

FUJITSU Software ServerView Resource Orchestrator Cloud Edition V3.3.0 [Citrix Xen] Automatic Quarantining Function Setup Guide

B1X1-0395-01ENZ0(01)
March 2018

Structure of Product DVDs

Resource Orchestrator is provided on two DVDs. The Cloud Edition program and manuals are contained on the first DVD-ROM.

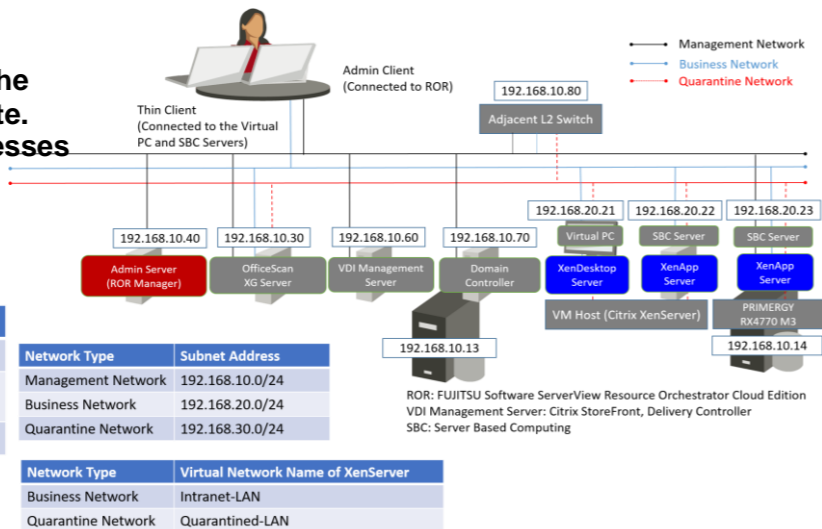
System Configuration

- Connect the hardware devices shown in the figure to the LAN so they can communicate.
- In the following explanations, the IP addresses shown in the figure are used.

* Prepare the admin server with a freshly installed Windows OS.

Server Type	OS Type
Admin server	Windows Server 2008 R2 or later
VM host on which the virtual PC and an SBC server operate	XenServer 7.2 or later
Physical servers on which SBC servers operate	Windows Server 2008 R2 or later

Server Type	Server Name
VM Host (XenServer)	xenserver000
Physical server	xenapp000



Note: This system configuration is only an example and does not indicate the entire support scope of the automatic quarantining function. The environment necessary for management of XenDesktop/XenApp is not explained here.

Before Installing Resource Orchestrator

Perform the following preparations beforehand.

(1) Configure SNMP

To receive hardware monitoring messages, perform configuration so the "SNMP service" starts on the admin server and managed servers.

Specify the IP address of the admin server (192.168.10.40) as the SNMP trap destination of managed servers.

(2) Confirm Required Software

Confirm that the following software has been installed:

- OfficeScan XG Server

(3) Execute the Environment Setup Conditions Check Tool

Execute the environment setup conditions check tool to confirm that the configuration is correct.

(4) Virtual PC

Use Citrix XenDesktop to confirm that a virtual PC is deployed on VMware ESXi.

Install the OfficeScan XG agent on the deployed virtual PC, and perform configuration so the virtual PC is managed by the OfficeScan XG server.

(5) SBC Server Deployed on the VM Host

Confirm that Citrix XenApp server is installed on VMware ESXi.

Install the OfficeScan XG agent on the Citrix XenApp server, and perform configuration so the Citrix XenApp server is managed by the OfficeScan XG server.

(6) SBC Server Deployed on the Physical Server

Confirm that Citrix XenApp server is installed on the physical server.

Install the OfficeScan XG agent on the Citrix XenApp server, and perform configuration so the Citrix XenApp server is managed by the OfficeScan XG server.

Install ServerView Agents for Windows on the Citrix XenApp server.

(7) 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 notification 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.

(8) ROR Manager

Install Windows PowerShell 3.0 or later.

(9) VM Host(Citrix XenServer)

Create a virtual network.

Installation

Refer to the "Automatic Quarantining Function User's Guide" for details.

STEP 1 Install the Product

Installing the Manager(Windows)

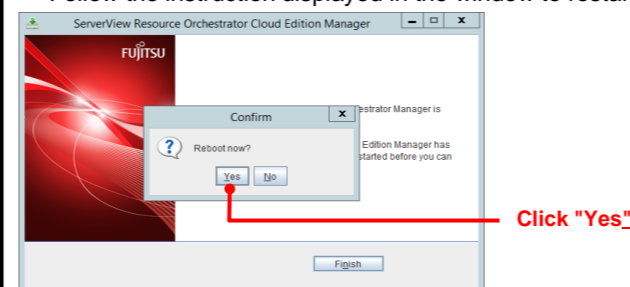
1. Insert the DVD-ROM on the admin server and then select "Cloud Edition" - "Manager installation".



2. Follow the instructions on the wizard to perform the installation. Specify the following values on each screen.

Window	Entry	Value to Enter or Select
Installation Folder Selection	Installation Folder	C:\Program Files (x86)\Resource Orchestrator
Admin LAN Selection	Network to use for the admin LAN	192.168.10.40
Authentication Method Selection	Authentication Method	Select "Internal Authentication".
Privileged User Creation	User Account	manage
	Password	Password for "manage" *Displayed as ●●● on the screen.
	Retype password	Password for "manage" *Displayed as ●●● on the screen.

3. When the installation is complete, the completion window is displayed. Follow the instruction displayed in the window to restart the system.



Installing the Agent (Windows)

1. Insert the DVD-ROM on the admin server and then select "Cloud Edition" - "Agent installation".



2. Follow the instructions on the wizard to perform the installation. Specify the following values on each screen.

Window	Entry	Value to Enter or Select
Installation Folder Selection	Installation Folder	C:\Program Files (x86)\Resource Orchestrator
Admin Server Registration	Admin LAN IP Address of the Admin Server	192.168.10.40
License Authentication	License Authentication Information for the Windows Volume License	Select [Next].

3. When the installation is complete, the completion window is displayed. Follow the instruction displayed in the window to restart the system.

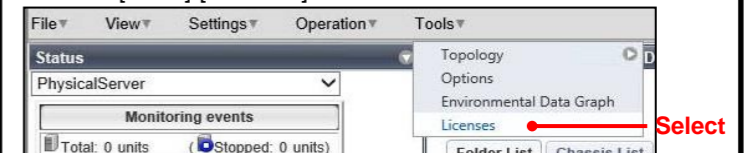
Continued on the Upper Right

STEP 2 Register the License

1. Start the ROR console from a Web browser.
[URL] https://192.168.10.40:23461
2. The login window is displayed. Enter "manage" for the user ID and the password for the "manage" user.



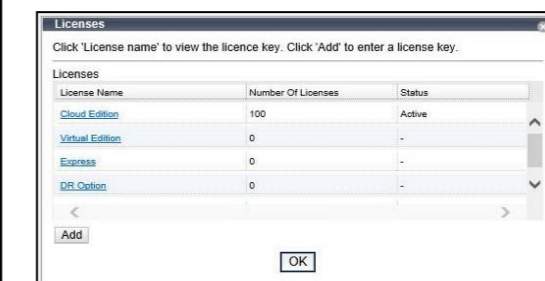
3. From the menu in the displayed window, select [Tools]-[Licenses].



4. Click the [OK] button on the Register License window to register the license.



5. Confirm that the license is registered.



STEP 3 Configure Environment Variables

Configure the following as a system environment variable.

Variable Name	Value
ROR_MGR	Installation_folder\SVROR\Manager\

Refer to "2.3.1 Configuring Environment Variables" in the "Automatic Quarantining Function User's Guide" for details.

Continued on the Next Page

STEP 4 Create Definition Files

Create definition files. If the definition files already exist, add definitions using the following format.

Definition Files when Using Virtual PCs or SBC Servers Deployed on VM Hosts

■ Storage Location on the Admin Server (ROR Manager)

C:\Program Files(x86)\Resource Orchestrator\SVROR\Manager\etc\vm

Definition File Name	Value to Set in the Definition File
register_ipmiless	None (Create an empty file)

■ Storage Location on the Admin Server (ROR Manager)

C:\Program Files(x86)\Resource Orchestrator\SVROR\Manager\etc\customize_data

Definition File Name	Value to Set in the Definition File
l_server.rcxprop	reserve_ip_address=true
vnetwork_citrixen.rcxprop	"Intranet-LAN"=20 "Quarantined-LAN"=30
avmgr_network.rcxprop	Intranet-LAN=Quarantine-LAN
server_control.rcxprop	ServerControl,V1.1 ##### # server_control.rcxprop # #All Rights Reserved, Copyright(C) FUJITSU LIMITED 2011 ##### # physical_server, ipmi # xenserver000,false

Common Definition Files for Virtual PCs and SBC Servers

(1) Create a work folder.

```
> mkdir D:\avmgr <RETURN>
```

(2) On the ROR console, select [File]-[System Configuration File]-[Download Template].
The [File Download] window is displayed.

(3) Click the [Save] button.

(4) Specify the storage directory (D:\Avmgr) and the file name (rcx-import-avmgr.csv).

(5) Click the [Save] button.

(6) Edit the content of the system configuration file (D:\Avmgr\rcx-import-avmgr.csv) as shown below.

Value to Set in the System Configuration File (rcx-import-avmgr.csv)	
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	
[ServerVMHost]	
Operation,server_name,vm_login_name,vm_login_passwd,vm_passwd_enc	
new,xenserver000,root,xenserver000_password,plain	
[ServerAgent]	
operation,server_name	
new,xenapp000	

STEP 5 Create Rulesets

(for the SBC Server Deployed on the Physical Server)

When using the SBC server deployed on the physical server and register rulesets for the configuration of VLAN settings for the adjacent L2 switch.

Create rulesets with the following names.

■ Storage Location on the Admin Server (ROR Manager)

C:\Program Files(x86)\Resource Orchestrator\SVROR\Manager\etc\scripts\network_resource\

Network Type	Ruleset Name
Management network	untag_vlan_admin-net
Business network	tag_vlan_intra-net
Quarantine network	tag_vlan_quarantined-net

Refer to "2.5.8 Rulesets (Scripts) for L2 Switches" in the "Automatic Quarantining Function User's Guide" for

Continued on the Upper Right

STEP 6 Enable Notification

Refer to the "Automatic Quarantining Function User's Guide" for details.

(1) Enable message notifications. Execute the following

```
> msgnotice register -name vdimgr -ip 192.168.10.60 -user_name admin -passwd  
VD\password_of_the_admin_server <RETURN>  
> msgnotice enable <RETURN>
```

(2) Authorize remote management. Execute the following command, and confirm that the content of TrustedHosts is a single asterisk (*) or the IP address for connection to the VDI management server (192.168.10.60).

```
> winrm get winrm/config/client <RETURN>
```

(3) 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 <RETURN>
```

(4) 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".

```
> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned <RETURN>
```

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

```
> msgnotice info <RETURN>
```

STEP 7 Register Resources

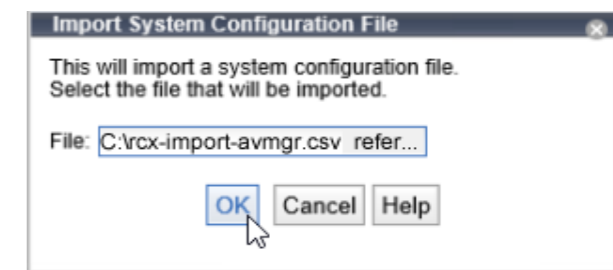
Refer to the "Automatic Quarantining Function User's Guide" for details.

(1) On the ROR console, select [File]-[System Configuration File]-[Import].

The [Import System Configuration File] dialog is displayed.

(2) Specify the system configuration file (rcx-import-avmgr.csv) prepared in "STEP 4 Create Definition Files".

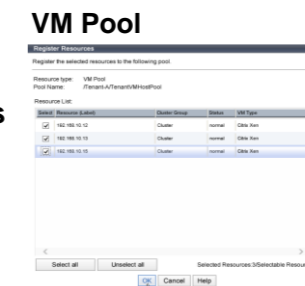
(3) Click the [OK] button.



STEP 8 Register Resource Pools

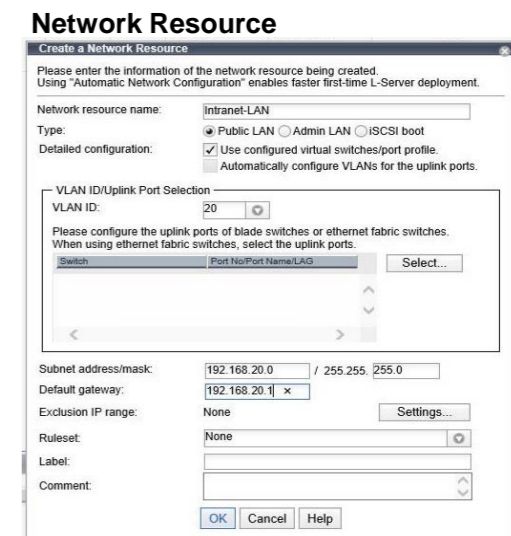
When Using Virtual PCs and SBC Servers Deployed on VM Hosts

(1) From the orchestration tree, right-click the target VM pool, then register the VM host.



(2) From the orchestration tree, right-click the target network pool and select [Create Network Resource]-[New].

Register the business network and the quarantine network.



Business Network

Window	Entry	Value to Enter or Select
Network resource name	The resource name of the business network	Intranet-LAN
Type	The type of the network resource	Public LAN
Detail configuration		Use configured virtual switches/port profile
VLAN ID	The VLAN ID of the business network	20
Subnet address/mask	Subnet address/mask	192.168.20.0/24
Default gateway	Default gateway	192.168.20.1

Quarantine Network

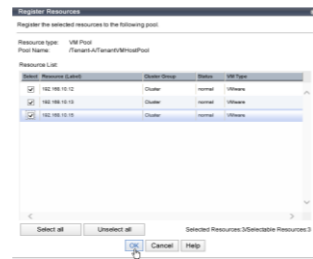
Window	Entry	Value to Enter or Select
Network resource name	The resource name of the quarantine network	Quarantine-LAN
Type	The type of the network resource	Public LAN
Detail configuration		Use configured virtual switches/port profile
VLAN ID	The VLAN ID of the quarantine network	30
Subnet address/mask	Subnet address/mask	192.168.30.0/24
Default gateway	Default gateway	192.168.30.1

Continued on the Next Page

When Using the SBC Server Deployed on the Physical Server

- From the orchestration tree, right-click the target server pool, then register the target physical server (xenapp000).

Server Pool



- Create the network configuration information XML file for the registration of the adjacent L2 switch.

Network Configuration Information XML File for the Registration of the Adjacent Switch

```
<?xml version="1.0" encoding="utf-8"?>
<NetConfig>
<Netdevices>
<Mode>add</Mode>
<Netdevice ip="192.168.10.80" name="Catalyst3750-1">
<Types>
<Type>L2-Switch</Type>
</Types>
<ApplianceType>physical</ApplianceType>
<Maintenance>false</Maintenance>
<AutoConfiguration>true</AutoConfiguration>
<MgmtInfos>
<Snmps>
<ReadCommunity>snmp_community</ReadCommunity>
</Snmps>
<LoginInfos>
<LoginInfo protocol="remote_login" auth_type="local password" authority="user" check="false">
<User>user1</User>
<Password>user_pass</Password>
<PrivilegedPassword>admin_pass</PrivilegedPassword>
<PasswordEncryption>false</PasswordEncryption>
</LoginInfo>
</LoginInfos>
<Monitoring method="1">
<Methods>
<Method>SNMP</Method>
</Methods>
<Interval>300</Interval>
<RetryCount>3</RetryCount>
<Timeout>30</Timeout>
</Monitoring>
</MgmtInfos>
</Netdevice>
</Netdevices>
<Links>
<Link>
<Devices>
<Device ip="192.168.10.80" kind="netdevice" name="Catalyst3750-1">
<Port>Gi1/0/1</Port>
</Device>
<Device ip="192.168.10.14" kind="server" name="xenapp000">
<Port>1</Port>
<NicIndex>1</NicIndex>
</Device>
</Devices>
</Link>
<Link>
<Devices>
<Device ip="192.168.10.80" kind="netdevice" name="Catalyst3750-1">
<Port>Gi1/0/2</Port>
</Device>
<Device ip="192.168.10.14" kind="server" name="xenapp000">
<Port>2</Port>
<NicIndex>2</NicIndex>
</Device>
</Devices>
</Link>
</Links>
</NetConfig>
```

Continued on the Upper Right

- Register the adjacent L2 switch. Execute the following command.

```
> rcxadm netconfig import -file D:\avmgr\netdevice_info.xml <RETURN>
```

- Confirm that the adjacent L2 switch has been registered successfully. Execute the following command.

```
> rcxadm netdevice list <RETURN>
```

- From the orchestration tree, right-click "AdminLan", then click [Delete] in the displayed menu. "AdminLan" will be deleted.

- From the orchestration tree, right-click the target network pool and select [Create Network Resource]-[New]. Register the business network and the quarantine network.

Business Network

Window	Entry	Value to Enter or Select
Network resource name	The resource name of the business network	Phy-Intranet-LAN
Type	The type of the network resource	Public LAN
Detail configuration		Use configured virtual switches/port profile
VLAN ID	The VLAN ID of the business network	21
Subnet address/mask	Subnet address/mask	192.168.20.0/24
Default gateway	Default gateway	192.168.20.1
Ruleset	Ruleset	tag_vlan_intra-net

Quarantine Network

Window	Entry	Value to Enter or Select
Network resource name	The resource name of the business network	Phy-Intranet-LAN
Type	The type of the network resource	Public LAN
Detail configuration		Use configured virtual switches/port profile
VLAN ID	The VLAN ID of the business network	21
Subnet address/mask	Subnet address/mask	192.168.20.0/24
Default gateway	Default gateway	192.168.20.1
Ruleset	Ruleset	tag_vlan_intra-net

Network Resource

- From the orchestration tree, right-click the target network pool and select [Create Network Resource]-[Using existing admin LAN subnet]. Register the management network.

Management Network

Window	Entry	Value to Enter or Select
Network resource name	The resource name of the management network	Phy-Admin-LAN
Type	The type of the network resource	Admin LAN
Detail configuration		Use configured virtual switches/port profile
VLAN ID	The VLAN ID of the management network	11
Subnet address/mask	Subnet address/mask	192.168.10.0/24
Default gateway	Default gateway	192.168.10.1
Ruleset	Ruleset	untag_vlan_admin-net

STEP 9 Register Antivirus Software

- Register antivirus software. Execute the following command.

```
> rcxadm avmgr create -name corpxg -mgmt_soft_name corp -ip 192.168.10.30 <RETURN>
```

- Confirm that the antivirus software is successfully registered. Execute the following command.

```
> rcxadm avmgr list <RETURN>
```

Continued on the Next Page

STEP 10 Import the Virtual PC and SBC Server Deployed on the VM Host

(1) Create the CSV configuration file. Execute the following command.

```
> convertVMtoLServer -exportfile D:\%avmgr <RETURN>
```

(2) Import the virtual PC and SBC server deployed on the VM host so they can be managed by ROR. Execute the following command.

```
> convertVMtoLServer -file D:\%avmgr\convertVMtoLserver_20170831000000.csv <RETURN>
```

STEP 11 Import the SBC Server Deployed on the Physical Server

Link the Physical Server with a Physical L-Server, and Load the IP Address of the Management Network

(1) Perform linking of the physical server. Execute the following command.

```
> rcxadm lserver convert -with xenapp000 <RETURN>
```

Load the IP Address of the Business Network Assigned to the Physical Server

(2) Execute the following command. The base XML file for changing the network will be output.

```
> rcxadm lserver show -name xenapp000 -format xml > D:\%avmgr\intranet_xenapp000.xml <RETURN>
```

(3) Edit the file output in step (2) as shown below.

```

For the Business Network (intranet_xenapp000.xml)
<?xml version="1.0" encoding="utf-8"?>
<Resources>
<LServer name="xenapp000" label="for Intranet-LAN">
<NICs>
<NIC>
<NICIndex>0</NICIndex>
<MacAddress auto="false"></MacAddress>
<NetworkLinks>
<NetworkLink name="Phy-Admin-LAN" index="0" vlan_mode="untagged">
<IpAddress auto="false" address="192.168.10.14"/>
</NetworkLink>
</NetworkLinks>
</NIC>
<NIC>
<NICIndex>1</NICIndex>
<MacAddress auto="false"></MacAddress>
<NetworkLinks>
<NetworkLink name="Phy-Intranet-LAN" index="0" vlan_mode="tagged">
<IpAddress auto="false" address="192.168.20.23"/>
</NetworkLink>
</NetworkLinks>
</NIC>
</NICs>
</LServer>
</Resources>

```

(4) Using the XML file created in step (3), specify the network resources and IP addresses corresponding to the NICs of the physical L-Server. Execute the following command.

```
> rcxadm lserver modify -name xenapp000 -type physical -file D:\%avmgr\businesslan_xenapp000.xml
```

Continued on the Upper Right

Create and Store the XML File for Transfer to the Quarantine Network

(5) Execute the following command. The base XML file for changing the network will be output.

```
> rcxadm lserver show -name xenapp000 -format xml > D:\%avmgr\quarantine_xenapp000.xml <RETURN>
> rcxadm lserver show -name xenapp000 -format xml > D:\%avmgr\unquarantine_xenapp000.xml <RETURN>
```

(6) Edit the XML file output in step (5) as shown below.

For the Management and Business Networks (unquarantine_xenapp000.xml)	For the Quarantine Network (quarantine_xenapp000.xml)
<pre> <?xml version="1.0" encoding="utf-8"?> <Resources> <LServer name="xenapp000" label="for Unquarantined-LAN"> <NICs> <NIC> <NICIndex>0</NICIndex> <MacAddress auto="false"></MacAddress> <NetworkLinks> <NetworkLink name="Phy-AdminLAN" index="0" vlan_mode="untagged"> <IpAddress auto="false" address="192.168.10.14"/> </NetworkLink> </NetworkLinks> </NIC> <NIC> <NICIndex>1</NICIndex> <MacAddress auto="false"></MacAddress> <NetworkLinks> <NetworkLink name="Phy-Internet-LAN" index="0" vlan_mode="tagged"> <IpAddress auto="false" address="192.168.20.23"/> </NetworkLink> </NetworkLinks> </NIC> </NICs> </LServer> </Resources> </pre>	<pre> <?xml version="1.0" encoding="utf-8"?> <Resources> <LServer name="xenapp000" label="for Quarantined-LAN"> <NICs> <NIC> <NICIndex>0</NICIndex> <MacAddress auto="false"></MacAddress> <NetworkLinks> <NetworkLink name="Phy-Internet-Quarantined-LAN" index="0" vlan_mode="tagged"> <IpAddress auto="false" address="192.168.30.34"/> </NetworkLink> </NetworkLinks> </NIC> <NIC> <NICIndex>1</NICIndex> <MacAddress auto="false"></MacAddress> <NetworkLinks> <NetworkLink name="Phy-Internet-Quarantined-LAN" index="0"> <IpAddress auto="false" address="192.168.30.33"/> </NetworkLink> </NetworkLinks> </NIC> </NICs> </LServer> </Resources> </pre>

Tryout

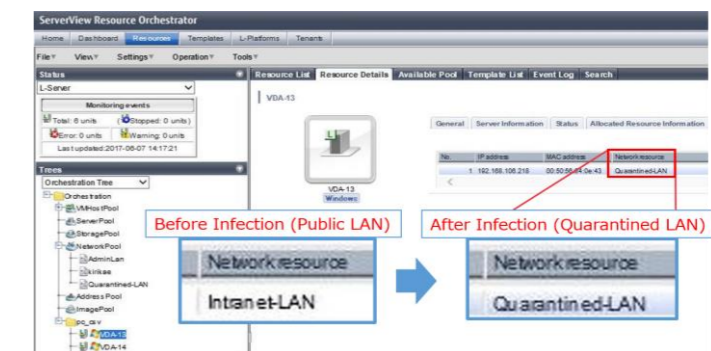
■ Download a dummy virus to a virtual PC and an SBC server, and confirm that the corresponding L-Servers are transferred to the quarantine network.

(1) Download a dummy virus to a virtual PC and SBC server.

(2) Confirm that security risks have been detected through email notifications sent by the antivirus software or by checking the system log of the admin server.

(3) Confirm the following:

- From the ROR console, confirm that the networks of the target virtual PC and SBC server have been switched to the quarantine network.
- Confirm the IP addresses of the target virtual PC and SBC server.



How to Reference the Electronic Manuals

Perform the following procedure to refer to the electronic manuals for Resource Orchestrator:

1. Insert the first DVD-ROM of Resource Orchestrator into the DVD drive.
2. On the initial window that is displayed automatically, click [Documentation] from the left menu and then [Manual].
3. The online manuals are listed in the Web browser. Refer to those in the Cloud Edition section.

For the most recent manuals, visit the Fujitsu Web site.

<http://software.fujitsu.com/jp/manual/manualindex/p17000045e.html> (As of March 2018)