with a physical L-Server, only the IP address of the management network is loaded.

This section explains how to load the IP address of the business network assigned to a physical server.

Procedure

1. Create the XML file necessary for specifying the network resources and IP addresses corresponding to the NICs for the physical L-Server.

    a. Execute the following command to output the base XML file for changing the network.

    ```
    > rcxadm lserver show -name Physical_L-Server_name -format xml
    ```

    b. Delete any unnecessary information from the output XML file and edit the content as shown below. However, do not delete the information specified in the NIC elements for the management network.

    The Resources, LServer, and NICs elements must be included.

    Depending on the details of the business network of the physical server, add the values for "name" in the NetworkLink element and "address" in the IpAddress element.

    For details on the XML file, refer to "Table A.2 Excerpt from Definition Information for Physical L-Servers (XML)".

    ```xml
    <?xml version="1.0" encoding="utf-8"?>
    <Resources>
      <LServer name="L-Server_name">
        <NICs>
          <NIC>
            <NICIndex>NIC_index</NICIndex>
            <MacAddress auto="false"></MacAddress>
            <NetworkLinks>
              <NetworkLink name="Network_name" index="Network_index" vlan_mode="VLAN_mode">
                <IpAddress auto="Automatic_IP_configuration" address="IP_address"/>
              </NetworkLink>
            </NetworkLinks>
          </NIC>
          <NIC>
            <NICIndex>NIC_index</NICIndex>
            <MacAddress auto="false"></MacAddress>
            <NetworkLinks>
              <NetworkLink name="Network_name" index="Network_index" vlan_mode="VLAN_mode">
                <IpAddress auto="Automatic_IP_configuration" address="IP_address"/>
              </NetworkLink>
            </NetworkLinks>
          </NIC>
            *Specify as many NIC elements as the number of NICs connected to the business network
        </NICs>
      </LServer>
    </Resources>
    ```

2. Execute the following command using the XML file that was created in step 1 to specify the network resources and IP addresses corresponding to the NICs for the physical L-Server.

    ```
    > rcxadm lserver modify -name Physical_L-Server_name -type physical -file file.xml [-nowait]
    ```

3. Refer to "Confirmation of Results" and confirm that the changes you made in step 2 have been reflected.

Confirmation of Results

Execute the following command and confirm that the changes you made in step 2 have been reflected.

```
> rcxadm lserver show -name Physical_L-Server_name -format xml
```

2.13.3 Creating and Storing the XML File for Changing the Network of Physical L-Servers from the Operation Network to the Quarantine Network

This section explains the procedure for creating and storing the XML file for changing the network of physical L-Servers from the operation network to the quarantine network.

Procedure

1. Execute the following command to output the base XML file for changing the network.

```
> rcxadm lserver show -name Physical_L-Server_name -format xml
```

2. Delete any unnecessary information from the output XML file and edit the content according to the configuration of the quarantine network.

   Storage Location

   Installation_folder\SVROR\Manager\etc\files\avmgr

   File Name

   quarantine_Physical_L-Server_name.xml

   Be sure not to accidentally delete any NIC elements of networks that are not the target of modification from the XML file.

   For details on the XML file, refer to "Table A.2 Excerpt from Definition Information for Physical L-Servers (XML)".

```xml
<?xml version="1.0" encoding="utf-8"?>
<Resources>
  <LServer name="L-Server_name">
    <NICs>
      <NIC>
        <NICIndex>NIC_number</NICIndex>
        <MacAddress auto="false"></MacAddress>
        <NetworkLinks>
          <NetworkLink name="Network_name" index="Network_index" vlan_mode="VLAN_mode">
            <IpAddress auto="IPAuto-configuration" address="IP_address"/>
          </NetworkLink>
        </NetworkLinks>
      </NIC>
      <NIC>
        <NICIndex>NIC_number</NICIndex>
        <MacAddress auto="false"></MacAddress>
        <NetworkLinks>
          <NetworkLink name="Network_name" index="Network_index" vlan_mode="VLAN_mode">
            <IpAddress auto="IPAuto-configuration" address="IP_address"/>
          </NetworkLink>
        </NetworkLinks>
      </NIC>
    </NICs>
  </LServer>
</Resources>
```

2.13.4 Creating and Storing the XML File for Changing the Connected Network of Physical L-Servers to the Operation Network

This section explains the procedure for creating and storing the XML file for changing the connected network of physical L-Servers to the operation network.

Procedure

1. Execute the following command to output the base XML file for changing the network.

```
> rcxadm lserver show -name Physical_L-Server_name -format xml
```

2. Delete any unnecessary information from the output XML file and edit the content according to the configuration of the operation network.

Storage Location

Installation_folder\SVROR\Manager\etc\files\avmgr

File Name

unquarantine_*Physical_L-Server_name*.xml

For details on the XML file, refer to "Table A.2 Excerpt from Definition Information for Physical L-Servers (XML)".

```xml
<?xml version="1.0" encoding="utf-8"?>
<Resources>
  <LServer name="L-Server_name">
    <NICs>
      <NIC>
        <NICIndex>NIC_number</NICIndex>
        <MacAddress auto="false"></MacAddress>
        <NetworkLinks>
          <NetworkLink name="Network_name" index="Network_index" vlan_mode="VLAN_mode">
            <IpAddress auto="IPAuto-configuration" address="IP_address"/>
          </NetworkLink>
        </NetworkLinks>
      </NIC>
      <NIC>
        <NICIndex>NIC_number</NICIndex>
        <MacAddress auto="false"></MacAddress>
        <NetworkLinks>
          <NetworkLink name="Network_name" index="Network_index" vlan_mode="VLAN_mode">
            <IpAddress auto="IPAuto-configuration" address="IP_address"/>
          </NetworkLink>
        </NetworkLinks>
      </NIC>
    </NICs>
  </LServer>
</Resources>
```

2.14 Testing When Handling Security Risks

This section explains the procedure for testing whether the corrective action for handling a security risk is executed correctly.

Download a dummy virus to a virtual PC or SBC server, and confirm that the virtual L-Server corresponding to each virtual PC or SBC server executes the configured action. If it is executed correctly, refer to "3.1 Operation When Handling Security Risks" and perform the procedure for when security risks have been removed.

If the action is not executed, check if there are any errors in the settings.

In configurations where there are multiple Resource Orchestrator managers, perform testing on all of the managers. Download a dummy virus to a virtual PC or SBC server managed by each Resource Orchestrator manager, and confirm that the virtual L-Server corresponding to each virtual PC or SBC server executes the configured action.

Chapter 3 Operation Using the Automatic Quarantining Function

This chapter explains how to operate this function.

3.1 Operation When Handling Security Risks

This section explains the procedures for operation when handling security risks.
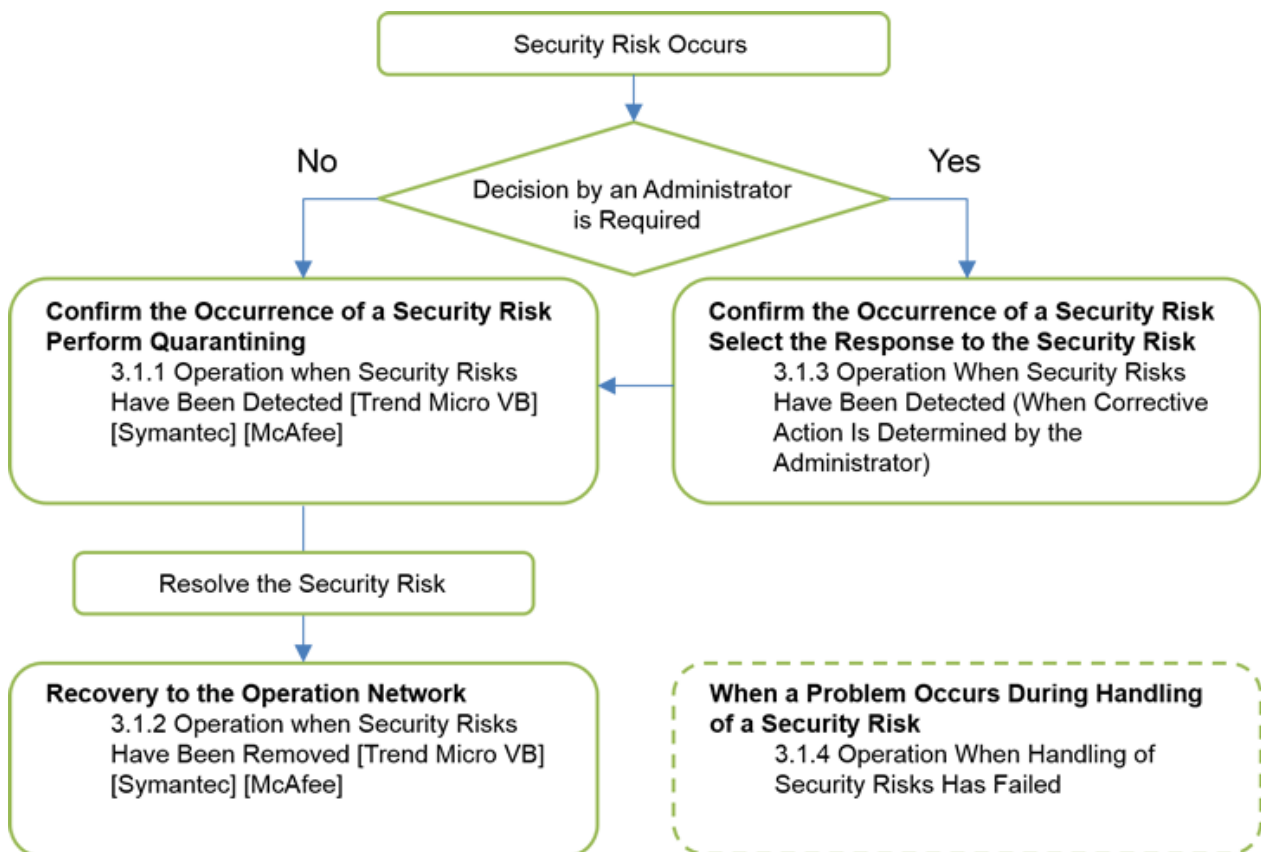
3.1.1 Operation When Security Risks Have Been Detected [Trend Micro VB] [Symantec] [McAfee]

Procedure

1. The infrastructure administrator learns that security risks have been detected through email notifications or by checking the system log of the server on which the Resource Orchestrator manager operates.

   📖 **Note**

   ....

   If the antivirus software coordinating with Resource Orchestrator is the following, information regarding detected security risks will not be output to the system log of the Resource Orchestrator manager server.

   - Symantec Endpoint Protection

   ....

2. The Resource Orchestrator manager responds to a notification from the following server and performs corrective action on the L-Server on which security risks have occurred, in accordance with either the settings for action to be taken automatically, or the action selected by the administrator.

[Trend Micro OfficeScan]

- OfficeScan 11.0 server

- OfficeScan XG server

[Symantec]

- Symantec Endpoint Protection Manager

[McAfee]

- McAfee ePolicy Orchestrator server

3. The infrastructure administrator checks whether the manager has correctly performed the corrective action by confirming the following.

- No error messages are displayed on the GUI (ROR console)

- When an L-Server was quarantined

From the GUI (ROR console), confirm that the network of the relevant L-Server has been switched to the quarantine network, and the IP address of the L-Server.

- When an L-Server was restarted

From the GUI (ROR console), confirm that the relevant L-Server is operating. When restarting has removed the security risk, proceed with operation as when security risks have been removed.

- When multiple Resource Orchestrator managers are configured

Identify the Resource Orchestrator manager that manages the L-Server on which security risks have been detected.

[Trend Micro OfficeScan] [McAfee]

To identify the relevant manager, check the following message that will have been output to the SYSLOG of the server on which the first manager of Resource Orchestrator operates.

```
Send information of SNMP trap to remote manager [Resource_Orchestrator_manager_IP_address]
```

[Symantec]

To identify the manager, check the following message that will have been output on the GUI (ROR console) of the first manager of Resource Orchestrator.

```
FJSVrcx:INFO:21143:quarantine L-
Server(submgr:Resource_Orchestrator_manager_IP_address):started
```

If the above message indicates that an error has been detected, perform the procedure in "3.1.4.1 Corrective Action When Automatic Action Taken When a Security Risk Is Detected Fails [Trend Micro VB] [Symantec] [McAfee]".

4. When quarantining has been performed, environments on which security risks have been detected can no longer be used.

In virtual PC environments, users of quarantined virtual PCs can access other virtual PCs by making requests to the infrastructure administrator.

5. When quarantining has been performed, the infrastructure administrator opens the consoles of the virtual PCs and SBC servers on which security risks have been detected, and performs the following quarantine processing.

   a. Modify the network settings of the OS based on the L-Server IP addresses and the network information confirmed in step 3.

   b. Perform corrective actions according to the manual for the antivirus software and then perform a virus scan.

   Confirm that no viruses are detected.

6. When quarantining has been performed, log off from the virtual machine.

When the quarantine processing in step 5 is complete, log off from the virtual machine.

3.1.2 Operation When Security Risks Have Been Removed [Trend Micro VB] [Symantec] [McAfee]

Procedure

1. When an L-Server has been quarantined

   a. The infrastructure administrator connects the L-Server to the operation network.

      Use the rcxadm avmgr unquarantine command on the Resource Orchestrator manager to reconnect the quarantined L-Servers to the operation network. Alternatively, you can use the procedure for reverting L-Servers included in an email notification of quarantining completion for the same outcome.

      For details on the command, refer to "4.1 rcxadm avmgr".

   b. The infrastructure administrator uses the GUI (ROR console) to confirm that the network of the L-Servers has been switched to the operation network and the IP addresses of the L-Servers.

   c. The infrastructure administrator opens the consoles of the virtual PCs and SBC servers and modifies the network settings of the OS based on the L-Server IP addresses and the network information confirmed in step b.

2. The infrastructure administrator informs the users of the virtual PCs and SBC servers on which security risks were detected that those virtual PCs and SBC servers can be used again.

3.1.3 Operation When Security Risks Have Been Detected (When Corrective Action Is Determined by the Administrator)

Procedure

1. The infrastructure administrator learns that security risks have been detected through email notifications.

2. The infrastructure administrator selects either of the following corrective actions to be performed.

   - Quarantining of the L-Server

   The relevant L-Server is quarantined. For the procedure for confirming that an L-Server has been quarantined, refer to either of the following:

   - "3.1.1 Operation When Security Risks Have Been Detected [Trend Micro VB] [Symantec] [McAfee]"

   It is possible to reconnect the L-Server to operation network included in an email notification of quarantining completion. For the procedure when security risks have been removed, refer to either of the following:

   - "3.1.2 Operation When Security Risks Have Been Removed [Trend Micro VB] [Symantec] [McAfee]"

   - Restarting the L-Server after it has been quarantined

   The L-Server is restarted after it has been quarantined. For the procedure for confirming that an L-Server has been quarantined, refer to either of the following:

   - "3.1.1 Operation When Security Risks Have Been Detected [Trend Micro VB] [Symantec] [McAfee]"

   It is possible to reconnect the L-Server to operation network included in an email notification of quarantining completion. For the procedure when security risks have been removed, refer to either of the following:

   - "3.1.2 Operation When Security Risks Have Been Removed [Trend Micro VB] [Symantec] [McAfee]"

   - Restarting the L-Server

   Request restart of the L-Server. Once the L-Server has been restarted, confirm that the security risks have been removed.

3.1.4 Operation When Handling of Security Risks Has Failed

This section explains operation when an error occurs during the handling of security risks. Explanations are divided according to the event during which the error occurred.

3.1.4.1 Corrective Action When Automatic Action Taken When a Security Risk Is Detected Fails [Trend Micro VB] [Symantec] [McAfee]

Procedure

When restarting fails

- For Virtual PCs

    Use the virtualization management software to restart the virtual PCs.

- For SBC Servers

    Restart the SBC servers from the administration screen of the iRMC.

When quarantining fails

a. Switch the connected network

   - For Virtual PCs

       Use the virtualization management software to switch the network that the virtual NICs of virtual PCs are connected to over to the quarantine network.

   - For SBC Servers

       Operate (change the VLAN of) the switches adjacent to the physical servers to switch the network that the physical servers are connected to over to the quarantine network.

b. Switch over to the quarantine network

   Execute the rcxadm avmgr quarantine command on the corresponding L-Servers to perform switchover to the quarantine network.

- If "3.1.2 Operation When Security Risks Have Been Removed [Trend Micro VB] [Symantec] [McAfee]" is performed before the above operation, discrepancies may occur in network information between the following:

    - Management information of virtual PCs and Resource Orchestrator

    - Management information of SBC servers and Resource Orchestrator

- When switching SBC servers over to the quarantine network, the statuses of those servers on the GUI (ROR console) will become "unknown".

In configurations where there are multiple Resource Orchestrator managers, if a problem occurs in switchover to the quarantine network, use the following procedure to perform corrective action.

1. On the GUI (ROR console) of the first manager of Resource Orchestrator, check whether the following message has been output.

   ```
   FJSVrcx:ERROR:67198:command execution error.quarantine failed(detail=detail)
   ```

2. If it has been output, refer to the "detail" of the message, and check the information of the Resource Orchestrator manager where the problem occurred and the error message.

    - When "submgr:*Resource_Orchestrator_manager_IP_address_or_FQDN*" is included in *detail*

      A problem has occurred on the Resource Orchestrator manager corresponding to the IP address or the FQDN.

    - When "submgr:*Resource_Orchestrator_manager_IP_address_or_FQDN*" is not included in *detail*

      A problem has occurred on the first manager of Resource Orchestrator.

3. Connect to the Resource Orchestrator manager where the problem occurred and take corrective action based on the error message.

If an error occurs during the network switchover operation of this function, the behavior will differ depending on the status of the corresponding virtual PCs or SBC servers.

- For Virtual PCs

    - When the virtual NICs of the virtual PCs have been switched to the quarantine network

    To prevent the spread of infection, the virtual NICs of virtual PCs remain connected to the quarantine network. The network of the NICs of the virtual L-Servers is switched back to the operation network.

    - When the virtual NICs of the virtual PCs have not been switched to the quarantine network

    The network of the NICs of the virtual L-Servers is switched back to the operation network.

- For SBC Servers

- When the NICs of the SBC servers have been switched to the quarantine network

  To prevent the spread of infection, the NICs of the SBC servers remain connected to the quarantine network. The network of the NICs of the physical L-Servers is switched back to the operation network.

- When the NICs of the SBC servers have not been switched to the quarantine network

  The network of the NICs of the physical L-Servers is switched back to the operation network.

3.2 Modification of Configuration

This section explains the procedure for modifying a configuration.

3.2.1 Adding Virtual PCs

Procedure

1. Confirm that the preparations in "2.1 Preparations for Using the Automatic Quarantining Function" have been completed for the created virtual PCs.

2. Perform the following operations:

   "2.12 Linking Virtual L-Servers with Configured Virtual PCs"

3.2.2 Adding VM Hosts

Procedure

1. Create a system configuration file for performing batch registration of added VM hosts as managed servers in the Resource Orchestrator manager.

   For details, refer to "2.5.2 Definition File Setting Action Selection".

2. Add the physical servers on which the added VM hosts operate to server_control.rcxprop.

   For details, refer to "2.5.7.1 server_control.rcxprop".

3. Use the system configuration file created in step 1 to register the VM hosts as managed servers with the Resource Orchestrator manager.

   For details, refer to "2.9.1 Importing the System Configuration File".

4. Register the VM hosts in VM pools.

   For details, refer to "2.10.1 Registering VM hosts in VM pools".

5. Add the virtual PCs that were created on the VM hosts.

   For details, refer to "3.2.1 Adding Virtual PCs".

3.2.3 Adding SBC Servers

Procedure

1. Confirm that the preparations in "2.1 Preparations for Using the Automatic Quarantining Function" have been completed for the created SBC servers.

2. Install Resource Orchestrator agents on the SBC servers.

   For details, refer to "2.4 Installing the Resource Orchestrator Agent".

3. Create the system configuration file necessary for batch import of SBC servers.

   For details, refer to "2.5.2 Definition File Setting Action Selection".

4. Import the SBC servers using the system configuration file created in step 3.

For details, refer to "2.9.1 Importing the System Configuration File".

5. Register the SBC servers in server pools.

   For details, refer to "2.10.2 Registering Physical Servers in Server Pools".

6. When adding SBC servers, if network devices (adjacent switches) that are different models from existing ones are added, register rulesets (scripts) for the newly added L2 switches in folders of Resource Orchestrator.

   For details, refer to "2.5.9 Rulesets (scripts) for L2 switches".

7. Add information for the connections between the SBC servers and the adjacent network devices.

   For details, refer to "2.10.3 Registering Network Devices (Adjacent Switches)".

8. Link the SBC servers with physical L-Servers.

   For details, refer to "2.13 Linking Physical L-Servers with Configured SBC Servers".

3.2.4 Automatically Linking Added Virtual PCs with L-Servers

This section explains the procedure for automatically linking added virtual PCs with L-Servers.

📝 Note

. . . .

- When linking virtual PCs with each tenant, use the -setfolder option.

  Add the option after the "call RUN_SCRIPT -exportfile "%CSVPATH%" -fixfilename" command in the script for linking with L-Servers.

. . . .

3.2.4.1 Creating the Script for Linking with L-Servers

When automatically linking added virtual PCs with L-Servers, the administrator creates the following scripts and definition files.

Storage Destination Server for the Script for Linking with L-Servers

The Resource Orchestrator admin server

File Name of the Script for Linking with L-Servers

Any desired string of alphanumeric characters, with the extension "bat".

Character Code

Shift-JIS

Exit Status

0

The command executed successfully.

non-zero

An error has occurred.

Content of the Script for Linking with L-Servers

The content of the script for linking with L-Servers is as follows.

```
@echo off

setlocal enabledelayedexpansion

set AUTO_CONVERT_PATH=%~dp0
set RUN_SCRIPT="Installation_folder\SVROR\Manager\bin\convertVMtoLServer"
set CSVPATH=Absolute_path_of_the_folder_for_storing_the_CSV_configuration_file
set CSVFILE=convertVMtoLserver.csv
set CSVFULLPATH=%CSVPATH%\%CSVFILE%
set CSVTEMP=%CSVPATH%\temp.csv
```

```
set UNCONVERT_VMNAMES=%AUTO_CONVERT_PATH%\unconvert_vmname.txt
set RESULTCSVFILE=%CSVPATH%\convertVMtoLserver_result.csv

echo [%DATE:/=-% %TIME%] auto convert Start
call %RUN_SCRIPT% -exportfile "%CSVPATH%" -fixfilename

if not !errorlevel!==0 (
 echo make csv file failed.
 echo [%DATE:/=-% %TIME%] auto convert End
 exit /b 1
) else (
 if exist "%UNCONVERT_VMNAMES%" (
  for %%a in ("%UNCONVERT_VMNAMES%") do (
   if not "%%~za" equ "0" (
    for /f "tokens=1 delims=" %%i in ('findstr /v /g:"%UNCONVERT_VMNAMES%" "%CSVFULLPATH%"') do (
                                                          echo %%i>>"%CSVTEMP%")
    del "%CSVFULLPATH%"
    ren "%CSVTEMP%" "%CSVFILE%"
   )
  )
 )
 call %RUN_SCRIPT% -file "%CSVFULLPATH%"
 if not !errorlevel!==0 (
  echo display convertVMtoLserver.csv start
  for /f "tokens=*" %%a in (%RESULTCSVFILE%) do echo %%a
  echo display convertVMtoLserver.csv end
  echo convert lserver or make xml file failed.
  echo [%DATE:/=-% %TIME%] auto convert End
  exit /b 1
 )
)
echo convert lserver is successfully completed.
echo [%DATE:/=-% %TIME%] auto convert End
exit /b 0
```

📌 Note

. . . .

- If you linked virtual PCs by executing the convertVMtoLServer command with the -fixfilename option specified, the CSV results file will always be named "convertVMtoLserver_result.csv".

- If there is already a CSV results file with the same name in the output destination directory, that CSV file will be deleted and then re-created. If the convertVMtoLServer command is executed with the -file option specified and the exit status is something other than "0", the contents of the CSV results file will be output to standard output.

- Only alphanumeric characters, underscores ("_"), and hyphens ("-") can be used in the absolute path of the folder for storing the CSV configuration file.

. . . .

Content of the Definition File for Excluding Virtual PCs from the Targets of Batch Linking

The content of the definition file for excluding virtual PCs from the targets of batch linking is shown below.

By specifying resource pool names, VM host names, and virtual PC names, it is possible to exclude specific virtual PCs from being linked as a batch.

Format of the Definition File for Excluding Virtual PCs from the Targets of Batch Linking

Location of the Definition File

The same folder as the script for linking with L-Servers

Name of the Definition File

unconvert_vmname.txt

Character Code

Shift-JIS

Line Break Code

CR/LF

Format of the Definition File

Describe the file using the following format. Do not enter blank spaces or empty lines.

```
/Resource_pool_name/VM_host_name/
Name_of_virtual_PC_1_to_be_excluded_from_the_targets_of_batch_linking
/Resource_pool_name/VM_host_name/
Name_of_virtual_PC_2_to_be_excluded_from_the_targets_of_batch_linking
```

📝 Example
. . . .

/VMHostPool/vmesx3/win2008

/VMHostPool/vmesx2/win2003
. . . .

3.2.4.2 Executing the Script for Linking with L-Servers

It is possible to automatically link added virtual PCs with L-Servers by registering the script created in "3.2.4.1 Creating the Script for Linking with L-Servers" in the OS Task Scheduler so it is executed periodically.

The procedure for registering the script for linking with L-Servers in the OS Task Scheduler and configuring it to be executed periodically is as follows:

1. Copy the script file created in "3.2.4.1 Creating the Script for Linking with L-Servers" to the desired storage location.

   In addition, if there are virtual PCs which are excluded from the targets of batch linking, copy the definition file for excluding virtual PCs from the targets of batch linking to the same location.

2. Log in to the admin server as the OS administrator.

3. Start the Task Scheduler.

   The icons to click to start the Task Scheduler are as follows:

   - For Windows Server 2012 and Windows Server 2012 R2

     [Start]-[Administrative Tools]-[Task Scheduler]

   - For Windows Server 2016

     [Start]-[Windows Administrative Tools]-[Task Scheduler]

4. Set the following in the Task Scheduler:

   - Task name

   - Task start date and time

   - The script file copied in step 1 as the program to be executed.

📝 Example
. . . .

- Specifying so that execution results will be output to D:\tmp\auto_convert.log

```
Script_for_linking_with_L-Servers >> D:\tmp\auto_convert.log 2>&1
```

- Sample execution results

```
[2017-07-28 10:57:34.62] auto convert Start
VmGuest export Start
VmGuest export End
VmGuest Convert Start
VmGuest:/VMHostPool/vmesx2/win2003 convert failed
VmGuest Convert End
display convertVMtoLserver.csv start
VMGuestName,Label,Comment,FolderName,Result,Note
/VMHostPool/vmesx2/win2003,,,,NG,FJSVrcx:ERROR:67154:/VMHostPool/vmesx2/win2003:not found
display convertVMtoLserver.csv end
convert lserver or make xml file failed.
[2017-07-28 10:57:37.92] auto convert End
```

3.2.5 Procedure for Modifying or Adding Network Change Settings for Virtual L-Servers

When re-creation of the XML files for changing the network is necessary because the definition files for configuring the operation and quarantine networks were modified due to modification or addition to the network change settings for virtual L-Servers, perform the following procedure.

Procedure

1. Reflect the changes made to the network settings for virtual L-Servers on the definition file for configuring the operation and quarantine networks (avmgr_network.rcxprop).

2. Execute the following command to re-create the XML files for changing the network.

   ```
   > convertVMtoLServer -createxml
   ```

Confirmation of Results

Confirm that the XML files for changing the networks of virtual L-Servers have been updated.

Storage Location of the XML Files for Changing the Network

[Windows Manager]

Installation_folder\SVROR\Manager\etc\files\avmgr

Names of the XML Files for Changing the Network

quarantine_*L-Server_name*.xml

unquarantine_*L-Server_name*.xml

See
- For details on avmgr_network.rcxprop, refer to "2.5.6 Definition File for Configuring the Business and Quarantine Networks".
- For details on the convertVMtoLServer command, refer to "4.2 convertVMtoLServer".
- For details on XML files for changing the network, refer to "A.4 XML Files for Changing the Network".

3.2.6 Deleting L-Servers

Procedure

1. Execute the following command to delete an L-Server.

   ```
   > rcxadm lserver delete -name L-Server_name -allow deldisk [-nowait]
   ```

Note

. . . .

Deleting an L-Server also deletes the content of the disks connected to it.

If you do not want to delete the content of disks, execute the rcxadm lserver revert command to cancel the link between the target L-Server and all connected disks.

. . . .

2. The names of L-Servers are included in the names of the XML files for changing the network.

   Delete any XML files for changing the network which correspond to the L-Server deleted in step 1.

Confirmation of Results

Execute the following command and confirm that the target L-Server has been deleted.

```
> rcxadm lserver list
```


See

. . . .

- For details on the rcxadm lserver command, refer to "4.3 rcxadm lserver".

- For details on XML files for changing the network, refer to "A.4 XML Files for Changing the Network".

. . . .

3.2.7 Changing the IP Addresses of L-Servers

Procedure

Execute the following commands to change L-Server IP addresses.

For Virtual L-Servers

1. Modify the network settings of the OS installed on the L-Server, referring to the IP address and network information of the modified L-Server.

2. Execute the following command, and confirm the value for Refreship.

   If "true" is displayed, then the target virtual L-Server is configured so its IP address is changed automatically when the IP address of the virtual PC linked to it is changed. Therefore, it is not necessary to change the IP address of the L-Server in step 3.

   ```
   > rcxadm lserver show -name Virtual_L-Server_name
   ```

3. Execute the following commands to change L-Server IP addresses.

   ```
   > rcxadm lserver modify -name Virtual_L-Server_name -file XML_file_for_changing_the_network [-
   nowait]
   ```

For Physical L-Servers

1. Modify the network settings of the OS installed on the L-Server, referring to the IP address and network information of the modified L-Server.

2. Execute the following commands to change L-Server IP addresses.

   ```
   > rcxadm lserver modify -name Physical_L-Server_name -type physical -file
   XML_file_for_changing_the_network [-nowait]
   ```

Confirmation of Results

Execute the following command and confirm that L-Server IP addresses have been changed.

If the target L-Server is a virtual L-Server and the value "true" is displayed for Refreship (as checked in step 2), it may take a while for the change of the network settings of the OS to be reflected on the IP address of the L-Server.

```
> rcxadm lserver show -name L-Server_name -format xml
```

📇 **See**
. . . .

- For details on the rcxadm lserver command, refer to "4.3 rcxadm lserver".

- For details on XML files for changing the network, refer to the following:

    - For Virtual PCs

      "Format of XML Files for Changing the Network of Virtual L-Servers"

    - For SBC Servers

      "Format of XML Files for Changing the Network of Physical L-Servers"
. . . .

🔶 **Note**
. . . .

[Trend Micro OfficeScan]

Modifying the IP addresses of L-Servers may also require modification to the settings of OfficeScan 11.0 or OfficeScan XG.

For details, refer to the manuals of OfficeScan 11.0 or OfficeScan XG.

[Symantec]

Modifying the IP addresses of L-Servers may also require modification of the settings of Symantec Endpoint Protection.

For details, refer to the manuals of Symantec Endpoint Protection.

[McAfee]

Modifying the IP addresses of L-Servers may also require modification of the settings of McAfee ePolicy Orchestrator.

For details, refer to the manuals of McAfee ePolicy Orchestrator.
. . . .

3.2.8 Changing the IP Address of the Antivirus Software Server

This section explains the procedure for changing the IP address of the antivirus software server.

When coordinating either of the following antivirus software with the Automatic Quarantining Function, it is not necessary to change the IP address of the antivirus software server.

- Trend Micro Control Manager

- Symantec Endpoint Protection

Procedure

1. Change the IP address of the server on which the antivirus software server operates.

2. Confirm the IP address of the SNMP trap agent of the antivirus software server using the following method.

    [Trend Micro OfficeScan]

    Using the Web console of OfficeScan 11.0 Server or OfficeScan XG, from the top menu, select [Administration]-[Settings]-[Agent Connection]. The IP address of the antivirus software server can be confirmed on the screen.

    [McAfee]

    Using the McAfee ePolicy Orchestrator Web console, from the menu, select [Configuration]-[Server Settings]-[Server Information]. The IP address of the antivirus software server can be confirmed on the screen.

3. Use the rcxadm avmgr list command to confirm the antivirus software which has already been registered.

    Execute the following command.

```
> rcxadm avmgr list
```

4. Using the rcxadm avmgr modify command, change the IP address of the registered antivirus software.

   Execute the following command. Specify the IP address that you changed in step 1.

```
> rcxadm avmgr modify -name Name_of_the_antivirus_software -ip
IP_address_of_the_server_on_which_the_antivirus_software_server_operates
```

See
. . . .
For details on the rcxadm avmgr command, refer to "4.1 rcxadm avmgr".
. . . .

Note
. . . .
It is not possible to change the IP address or identifier of antivirus software so that they match those of any of the registered antivirus software confirmed in step 3.
. . . .

3.2.9 Changing the IP Addresses of Virtual PCs from Static Addresses to DHCP Addresses

This section explains the procedure for changing the IP addresses of virtual PCs from static addresses to DHCP addresses.

Prerequisites

The settings of virtual PCs must be modified beforehand.

Procedure

1. Cancel the link with the virtual L-Server.

   Execute the following command.

```
> rcxadm lserver revert -name Virtual_L-Server_name [-force] [-nowait]
```

2. Delete the XML files for changing the network.

3. Perform linking with virtual L-Servers and re-creation of files for changing the network.

   For details, refer to "2.12 Linking Virtual L-Servers with Configured Virtual PCs".

See
. . . .
- For details on the rcxadm lserver command, refer to "4.3 rcxadm lserver".

- For details on XML files for changing the network, refer to "Format of XML Files for Changing the Network of Virtual L-Servers".
. . . .

3.2.10 Adding Sub Managers

This section explains the procedure for registering information of sub managers, in configurations where there are multiple Resource Orchestrator managers.

For the configuration of the sub managers to add, refer to "Chapter 2 Implementing the Automatic Quarantining Function".

Procedure

・ Register sub manager information.

   Execute the following command on the first manager of Resource Orchestrator.

```
> rcxadm submgr create -host IP_address_or_FQDN_of_the_sub_manager -port
Port_number_used_for_the_rcxweb_service -user
User_name_of_the_user_with_administrator_privileges_for_the_OS_of_the_sub_manager -password
Password_of_the_user_with_administrator_privileges_for_the_OS_of_the_sub_manager -ror_user
User_name_of_the_privileged_user_of_the_sub_manager -ror_password
Password_of_the_privileged_user_of_the_sub_manager
```

Confirmation of Results

Execute the following command, and confirm that the information of the sub manager has been registered.

```
> rcxadm submgr list
```

See
....
For details on the rcxadm submgr command, refer to "4.7 rcxadm submgr".
....

3.2.11 Deleting Sub Managers

This section explains the procedure for deleting sub managers, in configurations where there are multiple Resource Orchestrator managers.

Procedure

· Delete sub manager information.

   Execute the following command on the first manager of Resource Orchestrator.

```
> rcxadm submgr delete -host IP_address_or_FQDN_of_the_sub_manager
```

Confirmation of Results

Execute the following command, and confirm that the information of the sub manager has been deleted.

```
> rcxadm submgr list
```

See
....
For details on the rcxadm submgr command, refer to "4.7 rcxadm submgr".
....

3.2.12 Modifying User Information of Sub Managers

This section explains the procedure for modifying user information of sub managers, in configurations where there are multiple Resource Orchestrator managers.

Procedure

· Modify sub manager information.

   Execute the following command on the first manager of Resource Orchestrator.

```
> rcxadm submgr modify -host IP_address_or_FQDN_of_the_sub_manager {-user
User_name_of_the_user_with_administrator_privileges_for_the_OS_of_the_sub_manager |-password
Password_of_the_user_with_administrator_privileges_for_the_OS_of_the_sub_manager |-user
User_name_of_the_user_with_administrator_privileges_for_the_OS_of_the_sub_manager |-password
Password_of_the_user_with_administrator_privileges_for_the_OS_of_the_sub_manager| -ror_user
User_name_of_the_privileged_user_of_the_sub_manager |-ror_password
Password_of_the_privileged_user_of_the_sub_manager |-ror_user
User_name_of_the_privileged_user_of_the_sub_manager |-ror_password
Password_of_the_privileged_user_of_the_sub_manager}
```

Confirmation of Results

Execute the following command, and confirm that the information of the sub manager has been registered.

```
> rcxadm submgr list
```

See

For details on the rcxadm submgr command, refer to "4.7 rcxadm submgr".

3.2.13 Changing the Quarantine Policy for Security Risks and Action Selection Settings

In order to change the setting for whether an L-Server on which a security risk has been detected is quarantined, it is necessary to update the definition file of the quarantine policy for security risks.

Once the definition file has been updated, the way this function operates will change immediately.

For this reason, create the updated definition file in advance and replace the current definition file at the desired timing for changing the way this function operates.

3.2.14 Enabling, Disabling, and Changing the Operation of Message Notification

The following changes regarding operation and system configuration can be made to the settings for message notifications.

Changes are reflected in operation once all of the procedures have been performed.

Enabling or disabling message notification

To turn off message notification, disable the function for message notification during quarantining. To turn message notification back on, re-enable the function.

Execute the following commands.

[To enable]

```
> msgnotice enable
```

[To disable]

```
> msgnotice disable
```

See

For details on these commands, refer to "4.9 msgnotice".

Message to be sent

When changing the content of the message, configure it in the definition file.

See

For details on the definition results file, refer to "2.5.4 Definition File for Enabling Notification".

VDI management server information

The following information of the VDI management server can be changed:

- IP address

- Administrator user ID

- Administrator user password

Use the following procedure to change the information of the VDI management server.

Procedure

1. When changing the information of the VDI management server such as IP addresses, etc., it is first necessary to change the authentication information. Perform steps 3, 4, and 5 in "2.6 Procedure for Enabling Notification of Switchover to the Quarantine Network".

2. Execute the following command on the Resource Orchestrator manager, specifying the information you want to change.

```
> msgnotice modify -name VDI_management_server_name [ -ip VDI_management_server_IP_address]
[ -user_name Administrator_user_ID_for_the_VDI_management_server][ -passwd
Administrator_password_for_the_VDI_management_server]
```

 See
. . . .
For details on this command, refer to "4.9 msgnotice".
. . . .

3.2.15 Enabling, Disabling, and Changing the Operation of Email Notification

The following changes regarding operation and system configuration can be made to the settings for email notifications.

Changes are reflected in operation once all of the procedures have been performed.

Email address for notification

- [Virtual Edition]

  Execute the following command to change the email address of the administrator of the tenant information.

  ```
  > rcxadm tenant modify -name name -mail mail_address
  ```

- [Cloud Edition]

  Refer to "11.4 Modifying a Tenant" in the "User's Guide for Infrastructure Administrators".

 See
. . . .
For details on this command, refer to "4.4 rcxadm tenant".
. . . .

Enabling or disabling email notification

To turn off email notification, disable the function for email notification during quarantining. To turn message notification back on, re-enable the function. Execute the following commands.

[To enable]

```
> mailnotice enable
```

[To disable]

```
> mailnotice disable
```

 See
. . . .
For details on these commands, refer to "4.10 mailnotice".
. . . .

SMTP server information

The following information of the SMTP server can be changed:

- IP address

- Port number

- Sender's email address

Use the following procedure to change the information of the SMTP server.

Procedure

Execute the following command using the Resource Orchestrator manager.

```
> mailnotice modify -name Name [ -ip SMTP_server_IP_address][ -port SMTP_server_port_number][ -from Sender_email_address]
```

See
••

For details on this command, refer to "4.10 mailnotice".
••

3.3 Tuning Methods

This section explains tuning methods.

3.3.1 [Trend Micro OfficeScan] Tuning the Security Risks to Be Quarantined

When security risks which do not require quarantining are causing L-Servers to be quarantined, modify the definition files of keywords for exclusion from the targets of quarantine or the definition files of keywords for the targets of quarantine, based on the content of the messages beginning with "Security event occurred" output to the system log of the admin server.

For details, refer to "A.2 Definition files of keywords for exclusion from the targets of quarantining" and "A.3 Definition files of keywords for the targets of quarantining".

Note
••

When coordinating with McAfee ePolicy Orchestrator or Symantec Endpoint Protection, it is not possible to fine-tune antivirus software settings using Resource Orchestrator.
••

Chapter 4 Reference

This chapter explains the commands for this function.

4.1 rcxadm avmgr

Name

Installation_folder\SVROR\Manager\bin\rcxadm avmgr - Antivirus software operations

Format

```
rcxadm avmgr create -name name -mgmt_soft_name ident -ip ipaddress [-nowait]
rcxadm avmgr list
rcxadm avmgr modify -name name -ip ipaddress [-nowait]
rcxadm avmgr delete -name name [-nowait]
rcxadm avmgr quarantine -lserver lserver [-nowait]
rcxadm avmgr unquarantine -lserver lserver [-nowait]
```

Description

rcxadm avmgr is the command used to perform operations of antivirus software.

Subcommands

create

Registers antivirus software to enable the receipt of SNMP traps by Resource Orchestrator.

When antivirus software is registered, Resource Orchestrator can analyze any SNMP traps it receives from that software, and automatically quarantine L-Servers as necessary.

list

Displays a list of registered antivirus software.

The following information is displayed.

Table 4.1 Antivirus Software Information

Item Name	Description
MGMT_SOFT	Antivirus software identifier
IPADDRESS	IP address of the SNMP trap agent
NAME	Antivirus software name

modify

Changes the IP addresses of registered antivirus software.

Changes are reflected immediately. Restarting of the Resource Orchestrator manager is not necessary.

delete

Unregisters registered antivirus software.

When antivirus software is deregistered, automatic quarantining is no longer performed.

quarantine

Connects the specified L-Server to the quarantine network, isolating it from the operation network.

It is necessary to create an XML file for changing the network which describes the quarantine network beforehand.

Information

....

After this subcommand is executed, the connected network is changed by the rcxadm lserver modify command.

....

unquarantine

Connects the specified L-Server to the operation network.

It is necessary to create an XML file for changing the network which describes the operation network beforehand.

Information

....

After this subcommand is executed, the connected network is changed by the rcxadm lserver modify command.

....

Options

-name *name*

In *name*, specify the resource name of the target antivirus software.

Specify a character string that is up to 15 characters long, starts with an alphabetic character, and is composed of alphanumeric characters and hyphens ("-").

-mgmt_soft_name *ident*

In *ident*, specify the identifier of the antivirus software. The following identifier can be specified.

[Trend Micro OfficeScan]

- For OfficeScan 11.0 server

  Specify "corp".

- For OfficeScan XG server

  Specify "corp".

[McAfee]

- For McAfee ePolicy Orchestrator server

  Specify "epo".

-ip *ipaddress*

In *ipaddress*, specify the IP address of the SNMP trap agent.

[Trend Micro OfficeScan]

- For OfficeScan 11.0 server

  Specify the IP address of the SNMP trap agent of the OfficeScan 11.0 server.

- For OfficeScan XG server

  Specify the IP address of the SNMP trap agent of the OfficeScan XG server.

[McAfee]

- For McAfee ePolicy Orchestrator server

  Specify the IP address of the SNMP trap agent of the McAfee ePolicy Orchestrator server.

-lserver *lserver*

In *lserver*, specify the name of the L-Server whose network will be changed.

-nowait

Use this option to return directly to the command prompt without waiting for the antivirus software operation specified in the subcommand to complete its execution.

Requirements

Permissions

OS Administrator

Location

Admin server

Usage Example

- To display the list of antivirus software information

```
> rcxadm avmgr list
NAME MGMT_SOFT IPADDRESS
---- --------- ---------
avmgr corp 192.168.1.10
```

Exit Status

This command returns the following values:

0

The command executed successfully.

non-zero

An error has occurred.

4.2 convertVMtoLServer

Name

Installation_folder\SVROR\Manager\bin\convertVMtoLServer - Linking virtual PCs with virtual L-Servers

Format

```
convertVMtoLServer -exportfile folder [-fixfilename] [-setfolder]
convertVMtoLServer -file file.csv
convertVMtoLServer -createxml
```

Description

convertVMtoLServer is the command used to perform batch linking of configured virtual PCs with virtual L-Servers and batch creation of XML files for changing the network.

Options

-exportfile *folder*

Use this option create the CSV configuration file to be specified for the -file option.

For *folder*, specify the folder for storing the CSV configuration file using an absolute path.

For the folder name, specify a character string containing alphanumeric characters, underscores ("_"), hyphens ("-") and periods (".").

Paths containing single-byte spaces cannot be specified.

In all of the following VM hosts registered in the VM pool, all of the information of the virtual PCs that are not linked with virtual L-Servers is output to the CSV configuration file.

- VMware

- Hyper-V

- XenServer

If -fixfilename is specified, the CSV configuration file will be named convertVMtoLserver.csv.

If the file already exists, it will be deleted and then re-created.

-fixfilename

Use this option when periodically linking virtual PCs with L-Servers.

The CSV configuration file that is output will be named convertVMtoLserver.csv. If the file already exists, it will be deleted and then re-created.

-setfolder

Specify this when linking virtual PCs with each tenant.

For the output CSV configuration file, either the resource folder or the tenant that the VM host of the virtual PC belongs to is output as the FolderName where the L-Server is located.

-file *file.csv*

Specify this option to perform batch linking of virtual PCs with virtual L-Servers and batch creation of XML files for changing the network.

For *file*.csv, specify the CSV configuration file containing the definitions of the information regarding the virtual PCs that are already configured in the following VM hosts registered in the VM pool of Resource Orchestrator.

- VMware

- Hyper-V

- XenServer

The CSV configuration file can be created automatically by executing the command with the -exportfile option specified.

If the information of virtual PCs that you want to exclude from the operation target is contained in the CSV configuration file to be output using the -exportfile option, delete the lines corresponding to those virtual PCs from the CSV configuration file.

Alphanumeric characters, underscores ("_"), and hyphens ("-") can be used in the file name of the CSV configuration file.

In addition, the extension of the CSV configuration file must be "csv".

For the virtual L-Servers that are successfully linked, the XML files for changing the network are output to the storage directory of the XML files for changing the network. If XML files for changing the network that have the same names as the XML files to be output already exist, the existing files will be overwritten.

 See
....

For details, refer to "A.4 XML Files for Changing the Network".
....

-createxml

Specify this option to create XML files for changing the network.

Specify in the following cases:

- When linking virtual PCs with virtual L-Servers was performed using the -file option but the XML files for changing the network were not created

- When re-creation of the XML files for changing the network is necessary because the definition files for configuring the operation and quarantine networks were modified due to modification of or addition to the network change settings for virtual L-Servers

It is necessary to create the definition files for configuring the operation and quarantine networks beforehand.

 See
....

For details, refer to "2.5.6 Definition File for Configuring the Business and Quarantine Networks".
....

CSV Configuration File

The format of the file is as follows.

If the CSV configuration file has been created using the -exportfile option, only the first line and the VMGuestName values in the subsequent lines are output.

CSV configuration files are named using the following format and stored in *folder*.

Name of the CSV Configuration File

- If -fixfilename is specified

  convertVMtoLserver.csv

- If -fixfilename is not specified

  convertVMtoLserver_*yyyymmddhhmmss*.csv

  yyyymmddhhmmss is the date and time when the CSV configuration file was created.

Format of the CSV Configuration File

- In the first line, specify the definition of the names of the configuration items. The first line cannot be omitted.

  VMGuestName,Label,Comment,FolderName

- In the second and later lines, specify the data.

  Specify configuration values in the order of the configuration item names defined in the first line, separated by commas.

VMGuestName

Specify the names of the virtual PCs to link to L-Servers. Specify using full paths. Use slashes ("/") to connect the names of the resource pool and the VM host of each virtual PC.

For each virtual PC name, enter a string beginning with an alphanumeric character, and containing up to 64 alphanumeric characters, underscores ("_") and hyphens ("-"). Both upper and lower case letters can be used.

Virtual PC names containing periods (".") are not supported.

Example

. . . .

/Resource_pool_name/VM_host_name/Virtual_PC_name

. . . .

Label

Optional.

Enter a string of up to 32 alphanumeric characters (Both double-byte and single-byte characters can be used).

Comment

Optional.

Enter a string of up to 256 alphanumeric characters (Both double-byte and single-byte characters can be used).

FolderName

Optional.

For the folder name, enter a string beginning with an alphanumeric character, and containing up to 32 alphanumeric characters, underscores ("_") and hyphens ("-"). Both upper and lower case letters can be used.

Specify this item when grouping the resources of a virtual L-Server. When specifying FolderName, it is necessary to create the corresponding resource folder under the orchestration tree on the ROR [Resource] tab in advance.

For details, refer to "21.2 Creating" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

For a hierarchized resource folder, specify the folder name using slashes ("/").

If omitted, the configuration file is placed in the home folder.

📝 Example
. . . .

Example of the CSV Configuration File

```
VMGuestName,Label,Comment,FolderName
/VMHostPool/192.168.24.138/test1
/VMHostPool/192.168.24.138/test2,,
/VMHostPool/192.168.24.138/test3,,,FolderA
```

. . . .

🅿 Point
. . . .

The relationships between virtual PC names and resources can be confirmed using the following command.

```
> rcxadm pool list -name /VMHostPool -resource -info lserver
```

For details on this command, refer to "4.8 rcxadm pool".
. . . .

CSV Results File

The format of the CSV results files is as follows.

Storage Location of CSV Results Files

The same location as the storage folder for CSV configuration files.

Name of the CSV Results File

convertVMtoLserver_*yyyymmddhhmmss*_result.csv

yyyymmddhhmmss is the date and time when the CSV configuration file was created.

If -fixfilename is specified, the CSV results file will be named convertVMtoLserver_result.csv.

Format of the CSV Results File

VMGuestName

The details configured in the CSV configuration file are displayed as is.

Label

The details configured in the CSV configuration file are displayed as is.

Comment

The details configured in the CSV configuration file are displayed as is.

FolderName

The details configured in the CSV configuration file are displayed as is.

Result

The post-execution status of the loading operation for each VM is displayed.

"OK" indicates that loading was successful, while "NG" indicates failure.

Note

Error messages generated after failed operations are displayed.

Example

Output Example of the CSV Results File

```
VMGuestName,Label,Comment,FolderName,Result,Note
/VMHostPool/192.168.24.138/test1,,,FolderA,NG,FJSVrcx:ERROR:67280:test1:convert not supported.
(already in use)
/VMHostPool/192.168.24.138/test2,,,FolderA,NG,FJSVrcx:ERROR:67280:test2:convert not supported.
(already in use)
/VMHostPool/192.168.24.138/ls-test,,,,NG,FJSVrcx:ERROR:69133:operation not possible because power is
OFF
/VMHostPool/192.168.24.138/test3,,,,OK,
/VMHostPool/192.168.24.138/test4,,,,OK,
/VMHostPool/192.168.24.138/test5,,,,OK,
/VMHostPool/192.168.24.138/test6,,,,OK,
/VMHostPool/192.168.24.138/test7,,,,OK,
/VMHostPool/192.168.24.138/test8,,,,OK,
/VMHostPool/192.168.24.138/test9,,,,OK,
/VMHostPool/192.168.24.138/test10,,,,OK,
```

Requirements

Privileges

OS administrator

Location

Admin server

Usage Example

```
> convertVMtoLServer -file D:\convert_test\vm_test1.csv
VmGuest Convert Start
VmGuest:test3 is converting
VmGuest:test4 is converting
VmGuest:test3 convert completed
VmGuest:test4 convert completed
VmGuest Convert End
```

Exit Status

This command returns the following values:

0

The command executed successfully.

non-zero

An error has occurred.

> 📝 **Note**
> ....
>
> - Specify the CSV configuration file name using an absolute path. If single-byte blank spaces are included in the specified path, the command cannot be executed.
>
> - Do not open the CSV results file during execution of the convertVMtoLServer command.
> ....

4.3 rcxadm lserver

Name

Installation_folder**SVROR\Manager\bin\rcxadm lserver** - L-Server operations

Format

```
rcxadm lserver delete -name name -allow deldisk [-nowait]
rcxadm lserver modify -name name [-type physical] -file file.xml [-nowait]
rcxadm lserver list rcxadm lserver show -name name [-format {text|xml}]
rcxadm lserver convert [-name name] -with with [-label label] [-comment comment] [-to folder] [-nowait]
[-refreship]
rcxadm lserver revert -name name [-force] [-nowait]
```

Description

rcxadm lserver is the command used to manage and operate L-Servers.

> 📝 **Note**
> ....
>
> As a result of performing virtual PC operations, processes that are executed after a virtual PC is migrated to another VM host may fail.
>
> For details, refer to "9.2.2 Functional Differences between Products" in the "Design Guide VE".
> ....

Subcommands

delete

Deletes an L-Server. The resources allocated to the L-Server are released automatically and the definitions for the L-Server are also deleted.

modify

Changes the network resources comprising the L-Server.

- Changes the connection destination and the IP address of the network connected to the NIC of the L-Server.

    Multiple NICs can be specified as the modification target in the XML file.

    - For an L-Server linked with a configured virtual PC or SBC server

        - When the NIC is connected to network resources

        This command modifies the IP address of the NIC and the destination network of the target OS.

> 📝 **Note**
> ....
>
> **For Both Virtual L-Servers and Physical L-Servers**
>
> - When the NIC IP address is changed, the IP address used by the target OS to connect to the L-Server is not reconfigured automatically.
>
>   After modifying the IP address, log in to the target OS and then manually set the IP address displayed in the detailed information of the L-Server.

After setting the IP address, confirm that the changed NIC can communicate with external devices correctly.

For Virtual L-Servers

- Modification of the IP address and the destination network is performed for the NIC corresponding to the MAC address specified in the XML file. Therefore, ensure a MAC Address is specified.

  When there are no NICs, or multiple NICs, that have the MAC address specified in the XML file, NIC modification is not performed.

- When the NIC is connected to network resources

  When there are no VM guest NICs, or multiple VM guest NICs, that have the MAC address specified in the XML file, NIC modification is not performed for the VM guests.

  Only modification of the IP address and the destination network in the NIC definition is performed.

For Physical L-Servers

- Modification of the IP address and the destination network is performed for the NIC corresponding to the NICIndex specified in the XML file.

- During changing of the destination network, the existing NIC definition is compared to the contents of the XML file, and the following processing is performed.

  - New network connections are added for any NICs that have been added in the XML file.

  - Existing network connections corresponding to any NICs that have been omitted from the XML file are deleted.

  Therefore, be sure to include descriptions of all existing NICs in the XML file, even if no changes have been made to them.

P Point

Modification of a network using VM management software may cause differences in the network information of L-Servers and VM guests. In this case, perform one of the following procedures to make the network information consistent between L-Servers and VM guests.

- When adapting to VM management software

  Modify the destination network of the L-Server so it is aligned with the VM guest.

- When adapting to L-Servers

  Using the VM management software, modify the network of the target VM guest so it is aligned with the L-Server.

list

Displays a list of L-Server information.

The following information is displayed.

- For Physical L-Servers

  Table 4.2 Physical L-Server Information

Item Name	Description
NAME	L-Server name
TYPE	Server Type
SPEC (*)	CPU performance, CPU count, memory capacity
DISKS	Disk size
IPADDRESSES	IP address
STATUS	Operational status of the L-Server
RESOURCES	Resource allocation status

  * Note: Not displayed when using rack mount servers on which agents have not been registered

- For Virtual L-Servers

Table 4.3 Virtual L-Server Information

Item Name	Description
NAME	L-Server name
TYPE	Server Type
SPEC	CPU performance, CPU count, memory capacity
DISKS	Disk size When there are multiple disks, the disk sizes are displayed separated by commas. When disk size cannot be acquired, a hyphen ("-") is displayed.
IPADDRESSES	IP address When there are multiple IP addresses, they are displayed separated by commas.
STATUS	Operational status of the L-Server
RESOURCES	Resource allocation status

show

Displays the detailed information of the L-Server.

The following information is displayed.

![Note icon] **Note**

. . . .

The number and display order of the items may be changed by enhancement of Resource Orchestrator.

. . . .

- For Physical L-Servers

Table 4.4 Detailed Information of Physical L-Servers (Excerpt)

Item Name	Description
Name	L-Server name
Label	Label
Comment	Comment
PhysicalServer	Physical server name Displayed when the L-Server is in the following state. - Resources are already allocated (allocated)
OriginalServer	The physical server or resource pool to allocate to L-Servers
ServerPool	The name of the pool in which the physical servers allocated to L-Servers are registered Displayed when the L-Server is in the following state. - Resources are already allocated (allocated)
Status	Operational status of the L-Server
PowerStatus	Power status of the L-Server
Resources	Resource allocation status
ControlledResources	The scope of the controlled resources This is displayed for L-Servers linked to configured physical servers.
NumOfNIC	The number of NICs
NIC[*num*]	The name of the network resource to be allocated to the L-Server

Item Name	Description
	In *num*, the index number of the network element is displayed. The number is equal to or larger than 0.
NIC[*num*][MACAddress]	MAC address of NIC
NIC[*num*][PhysicalNum]	The number of the physical NIC corresponding to the NIC of an L-Server The number is equal to or larger than 0.
NIC[*num*][IPAddress]	IP address to allocate to the L-Server In *num*, the index number of the network element is displayed. The number is equal to or larger than 0.
NIC[*num*][*netlinknum*][IpAddress]	IP address
NIC[*num*][*netlinknum*][VlanMode]	VLAN mode
NIC[*num*][*netlinknum*][DNSServer]	DNS server address
NIC[*num*][*netlinknum*][DefaultGateway]	Default gateway address
NICGroup[*num*][*netlinknum*][IpAddress]	IP address
NICGroup[*num*][*netlinknum*][VlanMode]	VLAN mode
NICGroup[*num*][*netlinknum*][DNSServer]	DNS server address
NICGroup[*num*][*netlinknum*][DefaultGateway]	Default gateway address
NICGroup[*num*][*netlinknum*][NicLinks]	NIC number to be bound

* Note: Not displayed when using rack mount servers on which agents have not been registered.

- For Virtual L-Servers

Table 4.5 Detailed Information of Virtual L-Servers (Excerpt)

Item Name	Description
Name	L-Server name
Label	Label
Comment	Comment
VmHost	VM host name Displayed when the L-Server is in the following state. - Resources are already allocated (allocated)
VmGuest	VM name corresponding to the L-Server Displayed when the L-Server is in the following state. - Resources are already allocated (allocated)
OriginalServer	The VM host or the resource pool in which virtual PCs to be allocated to the L-Server are to be created
VMHostPool	The name of the pool in which the VM host with the virtual PCs allocated to the L-Server is registered Displayed when the L-Server is in the following state. - Resources are already allocated (allocated)
Status	Operational status of the L-Server
PowerStatus	Power status of the L-Server
Resources	Resource allocation status
ControlledResources	The scope of the controlled resources

Item Name	Description
	The combination of Server, Storage, and Network is displayed. This is displayed for the L-Servers linked with configured virtual PCs.
NumOfNIC	The number of NICs
NIC[*num*]	The name of the network resource to be allocated to the L-Server. In *num*, the index number of the network element is displayed. The number is equal to or larger than 0.
NIC[*num*][IPAddress]	IP address to allocate to the L-Server. In *num*, the index number of the network element is displayed. The number is equal to or larger than 0.
NIC[*num*][MACAddress]	MAC address to allocate to the L-Server. In *num*, the index number of the network element is displayed. The number is equal to or larger than 0.

RefreshIP	- When the IP addresses of virtual PCs are changed, the IP addresses of the virtual L-Servers linked to those virtual PCs are also changed accordingly, and "true" is displayed.
	
	  - true
	
	When the IP addresses of virtual PCs are changed, the IP addresses of the virtual L-Servers linked to those virtual PCs are also changed accordingly.
	
	- Displayed when there are virtual PCs operating on any of the following VM hosts.
	
	  - VMware
	  - Hyper-V
	  - XenServer

convert

Creates a link between an L-Server and a configured virtual PC or SBC server.

revert

Cancels the link between an L-Server and a configured virtual PC or SBC server.

Options

-file *file*.xml

In *file*.xml, specify the XML file with the definitions of the resources that comprise the L-Server.

When changing the basic information or specifications of an L-Server, multiple NICs can be specified as the modification target in the XML file.

For details on the XML file definition, refer to "Table A.2 Excerpt from Definition Information for Physical L-Servers (XML)" and "Table A.1 Excerpt from Definition Information for Virtual L-Servers (XML)".

-format text|xml

Specify the display format. "text" or "xml" can be specified.

When -format is omitted, it is displayed in text format.

-type physical

For this option, only "physical" can be specified. Specify when using the modify subcommand to target a physical L-Server with the operation.

-nowait

Use this option to return directly to the command prompt without waiting for the operation of the L-Server specified in the subcommand to complete its execution.

-name *name*

In *name*, specify the name of the target L-Server to perform an operation with.

For an L-Server allocated in a tenant or a resource folder, specify the tenant name or resource folder name using slashes ("/").

When specifying the convert subcommand, specify the name for the L-Server. For details on the characters that can be used for L-Server names, refer to the following section in the "Reference Guide (Command/XML) CE".

- "List of Items Specified in XML Definitions for Physical L-Servers" in "15.3.1 Definition Information for Physical L-Servers (XML)"

- "List of Items Specified in XML Definitions for Virtual L-Servers" in "15.3.2 Definition Information for Virtual L-Servers (XML)"

When the convert subcommand is specified without the -name option, the L-Server name is set as follows:

- When linking configured virtual PCs with virtual L-Servers

  - If the VM name of the configured virtual PC is a usable value for the L-Server name

    The VM name is set as the L-Server name.

  - If a value other than a usable value is used for the L-Server name

    The command exits with an error.

- When linking configured SBC servers with physical L-Servers

  - If the name of the physical server of the configured SBC server is a usable value for the L-Server name

    The physical server name will be set as the L-Server name.

  - If a value other than a usable value is used for the L-Server name

    - The command exits with an error.

-force

Specify this option when using the revert subcommand to forcibly cancel the link between a virtual L-Server and a virtual PC created using Resource Orchestrator.

-to *folder*

In *folder*, specify a resource folder to place L-Servers in. For the hierarchized resource folder, specify the resource folder name using slashes ("/"). If omitted, L-Servers are placed in the home folder.

When executed by a user who has multiple access scopes specified, it cannot be omitted. Specify a resource folder.

-allow deldisk

This option can only be specified for deldisk.

-label *label*

In *label*, specify the label for the L-Server.

-comment *comment*

In *comment*, specify any comments for the L-Server.

-with *with*

In *with*, specify the virtual PCs and SBC servers to link with the target L-Server.

Use slashes ("/") to connect the names of the resource folder and the resource pool.

```
/Resource_folder_name/Resource_pool_name/VM_host_name/Virtual_PC_name
/Resource_pool_name/VM_host_name/Virtual_PC_name
/Resource_folder_name/Resource_pool_name/SBC_server_name
/Resource_pool_name/SBC_server_name
```

-refreship

Automatically updates the IP addresses of the virtual L-Servers linked with virtual PCs when the IP addresses of those virtual PCs are changed by DHCP.

This option can only be specified for virtual PCs that operate on any of the following VM hosts. If it is specified for virtual PCs other than those that operate on VMware, an error occurs.

- VMware

- Hyper-V

- XenServer

Note

Even if this option is specified in either of the following cases, it will not be possible to automatically update the IP addresses of the corresponding L-Servers when the IP addresses of virtual PCs are changed by DHCP.

a. The modified IP addresses of the virtual PCs are not included in the IP address ranges of any network resources.

b. The modified IP addresses of the virtual PCs are already being used by other L-Servers.

In order to automatically update the IP addresses of L-Servers that are created by linking, execute the rcxadm lserver revert command to cancel the link between the virtual L-Servers and the virtual PCs and then create the link again, specifying this option.

Requirements

Permissions

OS Administrator

Location

Admin server

Usage Example

- When displaying a list of L-Server information

```
> rcxadm lserver list
NAME          TYPE       SPEC            DISKS          IPADDRESSES            STATUS    RESOURCES
----          ----       --------------  --------------  -----------            ------    ---------
L-Server1     Virtual    1.0GHz,1,2.0GB  30.0GB,100.0GB  10.20.30.40,10.20.40.50  normal
allocated
L-Server2     Virtual    1.0GHz,1,2.0GB  30.0GB,100.0GB  10.20.30.41             stop     preserved
L-Server3     Virtual    1.0GHz,1,2.0GB  30.0GB,100.0GB  -                       stop     defined
L-Server11    Physical   2.3GHz,2,72.0GB 30.0GB          10.30.40.2              normal   allocated
L-Server12    Physical   2.3GHz,2,72.0GB 30.0GB          10.30.40.3              stop     preserved
L-Server13    Physical   2.3GHz,2,72.0GB 30.0GB              -                       stop
defined
```

- When displaying a list of virtual L-Server information

```
> rcxadm lserver show -name /TenantA/test4
Name: test4
ServerType: Virtual
VMType: VMware
OSType: Microsoft Windows Server 2012
CPUArch: IA
CPUPerf: 1GHz
CPUReserve: 0.7GHz
CPUShare: 1000
NumOfCPU: 1
MemorySize: 1GB
```

```
MemoryReserve: 0.7GB
MemoryShare: 1000
VmHost: vmhost
VmGuest: test4-62
Status: stop
PowerStatus: off
Resources: allocated
NumOfDisk: 1
Disk[0]: test4-0-disk0
DiskSize[0]: 4GB
NumOfNIC: 1
NIC[0]: vnet1
NIC[0][IPAddress]: 192.168.1.2
NIC[0][MACAddress]: 00:50:56:91:09:21
Redundancy: None
Positioning: Fixed
Priority: 128
ReserveResources: true
OverCommit: true
Refreship: true
```

- When modifying the specifications of virtual L-Servers

```
> rcxadm lserver modify -name web-lserver1 -file web-lserver1.xml
```

Exit Status

This command returns the following values:

0

The command executed successfully.

non-zero

An error has occurred.

4.4 rcxadm tenant

Name

Installation_folder\SVROR\Manager\bin\rcxadm tenant - Tenant operations

Format

```
rcxadm tenant list [-name name]
rcxadm tenant show -name name
rcxadm tenant create -file file.xml [-nowait]
rcxadm tenant modify -name name {[-new_name name] [-label label] [-mail mail_address] [-comment
comment] [-global pool[,pool[,...]]]} [-nowait]
rcxadm tenant delete -name name [-nowait]
rcxadm tenant move -name name [-to folder] [-nowait]
```

Description

rcxadm tenant is the command used to perform tenant management and operations.

When using Cloud Edition, refer to "3.14 rcxadm tenant" in the "Reference Guide (Command/XML) CE".

Subcommands

list

Displays a list of tenants.

The following information is displayed.

- When not specifying -name for the option

Tenant Information (when omitting the -name option)

Item Name	Description
NAME	Tenant name
LABEL	Label for the tenant

- When specifying -name for the option

Tenant Information (when specifying the -name option)

Item Name	Description
TYPE	Type of resource folder, resource pool, or each resource
NAME	Name of the resource folder, resource pool, or each resource
LABEL	Label of the resource folder, resource pool, or each resource

show

Displays the detailed information for a tenant.

The following information is displayed.

Detailed Information for Tenants

Item Name	Description
NAME	Tenant name
LABEL	Label for the tenant
COMMENT	Comment for the tenant
GLOBAL POOL	Name of the global pool

create

Creates a tenant.

modify

Modifies one of the following. Specify at least one of the following items:

- Tenant Name

- Label

- E-mail address

- Comment Information

- Definition of the Global Pool

delete

Deletes a tenant.

When an L-Server is created in a tenant, deleting the tenant will also delete the L-Server.

For details on deleting L-Servers, refer to "3.6 rcxadm lserver" in the "Reference Guide (Command/XML) CE".

User groups and users are also deleted if the roles assigned to them are only targeting the tenant for deletion. When user information is managed using a directory service, the user information will be deleted from the management information of Resource Orchestrator. The user information in the directory service is not deleted.

move

Moves a tenant to the specified resource folder. If the destination resource folder is not specified, the folder is moved to the home folder.

It cannot be moved into a tenant.

Options

-file *file.xml*

In *file.xml*, specify the XML file that defines the information related to a tenant.

The XML definition for tenants is shown below.

```
<?xml version="1.0" encoding="utf-8"?>
<Tenant name ="Tenant name" label="Label">
<Comment>Comment</Comment>
<MailAddress>User's mail address</MailAddress>
<UserGroup name="User group name" label="Label">
<Comment>Comment</Comment>
<Role name="Role name">
<Scopes>
<Scope>Tenant name</Scope>
</Scopes>
</Role>
</UserGroup>
<User name="User ID" label = "Label" >
<Password>Password</Password>
<Comment>Comment</Comment>
<UserGroup>User Group Name</UserGroup>
</User>
<Pools>
<Pool name="Resource pool name" type="Resource pool type" label="Label">
<Comment>Comment</Comment>
<Priority>Priority</Priority>
</Pool>
</Pools>
<GlobalPoolLinks>
<GlobalPoolLink>Global pool name</GlobalPoolLink>
...
</GlobalPoolLinks>
</Tenant>
```

List of Items Specified in XML Definitions for Tenant

Element Name	Description	Remarks (Possible Values, Examples)
Tenant name (Tenant name)	Tenant Name	Specify a character string beginning with an alphanumeric character and containing up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-"). When creating it in a resource folder, specify the resource folder name using slashes ("/"). Creation in a tenant is not possible.
Label	Label for the tenant	Specify a string of up to 32 characters.

Element Name	Description	Remarks (Possible Values, Examples)
(Tenant label)	(optional)	
Comment (Comment)	Comment for the tenant (optional)	Specify a character string of up to 256 alphanumeric characters or symbols.
E-mail address (MailAddress)	Email address of the tenant administrator	Specify a character string of up to 64 alphanumeric characters or symbols.
User group name (UserGroup name)	Name of the user group to create in the tenant	Specify a user group name to create. If UserGroup is omitted, "supervisor" is set. For details on the elements inside the UserGroup tag, refer to "15.11 User Groups" in the "Reference Guide (Command/XML) CE". Create a user group when using directory service authentication.

User ID
(User name)
	Name of the user to create in the tenant	Specify the user ID to create.
		If the User element is omitted, no user is created.
		The following elements can be specified for User elements.
		  - *Label* (User label)
		  - *Password* (Password)
		  - *Comment* (Comment)
		  - *User Group Name* (UserGroup name)
		Role names (Role name) and access scopes (Scope) cannot be specified.
		For details on reach of the elements, refer to "15.10 User" in the "Reference Guide (Command/XML) CE".
		When using directory service authentication, register the users registered in the directory service with the manager.
		A user and a manager are not converted, when no users are registered in the directory service.

Resource pool name (Pool name)	Name of the resource pool to create in the tenant	Specify the name of the resource pool to create in the tenant. If the Pools element is omitted, no resource pool is created in the tenant.

Resource Pool Type
(Pool type)
	The type of the resource pool	Specify the type of the resource pool to create in the tenant.
		The following types can be specified:
		  - vm (VM pool)
		  - server (Server pool)
		  - storage (Storage pool)
		  - network (Network pool)
		  - address (Address pool)
		  - image (Image pool)

Label (Pool label)	Label for the resource pool (optional)	Specify a string of up to 32 characters.
Comment (Comment)	Comment for the resource pool (optional)	Specify a character string of up to 256 alphanumeric characters or symbols.
Priority	Resource pool priority	Specify the priority for the resource pool as between 1 and 10.

Element Name	Description	Remarks (Possible Values, Examples)
(Priority)	(optional)	If omitted, "5" is set. For the priority order, "1" is the highest and "10" is the lowest.
Name of the global pool (GlobalPoolLink)	Name of the global pool	Specify the resource pool name to be defined in a global pool of a tenant. If the GlobalPoolLinks element is omitted, no global pool is defined for the tenant. If specifying a resource pool in a resource folder, specify the resource folder name using slashes ("/").

Note

. . . .

The email addresses specified in the create and modify subcommands cannot be referred to using the show command. Therefore, retain the XML file or the option setting information used when executing the command.

. . . .

Example

. . . .

```xml
<?xml version="1.0" encoding="utf-8"?>
<Tenant name ="TenantFolder" label="TenantFolder Label">
  <Comment>TenantFolder Comment</Comment>
  <MailAddress>TenantAdministratorUser MailAddress</MailAddress>
  <UserGroup name="TenantUserGroup" label="TenantUserGroup Label">
    <Comment>TenantUserGroup Comment</Comment>
    <Role name="administrator">
        <Scopes>
          <Scope>TenantFolder</Scope>
        </Scopes>
    </Role>
  </UserGroup>
  <User name="TenantAdminUser" label="TenantAdministratorUser Label">
    <Password>tenant123</Password>
    <Comment>TenantAdministratorUser Comment</Comment>
    <UserGroup>TenantUserGroup</UserGroup>
  </User>
  <Pools>
    <Pool name="VMHostPool" type="vm" label="VMHostPool Label">
      <Comment>VMHostPool Comment</Comment>
      <Priority>5</Priority>
    </Pool>
    <Pool name="ServerPool" type="server" label="ServerPool Label">
      <Comment>ServerPool Comment</Comment>
      <Priority>5</Priority>
    </Pool>
    <Pool name="StoragePool" type="storage" label="StoragePool Label">
      <Comment>StoragePool Comment</Comment>
      <Priority>5</Priority>
    </Pool>
    <Pool name="NetworkPool" type="network" label="NetworkPool Label">
      <Comment>NetworkPool Comment</Comment>
      <Priority>5</Priority>
    </Pool>
    <Pool name="AddressPool" type="address" label="AddressPool label">
      <Comment>AddressPool Comment</Comment>
      <Priority>5</Priority>
    </Pool>
    <Pool name="ImagePool" type="image" label="ImagePool label">
      <Comment>ImagePool Comment</Comment>
      <Priority>5</Priority>
```

```
      </Pool>
    </Pools>
    <GlobalPoolLinks>
      <GlobalPoolLink>/VMHostPool</GlobalPoolLink>
      <GlobalPoolLink>/ServerPool</GlobalPoolLink>
          ...
    </GlobalPoolLinks>
</Tenant>
```

-nowait

Use this option to return directly to the command prompt without waiting for the operation specified in the subcommand to complete its execution.

-name *name*

In *name*, specify the name of the target tenant to perform an operation with. If a tenant created in a resource folder is specified, specify the resource folder name using slashes ("/").

-global *pool*

In *pool*, specify the resource pool name to be defined in a global pool of a tenant. If specifying a resource pool in a resource folder, specify the resource folder name using slashes ("/"). When specifying multiple resource pools, separate them using commas.

-new_name *new_name*

In *new_name*, specify the changed tenant name.

-mail *mail_address*

In *mail_address*, specify the email address of the tenant administrator.

-label *label*

In *label*, specify the new label.

-comment *comment*

In *comment*, specify the comment for a tenant.

-to *folder*

In folder, specify the destination resource *folder*. For the hierarchized resource folder, specify the resource folder name using slashes ("/"). It cannot be moved to a tenant or a resource folder in a tenant.

When omitted, the server is moved to the home folder.

When executed by a user who has multiple access scopes specified, it cannot be omitted. Specify a resource folder.

Requirements

Permissions

OS Administrator

Location

Admin server

Usage Example

- When displaying a list of tenant information

```
>rcxadm tenant list
NAME LABEL
---- -----
/Tenant01 -
/Tenant02 -
>rcxadm tenant list -name Tenant01
TYPE NAME LABEL
---- ---- -----
```

```
Pool AddressPool02 -
Pool ImagePool02 -
Pool NetworkPool02 -
Pool ServerPool02 -
Pool StoragePool02 -
Pool VMHostPool02 -
LServer lserver02 l_server 2
```

- When displaying details of tenant information

```
>rcxadm tenant show -name TenantA
name : tenantA
label : tenant A
comment : comment_A
global pool : /VMHostPool
global pool : /NetworkPool
global pool : /AddressPool
```

Exit Status

This command returns the following values:

0

The command executed successfully.

non-zero

An error has occurred.

4.5 rcxadm netconfig

Name

Installation_folder\SVROR\Manager\bin\rcxadm netconfig - network device batch operations

Format

```
rcxadm netconfig export -file file.xml
rcxadm netconfig import -file file.xml [-dryrun|-nowait]
```

Description

rcxadm netconfig is the command used to manage network devices in one operation.

Subcommands

export

Exports the network configuration information of all network devices registered in XML format.

import

Imports all network configuration information defined in the XML file.

For network device resources, they are created or modified according to the registration mode under the Netdevices element (the Mode element) defined in the network configuration information.

For link information, they are created or modified according to the registration mode under the Links element (the Mode element) defined in the network configuration information.

Information

- If importing is performed for network devices (with the status (unregistered)) detected by LAN switch searching, the import process is terminated and registration fails.

For registration of network devices with the status unregistered, after deleting those network devices, either import the network configuration information file again or create new network devices.

For creation and deletion of network devices, use the rcxadm netdevice command.

For details on the rcxadm netdevice command, refer to "4.6 rcxadm netdevice".

- For a network device with the status "registered", when importing the XML definitions specifying "add" for the registration mode (the Mode element under the Netdevices element), the target network device is not modified. The importing process will be continued for other network devices defined in the XML definitions.

When performing import operations by specifying the XML definitions to use "modify" for the registration mode (the Mode element under the Netdevices element), update operations are performed for the network devices registered using the same IP address as the admin IP address (Netdevice ip).

- For already registered link information, when importing the XML definitions specifying "add" for the registration mode (the Mode element under the Links element), already registered link information is not modified. The importing process will be continued for other link information defined in the XML definitions. To determine whether the link information has been registered, check the combination of "Admin IP Address of Device (Device ip)" and "Connection Port (Port)".

When importing the information specifying the XML definition using "modify" for the registration mode (the Mode element under the Links element), delete all registered link information, and then register the link information specified in the XML definitions.

Options

-dryrun|-nowait

-dryrun

Use this option to verify the XML file format that defines the network configuration information, without registering resources.

-nowait

Use this option to return the command without waiting for completion of the operation for the network configuration information specified in the subcommands.

-file *file*.xml

- For the Import Subcommand

In *file*.xml, specify the XML file that defines all network resources for creation.

- For the Export Subcommand

In *file*.xml, specify the destination file name for the XML file to be exported.

For details on the XML file definition, refer to "A.6 Network Configuration Information XML File".

Information

If an existing XML file name is specified for the -file option of the export subcommand, message number 65927 will be output and the export operation will fail.

Requirements

Privileges

OS administrator

Location

Admin server

Exit Status

This command returns the following values:

0

The command executed successfully.

non-zero

An error has occurred.

4.6 rcxadm netdevice

Name

Installation_folder\SVROR\Manager\bin\rcxadm netdevice - network device operations

Format

```
rcxadm netdevice create -file file.xml [-nowait]
rcxadm netdevice delete -name name [-nowait]
rcxadm netdevice list
rcxadm netdevice modify -name name -file file.xml [-nowait]
rcxadm netdevice set -name name -attr {mode={active [-with_va]|maintenance}|auto_conf={true|false}} [-
nowait]
rcxadm netdevice show -name name
rcxadm netdevice refresh -name  name [-recreate] [-nowait]
rcxadm netdevice cfbackup -name name [-type type] [-comment comment] [-redundancy] [-nowait]
rcxadm netdevice cfmodify -name name [-type config] -number number -comment comment [-nowait]
rcxadm netdevice cfmodify -name name -type environment -comment comment [-nowait] rcxadm netdevice
cfrestore -name name [-type type] [-nowait]
rcxadm netdevice cflist -name name
rcxadm netdevice cfexport -name name [-type config] -number number [-dir dir]
rcxadm netdevice cfexport -name name -type environment [-dir dir]
rcxadm netdevice cfclearerr -name name
```

Description

rcxadm netdevice is the command used to operate network devices.

Subcommands

create

Creates a network device.

ℹ️ Information
· ·

If two or more pieces of network device information are defined in the network configuration information definition file, the resource creation process is terminated and device registration fails.

When registering two or more network devices for resources in one operation, use the rcxadm netconfig command.
· ·

delete

Deletes a network device.

list

Displays a list of network devices.

The following information is displayed.

Table 4.6 Network Device Information

Item Name	Description
NAME	Network device name

Item Name	Description
IPADDRESS	Admin IP address for the network device
NETDEVICE_TYPES	Network device type When there is more than one, they are displayed separated by commas.

STATUS	Network device operation status
	
	One of the following is displayed:
	
	  - For normal status
	
	    "normal" is displayed.
	
	  - For error status
	
	    "error" is displayed.
	
	  - For warning status
	
	    "Warning" is displayed.
	
	  - For unknown status
	
	    "unknown" is displayed.

MAINTENANCE	Maintenance mode setting status for the network device
	
	Either of the following is displayed:
	
	  - When maintenance mode is set
	
	    "ON" is displayed.
	
	  - When maintenance mode is not set
	
	    "OFF" is displayed.

modify

Modifies a network device.

set

For a network device, switch the maintenance mode setting or the auto-configuration target.

show

Displays the detailed information for a network device.

The following information is displayed:

Table 4.7 Detailed Information for Network Devices (Excerpt)

Item Name	Description
Name	Network device name
SystemName	System name
IPAddress	Admin IP address
ProductName	Device name (product name)
ModelName	Model Name
VendorName	Vendor Name
Firmware	Firmware version
Location	The location of the device is displayed.
Status	Network device operation status One of the following is displayed: - For normal status

Item Name	Description
	"normal" is displayed.
	- For error status
	"error" is displayed.
	- For warning status
	"Warning" is displayed.
	- For unknown status
	"unknown" is displayed.
StatusCause	If the operational status of the network device is one other than "normal"
	One of the following is displayed:
	- When there is no response for ping
	"Ping unreachable" is displayed.
	- When there is no response for SNMP
	"SNMP unreachable" is displayed.
	- When there is no response for NETCONF
	"NETCONF unreachable" is displayed.
	- When automatic configuration failed
	"auto configuration failed" is displayed.
	If the operational status is normal, "-" is displayed.
NetdeviceTypes	Network device type
	When there is more than one, they are displayed separated by commas.
	When the type is omitted, only the item name is displayed and the type is not displayed.
Maintenance	Maintenance mode setting status for the network device
	Either of the following is displayed:
	- When maintenance mode is set
	"ON" is displayed.
	- When maintenance mode is not set
	"OFF" is displayed.
FabricId	Fabric ID
	This is only displayed when the network device type is "Fabric" and the fabric type is "C-Fabric".
Redundancy	Group ID
Redundancy[GroupDevice]	Group device name
	When there is more than one, they are displayed separated by commas.
Port[*num*]	Port name
	In *num*, the index number of a port element is displayed. The number is an integer starting from "0".
Port[*num*][Link]	Port link status
	One of the following is displayed:
	- For link-up status

Item Name	Description
	"up" is displayed.
	- For link-down status "down" is displayed.
	- For unknown status "unknown" is displayed.
	In *num*, the index number of a port element is displayed. The number is an integer starting from "0".
Port[*num*][PhysicalState]	Port communication status
	This is displayed in the format of line speed/communication mode. The unit of line speed is in Mbps.
	For the communication mode, one of the following is displayed:
	- For full duplex line "F" is displayed.
	- For half duplex lines "H" is displayed.
	- For unknown status A hyphen ("-") is displayed.
	In *num*, the index number of a port element is displayed. The number is an integer starting from "0".
Vlan[*num*]	VLAN ID
	In *num*, the index number of a VLAN element is displayed. The number is an integer starting from "0".
Vlan[*num*][UntaggedPort]	Name of the port belonging to an Untagged port of VLAN ID
	In *num*, the index number of a VLAN element is displayed. The number is an integer starting from "0".
	When there is more than one, they are displayed separated by commas.
	Some VLANs which have been configured with an AMPP function for VCS fabrics may not be displayed.
Vlan[*num*][TaggedPort]	Name of the port belonging to a Tagged port of VLAN ID
	In *num*, the index number of a VLAN element is displayed. The number is an integer starting from "0".
	When there is more than one, they are displayed separated by commas.
Link[*num*][NeighborResourceName]	Name of the resource linked to the port number [*num*]
	In *num*, the index number of a port element is displayed. The number is an integer starting from "0".
Link[*num*][NeighborPort]	Name of the port of the resource linked to the port number [*num*]
	In *num*, the index number of a port element is displayed. The number is an integer starting from "0".
LoginInfo[*num*][User]	User name of the account
	In *num*, the index number of an account element is displayed. The number is an integer starting from "0".
LoginInfo[*num*][IPAddress]	Destination IP address of the account

Item Name	Description
	In *num*, the index number of an account element is displayed. The number is an integer starting from "0".
LoginInfo[*num*][Port]	Destination port number of the account
	In *num*, the index number of an account element is displayed. The number is an integer starting from "0".
LoginInfo[*num*][Protocol]	Protocol name used by the account
	In *num*, the index number of an account element is displayed. The number is an integer starting from "0".
LoginInfo[*num*][Authority]	Account privileges
	Either of the following is displayed:
	- For administrator authority
	"administrator" is displayed.
	- For user authority
	"user" is displayed.
	In *num*, the index number of an account element is displayed. The number is an integer starting from "0".
LoginInfo[*num*][Tenant]	Tenant name of the account
	The tenant name is displayed only when the type is "Firewall" or "SLB" and the tenant name has been configured.
	In other cases, the item name and tenant name are not displayed.
	In *num*, the index number of an account element is displayed. The number is an integer starting from "0".
LoginInfo[*num*][AuthType]	Management method of account authentication information
	Either of the following is displayed:
	- When the information is managed within a network device
	"local password" is displayed.
	- When the information is managed within an external server
	"external server" is displayed.
	In *num*, the index number of an account element is displayed. The number is an integer starting from "0".
LoginInfo[*num*][LoginCheck]	Check results of account availability
	One of the following is displayed:
	- When the account can be used
	"Successful" is displayed.
	- When the account cannot be used
	"Failed" is displayed.
	- When the account has not been checked
	"Unchecked" is displayed.
	In *num*, the index number of an account element is displayed. The number is an integer starting from "0".
SnmpCommunityName	SNMP community name
FaultMonitoringMethod	Method of fault monitoring

Item Name	Description

	One of the following is displayed:
	
	- When alive monitoring is performed using ping
	
	  "ping" is displayed.
	
	- When the status is monitored using SNMP
	
	  "SNMP" is displayed.
	
	- When the status is monitored using NETCONF
	
	  "NETCONF" is displayed.
	
	When there are multiple monitoring methods employed, they are displayed separated by commas.

FaultMonitoringInterval(s)	Fault monitoring interval (unit: seconds)
FaultMonitoringRetry	Fault monitoring retry count
FaultMonitoringTimeout(s)	Fault monitoring timeout (unit: seconds)
RestoreHistory[Env][RestoreFileDate]	Time when the network device environment file was backed up If restoration has not been performed or the target file has been already deleted, "-" is displayed.
RestoreHistory[Env][RestoreExecDate]	Date when the network device environment file was backed up If restoration has not been performed, "-" is displayed.
RestoreHistory[Config][GenerationNumber]	Generation number of the network device configuration file If restoration has not been performed or the target file has been already deleted, "-" is displayed.
RestoreHistory[Config][RestoreFileDate]	Time when the restore network device configuration file to restore was backed up If restoration has not been performed, "-" is displayed.
RestoreHistory[Config][RestoreExecDate]	Date when the network device configuration file was backed up If restoration has not been performed, "-" is displayed.

refresh

Updates the configuration information of the network device.

cfbackup

Backs up network device files.

cfmodify

Modifies the comments displayed in COMMENT of the cflist command.

cfrestore

Restores network device files.

cflist

Displays the list of network device files that have already been backed up.

The following information is displayed.

Table 4.8 Information of Device Configuration Files

Item Name	Description
NUMBER	Generation number of the network device configuration file In the lines where backup failed, "-" is displayed (*).

Item Name	Description
	In the bottom line, "env", which represents an environment file, is displayed.
BACKUPDATE	Date when the network device file was backed up
TRIGGER	Trigger for performing network device file backup
	One of the following is displayed:
	- create
	When the network device was registered
	- command
	When the rcxadm netdevice cfbackup command was executed
	- auto
	When the network device was automatically configured
L-PLATFORM/NETWORK	If the type is "L2-Switch", the name of the network resource is displayed.
	This information is only displayed when TRIGGER is "auto".
TENANT	The name of the tenant of the L-Platform on which automatic configuration was performed
	This information is only displayed when TRIGGER is "auto".
OPERATION	One of the following is displayed:
	- create
	Creating a network resource
	- modify
	Modifying a network resource
	- delete
	Deleting a network resource
	- connect
	- disconnect
	Deleting an L-Server
	- recovery
	A recovery process
	This information is only displayed when TRIGGER is "auto".
COMMENT	Specified comment

* Note: Error lines disappear at one of the following timings:

- When the next generation of the network device configuration file is deleted due to the maximum number of generations being exceeded

- When the rcxadm netdevice cfclearerr command is executed

cfexport

Exports network device files.

cfclearerr

Deletes the error history of backup operations of network device configuration files.

Options

-attr {mode={active [-with_va]|maintenance}|auto_conf={true|false}}

For a network device, switch the maintenance mode settings or the auto-configuration target.

-attr mode=active

Checks the status of the device. If the device is in the normal state, this option will change the operational status to "normal" and release maintenance mode.

If an error is detected during the status check of the device, failure to release maintenance mode is notified as the command execution result. In this case, it is necessary to take corrective action according to the message that is output, and perform release of maintenance mode again.

-attr mode=maintenance

Places into maintenance mode.

-attr auto_conf=true

Use this option to select the network device as a target of auto-configuration.

-attr auto_conf=false

Use this option not to select the network device as a target of auto-configuration.

-file *file*.xml

In *file*.xml, specify the XML file that defines the network resource for creation.

For details on the XML file definition, refer to "A.6 Network Configuration Information XML File".

-name *name*

In *name*, specify the name of a network device.

If an unregistered network device name is specified for *name*, an error will occur.

-nowait

Use this option to return directly to the command prompt without waiting for the operation of the network device specified in the subcommand to complete its execution.

-type *type*

In *type*, specify the file type.

config

Specify when network device configuration file operations are performed.

environment

Specify when network device environment file operations are performed.

When omitted, "config" is specified.

For the handling of the file names corresponding to each model, refer to "Table: Network Devices that are Supported by Device Configuration File Management" in "10.2.1 Mechanism of Backup and Restoration" in the "Operation Guide CE".

-redundancy

Specify when operating a network device of the same redundant configuration group as the one that the network device specified for *name* belongs to.

-number *number*

Specify the generation number when a network device configuration file is to be operated.

The generation number can be checked using the cflist subcommand.

-dir *dir*

Specify the directory to which the file specified for export will be output.

Network device configuration files are output in the following format.

```
Backup_date_and_time-Network_device_configuration_file_name
```

20120921104043-running-config

If the file is an environment file, the file will be output using the filename of the target network device.

-comment *comment*

Specify the comment for the network device configuration file.

Specify a character string of up to 256 alphanumeric characters or symbols.

Requirements

Privileges

OS administrator

Location

Admin server

Usage Example

- To display a list of network device information.

```
>rcxadm netdevice list
NAME                      IPADDRESS        NETDEVICE_TYPES       STATUS    MAINTENANCE
----                      ---------        --------              ------    -----------
cat4503.network.com       192.168.5.17     L2-Switch             normal    OFF
```

Exit Status

This command returns the following values:

0

The command executed successfully.

non-zero

An error has occurred.

4.7 rcxadm submgr

Name

Installation_folder**SVROR\\Manager\\bin\\rcxadm submgr** - Operation of information for sub manager coordination

Format

```
rcxadm submgr create -host {ipaddress|FQDN} [-port port] -user user_name -password password -ror_user
ror_user_name -ror_password ror_password
rcxadm submgr modify -host {ipaddress|FQDN} {-user user | -password password | -user user_name -
password password | -ror_user ror_user_name | -ror_password ror_password | -ror_user ror_user_name -
ror_password ror_password}
rcxadm submgr delete -host {ipaddress|FQDN}
rcxadm submgr list
```

Description

The command for registering the host of the sub manager and the user information.

Perform this using the first manager.

Subcommands

create

Registers the host of the sub manager and the user information, and enables sending of requests to the sub manager.

modify

Modifies a registered user name or password.

delete

Deletes a registered host of a sub manager and the user information.

list

Displays a list of the registered sub managers.

Options

-host {*ipaddress|FQDN*}

Specify the IP address or FQDN of the sub manager.

When specifying the FQDN, execute the command after making it possible to resolve the name by adding information to the hosts file, etc.

-user *user_name*

Specify the user name for the sub manager.

When using a domain name, specify it using the format "domain_name\user_name" or "user_name@domain_name".

When not using a domain name, specify it using the format "computer_name\user_name".

-password *password*

Specify the password of the user specified for "-user".

The string can be composed of alphanumeric characters and symbols (excluding blank spaces), and can be up to 127 characters long.

-port *port*

Specify the port number to use for HTTP communication for the sub manager.

If this option is omitted, the default value (23461) will be set.

-ror_user *ror_user_name*

Specify the user name for the ROR manager.

The name must start with an alphabetic character and can be up to 16 alphanumeric characters long, including underscores ("_"), hyphens ("-"), and periods (".").

-ror_password *ror_password*

Specify the password of the user specified for "-ror_user".

The string can be composed of alphanumeric characters and symbols (excluding blank spaces), and can be up to 16 characters long.

Requirements

Permissions

OS Administrator

Location

Admin server

Usage Example

```
> rcxadm submgr create -host 192.168.1.3 -port 23462 -user Admin@domain.local -password passwd -
ror_user RORAdmin -ror_password ror_passwd
```

```
> rcxadm submgr modify -host 192.168.1.3 -user Admin02 -password passwd02


> rcxadm submgr delete -host 192.168.1.4


> rcxadm submgr list
HOST                        PORT  USER                  PASSWORD ROR_USER    ROR_PASSWORD
----                        ----  ----                  -------- --------    ------------
192.168.1.2                 23461 Admin@domain.local       ****** RORAdmin   ******
192.168.1.3                 23462 Admin02@domain.local     ****** RORAdmin   ******
```

Exit Status

This command returns the following values:

0

The command executed successfully.

non-zero

An error has occurred.

4.8 rcxadm pool

Name

[Windows Manager]

Installation_folder\SVROR\Manager\bin\rcxadm pool - resource pool operation

Format

```
rcxadm pool list [-reserve] [-extend attributes]
rcxadm pool list -name name [-template template_name] [-resource] [-info lserver] [-reserve] [-extend
attr[,attr[,...]]]
```

Description

rcxadm pool is the command used to manage resource pools. A resource pool is a type of resource folder in the orchestration tree, which stores the resources to select when creating or adding an L-Server. A resource pool type is specified when creating a resource pool, and only resources of a specific type are stored in each type of resource pool.

Resource pools enable you to manage all the resources allocated when creating an L-Server.

Subcommands

list

Displays a list of resource pools.

The following detailed information is displayed:

- When specifying -extend attributes for the option

Additional information is displayed.

- When not specifying -name for the option

The information for all the resource pools that can be accessed is displayed.

- For VM pools

When a calculation for the available space for the VM pool used for overcommit is set with a reservation value, it will be reflected on the information output in the following item names:

- CPU(max)

- MEMORY(max)

Table 4.9 VM Pool Information

Item Name	Description
NAME	VM pool name
TYPE	Resource pool type
PRIORITY	Priority
CPU(*max*)	The free size and the total size of the VM host CPUs In *max*, the maximum number of CPUs which can be allocated to a VM guest is displayed in "*Performance* GHz * *Cores*" format.
RESERVE-CPU (*1)	The CPU reservation size of the VM host For VM hosts for which the HA function provided by server virtualization software is available, the reserved capacity for a failover is displayed. For VM hosts for which the HA function is unavailable, or for operations with no reservation for failover, a hyphen ("-") is displayed.
MEMORY(*max*)	The free size and the total size of the VM host memory In *max*, the maximum memory that can be allocated to a VM host is displayed in "*Space* GB" format.
RESERVE-MEMORY (*1)	The memory reservation capacity of the VM host For VM hosts for which the HA function provided by server virtualization software is available, the reserved capacity for a failover is displayed. For VM hosts for which the HA function is unavailable, or for operations with no reservation for failover, a hyphen ("-") is displayed.

ATTRIBUTES (*2)	The calculation method for overcommit attributes and free space for VM pools.
	
	One of the following is displayed:
	
	- When calculating the free space with a reservation value, while overcommit is enabled
	
	  "OverCommit=true,CalculatedUsing=reserve" is displayed.
	
	- When calculating the free space with the upper limit value, while overcommit is enabled
	
	  "OverCommit=true,CalculatedUsing=limit" is displayed.
	
	- When overcommit is disabled
	
	  "OverCommit=false" is displayed.

*1: When specifying -reserve for the option, this is displayed.

*2: When specifying -extend attributes for the option, this is displayed. Immediately after performing upgrade of an admin server from ROR V2.2.0 or V3.0.0, this item cannot be displayed even if the -extend attributes option is specified. To display this item, delete the definition file explained in "2.3.1.2 Definition Files for Display Control of VM Pool Attribute Information" in the "Release Notes".

- For Server Pools

Table 4.10 Server Pool Information

Item Name	Description
NAME	Server pool name
TYPE	Resource pool type
PRIORITY	Priority
SERVER	The total and unused number of physical servers

- For storage pools

Table 4.11 Storage Pool Information

Item Name	Description
NAME	Storage pool name
TYPE	Resource pool type
PRIORITY	Priority
CAPACITY(*max*)	The total size and the free size of the virtual storage memory For a storage pool to which the thin provisioning attribute is applied, it is displayed as follows: - Virtual storage free space When the allocated size exceeds the total size of the virtual storage resource, the excess is displayed with a minus sign ("-"). - *max* In *max*, the maximum value is displayed. If free space values of all of registered virtual storage are negative values, the lowest value (the highest number with a minus sign) will be displayed. **[OVM for x86 2.2]** For the free space of virtual storage resources, refer to "8.5.9 Advisory Notes for OVM for x86 2.2 Usage" in the "Setup Guide CE". The total size of virtual storage resources will not be displayed when the virtual storage resource is an OVM for x86 2.2 storage repository. In *max*, the maximum disk space that can be allocated to a virtual storage resource is displayed in "*Space*GB" format. **[OVM for x86 2.2]** For the maximum disk space that can be allocated to a virtual storage resource, refer to "Virtual Storage Resource Free Space" in "8.5.9 Advisory Notes for OVM for x86 2.2 Usage" in the "Setup Guide CE".
ATTRIBUTES (*)	One of the following is displayed: - For a storage pool to which the thin provisioning attribute is applied "Thin=true" is displayed. - For a storage pool to which the thin provisioning attribute is not applied "Thin=false" is displayed.

* Note: When specifying -extend attributes for the option, this is displayed.

- For Network Pools

Table 4.12 Network Pool Information

Item Name	Description
NAME	Network pool name
TYPE	Resource pool type
PRIORITY	Priority
VLANID	Total number and unused number of VLAN IDs
NETWORKDEVICE(in use)	Total number of network devices, and the number of in use network devices

- For address pools

Table 4.13 Address Pool Information

Item Name	Description
NAME	Address pool name
TYPE	Resource pool type
PRIORITY	Priority
ADDRESS	Total number and unused number of addresses

- For image pools

Table 4.14 Image Pool Information

Item Name	Description
NAME	Image pool name
TYPE	Resource pool type
PRIORITY	Priority
IMAGE	Number of images

- When specifying -name for the option

  The specified resource pool and a list of the resources included in the resource pool are displayed.

  - For VM pools

    When a calculation for the available space for the VM pool used for overcommit is set with a reservation value, it will be reflected on the information output in the following item names:

    - CPU(*max*)

    - MEMORY(*max*)

    - CPU(*FREE*)

    - MEMORY(*FREE*)

Table 4.15 VM Pool Information

Item Name	Description
NAME	VM pool name
TYPE	Resource pool type
PRIORITY	Priority
CPU(*max*)	The free size and the total size of the VM host CPUs In *max*, the maximum number of CPUs which can be allocated to a VM guest is displayed in "*Performance* GHz * *Cores*" format.
RESERVE-CPU (*1)	The CPU reservation size of the VM host For VM hosts for which the HA function provided by server virtualization software is available, the reserved capacity for a failover is displayed. For VM hosts for which the HA function is unavailable, or for operations with no reservation for failover, a hyphen ("-") is displayed.
MEMORY(*max*)	The free size and the total size of the VM host memory In *max*, the maximum memory that can be allocated to a VM host is displayed in "*Space* GB" format.
RESERVE-CPU (*1)	The CPU reservation size of the VM host For VM hosts for which the HA function provided by server virtualization software is available, the reserved capacity for a failover is displayed. For VM hosts for which the HA function is unavailable, or for operations with no reservation for failover, a hyphen ("-") is displayed.

Item Name	Description
PER-TEMPLATE (*2)	Number of L-Servers which can be created in the specified L-Server template definition

ATTRIBUTES (*3)	The calculation method for overcommit attributes and free space for VM pools.
	
	One of the following is displayed:
	
	- When calculating the free space with a reservation value, while overcommit is enabled
	
	  "OverCommit=true,CalculatedUsing=reserve" is displayed.
	
	- When calculating the free space with the upper limit value, while overcommit is enabled
	
	  "OverCommit=true,CalculatedUsing=limit" is displayed.
	
	- When overcommit is disabled
	
	  "OverCommit=false" is displayed.

*1: When specifying -reserve for the option, this is displayed.

*2: When specifying -template for the option, this is displayed.

The number of possible L-Servers is displayed based on the VM type (VMtype) of the virtual L-Server template and the specified CPU architecture (CPUArch).

For details, refer to "20.6 Viewing" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

*3: When specifying -extend attributes for the option, this is displayed.

Table 4.16 Resource Information Included in VM Pools

Item Name	Description
NAME	Resource name included in the resource pool
TYPE	Type of resources included in the resource pools
CPU(*FREE*)	The free size and the total size of the VM host CPUs Free space is displayed in *FREE*:
RESERVE-CPU (*1)	The CPU reservation size of the VM host For VM hosts for which the HA function provided by server virtualization software is available, the reserved capacity for a failover is displayed. For VM hosts for which the HA function is unavailable, or for operations with no reservation for failover, a hyphen ("-") is displayed.
MEMORY(*FREE*)	The free size and the total size of the VM host memory Free space is displayed in *FREE*:
RESERVE-MEMORY (*1)	The memory reservation capacity of the VM host For VM hosts for which the HA function provided by server virtualization software is available, the reserved capacity for a failover is displayed. For VM hosts for which the HA function is unavailable, or for operations with no reservation for failover, a hyphen ("-") is displayed.
STATUS	Resource status
CLUSTER (*1)	The name of a cluster that the VM host belongs to For the VM hosts not belonging to a cluster, a hyphen ("-") is displayed.
MAINTENANCE	Maintenance mode
PER-TEMPLATE (*2)	Number of L-Servers which can be created in the specified L-Server template definition

*1: When specifying -reserve for the option, this is displayed.

*2: When specifying -template for the option, this is displayed.

The number of possible L-Servers is displayed based on the VM type (VMtype) of the virtual L-Server template and the specified CPU architecture (CPUArch).

For details, refer to "20.6 Viewing" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- When specifying -resource for the option

Table 4.17 Resource Information Included in VM Hosts

Item Name	Description
NAME	Virtual machine name
TYPE	Resource types
VM_HOST	VM host
L-SERVER (*)	The linked L-Server name

* Note: When specifying -info lserver for the option, this is displayed.

📒 **Note**

- -

When calculating the number of L-Servers using reservation values, if an L-Server template for which the CPU reservation performance and the memory reservation capacity of "0" is specified, "0" will be displayed for the number of possible L-Servers for creation.

- -

- For Server Pools

Table 4.18 Server Pool Information

Item Name	Description
NAME	Server pool name
TYPE	Resource pool type
PRIORITY	Priority
SERVER	The total and unused number of physical servers
PER-TEMPLATE (*)	Number of L-Servers which can be created in the specified L-Server template definition

* Note: When specifying -template for the option, this is displayed.

Table 4.19 Resource Information Included in Server Pools

Item Name	Description
NAME	Resource name included in the resource pool
TYPE	Type of resources included in the resource pools
MODEL	Physical server model name
CPU	Physical server CPU size
MEMORY	Memory size of a physical server
STATUS	Resource status
MAINTENANCE	Maintenance mode
L-SERVER (*1)	The linked L-Server name
PER-TEMPLATE (*2)	Number of L-Servers which can be created in the specified L-Server template definition

*1: When specifying -info lserver for the option, this is displayed.

*2: When specifying -template for the option, this is displayed.

- For Storage Pools

Table 4.20 Storage Pool Information

Item Name	Description
NAME	Storage pool name
TYPE	Resource pool type
PRIORITY	Priority

CAPACITY(*max*)	The total size and the free size of the virtual storage memory
	
	For a storage pool to which the thin provisioning attribute is applied, it is displayed as follows:
	
	- Virtual storage free space
	
	  When the allocated size exceeds the total size of the virtual storage resource, the excess is displayed with a minus sign ("-").
	
	- *max*
	
	  In *max*, the maximum value is displayed.
	
	  If free space values of all of registered virtual storage are negative values, the lowest value (the highest number with a minus sign) will be displayed.
	
	[OVM for x86 2.2]
	
	  For the free space of virtual storage resources, refer to "8.5.9 Advisory Notes for OVM for x86 2.2 Usage" in the "Setup Guide CE".
	
	  The total size of virtual storage resources will not be displayed when the virtual storage resource is an OVM for x86 2.2 storage repository.
	
	  In *max*, the maximum disk space that can be allocated to a virtual storage resource is displayed in "*Space*GB" format.
	
	[OVM for x86 2.2]
	
	  For the maximum disk space that can be allocated to a virtual storage resource, refer to "Virtual Storage Resource Free Space" in "8.5.9 Advisory Notes for OVM for x86 2.2 Usage" in the "Setup Guide CE".

PER-TEMPLATE (*1)	Number of L-Servers which can be created in the specified L-Server template definition

ATTRIBUTES (*2)	One of the following is displayed:
	
	- For a storage pool to which the thin provisioning attribute is applied
	
	  "Thin=true" is displayed.
	
	- For a storage pool to which the thin provisioning attribute is not applied
	
	  "Thin=false" is displayed.

*1: When specifying -template for the option, this is displayed.

Regarding the resources that can be used on the virtual L-Server, the number of possible L-Servers is displayed based on the VM type (VMtype) of the virtual L-Server template and the specified CPU architecture (CPUArch).

For details, refer to "20.6 Viewing" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

*2: When specifying -extend attributes for the option, this is displayed.

Table 4.21 Resource Information Included in Storage Pools

Item Name	Description
NAME	Resource name included in the resource pool

Item Name	Description
TYPE	Type of resources included in the resource pools
CAPACITY(*FREE*)	The total size and the free size of the virtual storage memory [OVM for x86 2.2] For the free space of virtual storage resources, refer to "8.5.9 Advisory Notes for OVM for x86 2.2 Usage" in the "Setup Guide CE". The total size of virtual storage resources will not be displayed when the virtual storage resource is an OVM for x86 2.2 storage repository. Free space is displayed in *FREE*:
STATUS	Resource status
PER-TEMPLATE (*)	Number of L-Servers which can be created in the specified L-Server template definition

* Note: When specifying -template for the option, this is displayed.

Regarding the resources that can be used on the virtual L-Server, the number of possible L-Servers is displayed based on the VM type (VMtype) of the virtual L-Server template and the specified CPU architecture (CPUArch).

For details, refer to "20.6 Viewing" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

- For Network Pools

Table 4.22 Network Pool Information

Item Name	Description
NAME	Network pool name
TYPE	Resource pool type
PRIORITY	Priority
VLANID	Total number and unused number of VLAN IDs
NETWORKDEVICE(in use)	Total number of network devices, and the number of in use network devices

Table 4.23 Resource Information Included in Network Pools

Item Name	Description
NAME	Resource name included in the resource pool
TYPE	Type of resources included in the resource pools
VLANID(*FREE*)	Total and unused number of VLAN IDs Unused numbers are displayed in *FREE*:
ADDRESS(*FREE*)	Total number and unused number of addresses Unused numbers are displayed in *FREE*:
STATUS	Network device status
NETDEVICE_TYPE	Network device type
RULESET	Ruleset name set for the network device When there is more than one, they are displayed separated by commas.
RESOURCE	Name of the resource that is using network devices When there is more than one, they are displayed separated by commas.
DEPLOYABLE_L-PLATFORM_NUMBER (*FREE*)	The number of L-Platforms which can be deployed (unused number and total number) The unused number is displayed in *FREE*:

- For Address Pools

Table 4.24 Address Pool Information

Item Name	Description
NAME	Address pool name
TYPE	Resource pool type
PRIORITY	Priority
ADDRESS	Total number and unused number of addresses

Table 4.25 Resource Information Included in Address Pools

Item Name	Description
NAME	Resource name included in the resource pool
TYPE	Type of resources included in the resource pools
ADDRESS(*FREE*)	Total number and unused number of addresses Unused numbers are displayed in *FREE*:

- For Image Pools

Table 4.26 Image Pool Information

Item Name	Description
NAME	Image pool name
TYPE	Resource pool type
PRIORITY	Priority
IMAGE	Number of images

Table 4.27 Resource Information Included in Image Pools

Item Name	Description
NAME	Resource name included in the resource pool
VERSION	Version of the image
TYPE	Type of resources included in the resource pools
IMAGE_TYPE	Type of image
VM_TYPE	Virtual image VM type identifier information [VMware] vmware-vc [Hyper-V] ms-scvmm [KVM] RHEL-KVM [Solaris Zones] SolarisContainer [OVM for SPARC] OVM-SPARC [Citrix Xen] Citrix-Xen [OVM for x86 3.x] ovmm-x86
OS	OS type of the image

Item Name	Description

DISKS (*1)	The disk sizes of the cloning image are displayed, with the system disk size first, then data disk size.
	
	Hyphens("-") are displayed for the following cloning images:
	  - A physical L-Server image
	  - Images with the VM type of Xen, KVM, or Oracle VM

RELATION (*2)	Name of server management software linked to cloning images
	
	When VM type identifier information is something other than "Solaris Container" or "OVM-SPARC", a hyphen ("-") is displayed.
	
	[Solaris Zones] [OVM for SPARC]
	  - When cloning images are linked to BladeLogic
	    "BladeLogic" is displayed.
	  - When there is no server management software linked to cloning images
	    "None" is displayed.

*1: When -extend disksize is specified for an option, the item is displayed. Disk size may not be displayed immediately after updating Resource Orchestrator from V3.0 or an earlier version or immediately after performing recovery operations using Disaster Recovery. Wait for a short while and then perform the operation again.

For details on Disaster Recovery, refer to the "DR Option Instruction".

*2: The item is displayed only when -extend relation is specified for an option.

Options

-name *name*

In *name*, specify the name of the target resource pool to perform an operation with.

For the resource pool allocated in the resource folder, specify the resource folder name using slashes ("/").

-template *template_name*

In *template_name*, specify the name of an L-Server template that can be created.

-extend *attr*

Specify when displaying additional information. When specifying multiple attributes, separate them using commas.

- attributes

Specify when displaying additional information. When using with the -name option, only storage pools or VM pools can be specified for the -name option.

- disksize

Specify this option to display the disk size of the cloning image. This option can only be specified when an image pool is selected for the -name option.

- relation

Specify when displaying the name of the server management software linked to the cloning image. This option can only be specified when an image pool is selected for the -name option.

-resource

Specify this option to display the elements of the resources registered in a resource pool.

This is valid when a VM pool is specified for the -name option.

-info lserver

Use this option to display the link between an L-Server and the resources or the elements of the resources registered in a resource pool.

This is valid when a VM pool or a server pool specified for the -name option.

-reserve

Specify this option to display the CPU and memory reservation capacities when the HA function is enabled on the VM host in a VM pool.

This is valid for VM pools when the -name option is specified with this option.

Requirements

Permissions

Refer to "5.1.2 Roles and Available Operations" in the "Design Guide CE".

Location

Admin server

Example

- To display the list of resource pools:

```
>rcxadm pool list -extend attributes <RETURN>
NAME                TYPE     PRIORITY CPU(max.)             MEMORY(max.)
----                ----     -------- ---------             ------------
/VMHostPool         VM       5        37.6/39.9(1.8GHz x 8)  23.3/26.6(8.0GB)

NAME                TYPE     PRIORITY SERVER
----                ----     -------- --------------
/ServerPool         Server   5        0/3

NAME                TYPE     PRIORITY CAPACITY(max.)         ATTRIBUTES
----                ----     -------- --------------         ------------
/StoragePool        Storage  5        449.7/3061.8(351.7GB)  Thin=false
/ThinStoragePool    Storage  5        449.7/3061.8(351.7GB)  Thin=true

NAME                TYPE     PRIORITY VLANID   NETWORKDEVICE(in use)
----                ----     -------- ------   ------
/NetworkPool        Network  5        0/0      10(5)

NAME                TYPE     PRIORITY ADDRESS
----                ----     -------- -------
/AddressPool        Address  5        249/257

NAME                TYPE     PRIORITY IMAGE
----                ----     -------- -----
/ImagePool          Image    5        10
```

When the calculation for the available space for a VM pool used for overcommit is set with a reservation value, in the case of the output example above, the following values will be the values calculated using the reservation value:

- 37.6 and (1.8 GHz x 8), which are displayed for CPU(max.)

- 23.3 and (8.0 GB), which are displayed for MEMORY(max.)

- To display the specified resource pool and a list of the resources included in the resource pool:

```
>rcxadm pool list -name /VMHostPool <RETURN>
NAME                TYPE     PRIORITY CPU(max.)             MEMORY(max.)
----                ----     -------- ---------             ------------
/VMHostPool         VM       5        37.6/39.9(1.8GHz x 8)  23.3/26.6(8.0GB)

NAME        TYPE     CPU(FREE)            MEMORY(FREE)   STATUS  MAINTENANCE
----        ----     ---------            ------------   ------  -----------
vmhost1     VMHost   1.9GHz x 4 (7.9GHz)  6.4GB (6.4GB)  normal  OFF
vmhost2     VMHost   1.9GHz x 8 (14.6GHz) 10.0GB (8.7GB) normal  OFF
vmhost3     VMHost   1.9GHz x 8 (14.9GHz) 10.0GB (8.0GB) normal  OFF
```

When the calculation for the available space for a VM pool used for overcommit is set with a reservation value, in the case of the output example above, the following values will be the values calculated using the reservation value:

- 37.6 and (1.8 GHz x 8), which are displayed for CPU(max.)

- 23.3 and (8.0 GB), which are displayed for MEMORY(max.)

- (7.9 GHz), (14.6 GHz), and (14.9 GHz), which are displayed for CPU(FREE)

- (6.4 GB), (8.7 GB), and (8.0 GB), which are displayed for MEMORY(FREE)

- To display the specified VM pool, and the CPU and memory reservation capacities of the VM hosts in the pool:

   - Cluster configuration and admission control are enabled (policy: Percentage of cluster resources reserved as failover spare capacity (10%))

```
>rcxadm pool list -name VMHostPool -reserve <RETURN>
NAME              TYPE     PRIORITY CPU(max.)              RESERVE-CPU MEMORY(max.)      RESERVE-
MEMORY
----              ----     -------- ---------              ----------- ------------
-------------
/VMHostPool       VM       5           5.4/11.1(1.2GHz x 2)  0.9GHz      19.2/27.4(8.4GB)  2.6GB

NAME        TYPE      CPU(FREE)             RESERVE-CPU MEMORY(FREE)   RESERVE-MEMORY STATUS
CLUSTER     MAINTENANCE
----        ----      ---------             ----------- ------------   -------------- ------
-------     -----------
vmhost1     VMHost    1.8GHz x 2 (1.2GHz)   0.3GHz      6.6GB (3.7GB)  0.6GB          normal
Cluster2    OFF
vmhost2     VMHost    1.8GHz x 2 (2.4GHz)   0.3GHz      10.4GB (8.4GB) 1.0GB          normal
Cluster2    OFF
vmhost3     VMHost    1.8GHz x 2 (1.8GHz)   0.3GHz      10.4GB (7.1GB) 1.0GB          normal
Cluster2    OFF
```

   - Cluster configuration and admission control are enabled (policy: Specify failover hosts (vmhost1))

```
>rcxadm pool list -name VMHostPool -reserve <RETURN>
NAME              TYPE     PRIORITY CPU(max.)              RESERVE-CPU MEMORY(max.)      RESERVE-
MEMORY
----              ----     -------- ---------              ----------- ------------
-------------
/VMHostPool       VM       5           5.0/11.1(1.4GHz x 2)  3.7GHz      17.5/27.4(9.4GB)  6.6GB

NAME        TYPE      CPU(FREE)             RESERVE-CPU MEMORY(FREE)   RESERVE-MEMORY STATUS
CLUSTER     MAINTENANCE
----        ----      ---------             ----------- ------------   -------------- ------
-------     -----------
vmhost1     VMHost    1.8GHz x 2 (0.0GHz)   3.7GHz      6.6GB (0.0GB)  6.6GB          normal
Cluster2    OFF
vmhost2     VMHost    1.8GHz x 2 (2.8GHz)   0.0GHz      10.4GB (9.4GB) 0.0GB          normal
Cluster2    OFF
vmhost3     VMHost    1.8GHz x 2 (2.2GHz)   0.0GHz      10.4GB (8.1GB) 0.0GB          normal
Cluster2    OFF
```

   - Cluster configuration and admission control are enabled (policy: The cluster tolerates host failures)

```
>rcxadm pool list -name VMHostPool -reserve <RETURN>
NAME              TYPE     PRIORITY CPU(max.)              RESERVE-CPU MEMORY(max.)      RESERVE-
MEMORY
----              ----     -------- ---------              ----------- ------------
-------------
/VMHostPool       VM       5           6.6/11.1(1.4GHz x 2)  0.0GHz      21.8/27.4(9.4GB)  0.0GB

NAME        TYPE      CPU(FREE)             RESERVE-CPU MEMORY(FREE)   RESERVE-MEMORY STATUS
CLUSTER     MAINTENANCE
----        ----      ---------             ----------- ------------   -------------- ------
```

```
-------         -----------
vmhost1         VMHost   1.8GHz x 2 (1.6GHz)  0.0GHz        6.6GB (4.3GB)  0.0GB            normal
Cluster2    OFF
vmhost2         VMHost   1.8GHz x 2 (2.8GHz)  0.0GHz        10.4GB (9.4GB) 0.0GB            normal
Cluster2    OFF
vmhost3         VMHost   1.8GHz x 2 (2.2GHz)  0.0GHz        10.4GB (8.1GB) 0.0GB            normal
Cluster2    OFF
```

- Cluster configuration and admission control are disabled

```
>rcxadm pool list -name VMHostPool -reserve <RETURN>
NAME             TYPE    PRIORITY CPU(max.)              RESERVE-CPU MEMORY(max.)      RESERVE-
MEMORY
----             ----    -------- ---------              ----------- ------------
-------------
/VMHostPool      VM      5        6.6/11.1(1.4GHz x 2)  -           21.8/27.4(9.4GB)  -

NAME            TYPE     CPU(FREE)              RESERVE-CPU MEMORY(FREE)   RESERVE-MEMORY STATUS
CLUSTER     MAINTENANCE
----            ----     ---------              ----------- ------------   -------------- ------
-------     -----------
vmhost1         VMHost   1.8GHz x 2 (1.6GHz)  -           6.6GB (4.3GB)  -              normal
Cluster2    OFF
vmhost2         VMHost   1.8GHz x 2 (2.8GHz)  -           10.4GB (9.4GB) -              normal
Cluster2    OFF
vmhost3         VMHost   1.8GHz x 2 (2.2GHz)  -           10.4GB (8.1GB) -              normal
Cluster2    OFF
```

- To display the specified VM pool, and a list of the VM hosts and virtual machines included in the pool:

```
>rcxadm pool list -name /VMHostPool -resource -info lserver <RETURN>
NAME             TYPE    PRIORITY CPU(max.)          MEMORY(max.)
----             ----    -------- ---------          ------------
/VMHostPool      VM      5        5.4/7.4(1.4GHz x 2)  5.3/9.5(4.6GB)

NAME            TYPE     CPU(FREE)              MEMORY(FREE)   STATUS  MAINTENANCE
----            ----     ---------              ------------   ------  -----------
VMHost1         VMHost   1.8GHz x 2 (2.5GHz)  2.9GB (0.7GB)  normal  OFF
VMHost2         VMHost   1.8GHz x 2 (2.9GHz)  6.6GB (4.6GB)  normal  OFF

NAME             TYPE            VM_HOST        L-SERVER
----             ----            -------        --------
Guest1           VirtualMachine  VMHost1        /L-Server1
Guest2           VirtualMachine  VMHost1        /folder/L-Server2
Guest3           VirtualMachine  VMHost1        -
Guest4           VirtualMachine  VMHost2        -
Guest5           VirtualMachine  VMHost2        -
```

- To display a list of address set resources contained in the specified address pool

```
>rcxadm pool list -name /AddressPool <RETURN>
NAME             TYPE    PRIORITY ADDRESS
----             ----    -------- -------
/AddressPool     Address 5        8872/8879

NAME             TYPE           ADDRESS(FREE)
----             ----           -------------
AAA              MacAddressSet  15(15)
AppLAN1          WwnAddressSet  17(17)
macset1          MacAddressSet  4272(4270)
name             MacAddressSet  255(251)
wwnset1          WwnAddressSet  4320(4319)
gip              GipAddressSet  15(15)
```

Exit Status

This command returns the following values:

0

The command executed successfully.

non-zero

An error has occurred.

4.9 msgnotice

Name

Installation_folder\SVROR\Manager\bin\msgnotice - Notification settings

Format

```
msgnotice register -name name -ip ipaddress -user_name user_name -passwd password
msgnotice unregister -name name
msgnotice modify -name name [-ip ipaddress] [-user_name user_name] [-passwd password]
msgnotice enable
msgnotice disable
msgnotice info
```

Description

When using the automatic quarantining function, msgnotice is the command used to configure notification of users.

When configuring notification of users, first use this command to set the connection information of the VDI management server, and then enable notification.

Note
. . . .

This command cannot be executed multiple times simultaneously.
. . . .

Subcommands

register

Registers the connection information of the VDI management server which will be used for notifying users.

Note
. . . .

It is not possible to register the connection information of multiple VDI management servers.
. . . .

unregister

Deletes the connection information of the registered VDI management server.

modify

Modifies the following information of the registered VDI management server.

- IP address

- Administrator user ID

- Administrator password

enable

Enables notification of users when an L-Server is transferred to the quarantine network.

disable

Disables notification of users when an L-Server is transferred to the quarantine network.

info

Displays information related to notification of users.

The following information is displayed.

Table 4.28 Information Related to Notification of Users

Item Name	Description

Notice	Enabling or disabling of notification
	
	 One of the following is displayed:
	
	 - enable
	
	   Displayed when notification is enabled.
	
	 - disable
	
	   Displayed when notification is disabled.
	
	 By default, this will be empty. (Notification is disabled)

Name	VDI management server name
IP address	IP address used to connect to the VDI management server
User name	Administrator user ID for the VDI management server
Password	Administrator password for the VDI management server

Options

-name *name*

In *name*, specify the registration name for the VDI management server.

For the registration name, specify a character string that is up to 15 characters long, starts with an alphabetic character, and is composed of alphanumeric characters and hyphens ("-").

-ip ipaddress

In *ipaddress*, specify the IP address of the VDI management server.

-user_name *user_name*

In *user_name*, specify the user ID of an account with administrator privileges for the VDI management server.

For the user ID, specify a character string that is up to 84 characters long, and is composed of alphanumeric characters and symbols (ASCII characters (0x20 to 0x7e)).

-passwd *password*

In *password*, specify the password for an account with administrator privileges for the VDI management server.

For the password, specify a character string that is up to 128 characters long, and is composed of alphanumeric characters and symbols (ASCII characters (0x20 to 0x7e)).

Requirements

Privileges

OS administrator

Location

Admin server

Usage Example

- Registering the connection information of the VDI management server

```
> msgnotice register -name vdimgr -ip 192.168.100.10 -user_name administrator -passwd admin00
```

- Modifying the connection information of the VDI management server

```
> msgnotice modify -name vdimgr -ip 192.168.100.20
```

- Enabling notification of transfer to the quarantine network

```
> msgnotice enable
```

- Displaying the information sent during notification

```
> msgnotice info
Notice: enable

Name: vdimgr
IP address: 192.168.100.20
User name: administrator
Password: *******
```

- Deleting the connection information of the VDI management server

```
> msgnotice unregister -name vdimgr
```

Exit Status

This command returns the following values:

0

The command executed successfully.

non-zero

An error has occurred.

4.10 mailnotice

Name

Installation_folder\SVROR\Manager\bin\mailnotice - Enables/disables email notification, displays information, and registers/deletes/modifies connection information for the SMTP server

Format

```
mailnotice register -name name -ip ipaddress -from from_address [-port port]
mailnotice unregister -name name
mailnotice modify -name name [-ip ipaddress] [-port port] [-from from_address]
mailnotice enable
mailnotice disable
mailnotice info
```

Description

mailnotice is the command for configuring email notifications to the tenant administrator in response to detection of malware.

When sending email notifications to the tenant administrator, use this command to configure the connection information for the SMTP server in advance, and enable email notifications.

Note

⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯

This command cannot be executed multiple times simultaneously.

⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯

Subcommands

register

Registers the connection information for the SMTP server that will be used to send email notifications to the tenant administrator.

Note

⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯

It is not possible to register the connection information of multiple SMTP servers.

⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯

unregister

Deletes the connection information of the registered SMTP server.

modify

Modifies the following information of the registered SMTP server.

- IP address

- Port number

- Sender's email address

Note

⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯

It is not possible to change the name registered for the SMTP server. To change the registered name, first delete the information registered for the SMTP server, and then re-register it.

⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯

enable

Enables the sending of email notifications to the tenant administrator when executing an action on an L-Server on which malware has been detected.

disable

Disables the sending of email notifications to the tenant administrator when executing an action on an L-Server on which malware has been detected.

info

Displays information regarding the email notification sent to the tenant administrator.

The following information is displayed.

Table 4.29 Information Regarding the Email Notification Sent to the Tenant Administrator

Item Name	Description

Notice	Enables/disables email notifications
	
	One of the following is displayed:
	
	- enable
	
	   Displayed when email notifications are enabled.
	
	- disable
	
	   Displayed when email notifications are disabled.
	
	By default, this will be empty. (Email notifications are disabled)

Name	SMTP server name
IP address	IP address used to connect to the SMTP server
Port	Port number of the SMTP server
From address	Sender's email address

Options

-name *name*

In *name*, specify the registration name for the SMTP server.

For the registration name, specify a character string that is up to 15 characters long, starts with an alphabetic character, and is composed of alphanumeric characters and hyphens ("-").

-ip *ipaddress*

In *ipaddress*, specify the IP address of the SMTP server.

-port *port*

In *port*, specify the port number of the SMTP server. If this is omitted, the default port number, 25, is set.

For the port number, specify an integer between 0 and 65535 composed only of single-byte numbers.

-from from_address

In *from_address*, specify the sender email address.

For the email address, specify a character string that is up to 64 characters long, starts with an alphabetic character, and is composed of alphanumeric characters and symbols.

Requirements

Privileges

OS administrator

Location

Admin server

Usage Example

Registering the connection information of the SMTP server

```
>mailnotice register -name smtpsv -ip 192.168.100.11 -port 25 -from alert@ror.com
```

Modifying the connection information of the SMTP server

```
> mailnotice modify -name smtpsv -ip 192.168.100.21
```

Enabling email notifications when executing an action upon detection of malware.

```
> mailnotice enable
```

When displaying information regarding the email notification

```
> mailnotice info
Notice: enable

Name: smtpsv
IP address: 192.168.100.21
Port: 25
From address: alert@ror.com
```

When deleting the connection information of the SMTP server

```
>mailnotice unregister -name smtpsv
```

Exit Status

This command returns the following values:

0

The command executed successfully.

non-zero

An error has occurred.

4.11 [Symantec] rcx_register_ror.ps1

Name

Drive_on_which_Symantec_Endpoint_Protection_Manager_has_been_installed\Symantec\Symantec Endpoint Protection Manager\bin \ResourceOrchestrator\cmd\rcx_register_ror.ps1 - Script file for registering Resource Orchestrator user information

Format

```
rcx_register_ror.ps1 create -host host -user user -password password
rcx_register_ror.ps1 show
```

Description

rcx_register_ror.ps1 is the command for registering Resource Orchestrator user information with the server on which Symantec Endpoint Protection Manager operates.

Subcommands

create

Encrypts the information specified in the argument and uses it in creation of the following environment definition file.

If the environment definition file already exists, a message checking whether to overwrite it is output.

Location of the Environment Definition File

Storage Location

drive\Symantec\Symantec Endpoint Protection Manager\bin\ResourceOrchestrator\etc

File Name

rcx.config

show

Displays the content of the environment definition file created using "create".

Options

-host *host*

For *host*, specify the IP address or the host name (FQDN) of the Resource Orchestrator manager.

-user *user_name*

For *user_name*, specify the user name of a privileged user that was created during installation of the Resource Orchestrator manager.

-password *password*

For *password*, specify the password of a privileged user that was created during installation of the Resource Orchestrator manager.

Requirements

Privileges

OS administrator

Location

The server on which Symantec Endpoint Protection Manager operates

Usage Example

- When creating the environment definition file

```
PS C:\Symantec\Symantec Endpoint Protection
Manager\bin\ResourceOrchestrator\cmd> ./rcx_register_ror.ps1 create -host 192.168.10.40 -user
manage -password password
```

- When displaying the content of the environment definition file

```
PS C:\Symantec\Symantec Endpoint Protection
Manager\bin\ResourceOrchestrator\cmd> ./rcx_register_ror.ps1 show
HOST:192.168.10.40
PORT:23461
USER:manage
PASSWORD:*******
```

Exit Status

This command returns the following values:

0

The command executed successfully.

non-zero

An error has occurred.

Chapter 5 Messages

This section explains the messages that are output when using this function.

When messages other than those explained in this chapter are output, refer to "Messages".

5.1 Messages Output during Execution of the rcxadm avmgr Command

Information

. . . .

No changes have been made to the explanations of messages output during the changing of the connection destination network of a virtual L-Server as a result of execution of the rcxadm avmgr quarantine or rcxadm avmgr unquarantine commands.

. . . .

21143

FJSVrcx:INFO: 21143:*L-Server_name*:quarantine L-Server:started

Description

The process of transferring the L-Server (*L-Server_name*) to the quarantine network has been started.

Corrective Action

No action is necessary.

21144

FJSVrcx:INFO: 21144 *L-Server_name*:quarantine L-Server:completed

Description

The process of transferring the L-Server (*L-Server_name*) to the quarantine network has been completed.

Corrective Action

No action is necessary.

21171

FJSVrcx:INFO: 21171:security event occurred.*detail*

Description

A security event has been sent to Resource Orchestrator.

In *detail*, the following information is displayed.

- For mgmt_soft_name=the_identifier_of_the_antivirus_software oid=the_identifier_of_the_SNMP_trap_agent st=the_identifier_specific_to_the_SNMP_trap_device data=the_raw_data_received_from_the_SNMP_trap_agent

  A security risk has been sent to ROR through an SNMP trap from the antivirus software shown in *the_identifier_of_the_antivirus_software*.

  The identifier of the SNMP trap agent is displayed for oid.

  The identifier specific to the SNMP trap device is displayed for st.

  The raw data received from the SNMP trap agent is displayed for data.

  When checking the content of decoded data, refer to system logs.

  There is a few minutes difference in the time messages are output to the system log and to the event log of the GUI (ROR console).

Corrective Action

Take corrective action based on the content output for *detail*.

For mgmt_soft_name=*the_identifier_of_the_antivirus_software* oid=*the_identifier_of_the_SNMP_trap_agent* st=*the_identifier_specific_to_the_SNMP_trap_device* data=*the_raw_data_received_from_the_SNMP_trap_agent*

Corrective action is only necessary in the following case.

- When tuning is necessary for the security risks that are the targets of quarantining, based on the content of "data" in this message (which is output to the system log), modify the definition files of keywords for exclusion from the targets of quarantining or the definition files of keywords for the targets of quarantining.

21180

FJSVrcx:INFO:21180:*obj.function* was performed

Description

The processing of the *function* for *obj* has been performed.

The name of the L-Server is displayed in *obj*.

- When "message notifying of disconnect" is displayed for *function*

A message was sent to the user when the L-Server was connected to the quarantine network.

- When "email notifying of disconnect" is displayed for *function*

When an action is executed on an L-Server upon detection of a malware infection, the tenant administrator is notified by email.

Corrective Action

No action is necessary.

41123

FJSVrcx:WARNING:41123:*obj.function* was aborted. detail=*detail*

Description

The processing of the *function* for *obj* has not been performed.

L-Server_name is displayed in *obj*.

The reason the processing of *function* was not performed is displayed for *detail*.

- When "message notifying of disconnect" is displayed for *function*

When executing an action upon detection of a malware infection on an L-Server, no notification message was sent to the user.

- When "email notifying of disconnect" is displayed for *function*

When executing an action upon detection of a malware infection on an L-Server, no notification message was sent to the tenant administrator.

Corrective Action

- When "message notifying of disconnect" is displayed for *function*

Processing of a VDI management server remote command failed. There are the following possibilities:

- There is no connection information configured for the VDI management server, or there is a mistake in the connection information
- The VDI management server is not operating correctly
- The network settings of the VDI management server are incorrect

Check the connection information, operating status, and network settings of the VDI management server.

- When "email notifying of disconnect" is displayed for *function*

Processing of an SMTP server remote command failed.

Check the connection information, operating status, and network settings of the SMTP server.

When the cause is not one of the above, collect troubleshooting data, and contact Fujitsu technical staff.

67153

FJSVrcx:ERROR:67153:*obj*: already exists

Description

The specified object *obj* already exists.

One of the following messages is displayed in *obj*.

- When *obj* is "Antivirus software"

    An antivirus software resource with the same name already exists.

- When *obj* is an IP address or an FQDN

    If this message is displayed during operation of information for sub manager coordination, manager information already exists.

Corrective Action

Change the name of the object to be created, or delete the existing *obj* and then perform the operation again.

In any other cases, take corrective action based on the content of *obj*.

- When *obj* is "Antivirus software"

    Either change the resource name of the antivirus software resource to register or delete the already registered antivirus software, and then perform the operation again.

- When *obj* is an IP address or an FQDN

    If this message is displayed when operating information for sub manager coordination, change the IP address or FQDN if necessary, and then perform the operation again.

67154

FJSVrcx:ERROR:67154:*obj*:not found

Description

After checking the following for the displayed object, perform the operation again.

- That the object exists
- That the object was not deleted during deletion processing

If this error is displayed when a command is executed, check the following.

- If this message is displayed when a command was executed

Corrective Action

If this message is displayed when a command was executed

There is a chance that the resource type of the specified object name differs from the resource type that can be specified for the command argument.

Check the resource type of the specified object and then perform the operation again.

The name of the specified object is displayed for *obj*.

The object name is displayed as follows.

- When operating information for sub manager coordination

    - An IP address or an FQDN

- When the object is an antivirus software

    - The resource name of the target antivirus software

67198

FJSVrcx:ERROR:67198:command execution error.*detail*

Description

An error has occurred during execution of a manager command.

In *detail*, the following information is displayed.

Take corrective action based on the content output for *detail*.

- For "quarantine failed(detail=*detail*)"

  Transferring of the L-Server to the quarantine network failed.

  detail will be one of the following:

   - "L-Server not found. ip=*IP_address*"

   - "Two or more L-Server found. ip=*IP_address*,lserver_key=["*Resource_ID*", "*Resource_ID*",...]"

   - "already registered"

     The connection information of the SMTP server has already been registered using the mailnotice command.

   - "Other error messages (FJSVrcx:ERROR:xxxx)"

Corrective Action

For "quarantine failed(detail=*detail*)"

Take corrective action based on the content output for *detail*.

"L-Server not found. ip=*IP_address*"

The L-Server for which the IP address of the SNMP trap or REST API has been set was not found.

Check whether linking of the virtual machine or SBC server using this IP address with the L-Server is complete.

In configurations where there are multiple Resource Orchestrator managers, check the following:

- Check whether the 413 warning message "Target lserver not found in submanager." has been output in the system log of the first manager of Resource Orchestrator.

  If the 413 warning message has not been output, no corrective action is necessary.

- Check whether the L-Server is being managed using another sub manager.

  If it is being managed using another sub manager, check whether the information for sub manager coordination is configured correctly.

  If "submgr:*Resource_Orchestrator_manager_IP_address_or_FQDN*" is included in *detail*, the message can be ignored.

"Two or more L-Server found. ip=*IP_address*,lserver_key=["*Resource_ID*", "*Resource_ID*",...]"

Multiple L-Servers for which the IP address of the SNMP trap or REST API has been set were found.

Environments in which multiple L-Servers are configured with the same IP address for reasons such as tenants are being used, are not supported.

Only use an IP address for one virtual L-Server.

"already registered"

No corrective action is necessary as registration is already complete.

"Other error messages (FJSVrcx:ERROR:xxxx)"

An error occurred during the modification of the L-Server performed during the transfer process of the L-Server to the quarantine network.

Take corrective action explained for the corresponding error message in "Messages".

In configurations where there are multiple Resource Orchestrator managers, check the following, connect to the manager where the problem occurred, and perform corrective action based on the error message.

- When "submgr:*Resource_Orchestrator_manager_IP_address_or_FQDN*" is included in *detail*

    A problem has occurred on the Resource Orchestrator manager corresponding to the IP address or the FQDN.

- When "submgr:*Resource_Orchestrator_manager_IP_address_or_FQDN*" is not included in *detail*

    A problem has occurred on the first manager of Resource Orchestrator.

67280

FJSVrcx:ERROR:67280:*obj*:*function* not supported. *detail*

Description

obj does not support *function*.

In *function*, the name of the function that is not supported is displayed.

When *function* can be used with certain conditions, detailed information is displayed in the following *function* or *detail*.

In cases other than the following, this message is displayed when you attempt to use a function that cannot be used by *obj*. No action is necessary.

- When "modify network" is displayed for *function,* and "not linked physical-lserver" is displayed for *detail*

    As the physical L-Server in *obj* was created using a method other than linking, changing of the destination network is not supported.

Corrective Action

When "modify network" is displayed for *function*, and "not linked physical-lserver" is displayed for *detail*

    Refer to "2.13 Linking Physical L-Servers with Configured SBC Servers", and perform linking.

67295

FJSVrcx:ERROR:67295:*obj*:duplicate resource name found

Description

- When registering or modifying an antivirus software

    An antivirus software resource with the same IP address and antivirus software identifier as the resource in *obj* that is being registered or modified already exists.

- When connecting to the quarantine network or the operation network

    An L-Server with the same name as the L-Server described in the XML files for changing the network already exists.

Corrective Action

When registering or modifying an antivirus software

    In Resource Orchestrator, only one resource can use the same combination of IP address and antivirus software identifier.

    Change the IP address specified during registration or changing of the antivirus software, and perform the operation again.

When connecting to the quarantine network or the operation network

    The L-Server name described in the XML files for changing the network must be identical to the L-Server name contained in the name of the XML file for changing the network. Change either of the virtual L-Server names so they are identical.

- When connecting to the quarantine network

    Execute the rcxadm avmgr quarantine command.

- When connecting to the operation network

    Execute the rcxadm avmgr unquarantine command.

67355

FJSVrcx:ERROR:67355:connection error. target=*target*

Description

The program of *target* may not have been started.

Corrective Action

After checking if the destination server for communication has been started by referring to the following manuals, resolve the problem, and then perform the operation again.

- Check the communication destination

  [Virtual Edition]

  Refer to "Chapter 2 Starting and Stopping Managers and Agents" in the "Operation Guide VE", and start the destination server for communication.

  [Cloud Edition]

  Refer to "Chapter 2 Starting and Stopping Managers and Agents" in the "Operation Guide CE", and start the destination server for communication.

  - When *target* is 127.0.0.1

  The services of Resource Coordinator Manager on the admin server may not have been started. Start the services.

- Check the port numbers

  Check the port numbers of the admin server and managed servers.

  If there are any mistakes, change the port number to the right one.

  [Virtual Edition]

  For how to change port numbers, refer to "Appendix A Port List" in the "Design Guide VE".

  For how to change port numbers, refer to "8.2 Changing Port Numbers" or "9.1.6 Changing Port Numbers" in the "User's Guide VE".

  [Cloud Edition]

  For how to check port numbers, refer to "Appendix A Port List" in the "Design Guide CE".

  For how to change port numbers, refer to "6.2 Changing Port Numbers" or "7.1.6 Changing Port Numbers" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

67392

FJSVrcx:ERROR:67392:modifying VM guest failed. detail=*detail*

Description

Modification of a VM guest failed.

Take corrective action for the content displayed for *detail*.

If this message is displayed during modification of an L-Server, some of the information of that L-Server may have been successfully modified. To confirm whether information has been modified, wait for a while and then check the information of the relevant L-Server.

- When the format "(*message*,vmerrno=*error_number*,ip=*IP_address*)", or the format "(*message*,vmerrno=*error_number*,ip=*IP_address*,host=*VM_host_IP_address*)" is displayed

  An error occurred during control of the VM host or VM management software with the corresponding *IP_address*. Take corrective action based on the *error_number*.

  - For *error_number* "400"

    [Citrix Xen]

      - "xe vm-param-set::Error code: MEMORY_CONSTRAINT_VIOLATION" is displayed for detail

Corrective Action

When the format "(*message*,vmerrno=*error_number*,ip=*IP_address*)", or the format
"(*message*,vmerrno=*error_number*,ip=*IP_address*,host=*VM_host_IP_address*)" is displayed

For *error_number* "400"

Processing of a VM host remote command failed. Check the operating status and network settings of the VM host.

If nothing happens even if the modification operation is performed on the VM host, there is a problem with the VM host. Resolve the problem with the VM host, and then perform the operation again.

[Citrix Xen]

"xe vm-param-set::Error code: MEMORY_CONSTRAINT_VIOLATION" is displayed for *detail*

You may be using XenServer with a free license.

Resource Orchestrator does not support the use of XenServer with a free license.

Check the license of XenServer registered in the pool of CitrixXen, and apply a commercial license.

If performing the above corrective action does not resolve the problem, or if content different from any of the above is displayed in *detail*, collect the relevant message and troubleshooting data, and contact Fujitsu technical staff.

67999

FJSVrcx:ERROR:67999:internal error, *details*

Description

In the following case, an error has occurred.

- When *details* is antivirus software resources

An unknown error may have occurred in communication with the services of the Resource Coordinator manager on the admin server.

Corrective Action

When *details* is antivirus software resources

Collect the relevant message and troubleshooting data, and contact Fujitsu technical staff.

Information
. . . .

System Log Messages

The messages that are output to the system log on the admin server are as follows:

- Messages with the "application log" event type

- Messages with source names starting with "JSE_SWRC_FJSVRCX"

. . . .

5.2 Messages Output during Execution of the convertVMtoLServer Command

42501

FJSVrcx:WARNING:42501:invalid value in the configuration file (file=*file*, detail=*detail*)

Description

There is an invalid value in the definition file.

The file name is displayed for *file*.

The details of the error are displayed for *detail*. When multiple errors are detected, they are displayed separated by commas (",").

Corrective Action

- When *file* is "avmgr.rcxprop"

- When *detail* is "avmgr.lserver_xml_*dir*"

If the folder specified for avmgr.lserver_xml_*dir* does not exist, the XML file has been created in the following folder which is the default storage location.

- *Installation_folder*\SVROR\Manager\etc\files\avmgr

As network switchover upon virus detection fails in this state, correct the folder name specified for avmgr.lserver_xml_*dir* and then move the XML files stored in the default storage location to the folder specified for avmgr.lserver_xml_*dir*.

- When *file* is "avmgr_network.rcxprop"

- When *detail* is "*name of the connected network of virtual L-Servers*"

Check if the network that is specified as the connected network of virtual L-Servers exists.

- When *detail* is "*quarantine network name*"

Check if the specified quarantine network exists.

- When *detail* is "*name of the connected network of virtual L-Servers*" or "*quarantine network name*"

Check if the network that is specified as the connected network of virtual L-Servers and the quarantine network exist.

- When *detail* is "LNetwork's definition is empty"

Check if the avmgr_network.rcxprop file is empty.

- When *detail* is blank

Check if there is an error in the avmgr_network.rcxprop file.

62501

FJSVrcx:ERROR:62501:*VmGuestName*:is required

Description

No VM name is configured for *VmGuestName*.

Corrective Action

Specify a VM name using the full path in a CSV configuration file.

62512

FJSVrcx:ERROR:62512:*filename*:invalid file format, detail=*%1*

Description

There is a mistake in the format of the file specified for *filename*.

In *%1*, the details of the mistake are displayed.

Corrective Action

Take corrective action based on the content displayed in *%1*.

- For "file is empty"

The file specified for *filename* is empty. Correct the content of the file, and execute the command again.

62595

FJSVrcx:ERROR:62595:*param_names*:mandatory parameter not defined in *file*

Description

Necessary settings are not configured in the configuration file displayed in *file*.

In *param_names*, all parameters that are not configured are displayed.

Corrective Action

When *param_names* is "name of the connected network of virtual L-Servers"

Refer to the format of the avmgr_network.rcxprop definition file and review the settings.

When *param_names* is "reserve_ip_address=true"

Check if "reserve_ip_address=true" exists in the l_server.rcxprop definition file.

When *param_names* is blank

No IP address has been loaded in the linked virtual L-Server.

Refer to "B.2 When the IP Address of a Linked Virtual L-Server Is Not Displayed in the Network Information for the Virtual L-Server", and take corrective action.

65905

FJSVrcx:ERROR:65905:Access to *filename* failed

Description

The content of the file specified in *filename* may not be in CSV format.

Corrective Action

Check whether the content of the file specified in *filename* is in CSV format.

65926

FJSVrcx:ERROR:65926:The file extension of *filename* is not supported.

Description

The requested import process was stopped because a file with an extension other than "csv" was specified for import.

Corrective Action

Specify a file with the extension "csv", and then perform the operation again.

65927

FJSVrcx:ERROR:65927:*filename* already exists

Description

The file you attempted to create already exists.

Corrective Action

Perform the operation again.

67101

FJSVrcx:ERROR:67101:not privileged

Description

The executing user is not an OS administrator.

Corrective Action

Execute the command with OS administrator privileges.

In Windows Server 2012 and later, it is not possible for user accounts that have administrator privileges but do not have the user name "Administrator" to execute commands with administrator privileges simply by starting the command prompt from the menu.

Right-click Command Prompt on the menu and select [Run as administrator] on the displayed menu to start a new command prompt, and then execute the command.

67117

FJSVrcx:ERROR:67117:*obj*:failed to create file or directory

Description

Creation of the *obj* file is not possible.

Corrective Action

Check the following, resolve the cause of the error, and then perform the operation again.

- Confirm the access privileges for the storage directory of the XML files for changing the network.

- Check if there is sufficient disk space available in the storage directory of the XML files for changing the network.

- Confirm the access privileges for the CSV configuration file.

- Check if there is sufficient disk space available in the storage directory of CSV configuration files.

- Confirm that the storage directory of CSV configuration files is specified using the full path.

- Confirm that the name of the storage directory of CSV configuration files is a character string containing alphanumeric characters, underscores ("_"), hyphens ("-"), and periods (".").

- Confirm that the content of the avmgr_network.rcxprop definition file is correct.

- Confirm that the IP address is contained in the network information of the linked virtual L-Server.

67126

FJSVrcx:ERROR:67126:*obj*:No such directory

Description

The specified directory does not exist.

Corrective Action

- Specify an existing directory.

- Confirm that the name of the storage directory of CSV configuration files is a character string containing alphanumeric characters, underscores ("_"), hyphens ("-"), and periods (".").

67129

FJSVrcx:ERROR:67129:syntax error

Description

The command syntax is incorrect. "Usage" is displayed.

Corrective Action

Check and correct the syntax of the command, and then perform the operation again.

67131

FJSVrcx:ERROR:67131:*option*:argument too long

Description

The specified option argument is too long.

Option may not be displayed.

Corrective Action

After checking and correcting the option argument specified in the CSV configuration file, perform the operation again.

67137

FJSVrcx:ERROR:67137:command is already running

Description

The command is currently being executed. This execution of the command will not be executed.

Corrective Action

Wait for the current execution to complete, and then execute the command again if necessary.

67140

FJSVrcx:ERROR:67140:*filename*:permission denied

Description

You do not have access privileges for the file specified for *filename*.

Corrective Action

Check the owner, the owning group, and the access privileges of the specified file.

67141

FJSVrcx:ERROR:67141:*filename*:write failed

Description

Writing to the file specified for *filename* failed.

Corrective Action

Check the system log, resolve the cause of the error, and then perform the operation again.

- Check if any error messages regarding the disk or file system were output

- Check if any messages indicating a quota limit or insufficient file system space were output

67146

FJSVrcx:ERROR:67146:filename:*file* not found

Description

The target file for the operation does not exist.

Corrective Action

When *file* is "avmgr_network.rcxprop"

Check if avmgr_network.rcxprop exists. If it does not exist, create it.

For details on avmgr_network.rcxprop, refer to "2.5.6 Definition File for Configuring the Business and Quarantine Networks".

67151

FJSVrcx:ERROR:67151:*filename*:remove failed

Description

Deletion of the Resource Orchestrator file *filename* failed.

Corrective Action

Check the following, resolve the cause of the error, and then perform the operation again.

- Check the system log for any error messages regarding the disk or file system

- Check if there are any programs referring to the specified CSV results file or its storage folder

67154

FJSVrcx:ERROR:67154:*obj*:not found

Description

After checking the following for the displayed object, perform the operation again.

- Is the VM name configured correctly?

- Does the specified folder exist?

- Does the VM host exist?

- Does the VM guest exist?

- Does the VM guest have a name that can be used for a virtual L-Server?

- Are there virtual L-Servers with the same name in different folders?

Corrective Action

When the VM name is not configured correctly

Specify the VM name correctly using the full path in the CSV configuration file.

When the specified folder is not found

Check if the specified folder exists. If it does not exist, create it.

When the VM host cannot be found

Check that the VM host is registered in the specified VM pool.

When the VM guest cannot be found

Check that the VM guest exists on the VM host.

In addition, check that the host name displayed for "DNS Name" in the corresponding virtual PC summary information in the VM management software matches the VM name configured in the CSV configuration file. If the names do not match, execute the rcxadm lserver convert command to link the virtual PC to a virtual L-Server.

For details, refer to "B.1 When Linking of Virtual PCs with Virtual L-Servers Fails".

When the VM guest name cannot be used as the virtual L-Server name

Execute the rcxadm lserver convert command to link this virtual PC to a virtual L-Server.

For details, refer to "B.1 When Linking of Virtual PCs with Virtual L-Servers Fails".

When virtual L-Servers with the same name exist in different folders

Environments in which virtual L-Servers with the same name exist in different folders are not supported.

Change the name of the virtual L-Server and ensure that there are no other virtual L-Servers with the same name.

67268

FJSVrcx:ERROR:67268:*filename*:no such file or directory

Description

The file or folder specified for *filename* does not exist.

Corrective Action

Specify an existing file or folder.

Confirm that the file name of the CSV configuration file does not contain characters other than alphanumeric characters, underscores ("_"), or hyphens ("-").

69133

FJSVrcx:ERROR:69133:operation not possible because power is OFF

Description

As the VM guest is powered off, the loading of it to a virtual L-Server has been canceled.

Corrective Action

Power on the VM guest, wait a couple of minutes, and then execute the command again.

5.3 Messages Output during Execution of the convertVMtoLServer Command or the rcxadm lserver Command

67280

FJSVrcx:ERROR:67280:*obj*:*function* not supported. *detail*

Description

obj does not support *function*.

In *function*, the name of the function that is not supported is displayed.

When *function* can be used with certain conditions, detailed information is displayed enclosed by parentheses in the following *function* or *detail*.

In cases other than the following, this message is displayed when you attempt to use a function that cannot be used by *obj*. No action is necessary.

- When *function* is "convert" and *detail* is "(already in use)"

The VM guest has already been linked to a virtual L-Server.

When the CSV file contains two or more lines with the same VM guest name but with a different host name, linking of the second and subsequent VM guests is not supported.

- When *function* is "create.xml" and *detail* is "(Two or more LNetworks)"

Creation of the XML for changing the network of virtual L-Servers with multiple NICs is not supported.

- When *function* is "convert with refreship" and *detail* is "(PhysicalLServer)"

The -refreship option cannot be specified for linking of physical L-Servers.

- When *function* is "convert with refreship" and *detail* is "(VMType)"

    - When using the rcxadm lserver convert command

    The -refreship option cannot be specified when linking virtual PCs that are not supported by Resource Orchestrator.

    - When using the convertVMtoLServer command

    It is not possible to link virtual PCs that are not supported by Resource Orchestrator.

[Citrix Xen]

    - When *function* is "convert" and *detail* is "(not assign a home server)"

    As Home Server settings have not been configured, linking to an L-Server cannot be performed.

Corrective Action

When *function* is "convert" and *detail* is "(already in use)"

When the CSV file contains two or more lines with the same VM guest name but with a different host name, link the failed VM guest with a virtual L-Server using the rcxadm lserver convert command.

For details on the rcxadm lserver command, refer to "4.3 rcxadm lserver".

In other cases, no action is necessary.

When *function* is "create.xml" and *detail* is "(Two or more LNetworks)"

Refer to "A.4 XML Files for Changing the Network" and create an XML file for changing the network that handles multiple NICs.

When *function* is "convert with refreship" and *detail* is "(PhysicalLServer)"

The -refreship option cannot be specified for linking of physical L-Servers.

When *function* is "convert with refreship" and *detail* is "(VMType)"

When using the rcxadm lserver convert command

When specifying the -refreship option, specify one of the following types of virtual PC supported by Resource Orchestrator for the -with option, and perform the operation again.

- VMware

- Hyper-V

- XenServer

For details on the rcxadm lserver command, refer to "4.3 rcxadm lserver".

When using the convertVMtoLServer command

Delete the information of virtual PCs that are not supported by Resource Orchestrator from the CSV configuration file specified in the -file option and then perform the operation again.

For details on the convertVMtoLServer command, refer to "4.2 convertVMtoLServer".

[Citrix Xen]

When *function* is "convert" and *detail* is "(not assign a home server)"

After configuring Home Server settings, wait for a while and then perform the operation again.

In other cases, no action is necessary.

5.4 Messages Output during Execution of the msgnotice Command

21180

FJSVrcx:INFO:21180:*obj*:*function* was performed

Description

The processing of the *function* for *obj* has been performed.

The name of the L-Server is displayed in *obj*.

- When "message notifying of disconnect" is displayed for *function*

A message was sent to the user when the L-Server was connected to the quarantine network.

- When "email notifying of disconnect" is displayed for *function*

When an action is executed on an L-Server upon detection of a malware infection, the tenant administrator is notified by email.

Corrective Action

No action is necessary.

41123

FJSVrcx:WARNING:41123:*obj*:*function* was aborted. detail=*detail*

Description

The processing of the *function* for *obj* has not been performed.

L-Server_name is displayed in *obj*.

The reason the processing of *function* was not performed is displayed for *detail*.

- When "message notifying of disconnect" is displayed for *function*

When executing an action upon detection of a malware infection on an L-Server, no notification message was sent to the user.

- When "email notifying of disconnect" is displayed for *function*

When executing an action upon detection of a malware infection on an L-Server, no notification message was sent to the tenant administrator.

Corrective Action

- When "message notifying of disconnect" is displayed for *function*

Processing of a VDI management server remote command failed. There are the following possibilities:

  - There is no connection information configured for the VDI management server, or there is a mistake in the connection information
  - The VDI management server is not operating correctly
  - The network settings of the VDI management server are incorrect

Check the connection information, operating status, and network settings of the VDI management server.

- When "email notifying of disconnect" is displayed for *function*

Processing of an SMTP server remote command failed.

Check the connection information, operating status, and network settings of the SMTP server.

When the cause is not one of the above, collect troubleshooting data, and contact Fujitsu technical staff.

67198

FJSVrcx:ERROR:67198:command execution error.*detail*

Description

An error has occurred during execution of a manager command.

The details of the message are displayed for *detail*.

Take corrective action for the content displayed for *detail*.

- "already registered"

  The connection information of the VDI management server specified in the msgnotice command has already been registered.

Corrective Action

The target VDI management server is already registered. No action is required.

5.5 Messages Output during Execution of the mailnotice Command

21180

FJSVrcx:INFO:21180:*obj*.*function* was performed

Description

The processing of the *function* for *obj* has been performed.

The name of the L-Server is displayed in *obj*.

- When "message notifying of disconnect" is displayed for *function*

  A message was sent to the user when the L-Server was connected to the quarantine network.

- When "email notifying of disconnect" is displayed for *function*

  When an action is executed on an L-Server upon detection of a malware infection, the tenant administrator is notified by email.

Corrective Action

No action is necessary.

41123

FJSVrcx:WARNING:41123:*obj.function* was aborted. detail=*detail*

Description

The processing of the *function* for *obj* has not been performed.

L-Server_name is displayed in *obj*.

The reason the processing of *function* was not performed is displayed for *detail*.

- When "message notifying of disconnect" is displayed for *function*

  When executing an action upon detection of a malware infection on an L-Server, no notification message was sent to the user.

- When "email notifying of disconnect" is displayed for *function*

  When executing an action upon detection of a malware infection on an L-Server, no notification message was sent to the tenant administrator.

Corrective Action

- When "message notifying of disconnect" is displayed for *function*

  Processing of a VDI management server remote command failed. There are the following possibilities:

  - There is no connection information configured for the VDI management server, or there is a mistake in the connection information

  - The VDI management server is not operating correctly

  - The network settings of the VDI management server are incorrect

  Check the connection information, operating status, and network settings of the VDI management server.

- When "email notifying of disconnect" is displayed for *function*

  Processing of an SMTP server remote command failed.

  Check the connection information, operating status, and network settings of the SMTP server.

When the cause is not one of the above, collect troubleshooting data, and contact Fujitsu technical staff.

67198

FJSVrcx:ERROR:67198:command execution error.*detail*

Description

An error has occurred during execution of a manager command.

The details of the message are displayed for *detail*.

Take corrective action for the content displayed for *detail*.

- "already registered"

  The connection information of the SMTP server has already been registered using the mailnotice command.

Corrective Action

The target VDI management server is already registered. No action is required.

5.6 [Symantec] Messages Output during Execution of the rcx_register_ror.ps1 Command

When the rcx_register_ror.ps1 command is executed using the PowerShell console on the Symantec Endpoint Protection Manager server, the message output to standard output will be one of the following.

INFO:210:Information registered successfully

Description

The environment definition file was created successfully.

Corrective Action

No action is necessary.

INFO:220:Registration canceled

Description

Creation of the environment definition file was canceled.

Corrective Action

No action is necessary.

INFO:230:Information already exists. Overwrite it? [y/n]

Description

The environment definition file already exists.

Corrective Action

To overwrite the existing environment definition file, enter "y", "Y", or "yes".

To not overwrite it, enter "n", "N", or "no".

INFO:240:Enter [y/Y/yes] or [n/N/no]

Description

A value other than "y", "Y", "yes", "n", "N", or "no" was entered.

Corrective Action

To overwrite the existing environment definition file, enter "y", "Y", or "yes".

To not overwrite it, enter "n", "N", or "no".

WARNING:410:No information found

Description

The environment definition file was not found. It may not have been created yet. "usage" is displayed.

Corrective Action

Create the environment definition file, and then perform the operation again.

ERROR:610:Invalid argument

Description

The command argument is invalid. "usage" is displayed.

Corrective Action

Check and correct the command argument, and then perform the operation again.

ERROR:620:Reading information failed

Description

Reading of the environment definition file failed.

Corrective Action

Check whether it is possible to access the environment definition file.

5.7 [Symantec] Messages Output to the Event Log of the Symantec Endpoint Protection Manager Server

The following messages are output to the event log of the Symantec Endpoint Protection Manager server when it notifies the Resource Orchestrator manager of security risks.

UUID:rcx_quarantine_lserver.bat Started

Level

INFORMATION

Source

JSE_SWRC_FJSVRCXMGR

Event ID

201

Description

Execution of the Symantec coordination batch file (rcx_quarantine_lserver.bat) has started.

For *UUID*, a UUID assigned to each process is displayed.

Corrective Action

No action is necessary.

UUID:rcx_quarantine_lserver.bat Completed

Level

INFORMATION

Source

JSE_SWRC_FJSVRCXMGR

Event ID

202

Description

Execution of the Symantec coordination batch file (rcx_quarantine_lserver.bat) has completed.

For *UUID*, a UUID assigned to each process is displayed.

Corrective Action

No action is necessary.

UUID:Quarantine L-server Failed

Level

ERROR

Source

JSE_SWRC_FJSVRCXMGR

Event ID

601

Description

Execution of the Symantec coordination script file (rcx_quarantine_lserver.ps1) failed.

For *UUID*, a UUID assigned to each process is displayed.

Corrective Action

Collect the event log (application log), and contact Fujitsu technical staff.

UUID:rcx_quarantine_lserver.ps1 Started

Level

INFORMATION

Source

JSE_SWRC_FJSVRCXMGR

Event ID

211

Description

Execution of the Symantec coordination script file (rcx_quarantine_lserver.ps1) has started.

For *UUID*, a UUID assigned to each process is displayed.

Corrective Action

No action is necessary.

UUID:Success to get IP address of L-server to quarantine:[IP Address]

Level

INFORMATION

Source

JSE_SWRC_FJSVRCXMGR

Event ID

212

Description

A security risk has occurred on the virtual PC or physical server with the IP address displayed in "*IP Address*".

For *UUID*, a UUID assigned to each process is displayed.

Corrective Action

No action is necessary.

UUID:rcx_quarantine_lserver.ps1 Completed

Level

INFORMATION

Source

JSE_SWRC_FJSVRCXMGR

Event ID

213

Description

Execution of the Symantec coordination script file (rcx_quarantine_lserver.ps1) has completed.

For *UUID*, a UUID assigned to each process is displayed.

Corrective Action

No action is necessary.

UUID:Failed to invoke API. Retry in 1 second

Level

WARNING

Source

JSE_SWRC_FJSVRCXMGR

Event ID

411

Description

An attempt to issue a REST API to the Resource Orchestrator manager to quarantine an L-Server failed.

Issuing will be re-attempted in one second.

For *UUID*, a UUID assigned to each process is displayed.

Corrective Action

No action is necessary.

UUID:rcx.config not exist

Level

ERROR

Source

JSE_SWRC_FJSVRCXMGR

Event ID

611

Description

The environment definition file (rcx.config) does not exist.

Corrective Action

Use the rcx_register_ror.ps1 create command to create the environment definition file.

UUID:Failed to read rcx.config

Level

ERROR

Source

JSE_SWRC_FJSVRCXMGR

Event ID

612

Description

Reading of the environment definition file (rcx.config) failed.

For *UUID*, a UUID assigned to each process is displayed.

Corrective Action

Check whether it is possible to access the environment definition file.

UUID:Argument not Exist

Level

ERROR

Source

JSE_SWRC_FJSVRCXMGR

Event ID

613

Description

The IP address of the virtual PC or physical server on which a security risk occurred was not received in a notification from Symantec Endpoint Protection Manager.

Preparation of Symantec Endpoint Protection Manager may not have been performed correctly.

For *UUID*, a UUID assigned to each process is displayed.

Corrective Action

Refer to "2.1 Preparations for Using the Automatic Quarantining Function" to confirm that the settings of antivirus software are correct.

UUID:Failed to get IP address

Level

ERROR

Source

JSE_SWRC_FJSVRCXMGR

Event ID

614

Description

The IP address of the virtual PC or physical server on which a security risk occurred could not be obtained from the notification from Symantec Endpoint Protection Manager.

Preparation of Symantec Endpoint Protection Manager may not have been performed correctly.

For *UUID*, a UUID assigned to each process is displayed.

Corrective Action

Refer to "2.1 Preparations for Using the Automatic Quarantining Function" to confirm that the settings of antivirus software are correct.

UUID:Failed to invoke API to ROR Manager. Detail = [detail]

Level

ERROR

Source

JSE_SWRC_FJSVRCXMGR

Event ID

615

Description

An attempt to issue a REST API to the Resource Orchestrator manager to quarantine an L-Server failed.

For *UUID*, a UUID assigned to each process is displayed.

In *detail*, the detailed message is displayed.

Corrective Action

- Use the rcx_register_ror.ps1 show command to check whether Resource Orchestrator user information is registered correctly.

- Check whether the Resource Orchestrator manager is operating correctly.

- Confirm the content of *detail*, and take corrective action.

If taking the above corrective action does not solve the problem, collect the Windows event log (application log) and troubleshooting data of the Resource Orchestrator manager, and contact Fujitsu technical staff.

UUID:Failed to invoke API to ROR Manager for 3 times. Detail = [detail]

Level

ERROR

Source

JSE_SWRC_FJSVRCXMGR

Event ID

616

Description

An attempt to issue a REST API to the Resource Orchestrator manager to quarantine an L-Server failed. Issuing of a REST API failed three times in a row due to a service being temporarily unavailable.

For *UUID*, a UUID assigned to each process is displayed.

In *detail*, the detailed message is displayed.

Corrective Action

- Use the rcx_register_ror.ps1 show command to check whether Resource Orchestrator user information is registered correctly.

- Check whether the Resource Orchestrator manager is operating correctly.

- Confirm the content of *detail*, and take corrective action.

If taking the above corrective action does not solve the problem, collect the Windows event log (application log) and troubleshooting data of the Resource Orchestrator manager, and contact Fujitsu technical staff.

5.8 [Trend Micro VB] [McAfee] Messages Output in the Event Log of the Resource Orchestrator Manager

In environments where there are multiple Resource Orchestrator managers, the messages output to the event log when antivirus software notifies the first manager of Resource Orchestrator of a security risk are as follow.

UUID:Send information of SNMP trap to remote manager [ip/fqdn] successfully. Request information: [detail]

Level

Information

Source

JSE_SWRC_FJSVRCXMGR

Event ID

217

Description

Transfer of the SNMP trap to the sub manager with the IP address or FQDN indicated in "ip/fqdn" was successful.

For UUID, a UUID assigned to each process is displayed.

Detailed information is displayed in detail.

Corrective Action

No action is necessary.

UUID:Target lserver not found in submanager. ip = [ip].

Level

Warning

Source

JSE_SWRC_FJSVRCXMGR

Event ID

413

Description

There is no L-Server configured with the IP address indicated in the "ip" included in SNMPTrap in the sub manager.

For UUID, a UUID assigned to each process is displayed.

Corrective Action

From the Resource Orchestrator manager, check whether the virtual machine or SBC server that is using the relevant IP address is linked to an L-Server.

When it is linked to the first manager of Resource Orchestrator, corrective action is not necessary.

UUID:No content in avmgr_submgr

Level

Warning

Source

JSE_SWRC_FJSVRCXMGR

Event ID

415

Description

There is no content in the environment definition file.

Corrective Action

When using a configuration in which there are multiple Resource Orchestrator managers, register the information of sub managers using the rcxadm submgr command.

When using a configuration in which there are not multiple Resource Orchestrator managers, delete the following environment definition file.

    Installation_folder\SVROR\Manager\etc\conf\avmgr_submgr

UUID:Failed to read remote_ror.rcxprop

Level

Error

Source

JSE_SWRC_FJSVRCXMGR

Event ID

615

Description

Reading of the environment definition file failed.

For UUID, a UUID assigned to each process is displayed.

Corrective Action

Register the information of sub managers using the rcxadm submgr command.

UUID:Argument not Exist

Level

Error

Source

JSE_SWRC_FJSVRCXMGR

Event ID

617

Description

As the argument was not found, collection of information of the machine that was the target of action execution failed.

Settings for notification from OfficeScan or McAfee ePolicy Orchestrator may be incorrect.

For UUID, a UUID assigned to each process is displayed.

Corrective Action

Check the settings for notification from OfficeScan or McAfee ePolicy Orchestrator.

UUID:Failed to access to remote Manager, IP/FQDN:[ip/fqdn]. Detail information:[detail]

Level

Error

Source

JSE_SWRC_FJSVRCXMGR

Event ID

618

Description

Issuing of the API to the sub manager with the IP address or FQDN indicated in "ip/fqdn" failed.

For UUID, a UUID assigned to each process is displayed.

Corrective Action

Perform either of the following corrective actions. However, when there are security risks for which notification was not sent, as the action to be performed automatically will not be performed, perform corrective action manually.

- Check whether the sub manager is operating normally. If it is not operating, start the sub manager.

- Check whether the authentication settings for remote management of the first manager are correct. If there are any mistakes in the settings, correct them.

  For details on the settings, refer to [Trend Micro VB Corp] [McAfee] in "2.8 Registering Sub Manager Information".

UUID:Failed to invoke API to ROR Manager. Detail = [Msg]

Level

Error

Source

JSE_SWRC_FJSVRCXMGR

Event ID

619

Description

Issuing of the API to the sub manager failed.

For UUID, a UUID assigned to each process is displayed.

Detailed information is displayed in "Msg".

Corrective Action

Perform one of the following corrective actions. However, when there are security risks for which notification was not sent, as the action to be performed automatically will not be performed, perform corrective action manually.

- Check whether the information registered for the sub manager is correct. If the information is incorrect, use the rcxadm submgr command to correct the sub manager information.

  For details on the rcxadm submgr command, refer to "4.7 rcxadm submgr".

- The name of the FQDN registered for the sub manager cannot be resolved. Take corrective action, such as registering it in the hosts file, etc., to enable resolution of the name.

- Check whether the sub manager is operating normally. If it is not operating, start the sub manager.

UUID:Failed to invoke API to ROR Manager for 3 times. Detail = [Msg]

Level

Error

Source

JSE_SWRC_FJSVRCXMGR

Event ID

631

Description

Issuing of the API to the sub manager failed.

For UUID, a UUID assigned to each process is displayed.

Detailed information is displayed in "Msg".

Corrective Action

- Check whether the information registered for the sub manager is correct.

- Check whether the sub manager is operating normally.

Chapter 6 Advisory Notes

This appendix provides advisory notes regarding this function.

6.1 VM Host VM Maintenance Mode

When a VM host is in VM maintenance mode, the transfer of L-Servers to the quarantine network and the recovery of L-Servers to the business network may fail with the following error.

When a VM host is in maintenance mode, release it from maintenance mode.

```
FJSVrcx:ERROR:62704:name:virtual switch not found on server server
```

6.2 When VMware DRS Is Enabled

In environments in which VMware DRS is enabled, if you edit the results output by the rcxadm pool list command and then perform batch loading of virtual PCs to L-Servers, relationships between VM hosts and virtual servers may be lost.

In such cases, it is necessary to confirm the relationships between VM hosts and virtual servers, and execute the batch loading of virtual PCs to L-Servers again.

For details on this command, refer to "4.8 rcxadm pool".

6.3 Notes When Performing Upgrade or Applying Patches to Resource Orchestrator Managers

When performing the following operations in an environment with the automatic quarantining function enabled, perform the operation check according to "2.14 Testing When Handling Security Risks" after the operation.

- Upgrading a Resource Orchestrator manager

- Applying patches to a Resource Orchestrator manager

Appendix A Customization of Definition Files

This appendix explains the settings that can be configured when customizing definition files.

A.1 Definition File of the Quarantine Policy for Security Risks

This section explains the definition file of the quarantine policy for security risks.

Purpose

Set the action to be performed on L-Servers when the Resource Orchestrator manager receives notification of a security risk from antivirus software.

It is not necessary to restart the services of the Resource Orchestrator manager after editing this type of definition file.

[Trend Micro OfficeScan]

By defining specific security risks it is possible to only execute the configured actions for the defined security risks.

Set the security risks that the following servers will send notification of to the Resource Orchestrator manager.

- OfficeScan 11.0 server

- OfficeScan XG server

The settings of the actions to perform are the default settings, and are the recommended ones.

Format of the Definition File

Location of the Definition File

[Windows Manager]

Installation_folder\SVROR\Manager\etc\customize_data

📘 Information

. . . .

The sample definition file (avmgr.rcxprop.sample) is stored in the location above.

When using the sample as the definition file, place the file after deleting the ".sample" included in the file name.

. . . .

Name of the Definition File

avmgr.rcxprop

Character Code

[Windows Manager]

UTF-8

Line Break Code

[Windows Manager]

CR/LF

Format of the Definition File

Describe the file using the following format.

```
avmgr.action = {quarantine|reboot|none|quarantine_reboot}
avmgr.action.<lserver_path> = {quarantine|reboot|none|quarantine_reboot }
```

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

[Trend Micro OfficeScan]

```
avmgr.corp.action_filter_base={ALL_ENABLE|ALL_DISABLE}
```

Definition File Items

avmgr.action

Specify the action to be taken against the L-Server when a security risk is detected. Specify the following actions. The default operation is "quarantine".

- quarantine : Quarantines the L-Server.

- reboot : Reboots the L-Server. When using a PVS (Provisioning Services) environment, use of this setting is recommended.

- quarantine_reboot : Quarantines the L-Server and then reboots it. When using a client OS that has a simultaneous connection count of 1, use of this setting is recommended.

- none : No action is performed. An email that enables selection of the action to take is sent to the email address of the tenant administrator set in "4.10 mailnotice". The tenant administrator selects how the security risk will be handled according to the content of the email.

Example
. . . .
```
avmgr.action = reboot
```

avmgr.action.<lserver_path>

Specify the action to be taken against the L-Server when a security risk is detected. For L-Servers which do not have this specified, the action specified in avmgr.action will be executed.

When rebooting L-Server "folder01/lsv01, folder01/lsv02"

Example
. . . .
avmgr.action./folder01/lsv01 = reboot

avmgr.action./folder01/lsv02 = reboot
. . . .

Note
. . . .
When setting action to "none", assign the virtual PC to a tenant so you can receive the email notification that enables selection of the action to perform after malware is detected, and use the email notification function.

When not using the email notification function, there is a possibility that response to malware infections may be delayed.

Specify a full path for *lserver_path*. For this reason, specify "/" at the start of the path even when specifying an L-Server in the root folder.
. . . .
. . . .

[Trend Micro OfficeScan]

avmgr.corp.action_filter_base

Specifies the quarantine policy for security risks for all notifications sent from the following servers to the Resource Orchestrator manager.

- OfficeScan 11.0 server

- OfficeScan XG server

Specify one of the following options:

- "ALL_ENABLE": When executing an action on an L-Server.

By using this in combination with "A.2 Definition files of keywords for exclusion from the targets of quarantining", it is possible to specify exclusion of security risks from executed actions.

- "ALL_DISABLE": When not executing an action on an L-Server.

By using this in combination with "A.3 Definition files of keywords for the targets of quarantining", it is possible to specify inclusion of security risks for executed actions.

"ALL_ENABLE" is specified in the following cases:

- When the specification of "avmgr.corp.action_filter_base" is omitted

- When an invalid value is specified

When "avmgr.corp.action_filter_base" is set more than once, the last specification will be valid.

📝 Example
. . . .
```
avmgr.corp.action_filter_base=ALL_DISABLE
```
. . . .

A.2 Definition files of keywords for exclusion from the targets of quarantining

This section explains the definition files of keywords for exclusion from the targets of quarantining.

Purpose

Using the definition files of keywords for exclusion from the targets of quarantining in combination with the definition file of the quarantine policy for security risks, it is possible to exclude security risks sent in notifications from one of the following servers to the Resource Orchestrator manager from execution of the selected action.

[Trend Micro OfficeScan]

- OfficeScan 11.0 server

- OfficeScan XG server

Create these definition files when "ALL_DISABLE" is not specified in "avmgr.corp.action_filter_base" in the definition file of the quarantine policy for security risks, and there are security risks that you want to exclude from execution of the selected action.

When "ALL_DISABLE" is specified in "avmgr.corp.action_filter_base", the content specified in these definition files is ignored.

It is not necessary to restart the services of the Resource Orchestrator manager after editing this type of definition file.

Format of the Definition File

Location of the Definition File

[Windows Manager]

Installation_folder\SVROR\Manager\etc\customize_data

📖 Information
. . . .
The sample definition file (avmgr_corp_filter_disable.en.rcxprop.sample) is stored in the location above.

When using the sample as the definition file, place the file after deleting the ".sample" included in the file name.
. . . .

Names of the Definition Files

avmgr_corp_filter_disable.en.rcxprop

Character Code

[Windows Manager]

UTF-8

Line Break Code

[Windows Manager]

CR/LF or LF

Format of the Definition File

Separate multiple keywords using line breaks (CR/LF or LF).

```
Keyword 1 for exclusion from the targets of quarantining
Keyword 2 for exclusion from the targets of quarantining
Keyword 3 for exclusion from the targets of quarantining
```

Definition File Items

For avmgr_corp_filter_disable.en.rcxprop

Alphanumeric characters and symbols (ASCII characters (0x20 - 0x7e)) can be used in keywords.

```
keyword1<line break (CR/LF or LF)>
keyword2<line break (CR/LF or LF)>
keyword3<line break (CR/LF or LF)>
...
```

When the Resource Orchestrator manager is notified of a security risk containing any of the specified keywords, the corresponding L-Server will be excluded from execution of the selected action.

💟 **Example**
· ·
```
keyword_of_unquarantine<line break (CR/LF or LF)>
```
· ·

A.3 Definition files of keywords for the targets of quarantining

This section explains the definition file of keywords for the targets of quarantining.

Purpose

Using the definition file of keywords for the targets of quarantining in combination with the definition file of the quarantine policy for security risks, it is possible to specify all security risks sent in notifications from one of the following servers to the Resource Orchestrator manager to be targets for execution of an action.

[Trend Micro OfficeScan]

- OfficeScan 11.0 server

- OfficeScan XG server

Create these definition files when "ALL_DISABLE" is specified in "avmgr.corp.action_filter_base" in the definition file of the quarantine policy for security risks, and there are security risks that you want to make the targets of execution of the selected action.

When "ALL_DISABLE" is not specified in "avmgr.corp.action_filter_base", the content specified in this definition file is ignored.

It is not necessary to restart the services of the Resource Orchestrator manager after editing this type of definition file.

Format of the Definition File

Location of the Definition File

[Windows Manager]

Installation_folder\SVROR\Manager\etc\customize_data

The sample definition file (avmgr_corp_filter_enable.en.rcxprop.sample) is stored in the location above.

When using the sample as the definition file, place the file after deleting the ".sample" included in the file name.

Names of the Definition Files

avmgr_corp_filter_enable.en.rcxprop

Character Code

[Windows Manager]

UTF-8

Line Break Code

[Windows Manager]

CR/LF or LF

Format of the Definition File

Separate multiple keywords using line breaks (CR/LF or LF).

```
Keyword 1 for the targets of quarantining
Keyword 2 for the targets of quarantining
Keyword 3 for the targets of quarantining
```

Definition File Items

For avmgr_corp_filter_enable.en.rcxprop

Alphanumeric characters and symbols (ASCII characters (0x20 - 0x7e)) can be used in keywords.

```
keyword1<line break (CR/LF or LF)>
keyword2<line break (CR/LF or LF)>
keyword3<line break (CR/LF or LF)>
...
```

When the Resource Orchestrator manager receives notification of a security risk containing any of the specified keywords, the corresponding L-Server will be quarantined.

Example

```
keyword_of_quarantine<line break (CR/LF or LF)>
```

A.4 XML Files for Changing the Network

This section explains the XML files for changing the network.

A.4.1 XML Files for Changing the Connected Network of Virtual L-Servers to the Quarantine Network

This section explains XML files for changing the connected network of virtual L-Servers to the quarantine network.

Purpose

The XML files necessary for changing the connected network of virtual L-Servers to the quarantine network.

Creation and storing of XML files for changing the network to the quarantine network is possible even when Resource Orchestrator is operating.

Creating XML Files for Changing the Network to the Quarantine Network

1. Execute the following command to output the base XML file for changing the network.

```
> rcxadm lserver show -name L-Server_name -format xml
```

2. Delete any unnecessary information from the output XML file and edit the content as shown in "Format of XML Files for Changing the Network of Virtual L-Servers".

   The Resources, LServer, and NICs elements must be included.

   Depending on the details of the quarantine network, modify the values for "name" in the NetworkLink element and "address" in the IpAddress element.

Format of XML Files for Changing the Network of Virtual L-Servers

```xml
<?xml version="1.0" encoding="utf-8"?>
<Resources>
  <LServer name="L-Server_name">
    <NICs>
      <NIC>
        <NICIndex>NIC_index</NICIndex>
        <MacAddress>MAC_address</MacAddress>
        <NetworkLinks>
          <NetworkLink name="Network_name" index="0">
            <IpAddress auto="Automatic_IP_configuration" address="IP_address"/>
          </NetworkLink>
        </NetworkLinks>
      </NIC>
    </NICs>
  </LServer>
</Resources>
```

Table A.1 Excerpt from Definition Information for Virtual L-Servers (XML)

Element Name	Description	Remarks (Possible Values, Examples)
Network_name (NetworkLink name)	Name of the network that the L-Server connects to	Specify the name of an existing network resource. - When modifying an L-Server linked with a configured virtual PC Modification of a *Network* name is performed for the NIC corresponding to the specified MAC address. Therefore, ensure a MAC Address is specified.
MAC_address (MacAddress)	The MAC address to allocate to the L-Server NIC	When modifying an IP address and a Network name, ensure the MAC address is specified using the following format. <MacAddress>XX:XX:XX:XX:XX:XX</MacAddress> In addition, changing of MAC addresses cannot be performed.
IP_address (IpAddress)	IP address to allocate to the L-Server (optional)	The IP address can be specified using the following methods: - When specifying an IP address directly <IpAddress auto="false" address="xxx.xxx.xxx.xxx"/> - When assigning an IP address automatically from the address range set for the network resource <IpAddress auto="true"/> When the IP address of the virtual PC is managed using DHCP, do not specify the IpAddress element. Even if the IpAddress element is omitted, an IP address is automatically assigned from the address range set for the network resource. Modification of an IP address is performed for the NIC corresponding to the specified MAC address. Therefore, ensure a MAC Address is specified.

See

For details on the definition information for virtual L-Servers (XML), refer to the following manuals.

- "15.3.2 Definition Information for Virtual L-Servers (XML)" in the "Reference Guide (Command/XML) CE"

Storage Location of XML Files for Changing the Network to the Quarantine Network

[Windows Manager]

Installation_folder\SVROR\Manager\etc\files\avmgr

Name of the XML File for Changing the Network to the Quarantine Network

quarantine_*L-Server_name*.xml

Information

- For environments where multiple NICs are connected

When an L-Server in which multiple NICs are defined is quarantined, enter as many lines enclosed by the NIC elements as the defined NICs to set each NIC so all the NICs will be connected to the quarantine network.

Specifying the same network for each NIC will cause no problems.

- When modifying the default value of the storage directory of the XML files

To modify the default value of the storage directory of the XML files, create the definition file.

For details on the definition results file, refer to "A.5 Definition File of the Storage Directory of the XML Files for Changing the Network".

A.4.2 XML Files for Changing the Connected Network of Virtual L-Servers to the Operation Network

This section explains the network definition information (XML) for changing the connected network of virtual L-Servers to the operation network.

Purpose

The XML files necessary for changing the connected network of virtual L-Servers to the operation network.

Creation and storing of XML files for changing the network to the operation network is possible even when Resource Orchestrator is operating.

Creating XML Files for Changing the Network to the Operation Network

1. Execute the following command to output the base XML file for changing the network.

```
> rcxadm lserver show -name L-Server_name -format xml
```

2. Delete any unnecessary information from the output XML file and edit the content as shown in "Format of XML Files for Changing the Network of Virtual L-Servers".

The Resources, LServer, and NICs elements must be included.

Depending on the details of the operation network, modify the values for "name" in the NetworkLink element and "address" in the IpAddress element.

Format of XML Files for Changing the Network to the Operation Network

For details, refer to "Format of XML Files for Changing the Network of Virtual L-Servers".

Storage Location of XML Files for Changing the Network to the Operation Network

[Windows Manager]

Installation_folder\SVROR\Manager\etc\files\avmgr

Name of the XML File for Changing the Network to the Operation Network

unquarantine_*L-Server_name*.xml

Information

. . . .

- For environments where multiple NICs are connected

When an L-Server in which multiple NICs are defined is quarantined, enter as many lines enclosed by the NIC elements as the defined NICs to set each NIC so all the NICs will be connected to the operation network.

Specifying the same network for each NIC will cause no problems.

- When modifying the default value of the storage directory of the XML files

To modify the default value of the storage directory of the XML files, create the definition file.

For details on the definition results file, refer to "A.5 Definition File of the Storage Directory of the XML Files for Changing the Network".

. . . .

A.4.3 XML Files for Changing the Network of Physical L-Servers from the Operation Network to the Quarantine Network

This section explains XML files for changing the network of physical L-Servers from the operation network to the quarantine network.

Purpose

The XML files necessary for changing the network physical L-Servers are connected to from the operation network to the quarantine network.

Creation and storing of XML files for changing the network to the quarantine network is possible even when Resource Orchestrator is operating.

Creating XML Files for Changing the Network to the Quarantine Network

1. Execute the following command to output the base XML file for changing the network.

```
> rcxadm lserver show -name L-Server_name -format xml
```

2. Delete any unnecessary information from the output XML file and edit the content as shown in "Format of XML Files for Changing the Network of Physical L-Servers".

The Resources, LServer, and NICs elements must be included.

Depending on the details of the quarantine network, modify the values for "name" in the NetworkLink element and "address" in the IpAddress element.

Format of XML Files for Changing the Network of Physical L-Servers

```
<?xml version="1.0" encoding="utf-8"?>
<Resources>
  <LServer name="L-Server_name">
    <NICs>
      <NIC>
        <NICIndex>NIC_index</NICIndex>
        <MacAddress auto="false"></MacAddress>
        <NetworkLinks>
          <NetworkLink name="Network_name" index="Network_index" vlan_mode="VLAN_mode">
            <IpAddress auto="Automatic_IP_configuration" address="IP_address"/>
          </NetworkLink>
        </NetworkLinks>
      </NIC>
      <NIC>
```

```
            <NICIndex>NIC_index</NICIndex>
            <MacAddress auto="false"></MacAddress>
            <NetworkLinks>
              <NetworkLink name="Network_name" index="Network_index" vlan_mode="VLAN_mode">
                 <IpAddress auto="Automatic_IP_configuration" address="IP_address"/>
              </NetworkLink>
            </NetworkLinks>
          </NIC>
             *Specify as many NIC elements as the number of management network and business network NICs
       </NICs>
     </LServer>
</Resources>
```

Table A.2 Excerpt from Definition Information for Physical L-Servers (XML)

Element Name	Description	Remarks (Possible Values, Examples)
NIC index (NICIndex)	Number to identify the NIC definition to allocate to the L-Server	Specify an integer between 0 and 31 starting with "0". For physical L-Servers, specify the NIC number defined for the rack mount server decided in "9.3.5 Pre-configuring Managed Servers" in the "Design Guide CE" with 1 subtracted from it. 📝 **Example** . . . . If the NIC number of the leftmost NIC on the back of a rack mount server was defined as "1" in "9.3.5 Pre-configuring Managed Servers" in the "Design Guide CE", specify "0" here. . . . .

VLAN mode
 	
(NetworkLink vlan_mode)
	VLAN mode
	
	(optional)
		Specify a VLAN mode.
		
		The IP address can be specified using the following methods:
		  - Untagged VLAN communication
		    vlan_mode="untagged"
		  - Tagged VLAN communication
		    vlan_mode="tagged"
		
		When vlan_mode is omitted, tagged VLAN communication is used.

MAC_address (MacAddress)	The MAC address to allocate to the L-Server NIC	The WWN can be specified using the following methods: <MacAddress auto="false"></MacAddress>
Network_name (NetworkLink name)	Name of the network that the L-Server connects to	Specify the name of an existing network resource. If the target network resource is an admin LAN resource, specify "untagged" for vlan_mode. As a quarantine network resource cannot be an admin LAN resource, this condition does not apply when changing the definition of the quarantine network.
Network_index (Index)	The network index	Specify a network index. The index starts from "0".

IP_address
 	
(IpAddress)
	IP address to allocate to the L-Server	The IP address can be specified using the following methods:
		  - When specifying an IP address directly
		    <IpAddress auto="false" address="xxx.xxx.xxx.xxx"/>
		  - When assigning an IP address automatically from the address range set for the network resource
		    <IpAddress auto="true"/>

Element Name	Description	Remarks (Possible Values, Examples)
		Even if the IpAddress element is omitted, an IP address is automatically assigned from the address range set for the network resource.

📇 See
....

For details on the definition information for physical L-Servers (XML), refer to the following manual.

- "15.3.1 Definition Information for Physical L-Servers (XML)" in the "Reference Guide (Command/XML) CE"

....

Storage Location of XML Files for Changing the Network to the Quarantine Network

[Windows Manager]

Installation_folder\SVROR\Manager\etc\files\avmgr

Name of the XML File for Changing the Network to the Quarantine Network

quarantine_*L-Server_name*.xml

📖 Information
....

- For environments where multiple NICs are connected

When an L-Server in which multiple NICs are defined is quarantined, enter as many lines enclosed by the NIC elements as the defined NICs to set each NIC so all the NICs will be connected to the quarantine network.

Specifying the same network for each NIC will cause no problems.

- When modifying the default value of the storage directory of the XML files

To modify the default value of the storage directory of the XML files, create the definition file.

For details on the definition results file, refer to "A.5 Definition File of the Storage Directory of the XML Files for Changing the Network".

....

A.4.4 XML Files for Changing the Connected Network of Physical L-Servers to the Operation Network

This section explains the network definition information (XML) for changing the connected network of physical L-Servers to the operation network.

Purpose

The XML files necessary for changing the connected network of physical L-Servers to the operation network.

Creation and storing of XML files for changing the network to the operation network is possible even when Resource Orchestrator is operating.

Creating XML Files for Changing the Network to the Operation Network

1. Execute the following command to output the base XML file for changing the network.

```
> rcxadm lserver show -name L-Server_name -format xml
```

2. Delete any unnecessary information from the output XML file and edit the content as shown in "Format of XML Files for Changing the Network of Physical L-Servers".

The Resources, LServer, and NICs elements must be included.

Depending on the details of the operation network, modify the values for "name" in the NetworkLink element and "address" in the IpAddress element.

Format of XML Files for Changing the Network to the Operation Network

For details, refer to "Format of XML Files for Changing the Network of Physical L-Servers".

Storage Location of XML Files for Changing the Network to the Operation Network

[Windows Manager]

Installation_folder\SVROR\Manager\etc\files\avmgr

Name of the XML File for Changing the Network to the Operation Network

unquarantine_*L-Server_name*.xml

Information

- For environments where multiple NICs are connected

When an L-Server in which multiple NICs are defined is quarantined, enter as many lines enclosed by the NIC elements as the defined NICs to set each NIC so all the NICs will be connected to the operation network.

Specifying the same network for each NIC will cause no problems.

- When modifying the default value of the storage directory of the XML files

To modify the default value of the storage directory of the XML files, create the definition file.

For details on the definition results file, refer to "A.5 Definition File of the Storage Directory of the XML Files for Changing the Network".

A.5 Definition File of the Storage Directory of the XML Files for Changing the Network

This section explains the definition file of the storage directory of the XML files for changing the network.

Purpose

Create this definition file when you wish to modify the default value of the storage directory of the XML files for changing the network.

The default value for the storage directory of the XML files for changing the network which are used during the quarantining of L-Servers by this function is as follows.

Default Storage Directory of the XML Files for Changing the Network

[Windows Manager]

Installation_folder\SVROR\Manager\etc\files\avmgr

It is not necessary to restart the services of the Resource Orchestrator manager after editing this type of definition file.

Format of the Definition File

Location of the Definition File

[Windows Manager]

Installation_folder\SVROR\Manager\etc\customize_data

Information

The sample definition file (avmgr.rcxprop.sample) is stored in the location above.

When using the sample as the definition file, place the file after deleting the ".sample" included in the file name.

Name of the Definition File

avmgr.rcxprop

Character Code

[Windows Manager]

UTF-8

Line Break Code

[Windows Manager]

CR/LF

Format of the Definition File

Describe the file using the following format.

```
avmgr.lserver_xml_dir=Storage_directory
```

Definition File Items

avmgr.lserver_xml_dir

Specify the storage directory of the XML files for changing the network.

If the specified directory does not exist, the transfer of L-Servers to the quarantine network and the recovery of L-Servers to the operation network will fail.

When the format of the definition file is incorrect, the default value is used for the storage directory of the XML files for changing the network.

📝 **Example**

. . . .

```
avmgr.lserver_xml_dir=c:\xml
```

. . . .

A.6 Network Configuration Information XML File

The XML definition for network configuration information is shown below.

- XML definitions for creation of individual network devices

```xml
<?xml version="1.0" encoding="utf-8"?>
<Netdevice ip="Admin IP Address" name="Device Name">
  <Location>Location</Location>
  <Types>
    <Type>Type</Type>
  </Types>
  <Maintenance>Maintenance Mode</Maintenance>
  <AutoConfiguration>Auto-Configuration for Network Device</AutoConfiguration>
  <DeviceInfo>
    <SysObjectId>sysObjectID</SysObjectId>
    <Vendor>Vendor Name</Vendor>
    <ProductName>Device Name</ProductName>
    <ModelName>Model Name</ModelName>
    <Firmware>Firmware</Firmware>
  </DeviceInfo>
  <Redundancy group_id="Group ID"></Redundancy>
  <MgmtInfos>
    <Snmps>
      <ReadCommunity>Community Name</ReadCommunity>
    </Snmps>
    <LoginInfos>
      <LoginInfo="Protocol" auth_type="Management Method for Authentication Information"
authority="Administrator Authority" check="Account Confirmation">
        <IpAddress>Destination IP Address</IpAddress>
        <Port>Destination Port Number</Port>
```

```
        <User>Account</User>
        <Password>Password</Password>
        <PrivilegedPassword>Administrator Password</PrivilegedPassword>
        <PasswordEncryption>Password Encryption</PasswordEncryption>
      </LoginInfo>
    </LoginInfos>
    <Monitoring>
      <Methods>
        <Method>Monitoring method</Method>
      </Methods>
      <Interval>Monitoring interval</Interval>
      <RetryCount>Retry Count</RetryCount>
      <Timeout>Timeout</Timeout>
    </Monitoring>
    <MgmtURL>Web Management Window URL</MgmtURL>
  </MgmtInfos>
  <Ports>
    <Port name="Port Name">
      <Description>Port Overview</Description>
      <PhysicalState>Communication Status</PhysicalState>
      <Link ip="Management IP address for Link Destination Device" port="Port Name of Link
Destination" kind="Type of Link Destination Device" />
    </Port>
  </Ports>
</Netdevice>
```

- XML definitions for batch creation of multiple network devices

```
<?xml version="1.0" encoding="utf-8"?>
<NetConfig>
<Netdevices>
  <Mode>Registration Mode</Mode>
  <Netdevice ip="Admin IP Address" name="Device Name">
    <Location>Location</Location>
    <Types>
      <Type>Type</Type>
    </Types>
    <Maintenance>Maintenance Mode</Maintenance>
    <AutoConfiguration>Auto-Configuration for Network Device</AutoConfiguration>
    <DeviceInfo>
      <SysObjectId>sysObjectID</SysObjectId>
      <Vendor>Vendor Name</Vendor>
      <ProductName>Device Name</ProductName>
      <ModelName>Model Name</ModelName>
      <Firmware>Firmware</Firmware>
    </DeviceInfo>
    <Redundancy group_id="Group ID"></Redundancy>
    <MgmtInfos>
      <Snmps>
        <ReadCommunity>Community Name</ReadCommunity>
      </Snmps>
      <LoginInfos>
        <LoginInfo="Protocol" auth_type="Management Method for Authentication Information"
authority="Administrator Authority" check="Account Confirmation">
          <IpAddress>Destination IP Address</IpAddress>
          <Port>Destination Port Number</Port>
          <User>Account</User>
          <Password>Password</Password>
          <PrivilegedPassword>Administrator Password</PrivilegedPassword>
          <PasswordEncryption>Password Encryption</PasswordEncryption>
        </LoginInfo>
      </LoginInfos>
      <Monitoring>
```

```
              <Methods>
                <Method>Monitoring method</Method>
              </Methods>
              <Interval>Monitoring interval</Interval>
              <RetryCount>Retry Count</RetryCount>
              <Timeout>Timeout</Timeout>
            </Monitoring>
            <MgmtURL>"Web Management Window URL"</MgmtURL>
          </MgmtInfos>
          <Ports>
            <Port name="Port Name">
              <Description>Port Overview</Description>
              <PhysicalState>Communication Status</PhysicalState>
              <Link ip="Management IP address for Link Destination Device" port="Port Name of Link
Destination" kind="Type of Link Destination Device" />
            </Port>
          </Ports>
        </Netdevice>
      </Netdevices>
      <Links>
        <Mode>Link Information Registration Mode</Mode>
        <Link>
          <Devices>
            <Device ip="Admin IP Address of Device 1" name="Resource Name of Device 1" kind="Type of
Device 1">
              <Port>Connection Port Name of Device 1</Port>
            </Device>
            <Device ip="Admin IP Address of Device 2" name="Resource Name of Device 2" kind="Type of
Device 2">
              <Port>Connection Port Name of Device 2 </Port>
            </Device>
          </Devices>
        </Link>
      </Links>
    </NetConfig>
```

Table A.3 List of Items Specified in XML Definitions for Network Configuration Information (Excerpt)

Element Name	Description	Remarks (Possible Values, Examples)	Specification				Output Using Export
			Individual Registration	Individual Modification	Batch Registration	Batch Modification	
Network configuration information (NetConfig)	A collection of network configuration information	-	Not possible	Not possible	Mandatory	Mandatory	Yes
Network device information (Netdevices)	A collection of network device information	Specify one or more Netdevice elements. When registering two or more network devices for resources simultaneously, this element cannot be omitted.	Not possible	Not possible	Optional	Optional	Yes (*1)
Registration mode (Mode)	Registration mode	Specify the registration mode of the network device. Specify either of the following options: - add New registration	Not possible	Not possible	Optional	Mandatory	No

Element Name	Description	Remarks (Possible Values, Examples)	Specification				Output Using Export
			Individual Registration	Individual Modification	Batch Registration	Batch Modification	

		Network device information is not overwritten when the specified management IP address has already been used to register another resource.
		
		- modify
		
		  Modification
		
		  Network device information is overwritten when the specified management IP address has already been used to register another resource.
		
		If left blank, "add" is specified.					

Admin IP address (Netdevice ip)	Admin IP address for the network device	Specify an IPv4 address.	Mandatory	Optional	Mandatory	Mandatory	Yes
Device Name (Netdevice name)	Name of the network device	Specify a character string containing up to 32 alphanumeric characters, underscores ("_"), hyphens ("-"), and periods ("."). If left blank, the host name or IP address obtained from the network device is specified. If characters other than alphanumeric characters, underscores ("_"), hyphens ("-"), and periods (".") are used in the host name obtained from the network device, they will be replaced with underscores ("_"). However, when the obtained value is 33 characters or longer, only the first 32 characters will be specified.	Optional	Optional	Optional	Optional	Yes
Location (Location)	Location	Specify a character string containing up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").	Optional	Optional	Optional	Optional	Yes (*2)

Element Name	Description	Remarks (Possible Values, Examples)	Specification				Output Using Export
			Individual Registration	Individual Modification	Batch Registration	Batch Modification	
		If left blank, the location obtained from the network device is specified. If characters other than alphanumeric characters, underscores ("_"), hyphens ("-"), and periods (".") are used in the location obtained from the network device, they will be replaced with underscores ("_"). However, when the obtained value is 33 characters or longer, only the first 32 characters will be specified.					
Type Information (Types)	A collection of type information	Specify one or more Type elements.	Optional	Optional	Optional	Optional	Yes (*1)
Type (Type)	Network device type	Specify the type of the network device. Specify the following. - L2-Switch When omitted, the type obtained from the Network Device Model Definitions is specified.	Optional	Optional	Optional	Optional	Yes (*2)

Maintenance Mode (Maintenance)	Maintenance mode settings	Specify the status of maintenance mode. Specify either of the following options:
		 - true
		   Maintenance Mode
		 - false
		   Normal
		 If left blank, "false" is specified.
			Optional	-	Optional	-	Yes

Auto-configuration for the network device (AutoConfiguration)	Auto-configuration for network devices	Specify whether the network device can be selected as a target of auto-configuration. Specify either of the following options: - true Target of auto-configuration - false	Optional	Optional	Optional	Optional	No

Element Name	Description	Remarks (Possible Values, Examples)	Specification				Output Using Export
			Individual Registration	Individual Modification	Batch Registration	Batch Modification	
		Not the target of auto-configuration If left blank, "true" is specified. When the operational status of the network device is "error", changing the value to "false" is not possible.					
Device information (DeviceInfo)	Device information	Specify the information of the model of the network device.	Optional	-	Optional	-	Yes
SysObjectId (SysObjectId)	SysObjectId	When monitoring using SNMP, SysObjectID collected automatically is specified as an OID in number and period format.	-	-	-	-	Yes
Vendor Name (Vendor)	Vendor Name	Specify a character string beginning with an alphanumeric character and containing up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-"). Specify the same arbitrary name as used for the Vendor name of the folder where the rulesets for network resources (network device-specific) are registered. When omitted, the vendor name obtained from the Network Device Model Definitions is specified.	Optional	-	Optional	-	Yes
Device name (ProductName)	Device name (product name)	Specify a character string beginning with an alphanumeric character and containing up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-"). Specify the same arbitrary name as used for the unit_name or model_name of the folder where the rulesets for network resources (network device-specific) are registered.	Optional	-	Optional	-	Yes

Element Name	Description	Remarks (Possible Values, Examples)	Specification				Output Using Export
			Individual Registration	Individual Modification	Batch Registration	Batch Modification	
		When omitted, the unit name obtained from the Network Device Model Definitions is specified.					
Model Name (ModelName)	Model Name	Specify a character string beginning with an alphanumeric character and containing up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-"). Specify the same arbitrary name as used for the unit_name or model_name of the folder where the rulesets for network resources (network device-specific) are registered. When omitted, the model name obtained from the Network Device Model Definitions is specified.	Optional	-	Optional	-	Yes
Firmware (Firmware)	Firmware or IOS version	A character string is specified. Specification is unnecessary as it is automatically collected from the network device.	-	-	-	-	Yes
Group ID (Redundancy group_id)	Group ID	Specify a character string beginning with an alphanumeric character and containing up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-"). For the network devices belonging to the same group ID, use the same vendor name and device name.	Optional	Optional	Optional	Optional	Yes (*2)
Management information (MgmtInfos)	A collection of management information	Specify one or more Snmps elements, LoginInfo elements, or other similar elements.	Mandatory	Optional	Mandatory	Optional	Yes
SNMP Information (Snmps)	A collection of SNMP information	Specify the ReadCommunity element once.	Optional	Optional	Optional	Optional	Yes
Community name	Community name	Specify a character string containing up to 32 alphanumeric characters,	Optional (*10)	Optional	Optional (*10)	Optional	Yes

Element Name	Description	Remarks (Possible Values, Examples)	Specification				Output Using Export
			Individual Registration	Individual Modification	Batch Registration	Batch Modification	
(ReadCommunity)	(This cannot be omitted when specifying SNMP information)	underscores ("_"), and hyphens ("-").					
Login Information (LoginInfos)	A collection of login information	Specify one or more LoginInfo elements.	Optional	Optional	Optional	Optional	Yes (*1)
Protocol (LoginInfo protocol)	Protocol	Specify the protocol used when logging in using login information. Specify one of following items. - remote_login Specify when using Telnet or SSH login information. If login via Telnet is possible, use Telnet. If login via Telnet is not possible, use SSH. - telnet Specify when using Telnet login information. - ssh Specify when using SSH login information. When omitted, "remote_login" is specified.	Optional	Optional	Optional	Optional	Yes
Management method for authentication information (LoginInfo auth_type)	Management method for authentication information	Specify the management method for the authentication information. When the information is managed within a network device, specify "local password". If omitted, it will be automatically specified.	Optional	Optional	Optional	Optional	Yes (*3)
Administrator authority (LoginInfo authority)	Presence or absence of administrator authority	Specify the type of authority for the account. Specify either of the following options: - user Specify when it is possible to connect to the	Optional	Optional	Optional	Optional	Yes (*3)

Element Name	Description	Remarks (Possible Values, Examples)	Specification				Output Using Export
			Individual Registration	Individual Modification	Batch Registration	Batch Modification	
		target network device using an account with user privileges (the account specified for "Account (User)") and then switch to administrator privileges to modify definitions. - admin Specify only when it is possible to change the definition for the device to register using an account with administrator privileges (the account specified for "Account (User)"). When omitted, "user" is specified.					

Account confirmation
 	
(LoginInfo check)
	Presence or lack of account information checks	Specify whether to check the account information when the registration or modification is performed.
		
		Specify either of the following options:
		
		- true
		
		  Checking is performed. (*4)
		
		- false
		
		  Checking is not performed.
		
		If left blank, "false" is specified.
			Optional	Optional	Optional	Optional	No

Destination IP address (IpAddress)	Destination IP address	Specify the IP address in IPv4 format. Specify when performing checks of the auto-configuration settings for the network device and account information (when "true" is specified for the account check (LoginInfo check)) from an IP address other than the admin IP address (Netdevice ip). When a different IP address is specified, or partially	Optional	Optional	Optional	Optional	Yes (*3)

Element Name	Description	Remarks (Possible Values, Examples)	Specification				Output Using Export
			Individual Registration	Individual Modification	Batch Registration	Batch Modification	
		omitted, the auto-configuration settings for the network device and the account information of the connection IP address (IpAddress) in the login information with "user" specified in the administrator privileges (LoginInfo authority) are checked. If left blank, the admin IP address (Netdevice ip) is specified.					
Destination port number (Port)	Port number of the protocol to connect the destination	Specify an integer between 1 and 65535. Specify the port number of the network device to perform checking of auto-configuration settings and account information (when "true" is specified for the account check (Login Info check)). When a different port number is specified, or partially omitted, the auto-configuration settings for the network device and the account information of the port number in the login information with "user" specified in the administrator privileges (LoginInfo authority) are checked. If left blank, one of the following is specified based on the value specified for the protocol (LoginInfo protocol). - 23 or 22 For "remote_login" The default value (23 or 22) for the protocol (Telnet or SSH) that was successful when checking the account information is specified. However, when not performing a check of the	Optional	Optional	Optional	Optional	Yes (*3)

Element Name	Description	Remarks (Possible Values, Examples)	Specification				Output Using Export
			Individual Registration	Individual Modification	Batch Registration	Batch Modification	
		account information (when "false" is specified for the account check (LoginInfo check)), the default value for Telnet (23) is specified. - 21 For "ftp" - 23 For "telnet" - 22 For "ssh"					
Account (User)	User account for connection	When "user" is specified for Administrator authority (LoginInfo authority), specify an account with user privileges. When "admin" is specified for Administrator authority (LoginInfo authority), specify an account with administrator privileges. For the account, specify a character string containing up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").	Optional (*11)	Optional (*11)	Optional (*11)	Optional (*11)	Yes (*3)
Password (Password)	Password for connection	Specify a character string of up to 64 alphanumeric characters and symbols (!$% ()*+,-./:;=@[]^_`{|}~ and spaces).	Mandatory	Optional (*11)	Mandatory	Optional (*11)	Yes (*3)
Administrator password (PrivilegedPass word)	Administrator password	Specify a character string of up to 64 alphanumeric characters and symbols (!$% ()*+,-./:;=@[]^_`{|}~ and spaces). When "admin" is specified for Administrator authority (LoginInfo authority), the administrator password is regarded as invalid.	Optional	Optional	Optional	Optional	Yes (*3)
Password encryption (PasswordEncry ption)	Presence or absence of password encryption	Specify whether the password of the network device is encrypted. Specify either of the following options:	Optional	Optional	Optional	Optional	Yes (*3)

Element Name	Description	Remarks (Possible Values, Examples)	Specification				Output Using Export
			Individual Registration	Individual Modification	Batch Registration	Batch Modification	
		- true Encrypted - false Not encrypted If left blank, "false" is specified. Specify "false" for initial registration as the password is entered in plain text at that time. When exporting the information, the password will be encrypted and "true" is set for this element to ensure security. Specify "true" only when registering an external server using an encrypted password.					
Monitoring Information (Monitoring)	Monitoring Information	Specify the element of monitoring information.	Optional	Optional	Optional	Optional	Yes
Monitoring method information (Methods)	Collection of monitoring method information	Specify the monitoring method by specifying one or more Method elements. When this element is omitted, the following will be specified. - SNMP	Optional	Optional	Optional	Optional	Yes
Monitoring method (Method)	Monitoring method	Specify the monitoring method for the network device. Specify one of following items. - ping When using ping monitoring - SNMP When using SNMP monitoring When omitted, "no monitoring" is specified for monitoring of the network device.	Optional	Optional	Optional	Optional	Yes

Element Name	Description	Remarks (Possible Values, Examples)	Specification				Output Using Export
			Individual Registration	Individual Modification	Batch Registration	Batch Modification	
		When specifying multiple monitoring methods, specify multiple entries of this element.					
Monitoring interval (Interval) (*5)	Monitoring interval (seconds) (This cannot be omitted when modifying the monitoring method)	Specify an integer between 1 and 86400. If left blank, "300" is set.	Optional	Optional	Optional	Optional	Yes
Retry count (RetryCount) (*5)	Retry count (This cannot be omitted when modifying the monitoring method)	Specify an integer between 1 and 10. If left blank, "3" is specified.	Optional	Optional	Optional	Optional	Yes
Timeout (Timeout) (*5)	Timeout (seconds) (This cannot be omitted when modifying the monitoring method)	Specify an integer between 1 and 300. If left blank,"30" is specified.	Optional	Optional	Optional	Optional	Yes
Web Management Window URL (MgmtURL)	Web management window URL	Specify the URL for the Web management window. This can be specified when the Web management functions of the corresponding network devices are provided. If left blank, "http://*Admin IP address*/" is specified.	Optional	Optional	Optional	Optional	Yes
Port information (Ports)	A collection of port information	One or more Port elements are specified.	Optional	Optional	Optional	Optional	Yes (*1)
Port name (Port name)	Port name	Specify the port name configured in the network device using a string of up to 64 characters. Alphanumeric characters and symbols (ASCII characters (0x20 to 0x7e) can be specified. If left blank, the value for the port name obtained from the network device is specified.	Optional (*19)	Optional (*19)	Optional (*19)	Optional (*19)	Yes

Element Name	Description	Remarks (Possible Values, Examples)	Specification				Output Using Export
			Individual Registration	Individual Modification	Batch Registration	Batch Modification	
		For the procedure to confirm port names, refer to "9.4.8.1 When Creating Network Configuration Information (XML Definition)" in the "Design Guide CE".					
Overview of the port (description)	Overview of the port	The overview of the port (description) is specified. Specification is unnecessary as it is automatically collected from the network device.	-	-	-	-	Yes
Communication status (PhysicalState)	Communication status	The value of line speed and the communication mode are specified. Specification format:*Line_speed (bps)/ Communication_mode* For the communication mode, one of the following is specified: - F Represents full duplex. - H Represents half duplex. - - Represents unknown. Specification is unnecessary as it is automatically collected from the network device.	-	-	-	-	Yes
Management IP address for link destination device (Link ip)	Management IP address for link destination	An IP address in IPv4 format is specified.	-	-	-	-	Yes (*2)
Port Name of Link Destination (Link port)	The name of the link destination port of a physical interface	The name of the destination port to be linked to is specified.	-	-	-	-	Yes (*2)
Type of link destination device (Link kind)	Type of link destination device	The destination device to be linked to is specified. One of the following is specified: - netdevice	-	-	-	-	Yes (*2)

Element Name	Description	Remarks (Possible Values, Examples)	Specification				Output Using Export
			Individual Registration	Individual Modification	Batch Registration	Batch Modification	
		Represents a network device. - server Represents a server.					
Link information (Links)	Link information destination	This element consists of one or more Link elements. Link information specified with the Links element is registered after all of the currently registered link information is deleted. When modifying only device information, do not specify the Links element to avoid modifying the current link information. In order to delete all current link information, specify the following elements for the Links element: <Links><Link></Link></Links>	Not possible	Not possible	Optional	Optional	Yes (*1)
Link information registration mode (Mode)	Link information registration mode	Specify the registration mode of the link information. Specify either of the following options: - add New registration When the information is the same as that of an already registered link, the link information will not be overwritten. - modify Modification After deleting all already registered link information, register the new link information. If left blank, "modify" is specified.	Not possible	Not possible	Optional	Optional	No
Link (Link)	Link definition (This cannot be omitted when	Specify the Devices element once.	Not possible	Not possible	Optional	Optional	Yes (*1)

Element Name	Description	Remarks (Possible Values, Examples)	Specification				Output Using Export
			Individual Registration	Individual Modification	Batch Registration	Batch Modification	
	specifying link information)						
Device information (Devices)	Definition of device information (This cannot be omitted when specifying links)	Specify the Device element twice.	Not possible	Not possible	Optional	Optional	Yes (*1)
Admin IP address for the device (Device ip)	Admin IP address for the device	Specify the IP address in IPv4 format.	Not possible	Not possible	Optional (*12)	Optional (*12)	Yes
Device name (Device name)	Device name (Specification is not necessary)	The network device name registered from the admin IP address for devices is specified. When using devices other than network devices, the device name that is the connection destination set by auto-configuration functions is supplemented.	-	-	-	-	Yes

Device type (Device kind)	Device type	Specify the type of the device. Specify one of following items.
		 - netdevice
		   Represents a network device.
		 - server
		   Represents a server.
		If left blank, "netdevice" is specified.
			Not possible	Not possible	Optional	Optional	Yes

Connection port name of device (Port)	Connection port name of device	Specify a character string.
		 - When device type is "netdevice"
		   Specify the port name of the network device.
		   For the procedure to confirm port names, refer to "9.4.8.1 When Creating Network Configuration Information (XML Definition)" in the "Design Guide CE".
			Not possible	Not possible	Optional (*12)	Optional (*12)	Yes

Element Name	Description	Remarks (Possible Values, Examples)	Specification				Output Using Export
			Individual Registration	Individual Modification	Batch Registration	Batch Modification	
		- When device type is "server" Specify the server NIC number. Specify the NIC number of a rack mount server or a tower server. The NIC number is defined in the preparations explained in "9.3.5 Pre-configuring Managed Servers" in the "Design Guide CE". 📓 **Example** . . . . If "1" is defined for the NIC number placed on the upper left of the back face of a rack mount server, specify "1".					

-: Specification is unnecessary when registering or modifying. The information for the element is supplied by automatic configuration. The user is notified of the information when the network configuration information is exported.

Yes: The element is output when exporting the network configuration information.

No: The element is not output when exporting the network configuration information.

*1: The element is output only when the elements are defined under that element.

*2: The element is output only when values are specified for that element.

*3: The element is output only when login information is set. When login information is not set, the default value (the value used when omitted) for that element is output if available.

*4: Account information for network device models satisfying all of the following conditions can be confirmed.

Table A.4

Vendor Name	Model Name	Prompt Type	Prompt Character
Fujitsu	SR-X	Login prompt	Login:
		Password prompt	Password:
		Command prompt	*Arbitrary_character_string*#
			Arbitrary_character_string>
Cisco	Catalyst	Login prompt	Username:
		Password prompt	Password:
		Command prompt	*Arbitrary_character_string*#
			Arbitrary_character_string>
	Nexus	Login prompt	login:
		Password prompt	Password:
		Command prompt	*Arbitrary_character_string*#

Vendor Name	Model Name	Prompt Type	Prompt Character
			Arbitrary_character_string>
Brocade	VDX	Login prompt	Login:
		Password prompt	Password:
		Command prompt	*Arbitrary_character_string#*
			Arbitrary_character_string>

The command prompt treats the *arbitrary character string* and the "#" or ">" that follows it as a prompt character string.

*5: Only specify the values when there are special requirements.

*10: Required when specifying "SNMP" for the *monitoring method* (Method).

*11: Required when specifying the login information (LoginInfos).

*12: Required when specifying the device information (Devices).

*19: Required when specifying port information (Ports).

Appendix B Corrective Actions for Errors

This appendix explains the corrective actions to take when errors occur.

B.1 When Linking of Virtual PCs with Virtual L-Servers Fails

When linking of a virtual PC with a virtual L-Server fails, it is necessary to perform linking with the virtual L-Server by specifying the virtual L-Server name. Perform the following procedure.

When linking of a virtual PC with a virtual L-Server fails, if the virtual PC has been powered off, power it on and wait for a while, and then perform linking of it with the virtual L-Server again.

Procedure

1. Execute the following command.

```
> rcxadm lserver convert -name Virtual_L-Server_name -with Virtual_PC_name [-label label] [-
comment comment] [-to folder] [-nowait] -refreship
```

2. Refer to "Confirmation of Results", and confirm that linking with the virtual L-Server has been successfully completed.

3. Create the XML files for changing the network.

   Perform "B.3 When the XML Files for Changing the Network Have Not Been Created".

Confirmation of Results

Execute the following command and confirm that linking with the virtual L-Server has been successfully completed and that RefreshIP at the end is set to "true".

```
> rcxadm lserver show -name L-Server_name -format xml
```

See
. . . .
- For details on the rcxadm lserver command, refer to "4.3 rcxadm lserver".
. . . .

B.2 When the IP Address of a Linked Virtual L-Server Is Not Displayed in the Network Information for the Virtual L-Server

This section explains the corrective action to take when the IP address of a linked virtual L-Server is not displayed in the information for the network of the virtual L-Server when you check that information.

If either of the following conditions is satisfied, perform the procedure that follows.

- When you check the network information for the linked virtual L-Server, the IP address is not contained in the displayed information

- When "2.5.5 Definition File for Loading IP Addresses of Virtual PCs to Virtual L-Servers" has not been created

Procedure

1. Create the XML file that becomes necessary for specifying the network resources and IP addresses corresponding to the NICs for the virtual L-Server.

   1. Execute the following command to output the base XML file for changing the network.

   ```
   > rcxadm lserver show -name L-Server_name -format xml
   ```

   2. Delete any unnecessary information from the output XML file and edit the content as shown below.

The Resources, LServer, and NICs elements must be included.

Depending on the details of the operation network of the virtual PC, specify the values for "name" in the NetworkLink element and "address" in the IpAddress element.

```
<?xml version="1.0" encoding="utf-8"?>
<Resources>
  <LServer name="L-Server_name">
    <NICs>
      <NIC>
        <NICIndex>NIC_index</NICIndex>
        <MacAddress>MAC_address</MacAddress>
        <NetworkLinks>
          <NetworkLink name="Network_name" index="0">
            <IpAddress auto="Automatic_IP_configuration" address="IP_address"/>
          </NetworkLink>
        </NetworkLinks>
      </NIC>
    </NICs>
  </LServer>
</Resources>
```

2. Execute the following command using the XML file that was created in step 1 to specify the network resources and IP addresses corresponding to the NICs for the virtual L-Server.

```
> rcxadm lserver modify -name L-Server_name -file file.xml [-nowait]
```

3. Refer to "Confirmation of Results" and confirm that the changes you made in step 2 have been reflected.

4. If the XML files for changing the network have not been created, create them.

    Perform "B.3 When the XML Files for Changing the Network Have Not Been Created".

Confirmation of Results

Execute the following command and confirm that the changes you made in step 2 have been reflected.

```
> rcxadm lserver show -name L-Server_name -format xml
```

🔷 See
....
  - For the XML definitions for network resources (file.xml), refer to "Table A.1 Excerpt from Definition Information for Virtual L-Servers (XML)".

  - For details on the rcxadm lserver command, refer to "4.3 rcxadm lserver".
....

B.3 When the XML Files for Changing the Network Have Not Been Created

This section explains the corrective action to take when the XML files for changing the network have not been created.

The possible causes for absence of the XML files for changing the network are as follows:

  - Linking of virtual PCs with virtual L-Servers has been completed successfully but the XML files for changing the network have not been created due to a creation error of the definition file (avmgr_network.rcxprop)

  - As linking of virtual PCs with virtual L-Servers was performed using the rcxadm lserver convert command, the XML files for changing the network have not been created

Procedure

1. Create the definition file (avmgr_network.rcxprop).

2. Execute the following command.

```
> convertVMtoLServer -createxml
```

Confirmation of Results

Confirm that the XML files for changing the network of the linked virtual L-Servers have been created.

Storage Location of the XML Files for Changing the Network

[Windows Manager]

Installation_folder\SVROR\Manager\etc\files\avmgr

Names of the XML Files for Changing the Network

quarantine_*L-Server_name*.xml

unquarantine_*L-Server_name*.xml

 See
∙∙

- For details on avmgr_network.rcxprop, refer to "2.5.6 Definition File for Configuring the Business and Quarantine Networks".

- For details on the convertVMtoLServer command, refer to "4.2 convertVMtoLServer".
∙∙

B.4 Corrective Actions for Other Errors

When execution of a command is interrupted due to a server failure, etc., refer to "2.12.1 Batch Loading Virtual PCs Using the convertVMtoLServer Command" and execute the convertVMtoLServer command again.

Appendix C Stopping Use

This appendix explains how to stop using the automatic quarantining function.

1. Use the rcxadm avmgr list command to confirm the antivirus software which has already been registered.

   For details on the command, refer to "4.1 rcxadm avmgr".

2. Use the rcxadm avmgr delete command to unregister all antivirus software.

   For details on the command, refer to "4.1 rcxadm avmgr".

3. Confirm the storage directory of the XML files for changing the network.

   When the storage directory has not been customized, it will be as follows.

   [Windows Manager]

   > *Installation_folder*\SVROR\Manager\etc\files\avmgr

   When the storage directory has been customized, it will be described in avmgr.lserver_xml_dir in avmgr.rcxprop.

4. Delete any existing XML files for changing the network.

5. When a virtual PC was linked to an L-Server in order to use this function, release the link.

   For the procedure to release the link, refer to "18.6 Releasing an L-Server" in the "User's Guide for Infrastructure Administrators (Resource Management) CE".

6. Disable the email notification function and the message notification function.

   Refer to "4.9 msgnotice" and "4.10 mailnotice", and disable each of the functions.

7. Delete any definition files in the following directory.

   Location of the Definition Files

   [Windows Manager]

   > *Installation_folder*\SVROR\Manager\etc\customize_data

   Names of the Definition Files

   - avmgr.rcxprop
   - avmgr_msgnotice.rcxprop
   - avmgr_corp_filter_disable.en.rcxprop
   - avmgr_corp_filter_enable.en.rcxprop

8. When a VE license has been applied, delete the following file.

   Location of the File

   [Windows Manager]

   > *Installation_folder*\SVROR\Manager\etc\conf

   Name of the File

   > rorsetup.conf

9. Return the content set in "2.1 Preparations for Using the Automatic Quarantining Function" for the antivirus software back to the original content.

10. Check the registered information of sub managers using the rcxadm submgr list command.

    For details on the command, refer to "4.7 rcxadm submgr".

11. When there are sub managers registered, use the rcxadm submgr delete command to delete all of the sub manager information.

    For details on the command, refer to "4.7 rcxadm submgr".

12. Close any unnecessary ports.

    If the rules created in "2.2.3 Configuring the Windows Firewall" will no longer be used, delete them.

Example Procedure

```
netsh advfirewall firewall delete rule name="ServerView Resource Orchestrator(TCP)"
netsh advfirewall firewall delete rule name="ServerView Resource Orchestrator(UDP)"
netsh advfirewall firewall delete rule name="ServerView Resource Orchestrator(SMTP)"
```

Execution Results

```
> Deleted 1 rule(s).
> Ok.
```

Appendix D Preparations for Automatic Configuration and Operation of Network Devices

This section explains how to prepare automatic configuration and operation of network devices.

D.1 Creating Model Definitions for Network Devices

Rulesets used for the function that automatically configures network devices are registered by the network device model. Therefore, it is necessary to create model definitions for determining the models of network devices.

The created model definitions are enabled by registering the following XML definition file:

[Windows Manager]

Installation_folder\SVROR\Manager\etc\customize_data\network_device_model.xml

Newly added models can be supported by editing the model definitions.

For supported models, model definitions are automatically acquired, therefore, it is not necessary to enter them in the model definition file for network devices.

The network device model definitions provided with sample scripts for auto-configuration and operations of network devices are automatically acquired, therefore it is not necessary to enter them in the model definition file.

 Information
. . . .

 - When editing a model definition, check the sysObjectID of the network device using the snmpwalk command.

 Example
. . . .

snmpwalk -v 1 -c [*SNMP_community_name*] [*IP_address*] sysObjectID
. . . .

If the information is available from the manual or vendor of the destination device, obtain it from there.

 - Use the specified OID string as the SysObjectId element in the Model element to specify the model name of the network device.

   - The model definition file of network devices is searched from the start, and the first sysObjectID that matches will be used as the model name of the name attribute of the Model element.

   - When there is no matching OID string in the model definition file, the model name is not specified.

 - If the product name or model name is specified in the network configuration information used for network device registration, the specified product name or model name is regarded as a model.
. . . .

 See
. . . .
For details on model definitions for network devices, refer to "15.15 Network Device Model Definition" in the "Reference Guide (Command/XML) CE".
. . . .

D.2 Configuring the Execution Environment

This section explains how to configure execution environment for automatic configuration and operation of network devices.

D.2.1 When Connecting to Network Devices with SSH

When connecting to network devices with SSH in automatic configuration and operation of network devices, the infrastructure administrator prepares the SSH environment using the following procedure.

1. Prepare the SSH library used for scripts.

   When using sample scripts, download "Ganymed SSH-2 for Java (build 250)" from the Internet.

2. Store the prepared SSH library in the following location:

   [Windows Manager]

   Installation_folder\SVROR\Manager\etc\scripts*vendor_name**unit_name or model_name*\common\

   When using sample scripts, decompress the downloaded "Ganymed SSH-2 for Java (build 250)", and store "ganymed-ssh2-build250.jar".

D.2.2 When Using a Script Language other than Ruby

When using a script language other than ruby in automatic configuration and operation of network devices, the infrastructure administrator prepares the script language environment using the following procedure.

1. Store the script language library in any folder recognizable by the ROR manager.

2. Define the script language in the definition file of automatic configuration and operation of network devices.

   For details on how to define the script monitoring language, refer to "Script language" in "D.7.3 Definition File Format".

D.3 Creating a Folder for Registering Rulesets

When it is necessary to specify settings that differ according to the provided service, register these patterns as separate rules to manage them. This management is performed by the ruleset.

Create a folder with a unique name in the system for registering scripts, etc. for each ruleset.

Rulesets are registered in folders for network resources.

Information

. . . .

- For "*vendor_name*", "*unit_name*", and "*model_name*", specify the "*vendor name*", "*unit name*", and "*model name*" of the target network device for script execution, respectively.

  The "*Vendor name*", "*unit name*", and "*model name*" of a network device can be confirmed by checking the model definition (XML file) for that device or from the [Resource Details] in the [Resources] tab on the ROR console.

  For details on model definitions for network devices, refer to "15.15 Network Device Model Definition" in the "Reference Guide (Command/XML) CE".

- Specify the folder name of "*ruleset name*" using up to 32 characters, including alphanumeric characters, underscores ("_"), and hyphens ("-"). This name should start with an alphabetical character.

  Set a unique name for the folder name of "*ruleset name*", excluding the following folders in which sample scripts are registered.

  [Windows Manager]

  Installation_folder\SVROR\Manager\etc\scripts\

. . . .

D.3.1 Folders for Network Resources

Create folders for registering rulesets for automatic configuration of L2 switches.

Network device specific folders include rulesets in units of network device names or model names.

Create the following two types of folders.

- A folder common to network devices

  Register the ruleset selected when creating network resources.

  Create the folder with the following name.

  [Windows Manager]

  Installation_folder\SVROR\Manager\etc\scripts\network_resource*ruleset_name*\

- A folder for a specific network device

  Register a ruleset for each network device unit name or model name. This ruleset includes the scripts used by the ruleset common to network devices.

  Create the folder with the following name.

  [Windows Manager]

  Installation_folder\SVROR\Manager\etc\scripts*vendor_name**unit_name or model_name*\rulesets*ruleset_name*\

D.4 Basic Script Structure

This section explains the basic operation and structure of a script used for automatic configuration and operation of network devices.

The basic flow of configuration and operation of network devices using scripts is as follows:

1. Confirm the syntax of the script list file.

2. The following is processed starting from the start of the script list file.

    a. Specify the target network device.

    b. Complete the script file to convert variable information in the script file corresponding to "Script Name" with the information of the parameter file.

    c. When "cmd operand" is specified in a script list, complete the specified command file. In this process, variable information in the command file is converted using the information of parameter files.

    d. Script files are executed sequentially, from top to bottom.

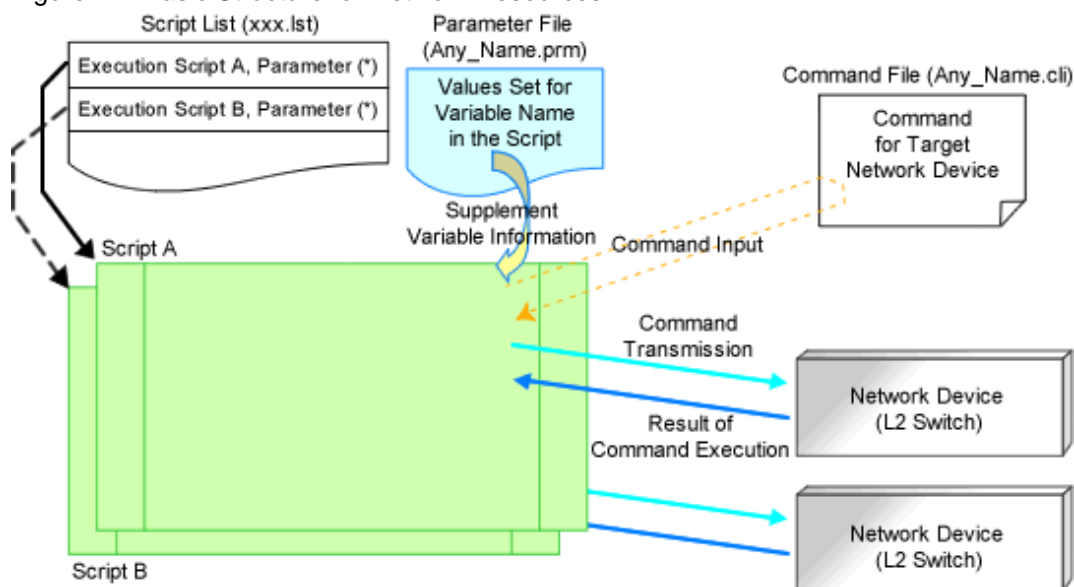   At this time, if necessary, commands are loaded from the command file.

For the function of each file, refer to "D.4.1 Function and Attributes of Each File".

As examples of basic script structure, the following basic structures are shown.

- Basic Structure for Network Resources

Basic Structure for Network Resources

Figure D.1 Basic Structure for Network Resources

Note: It is possible to specify parameters in a script without a parameter file.

Scripts A, B

These scripts are prepared by the infrastructure administrator and registered under a specific network device ruleset folder.

An example of the basic process in a script is as follows:

1. Define variables

2. Establish a telnet/ssh connection with the variable (IP address in admin LAN)

3. Send the variable (login account 1)

4. Send the variable (login password 1)

5. Process the command file

   - If command files exist

     Read the command file and send the content of the command file line by line. [Command transmission]

   - If command files do not exist

     Execute the process of sending and receiving commands. [Command transmission]

6. Command processing ends.

   - If command processing ends normally

     Set [Normal] for the return value.

   - If command processing ends abnormally

     Set [Abnormal] for the return value.

7. Send the variable (logout character string). [Command transmission]

8. Disconnect the telnet/ssh connection.

Script List (*xxx*.lst)

This script is prepared by the infrastructure administrator and registered under a specific network device ruleset folder.

For network devices related to the operated L-Platform.

Scripts specified in the script list are executed in order.

Parameter File (*Any_Name*.prm)

> The infrastructure administrator prepares this if necessary.

Command File (*Any_Name*.cli)

> The infrastructure administrator prepares the script.

> Define processes for after log in to devices with log in accounts, excluding command processes included in scripts.

D.4.1 Function and Attributes of Each File

This section explains the functions and attributes of each file which compose a script.

Table D.1 Function and Attributes of Each File

File Type	Function	File Name Rule	Extension
D.6.1 Script List Files	In this file, scripts are arranged in the order of execution for auto-configuration of network devices. Include all script lists for operating network devices in one operation (creation, modification, or deletion of L-Platforms or network resources).	-	lst
	For setup Script lists for adding settings to network devices according to the purpose of the ruleset, such as port VLAN settings, firewall rules for blocking unauthorized access, and server load balancing rules.	"create"	
	For setup error recovery Script lists for recovering configurations for network devices in case errors occur when creating L-Platforms or network resources. Preparation of this script is not necessary if the recovery process is not necessary when an error occurs while executing a script list for setup.	"create_recovery"	
	For modification Script lists for modifying parameters that were configured in the script lists for setup. In addition to modification of configuration parameter values, this type of script list can be used for addition or deletion of physical port settings or interface configurations when attaching or detaching servers. When adding or deleting configurations for physical ports or interfaces, it is necessary to reflect the configuration changes made by the script for modification onto the script list for setup or the script list for deletion.	"modify.lst"	
	For modification error recovery Script list for recovering configurations for network devices when an error occurs in the script lists for modification. This script list is needed only if the recovery process is needed after occurrence of an error.	"modify_recovery"	
	For deletion Script list for deleting parameters configured in the script lists for setup or modification.	"delete"	
	For creation of interface for adjoining server This script list is used to connect a physical L-Server and network resources when creating a physical L-Server. This script list adds configurations, for example, VLAN configurations corresponding to network resources, for the	"connect"	

File Type	Function	File Name Rule	Extension
	L2 switch port connected to the NIC of the rack server where the physical L-Server is created.		
	For error recovery of creation of an interface for an adjoining server This script list is used to recover configurations for network devices when an error occurs in the script lists for creation of an interface for an adjoining server. This script list is needed only if the recovery process is needed after occurrence of an error during creation of an interface for an adjoining server.	"connect_recovery"	
	For deleting an interface for an adjoining server This script list is used to release physical L-Server connection with network resource when deleting physical L-Server. This script list automatically deletes configurations, for example, VLAN configurations corresponding to network resource, from L2 switch port connected to NIC of Rack Server where physical L-Server is created.	"disconnect"	
	For operation Script lists for obtaining information from a network device by executing operation commands such as the ones for state display and log collection.	"operate"	
D.6.2 Script Files	In this file, the procedure for auto-configuration of network devices is written.	An arbitrary character string composed of alphanumeric characters, hyphens ("-"), and underscores ("_"). The valid characters and string lengths depend on the OS or the rules of the script language.	Language dependent
D.6.3 Command Files	In this file, the list of commands which will be sent to network devices are written.	A string of alphanumeric characters, hyphens ("-"), and underscores ("_"), within 32 characters in length.	cli
D.6.4 Parameter Files	In this file, the parameters which can be customized in the scripts are written.	- "default_param.prm" For rulesets for L-Platform templates, this name is fixed. - User defined name For rulesets used by network resources, specify this using up to 32 alphanumeric characters, including hyphens ("-") and underscores ("_").	prm

D.4.2 Location of Each File

This section explains the location of each file which composes a script.

Deployment Locations for Script List Files and Parameter Files

- Ruleset used by network resources

  [Windows Manager]

Installation_folder\SVROR\Manager\etc\scripts\network_resource*ruleset_name*|

Deployment Locations for Script Files and Command Files

- Ruleset for automatic configuration

   [Windows Manager]

   Installation_folder\SVROR\Manager\etc\scripts*vendor_name**unit_name or model_name*\rulesets*ruleset_name*\

- Ruleset for operation

   [Windows Manager]

   Installation_folder\SVROR\Manager\etc\scripts\vendor_name*unit_name or model_name*\operations*ruleset_name*|

D.5 Timing of Ruleset Execution

The timing at which rulesets in the folder for ruleset registration are executed is listed below.

Table D.2 Timing of Ruleset Execution

Operation	Registration Folder	Target Device	Remarks
L-Server creation L-Server modification L-Server deletion	Folders for Network Resources	L2 switches	When deploying a physical L-Server using a rack mount server, configure an L2 switch.
Network resource creation Network resource modification Network resource deletion	Folders for Network Resources	L2 switches	Sets the VLAN corresponding to network resources.

D.6 File Components of Rulesets

This section describes each file contents for configuration and operation according to the structure of the script described in "D.4 Basic Script Structure".

D.6.1 Script List Files

This section explains the format of script list files and how to write parameters in them.

Script List for Network Resources

This section explains the ruleset script list used by network resources.

Format

```
Script Path Script Name[,cmd=Script Command File Name],node=Network Device
Name[,paramfile=Parameter File Name][,param=(Parameter Name1=Parameter Value1,Parameter
Name2=Parameter Value2, ...)]
```

Description

This section explains each item.

Script Path

   Specify the folder path for the script to execute using an absolute path or relative path from the scripts folder.

   The folder path, including the execution script, is necessary.

Script Name

   Specify the name of the script you want to execute.

   Do not specify a script list name in this field. If you specify it, it is regarded as designating the name of the script to execute.

cmd=*Script Command File Name*

Specify the name of the script command file you want to execute.

The value specified for this operand will be configured for the reserved variable "command file name".

If you invoke multiple command files, it is necessary to use the "command file names" including a serial number (in ascending order from 1).

If you do not specify the command file name in the script, the command file is not invoked from the script.

node=*Network Device Name*

Specify the name of the network device to execute the script.

If you specify the wrong network device name in this field, an automatic configuration error or incorrect configuration occurs when the script is executed. Specify the network device name carefully.

paramfile=*Parameter File Name*

Specify the parameter file name of the variable information passed to the script.

If you use variable information from a parameter file, specify the name of the parameter file.

param=(*Parameter Name1=Parameter Value1,Parameter Name2=Parameter Value2,...*)

If you want to change the settings of variable parameters in the parameter file specified for the "paramfile" field per line of script list, use this operand.

Specify all parameter names and changed parameter values that you want to change.

Information

- Specified parameters are separated by "," and blank spaces between parameters and "," are ignored.

- The number of lines specified in a script list is limited to 100, excluding comment lines.

- Comments begin with "#" in the first column. Any characters can be used in the comment line.

  Write comments such as description of executed scripts when necessary.

  Comments are ignored when script lists are processed.

- Blank lines are regarded as comments and ignored when a script list is processed.

- When a script list processes the same network device, the script list is not executed at the same time but executed in order. On the other hand, when a script list does not process the same network device, the script list is executed at the same time.

Execution Image

Script lists are executed in the order of the list.

```
[Script Path]Script Name1,node=Network Device Name1,param=(Parameter Name1=Value,...)
[Script Path]Script Name2,node=Network Device Name2,param=(Parameter Name2=Value,...)
[Script Path]Script Name3,node=Network Device Name3,param=(Parameter Name3=Value,...)
```

D.6.2 Script Files

This section explains how to create script files.

Script Structure

This section explains the structure of scripts.

The process from establishing to releasing a telnet/ssh connection with the target network device is written in scripts.

The basic structure is shown in the following figure.

Variable Definition Section

Variable information is converted using information from the parameter file and DB and defined as a variable.

Connection (login)

Establishes a telnet connection to the admin LAN IP address defined in the variable.

Sends the login account defined in the variable.

Sends the login password defined in the variable.

Command Sending Section

- If command files exist

    Send the content of the command file line by line.

- If command files do not exist

    Executes the process of sending and receiving commands in a script.

Verification of execution results

If the command ends normally, the return value "normal" is set.

If the command process ends abnormally, the return value "error" is set.

Disconnection (logout)

Send the variable (logout string).

Disconnect the telnet connection.

Note

Define the process from connection to disconnection in the script.

Variable Information Usable in Scripts

Variables used in scripts are defined in the variable definition section.

Variables including variable information are defined between the reserved variables "%Unm_DefineStart%" and "%Unm_DefineEnd%" as follows.

```
# %Unm_DefineStart%

Define variables, including variable information.

# %Unm_DefineEnd%
```

Reserved variable names consist of character strings with "Unm" as a prefix and alphanumeric characters and an ampersand ("&"), underscores ("_"), and hyphens ("-"). "&" in a character string is a symbol utilized to split a character string into a meaningful string such as an L-Server name and a network resource name.

Reserved variable names which can be used in scripts are shown in the following table.

Table D.3 Reserved Variables that can be Used in Scripts

Information Type	Variable Name	Usage After Conversion
Variable information (beginning)	%Unm_DefineStart% (*1)	Specify the beginning of the range for variable conversion in a script. Include this as a comment line once in a script.
Variable information (end)	%Unm_DefineEnd% (*1)	Specify the end of the range for variable conversion in a script. Include this as a comment line once in a script.
Command file name	%Unm_CommandFileName% (*2)	Command file name

VLAN-ID	%Unm_VlanId% (*3)	VLAN-ID value
VLAN-ID	%Unm_VlanId&Network Resource Name% (*3)	VLAN-ID value
Admin IP address	%Unm_MyLoginIp%	IP address used for logging in to the target device via SSH/TELNET/FTP
Login account 1	%Unm_MyLoginAccount1%	Account name used for logging in to the target device via SSH/TELNET/FTP
Login account 2	%Unm_MyLoginAccount2%	Account name used for logging in to the target device via FTP
Login password 1	%Unm_MyLoginPass1%	SSH/TELNET password for logging in to the target device
Login password 2	%Unm_MyLoginPass2%	FTP password for logging in to the target device
Admin password 1	%Unm_MyAdminPass1%	Password to change to admin privileges of the target device
Admin account	%Unm_MyAdminAccount%	Admin account of the target device
Admin password 2	%Unm_MyAdminPass2%	Admin password of the target device
Login port	%Unm_LoginPort%	SSH/TELNET port for logging in to the target device
FTP admin IP address	%Unm_FtpLoginIp%	IP address for logging in from the target device via FTP
FTP login port	%Unm_FtpLoginPort%	Port used for logging in from the target device via FTP
FTP login account	%Unm_FtpLoginAccount%	Account name for logging in from the target device via FTP
FTP login password	%Unm_FtpLoginPass%	Password for logging in from the target device via FTP
Adjacent L2 switch 1	%Unm_SwNode1% (*4)	Network device name of the adjacent L2 switch connected to the physical rack server NIC (If a physical server has redundant NICs, specify the first L2 switch connected to the first NIC)
Adjacent L2 switch 2	%Unm_SwNode2% (*4)	Network device name of second adjacent L2 switch connected to physical rack server redundant NIC
Adjacent L2 switch port 1	%Unm_SwPort1% (*4)	Port name of the second adjacent L2 switch connected to the physical rack server redundant NIC Port name of the adjacent L2 switch connected to the physical rack server redundant NIC
Adjacent L2 switch port 2	%Unm_SwPort2% (*4)	Port name of second adjacent L2 switch connected to physical rack server redundant NIC
Network device IPv4 address	%Unm_Ipv4&Sequential Number&Network Resource Name% (*5)	IPv4 address configured on the interface of the automatic configuration target device

Network device IPv4 subnet	%Unm_Ipv4Subnet&Network Resource Name%	IPv4 subnet configured on the interface of the automatic configuration target device
Network device IPv4 subnet mask	%Unm_Ipv4SubnetMask&Network Resource Name%	IPv4 subnet mask configured on the interface of the automatic configuration target device
Network device IPv4 subnet mask length	%Unm_Ipv4SubnetMaskLength&Network Resource Name%	IPv4 subnet mask length configured on the interface of the automatic configuration device
Network device IPv6 address	%Unm_Ipv6&Sequential Number&Network Resource Name% (*5)	IPv6 address configured on the interface of the automatic configuration target device
Network device IPv6 prefix	%Unm_Ipv6Prefix&Network Resource Name%	IPv6 prefix configured on the interface of the automatic configuration target device
Network device IPv6 prefix length	%Unm_Ipv6PrefixLength&Network Resource Name%	IPv6 prefix length configured on the interface of the automatic configuration target device
VRID	%Unm_Vrid&Network Resource Name%	VRID configured on the interface of the automatic configuration target device
L-Platform name	%Unm_LplatformName%	Name of the L-Platform performing processing
L-PlatformID	%Unm_LplatformId%	Resource ID of the L-Platform performing processing
Firewall name	%Unm_FirewallName%	Name of the firewall processing the L-Platform
Firewall resource ID	%Unm_FirewallId%	Resource ID of the firewall processing the L-Platform
Server load balancer name	%Unm_SlbName%	The name of the processed SLB on the L-Platform
The server load balancer resource ID	%Unm_SlbId%	The resource ID of the processed SLB on the L-Platform
List of admin IP addresses of redundant network devices	%Unm_Group&Group Number%	List of admin IP addresses of the redundant network device corresponding to the group number of the script. The group number specified in the script list
Backup directory	%Unm_BackupDir% (*6)	Absolute path name of the backup directory
Current setting information	%Unm_Present&Variable name% (*7)	The content of the variable name used in the most recent configuration
Variable parameter specified by an infrastructure administrator	%Unm_Set_Variable_Character&Network_Resource_Name%	The value when a variable parameter excluding variable parameter limited by the system is specified in the interface configuration file

*1: The scope of the script lines converted by the script which converts variable information

- When %Unm_DefineStart% is defined, but %Unm_DefineEnd% is not defined

  Lines from %Unm_DefineStart% to the last line of script files are considered as variable parameters to be converted.

- When %Unm_DefineStart% is not defined, but %Unm_DefineEnd% is defined

  Variable parameter conversion is not executed in the script file.

- When that %Unm_DefineStart% and %Unm_DefineEnd% are multiply defined

  Variable parameters between first %Unm_DefineStart% and %Unm_DefineEnd% from first line of file are the targets of variable parameter conversion.

*2: Command file name

In variable information of the command file name, configure the name added to "exec_discrimination number (8 - 10 digits)" before the command file name prescribed by the system.

When you use multiple command files in a script, it is necessary that variable parameters of the script are written as variable information of the command file name + *n* (*n* is a sequential number).

```
Example
"%Unm_CommandFileName%1.cli"
"%Unm_CommandFileName%2.cli"
"%Unm_CommandFileName%3.cli"
...
```

*3: VLAN-ID value of network resources

VLAN-ID values that can be used as variable information differ depending on the device to be configured automatically.

When you use the VLAN-ID value of a network resource as variable information, specify it in the following format in the script and the value will be resolved by the system.

- When the automatically configured device is an L2 switch

  - VLAN-ID value : %Unm_VlanId%

  Specify the VLAN-ID configured for the network resource as variable information.

- When the automatically configured device is a firewall

  - VLAN-ID value: %Unm_VlanId & Network resource name (up to 32 characters)%

  The VLAN-ID configured in the network resource corresponding to the specified network resource name is configured as variable information.

  For the network resource name, the name of the network resource in the segment used by the L-Platform can be used.

- When the automatically configured device is a server load balancer

  - VLAN-ID value: %Unm_VlanId & Network resource name (up to 32 characters)%
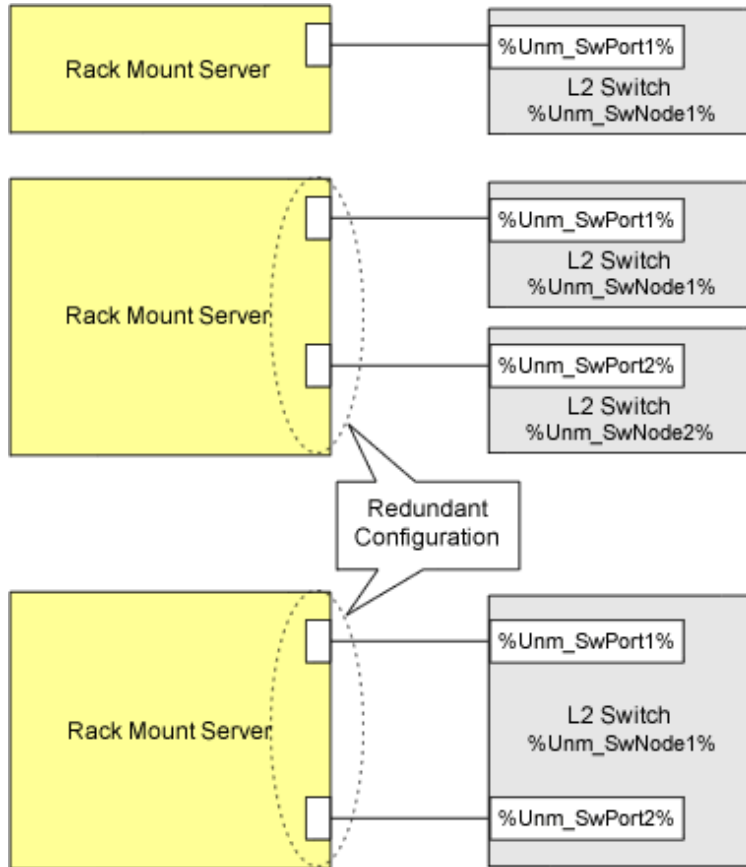
  The VLAN-ID configured in the network resource corresponding to the specified network resource name is configured as variable information.

  For the network resource name, the name of the network resource in the segment where the server load balancer is located can be used.

*4: Reserved variable names when physical rack servers have redundant NICs

For a physical rack server with redundant NICs, the reserved variable names are as follows:

Figure D.2 Reserved Variable Names for Physical Rack Mount Servers with Redundant NICs

Rack Mount Server — %Unm_SwPort1% / L2 Switch %Unm_SwNode1%

Rack Mount Server — %Unm_SwPort1% / L2 Switch %Unm_SwNode1% ; %Unm_SwPort2% / L2 Switch %Unm_SwNode2%

Redundant Configuration

Rack Mount Server — %Unm_SwPort1% / L2 Switch %Unm_SwNode1% ; %Unm_SwPort2%

*5: Sequential numbers

Ensure that specified sequential numbers are the values corresponding to the IPv4/IPv6 addresses for the desired purpose.

Assign sequential numbers for each purpose to the IPv4/IPv6 addresses required by network devices, such as physical IPv4/IPv6 addresses for active units and virtual IPv4/IPv6 addresses for standby units.

Specify the mapping of the IPv4/IPv6 addresses for each purpose and assign sequential numbers in the following elements in the interface configuration file:

  - The IPv4Address element

  - The IPv6Address element

*6: Backup directory

Parameters in the following definition files are configured as a backup directory name.

  - Location of the Definition Files

    [Windows Manager]

    Installation_folder\SVROR\Manager\etc\customize_data\manager_backup.rcxprop

  - Parameter Format of Definition Files

    ruleset_backup_dir=*backup directory*

    backup directory: specify the backup directory name using an absolute path.

    If this parameter is not specified, the following backup directory is specified by default.

    [Windows Manager]

    Installation_folder\SVROR\Manager\var\lserver_repair\ruleset_backup

*7: Current setting information

It is possible to obtain information from when creating resources for firewalls and server load balancers, until those resources are deleted.

When two or more types of scripts are executed during creation or modification of resources of firewalls or server load balancers, the variable name used by the script that was last executed can be used as the current setting information.

When using the current setting information, it is not possible to configure different values for individual scripts or to use different variable information names for individual scripts in the script list. The variable information name and value must be the same throughout the script list.

The variable names which can be specified for "variable name" of this reserved variable are the following reserved variable names, and user-defined variable names stated in the parameter file.

Table D.4 Reserved Variable Names that can be Used for "Variable Name"

Information Type	Reserved Variable Name
Command file name	%Unm_CommandFileName%
VLAN-ID	%Unm_VlanId&Network Resource Name%
L-Platform name	%Unm_LplatformName%
L-Platform resource ID	%Unm_LplatformId%
Firewall name	%Unm_FirewallName%
Firewall resource ID	%Unm_FirewallId%
Server load balancer name	%Unm_SlbName%
The server load balancer resource ID	%Unm_SlbId%
List of admin IP addresses of redundant network devices	%Unm_Group&Group Number%

Current setting information varies depending on how many times automatic configuration was performed.

"None" indicates that the variable name will not be converted because there is no value.

Table D.5 Example of Information Changed each time Auto-configuration is Executed

Number of Times Executed	Variable Name	Information of %Unm_Present & Variable name%	Variable Name Information
First time	A	None	1
	B	None	2
	C	None	3
Second time	A	1	11
	B	2	2
	C	3	None
Third time	A	11	11
	B	2	2
	C	None	1

Information

- Reserved variable names are written in the following locations.

  - Any place in a command file

  - In the "node" operand and "param" operand in script lists

  - Between the "%Unm_DefineStart%" line and "%Unm_DefineEnd%" line in a script

- When you do not use a sample script (as in cases where an infrastructure administrator creates their own new script), specify variable information which is usable in command files and scripts using character strings enclosed by % as in "% %". The maximum length of a variable information string is 128 characters.

- In the character string enclosed by %, alphanumeric characters, underscores ("_"), and hyphens ("-") can be used. "Unm_" is a reserved variable name, so it cannot be included in variable names specified by users.

- Variable information can be written in the following locations.

    - Any place in a command file

    - Between the "%Unm_DefineStart%" line and "%Unm_DefineEnd%" line in a script

··

Operation when Variable Information Conversion in a Script Fails

If conversion of variable information fails, variable information parameters are not converted and the script is executed.

If variable information in the command file is a character string before conversion, the script will not send that command or any associated commands to the network device.

A script execution error is not returned just because the conversion of variable information fails.

If conversion of the following variable information related with the adjacent L2 switch fails, the script is not executed and an error is returned because there is a problem when constructing information of the network device.

- %Unm_SwNode1%

- %Unm_SwNode2%

- %Unm_SwPort1%

- %Unm_SwPort2%

Return Codes Used by Scripts

The results of script execution are determined to be normal or abnormal based on their return code.

Based the code returned by a script, the process ends normally or recovery action is executed.

Return codes used for scripts are as follows.

Table D.6 Return Codes Used by Scripts

Return Code	Return Code Meaning
0	Processing of the script ended normally.
4	An error occurred in script execution, but the script can be executed again. (Connection closed or connection time out)
6	An error occurred in script execution, but the script can be executed again. (An error occurred before reflection of the definition on the network device)
8	An error occurred in script execution, and the script cannot be executed again. (Errors other than the above) Changes the status of the network device for which the script was executed and the redundant network device into "error" and places them into "maintenance mode". Take corrective action and then execute the following command to release "maintenance mode", which will change the status of the devices back to "normal". - Execute the rcxadm netdevice set command with the -attr mode=active option specified For information about the rcxadm netdevice command, refer to "3.8 rcxadm netdevice" in the "Reference Guide (Command/XML) CE".

Confirming Results of Script Execution

In order to check the progress of script execution and any errors in a script, create the script so that process content is logged to an arbitrary file.

Refer to the contents of the output log file to confirm results of script execution.

Sample scripts generate logs in the folder where rulesets are placed to provide reference information for infrastructure administrators.

When checking the content, copy the log file to an arbitrary user directory and then open the copied log file.

 Note

- The above log file is used when infrastructure administrators check script action. Use of this log file by tenant users and administrators has not been considered. Accordingly, there is no protection between tenants.

- Do not perform standard output or standard error output of script execution results, except for script files used by the rulesets for operations. If scripts which perform standard output or standard error output are used, automatic network device configuration may be aborted.

- To perform standard output and standard error output of script execution results using the script files used by a ruleset for operations, it is necessary to specify the same processing method as the one used in the sample script. If you create and use an original processing method for standard output and standard error output, the execution result of the scripts for operations cannot be obtained and L-Platform operations may fail.

Operation when Script Executions Results are Abnormal

When there are abnormal script execution results when executing a script list, the operations that follow vary depending on the type of script list and the specifications of the definition file.

Script Lists	Operation when Script Executions Results are Abnormal	
	SCRIPT_EXECUTION_MODE= continue	SCRIPT_EXECUTION_MODE= stop
- Script lists for setup - Script list for modification - Script lists for setup (physical server added) - Script lists for operations	Execution of the script is canceled. If a script for recovery has been prepared, the script for recovery is executed. (*1)	
- Script list for deletion - Script lists for deletion (physical server deleted)	Execution of the script is continued.	Execution of the script is canceled.
- Script lists for setup error recovery - Script lists for modification error recovery - Script lists for setup error recovery (physical server added)	Execution of the script is continued, without canceling execution of the script for recovery.	Execution of the script for recovery is canceled. When the execution results are not abnormal, the script for recovery will be executed for all network devices.

*1: There are no scripts for recovery in script lists for operations.

For details of the specified parameters and possible parameter values of the definition file "SCRIPT_EXECUTION_MODE", refer to "D. 7 Network Device Automatic Configuration and Operation Definition Files".

Differences in Operations Depending on Specifications in the Definition File "SCRIPT_EXECUTION_MODE"

The operations when executing scripts change depending on the specified values in the definition file "SCRIPT_EXECUTION_MODE". Decide the value to specify in "SCRIPT_EXECUTION_MODE" based on the specifications of the scripts being used.

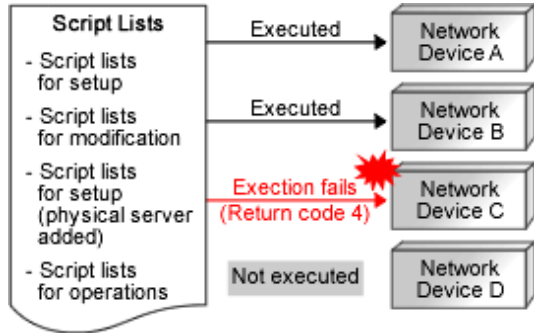Figure D.3 Example Script Operation not Reliant on SCRIPT_EXECUTION_MODE Specifications

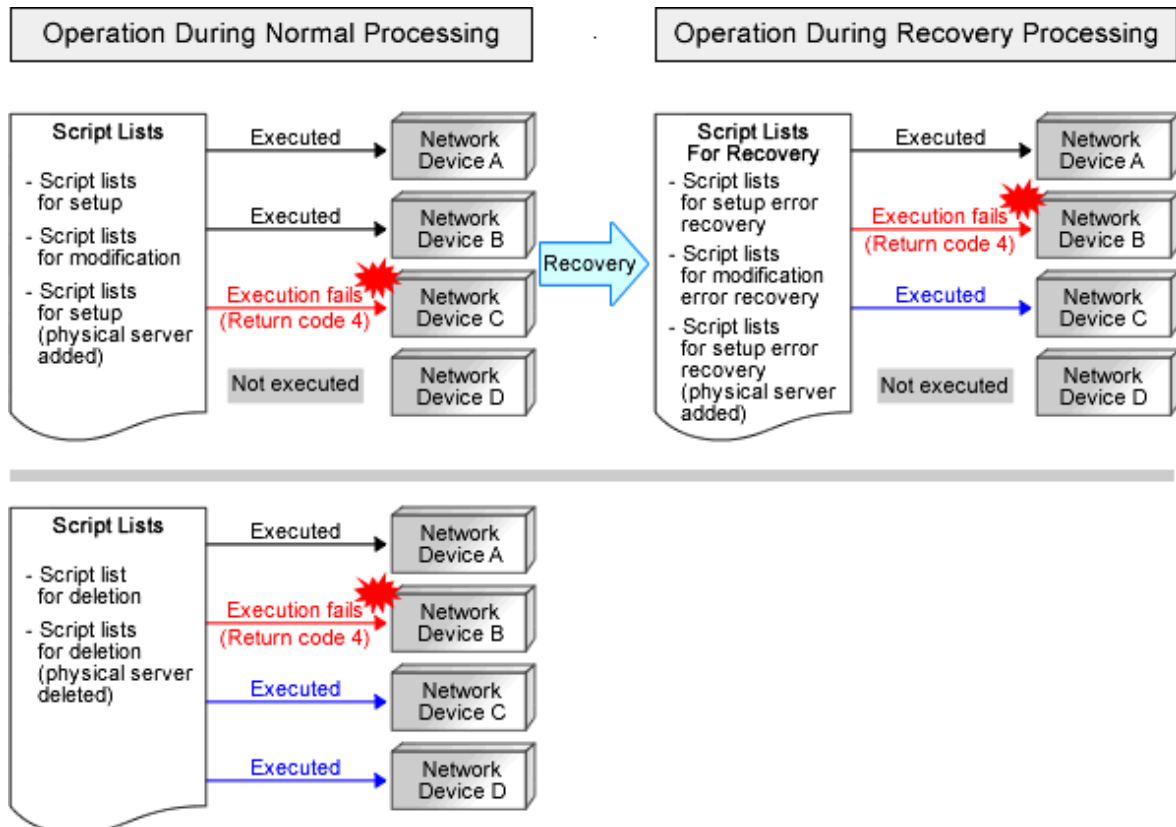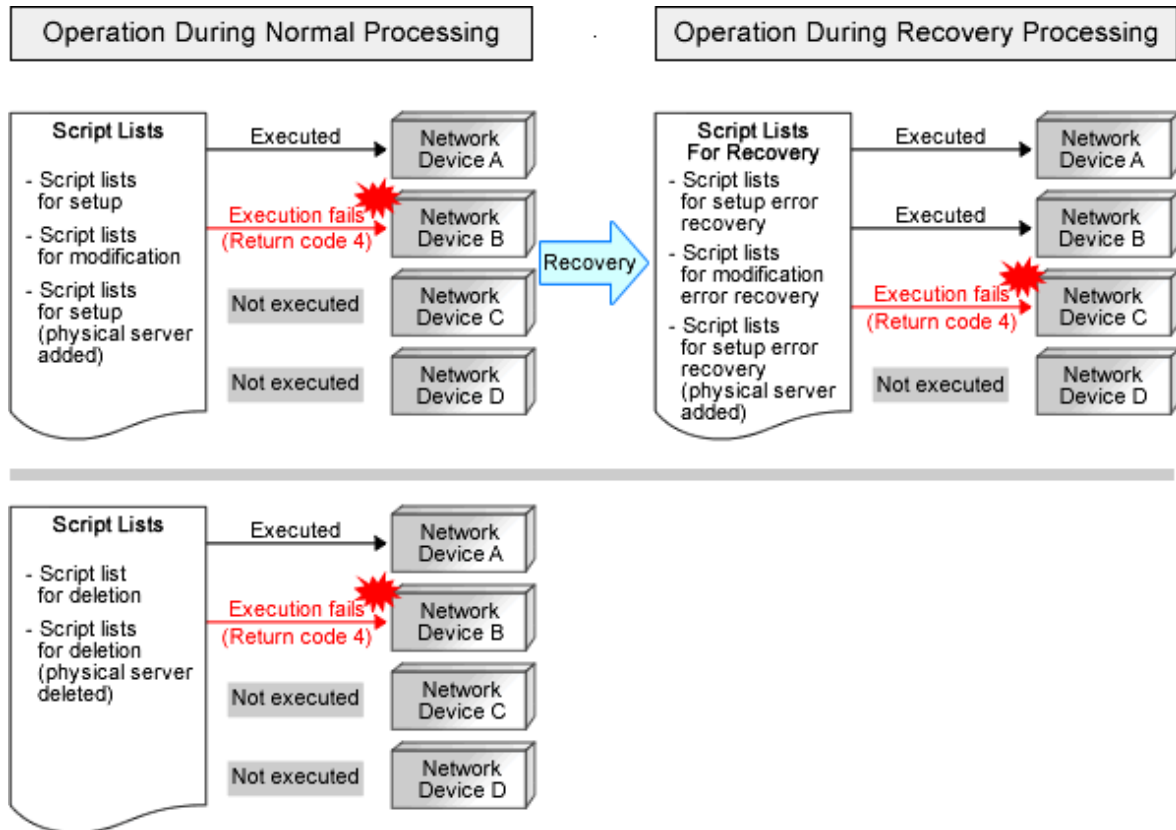Figure D.4 Example Script Operation for SCRIPT_EXECUTION_MODE=continue

Figure D.5 Example Script Operation for SCRIPT_EXECUTION_MODE=stop

Execution Conditions for Scripts for Recovery

This section explains the execution conditions for scripts for recovery.

- When "SCRIPT_EXECUTION_MODE=continue" is specified in the definition file

When an error occurs in a script for configuration or modification, the script for recovery will be executed for the network device the script was being executed on. Execution of the script for recovery is determined based on the return code of the script for configuration or modification.

Return Code of the Script for Configuration or Modification	Application of the Script for Recovery	Status of the Network Device after Script Execution
0	The script for recovery is executed	Unchanged
4	The script for recovery is executed	Unchanged
6	The script for recovery is not executed	Unchanged
8	The script for recovery is not executed	It is placed into maintenance mode.

- When "SCRIPT_EXECUTION_MODE=stop" is specified in the definition file

When an error occurs in a script for configuration or modification, all scripts in the script list for recovery will be executed.

For details of the specified parameters and possible parameter values of the definition file, refer to "D.7 Network Device Automatic Configuration and Operation Definition Files".

D.6.3 Command Files

This section explains the format of command files.

Format

```
Command for Network Device
.....
Command for Network Device
```

Only include commands for the target network device in the command file.

📖 **Information**

....

- Command format depends on the type of network device.

- When creating scripts referring to sample scripts, initial commands executed after logging in to a network device depend on the type of network device. So, it is necessary to change the initial commands and their responses in the script.

- If the structure of a script is same as that of a sample script, commands in the command file are executed after the execution of initial commands.

....

Creation Example

```
class-map match-all %classmapname%
    match source-address ip %ip%
    match source-port %port%
    match destination-address ip %Unm_IPv4& LServer_name&network_resource_name %
    match destination-port %serverport%
    ...
interface %ifname%
    rule access %num% in %classmapname% accept  audit-session-norma audit-match-none
    ...
commit
save startup-config
```

📄 **Point**

....

- All variable information in a command file is within the conversion range and converted before script execution.

  For the variable information which can be used, refer to "Variable Information Usable in Scripts".

- When not using any sample scripts (such as when the infrastructure administrator creates their own new script), create command files in the appropriate format for the created script.

- When scripts do not invoke command files, such as when not using sample scripts, it is no necessary to create a command file.

....

D.6.4 Parameter Files

This section explains the format of the parameter file.

Format

The parameter file is in XML format.

Refer to "15.16 Parameter Files (for Scripts)" in the "Reference Guide (Command/XML) CE" for details.

D.6.5 Script Operation Pre-checks

This appendix explains the procedure for checking the operation of created scripts in advance. Please perform checks in a separate environment in order to prevent the operation check affecting the operational environment.

Operation Checks of Scripts other than "Variable Information"

Check the operation of scripts excluding their "variable information".

1. Prepare the network devices to use for the operation check.

Prepare a network using network devices other than those used in the operating public LAN and admin LAN.

2. Register the network devices for the operation check.

   When using firewalls or server load balancers, create a network pool for the operation check and then register the network devices.

3. Prepare the script for the operation check, basing it on the script you plan to use in actual operation.

   At this time, make the following modifications to enable the operation check.

   - Replace the "variable information" of the script with the post-conversion values.

   - Change the log output settings to save the log in the desired location so that the execution results can be checked.

4. Use the auto-configuration function to perform auto-configuration of the network devices to be used in the operation check.

5. Check the operation results of the script in the output log.

6. Connect to the network devices and delete the definition set for the operation check.

Conversion Checks of "Variable Information"

Check whether the "variable information" specified in the script file and command file was converted as intended.

1. Prepare the network devices to use for the operation check.

   Prepare a network using network devices other than those used in the operating public LAN and admin LAN.

2. Register the network devices for the operation check.

   When using firewalls or server load balancers, create a network pool for the operation check and then register the network devices.

3. Prepare the script that will be used in actual operation as the operation check script.

   - As configuration of network devices is not necessary, change the script to finish before it connects to the network devices.

   - Change the settings to save the log in the desired location so that the post-conversion "variable information" can be checked.

4. Use the auto-configuration function to perform auto-configuration of the network devices to be used in the operation check.

5. Check the conversion results of the "variable information" in the output log.

Figure D.6 Update Checks of Variable Information
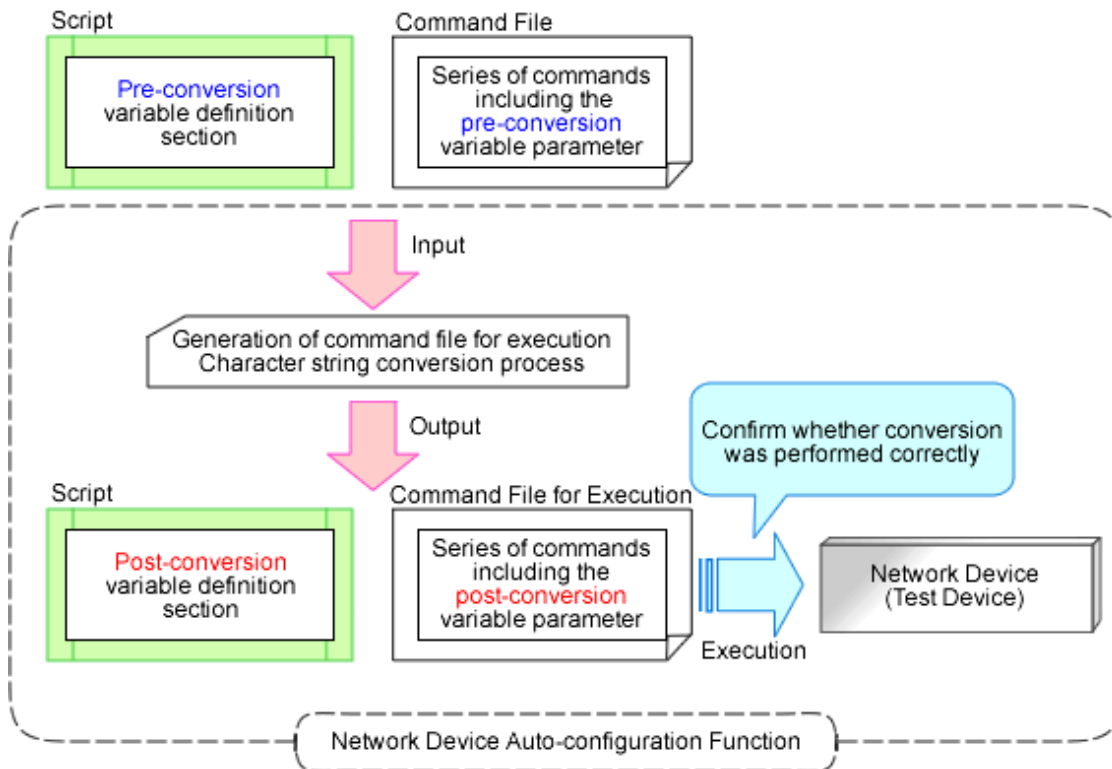
D.7 Network Device Automatic Configuration and Operation Definition Files

The definition used for network device automatic configuration or operation can be changed by setting the value in the following definition file beforehand.

D.7.1 Storage Location of the Definition File

[Windows Manager]

Installation_folder\SVROR\Manager\etc\customize_data

D.7.2 Definition File Name

Name of the Definition File

unm_provisioning.rcxprop

Sample Definition File

unm_provisioning.rcxprop.sample

D.7.3 Definition File Format

Script language

Specify the script language when you want to use a language other than ruby.

📖 Information

Ruby is used as the script language in sample scripts.

Parameter Format of Definition Files

```
extension_Extension=Execution file path
```

Specify the extension of the script language such as "rb" or "pl" for *Extension*.

When there is no specification for the *Extension*, jruby is used.

Execution file path specifies the absolute path.

📋 Example

extension_rb=/usr/bin/jruby

Monitoring Time of Script

Specify the monitoring time when you want to change it to a value besides 300 (seconds).

📖 Information

In the network device automatic configuration function, script execution time is monitored.

When the monitoring time has passed since the beginning of the script execution, the processing of the script is terminated.

Parameter Format of Definition Files

```
EXECUTE_TIMEOUT=monitoring time
```

Specify the monitoring time within the range of 1 to 7200 (seconds).

When the specified value is non-numeric or is outside of the above-mentioned range, 300 (seconds) is used.

 Example
. . . .
EXECUTE_TIMEOUT=600
. . . .

Upper Output Limit of Operation Rulesets

Specify the upper output limit of operation ruleset when you want to change it to a value other than 500 (KB).

 Information
. . . .
When a large amount of data is output as a result of executing a ruleset for operations on network devices, a large amount of memory resources is consumed. Memory consumption can be limited by customizing the upper output limit.
. . . .

Parameter Format of Definition Files

```
SCRIPT_OUTPUT_SIZE_LIMIT= upper output limit
```

Specify the *upper output limit* within the range of 1-10000 (KB).

When the specified value is non-numeric or is outside the range mentioned above, 500 (KB) is used.

 Example
. . . .
SCRIPT_OUTPUT_SIZE_LIMIT=300
. . . .

Operation Specifications when Script Executions Results are Abnormal

This section explains the operations when there are abnormal script execution results when executing a script list. The following script lists are the targets.

- Script lists for setup error recovery

- Script lists for modification error recovery

- Script list for deletion

- Script lists for setup error recovery (physical server added)

- Script lists for deletion (physical server deleted)

For details on the operations when scripts are executed based on specified values, refer to "Differences in Operations Depending on Specifications in the Definition File 'SCRIPT_EXECUTION_MODE'".

Parameter Format of Definition Files

- To execute successive scripts listed in the script list

```
SCRIPT_EXECUTION_MODE=continue
```

- To cancel successive scripts listed in the script list

```
SCRIPT_EXECUTION_MODE=stop
```

If a value other than continue or stop is specified, or no value is specified, stop will be used.

Example

....

SCRIPT_EXECUTION_MODE=continue

....