CA92344-1482-03

FUJITSU Software
ServerView Infrastructure Manager V2.0
Settings for Monitoring Target OS and
Cloud Management Software

March, 2017
FUJITSU LIMITED

To manage an OS by using ServerView Infrastructure Manager V2.0 (hereafter referred to as “ISM 2.0”), set up on the OS side is required. This document provides the required information for the settings.

For abbreviations used within this document and details of Node Management, refer to the manuals below.

・FUJITSU Software ServerView Infrastructure Manager V2.0 User’s Manual
・FUJITSU Software ServerView Infrastructure Manager V2.0 Glossary

1. List of Settings Required per Monitoring Target OS/Could Management Software

To utilize the display of virtual machine information, device information (OS information and disk volume), Log Manager (OS log collection) and firmware update (Online PCI card) from ISM 2.0, it is required to perform setup for each OS/Cloud Management Software. Perform the change in settings according to the tables shown below.

✓: Settings required ×: Settings not required -: Not applicable

		Service		Security			Domain	
		sshd	WinRM	Firewall	sslv3	PowerShell	SPN	ISM-VA Settings
Red Hat Enterprise Linux	6.x	✓	-	×	-	-	-	✓
	7.x	✓	-	×	-	-	-	✓
SUSE Linux Enterprise Server	11	✓	-	✓	-	-	-	✓
	12	✓	-	✓	-	-	-	✓
Windows Server	2008R2	-	✓	✓	-	✓	✓	✓
	2012	-	✓	✓	-	✓	✓	✓
	2012R2	-	✓	✓	-	✓	✓	✓
	2016	-	✓	✓	-	✓	✓	✓
Windows Server VMware ESXi	5.x	-	-	-	✓	-	-	✓
	6.x	-	-	-	✓	-	-	✓

Table 1. List of Required Settings per Monitoring OSes

		Settings for each host	Domain		
		WinRM	SPN	ISM-VA Settings	Kerberos delegation configuration
vCenter Server	5.5 or later	-	-	✓	-
	6.x	-	-	✓	-
Microsoft Failover Cluster	Windows Server 2012 or later	✓	✓	✓	✓

Table 2. List of Required Settings per Monitoring Cloud Management Software

[Note]

・To monitor a target server, it is required to register OS information, with the user account having administrator privilege.

- To manage Emulex LAN/FC/CNA cards mounted on Windows/Linux, it is required that Emulex OneCommand Manager CLI is already installed on the OS of the target server.
- To manage the QLogic FC card mounted on Windows/Linux, it is required that QLogic QConvergeConsole CLI is already installed on the OS of a target server.
- To manage LAN/FC/CNA cards mounted on Linux, it is required that "lspci command" is executable on the Linux of the target server.
- Use the latest Emulex OneCommand Manager CLI or QLogic QConvergeConsole CLI. Apply the latest drivers for LAN/FC/CNA cards.
- To monitor the performance of the disk speed and network speed of Linux, it is required that the systat package is already installed on the OS of a target server.
- Even when having changed the domain user password from Active Directory, you can get the information without immediately making it effective. However, immediately changing the password in ISM 2.0 is recommended.

2. Settings Procedure for Monitoring Target (OS)

2.1. Settings Procedure for Windows

ISM 2.0 uses WS-Management protocol for the monitoring devices, with Windows Server installed. Https Protocol + Basic authentication is used as the communication method. The following are the required settings.

- Checking WinRM service has started
- Settings for WinRM service
- Opening the firewall port
- Changing execution policy for Windows PowerShell script

2.1.1. Checking WinRM Service Has Started

Open the command prompt as administrator and execute the following command to check that WinRM service has started.

```
>sc query winrm
```

Check the following result and check that the STATE is RUNNING.

```
        TYPE               : 20   WIN32_SHARE_PROCESS
        STATE              : 4   RUNNING
                                 (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0   (0x0)
        SERVICE_EXIT_CODE  : 0   (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

Execute the following command to start WinRM service if the WinRM service has not started.

```
>sc start winrm
```

[Note]

In some cases, WinRM service does not start automatically depending on the conditions. It is required to change the settings so that WinRM service can be auto-started (auto) or delayed-auto-started (delayed-auto).

The following is an example of the automatic start setting.

```
>sc config winrm start=auto
```

2.1.2. Settings for WinRM Service

(1) Settings for WinRM Service

Since Basic authentication is not allowed in the initial settings (refer to 1-1), the settings to allow Basic authentication is required.

Since https communication is used, communication with Basic authentication is encrypted.

Open the command prompt as administrator and execute the following command.

```
>winrm quickconfig
```

In cases where the following message is displayed, although WinRM service is running, remote access permission is not yet set. Therefore, proceed to the following steps. The settings are already complete if the message “WinRM service already runs on this computer” is displayed. In this case, proceed to “(2) Settings for Https Communication.” After entering “y”, press the [Enter] key.

```
WinRM service is already running on this machine.
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:

Configure LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.
Make these changes [y/n]? y
```

The following message is shown.

```
WinRM has been updated for remote management.

Configured LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.
```

(1-1) Allowing Basic Authentication

Execute the following command.

```
>winrm set winrm/config/service/Auth@{Basic="true"}
```

(1-2) Additional Settings Item (Windows Server 2008R2)

Execute the following command to increase the numerical value of MaxConcurrentOperationsPerUser depending on the type and the number of cards, if the OS of a target server is Windows Server 2008 R2.

Execute the following command.

```
>winrm set winrm/config/Service @{MaxConcurrentOperationsPerUser="numerical value"}
```

Ex. In the case where the above value is set as 1500(1500 is recommended because 1500 is set by default in Windows Server 2012/2012R2.)

```
>winrm set winrm/config/Service @{MaxConcurrentOperationsPerUser="1500"}
```

(2) Settings for Https Communication

To establish https communication, certificate setup is required.

(2-1) Preparation of Required Tools

Two tools are required for creating a certificate. You can create the certificate without depending on the execution conditions.

・.NET Framework 4.5 (Download site)

https://www.microsoft.com/en-us/download/details.aspx?id=30653

・Windows Software Development Kit (Download site)

https://developer.microsoft.com/en-us/windows/downloads/windows-10-sdk

[Note]

The Windows Software Development Kit of the above URL is supported in Windows 8.1 and Windows Server 2012 or later.　When installing OS of other than mentioned, install the appropriate Windows Software Development Kit.

Windows Software Development Kit includes two tools required for creating the certificate.

Certificate creation tool (makecert.exe）

https://msdn.microsoft.com/en-us/library/bfsktky3(v=vs.80).aspx

Personal information exchange file creation tool (pvk2pfx.exe)

https://msdn.microsoft.com/en-us/library/windows/hardware/ff550672(v=vs.85).aspx

(3) Creating Certificate

Use the certificate creation tool and personal information exchange file creation tool to create the following three files.

・CER file (Certificate)

・PVK file (Private key file)

・PFX file (Service certificate)

For more detailed procedure of certificate creation, refer to the following URL.

https://blogs.technet.microsoft.com/junichia/2010/11/09/azure-for-itpro-3

(4) Creating a Certificate and Private Key Files

In order to create the certificate and private key files, it is required to execute commands suitable for the conditions of a target server.

The following is a command example where the server name of the target server is set as “192.168.10.10” and the effective period of the certificate is set to March 30th, 2017.

```
>makecert.exe -r -pe -n "CN=192.168.10.10" -e 03/30/2017 -eku 1.3.6.1.5.5.7.3.1 -ss My
-sr localMachine -sky exchange <certificate file name.cer> -sv <private key file name.pvk>
```

For detailed settings on the certificate configuration, refer to the following URL.
https://technet.microsoft.com/ja-jp/library/ms186362(v=sql.105).aspx

(5) Creating a Service Certificate

Execute the following command.

```
>pvk2pfx.exe -pvk <private key file name.pvk> -spc <certificate file name.cer> -pfx <service certificate file name.pfx>
```

(6) Registering Certificate and Service Certificate

Open the Certificate Snap-In and register the certificate created above in steps (4) and (5).

1. Execute mmc. exe on the target server.
2. From [File] >, select [Add and Remove Snap-In].
3. From [Available Snap-in], select “Certificate” to [Add].
4. Select “Computer Account” and click on [Next] > [Finish] in sequence.
5. Click on [OK].

(7) Registering SSL certificate

1. Register <certificate file name.cer> with Trusted Root Certification Authority.
   From [Console Root] > [Certificates (Local Computer)] >, and right-click on [Trusted Root Certificate Authority]. From [ALL Tasks] > [Import], select <certificate file name.cer> file, and finish Certificate Import Wizard.
2. Confirm if <certificate file name.cer> is successfully registered with [Trusted Root Certificate Authority].
   Select [Console Root] > [Certificate (Local Computer)] > [Trusted Root Certificate Authority] > [Certificate] in sequence and confirm if “Issued to” and “Issued by” are the server names specified as CN, and “Authentication Purpose” is specified as “Server Authentication.”
3. Register <service certificate file name.pfx> in ‘personal’.
   From [Console Root] > [Certificate (Local Computer)] >, right-click on [Personal]. From [All Tasks] > [Import], select<service certificate file name.pfx>, and finish Certificate Import Wizard.
4. Confirm if <service certificate file name.pfx> is successfully registered with [Personal].
   From [Console Root] > [Certificate (Local Computer)] > [Personal] in sequence and confirm if “Issued to” and “Issued by” are the server name specified as CN, and “Authentication Purpose“ is specified as “Server Authentication.”

(8) Register the Thumbprint Described on the Certificate to WinRM Service.

(8-1) Check Thumbprint

The following shows how to check if the certificate is saved in LocalMachine¥my.

1. Start PowerShell from a command prompt.
2. Check the Thumbprint. Execute the following command.

```
>ls cert:LocalMachine¥my
```

This is shown as follows.

```
WinRM service is already running on this machine.
PS C:¥Windows¥system32> ls cert:LocalMachine¥my


Directory: Microsoft.PowerShell.Security¥Certificate::LocalMachine¥my
Thumbprint                                          Subject
----------                                           -------
1C3E462623BAF91A5459171BD187163D23F10DD9     CN=192.168.10.10
```

(8-2) Register the Thumbprint Described on the Certificate with WinRM Listener.

Finish Powershell and execute the following command. Space is required between "HTTPS" and "@".

```
>winrm create winrm/config/listener?Address=*+Transport=HTTPS @{Hostname="<CN Name that was specified
 above in step (4)Creating a Certificate and Private Key Files>";CertificateThumbprint="<created certificate
 thumbprint>"}
```

(8-3) Checking WinRM Listener is registered

Execute the following command.

```
>winrm get winrm/config/listener?Address=*+Transport=HTTPS
```

If the command result as shown below is returned, WinRM Listener is successfully registered.

```
Listener
    Address = *
    Transport = HTTPS
    Port = 5986
    Hostname = 192.168.10.10
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint = 1C3E462623BAF91A5459171BD187163D23F10DD9
    ListeningOn = 192.168.10.10, 127.0.0.1, ::1, 2001:258:8402:200:bd8a:1c1:c50d
:8704, fe80::5efe:192.168.10.10%13, fe80::bd8a:1c1:c50d:8704%12
```

2.1.3. Opening a Firewall Port

You need to open the port that you have set up in the above WinRM Listener, so that WinRM services can accept requests. The default port number of https communication is 5986.

(1) In the Case of Windows Server 2008 R2

Execute the command as shown below.

```
>netsh advfirewall firewall add rule name= <firewall rule name> enable=yes localip=any remoteip=any
protocol=tcp localport=<port number> remoteport=any edge=no dir=in profile=domain,private,public action=allow
```

(Ex.) Set the name “WinRM” as the rule to open port number 5986.

```
>netsh advfirewall firewall add rule name=WinRM enable=yes localip=any
remoteip=any protocol=tcp localport=5986 remoteport=any edge=no dir=in profile=domain,private,public
action=allow
```

(2) In the Case of Windows Server 2012/2012R2/2016

1. Open the PowerShell from the command prompt.
2. Execute the command as shown below.

```
>New-NetFirewallRule -DisplayName <firewall rule name> -Action Allow -Direction Inbound -Enabled True -Protocol
TCP -LocalPort <port number>
```

Ex.) Set the name “WinRM” as the rule to open the port number 5986.

```
>New-NetFirewallRule -DisplayName WinRM -Action Allow -Direction Inbound -Enabled True  -Protocol TCP -
LocalPort 5986
```

[Note]

The firewall settings differ depending on the environment of managed servers.

2.1.4. Changing Execution Policy for Windows PowerShell

Open Windows PowerShell as administrator and execute the following command.

```
>set-executionpolicy remotesigned
```

If the following message appears, enter [Y] and press the [Enter] key.

```
Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might
expose you to the security risks described in the about_Execution_Policies help topic at
http://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes  [N] No  [S] Suspend   [?] Help (default is "Y"): y
```

2.1.5. Settings When Using Domain User Account

Monitoring by using a domain user account is the function supported in ISM2.0.0.a or later.
You cannot monitor multiple different domain environments concurrently.

(1) Adding SPN to Active Directory

It is required to correctly register the Service Principal Name (SPN) of a managed server on Active Directory when monitoring a Windows Server using the domain user account. Execute the following procedure to register the Service Principal Name of the managed server.

```
>setspn –A HOST/[monitoring target IP address] [monitoring target host name]
```

Checking command

```
>setspn –L [monitoring target host name]
```

Removal command

```
>setspn –D HOST/[monitoring target IP address] [monitoring target host name]
```

(2) Adding domain information to ISM-VA

When carrying out monitoring using a domain user account, execute the procedures in "3.4.2 Initial Settings of ISM" (ISM 2.0 User's Manual).

(3) Adding DNS information to ISM-VA

When carrying out monitoring using the domain user account, execute the procedures in "ISM2.0_ User's Manual (4.9 Network Settings Add DNS server)" to register the DNS server on ISM-VA.

2.2. Settings Procedure for Red Hat Enterprise Linux

ISM 2.0 communicates with the target servers with Red Hat Enterprise Linux installed, by using SSH (Secure Shell service). The following settings are required.

・Starting SSH service

2.2.1. Checking SSH Service Has Started

Configure so that sshd can be started. The command differs depending on the OS versions.

(1) In the Case of Red Hat Enterprise Linux 6

Execute the following command and confirm if sshd is started.

```
#chkconfig –list sshd
```

The start of sshd is disabled if the result shown below is displayed.

```
sshd                0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

Execute the following command to cause ssdh to start automatically if the item of the number (corresponding to the run level of the management target server) is "off."

Copyright 2017 FUJITSU LIMITED

```
#chkconfig sshd on
```

(2) In case of Red Hat Enterprise Linux 7

Execute the following command and confirm if sshd is started.

```
#systemctl is-enabled sshd
```

The starting of sshd is disabled if the result as shown below is displayed.

```
disabled
```

Execute the following command if starting sshd is disabled.

```
#systemctl enable sshd
```

2.2.2. Settings When Using Domain User Account

Monitoring by using a domain user account is the function supported in ISM2.0.0.a or later.

Pay attention to the following points in monitoring by using the domain user account.

(1) Adding domain information to ISM-VA.

When carrying out monitoring using the domain user account, execute the procedures in “3.4.2 Initial Settings of ISM” (ISM 2.0 User’s Manual).

(2) Adding DNS information to ISM-VA

When carrying out monitoring using the domain user account, execute the procedures in “ISM2.0_ User’s Manual (4.9 Network Settings Add DNS server)” to register the DNS server on ISM-VA.

(3) Restriction on domain user account name

Also pay attention to the restriction on the user names of Linux when you use the domain user name, registered on Active Directory, for Linux.

＜Representative examples unavailable for Linux user names＞

・ Uppercase letters, numeric characters at the beginning, and symbols, such as dot (.)

(4) Restriction when collecting Emulex card information

Use “hbacmd” to collect the card information for the devices on which the card provided by Avago/Emulex is mounted.

When collecting the card information with other than the root user authorization, give “hbacmdan” administrator privilege. For details, refer to “OneCommandManager Command Line Interface User Manual“.

(5) Restriction when collecting QLogic card information

You cannot get the information about the devices on which the card provided by QLogic is mounted, by using the domain user account. Register the root user from Edit OS Information screen to get the information.

(6) Restriction when collecting ServerView logs

You cannot collect ServerView logs by using the domain user account. Register the root user from Edit OS Information screen to collect the information.

(7) Restriction when updating firmware

You cannot execute online firmware update by using the domain user account. Register the root user from Edit OS Information screen to execute firmware update.

2.2.3 Setting Up the Account Used for Monitoring

(1) Setting ".bashrc"

Open ".bashrc" file in the home directory of an applicable account. Create the file if there is no ".bashrc" file.

```
#vi ~/.bashrc
```

Add the paths to "/sbin", "/usr/sbin" and "/usr/loca/sbin" to ".bashrc" file.

```
PATH=$PATH:/sbin
PATH=$PATH:/usr/sbin
PATH=$PATH:/usr/local/sbin
```

(2) Setting Up the Environment Variable

To execute the Log Collection function of ServerView, log in to a monitoring target with SSH by using the OS account registered with an ISM node, and confirm if the following conditions have been met (*).

・Directed to home directory upon login.
・'~' is included in the prompted strings upon login.
・'$' or '#' is included after ' ~' in the prompted strings upon login.
Ex. 1) [root@hostname ~]#
Ex. 2) ADUSER¥ismuser@hostname ~ $

* You can change the prompted strings by changing the value of environment variable $PS1.
Example of parameter of environment variable $PS1)

```
[root@localhost ~]# echo $PS1
[¥u@¥h ¥W]¥$
```

2.3. Settings Procedure for SUSE Linux Enterprise Server

ISM 2.0 communicates with target servers with SUSE Linux Enterprise Server installed, by using SSH (Secure Shell service). The following are required settings.

・Checking SSH service is started
・Opening the firewall port

2.3.1. Checking SSH Service Has Started

The start of sshd is disabled by default in SUSE Linux Enterprise Server.

Make settings so that sshd can be started. The command differs depending on OS versions.

(1) SUSE Linux Enterprise Server 11

Execute the following command and confirm if sshd is started.

```
#chkconfig –list sshd
```

The start of sshd is disabled if the result is shown as follows.

```
sshd                0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

Execute the following command so that sshdcan be started automatically if the item of the number (corresponding to the run level of the target server) is "off."

```
#chkconfig sshd on
```

(2) SUSE Linux Enterprise Server 12

Execute the following command and confirm if sshd is started.

```
#systemctl is-enabled sshd
```

The start of sshd is disabled if the result is as shown below.

```
disabled
```

Execute the following command if the start of sshd is disabled.

```
#systemctl enable sshd
```

2.3.2. Opening the Firewall Port

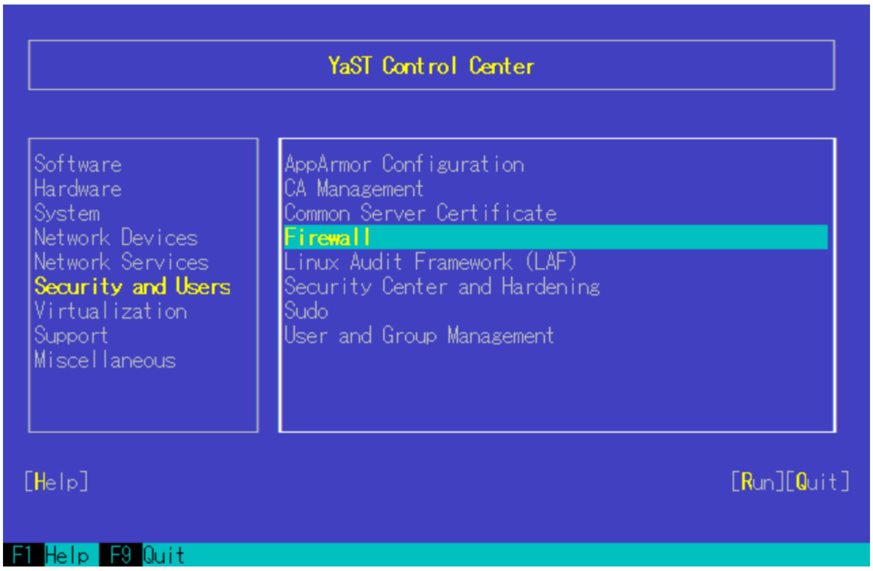
The firewall of SUSE Linux Enterprise Server closes its SSH port by default. It is required to allow SSH communication within the firewall settings.

The firewall settings differ depending on the conditions of the target servers. The example as shown below is the firewall settings in which YaST is used.

1. Execute the following command to show YaST Control Center.

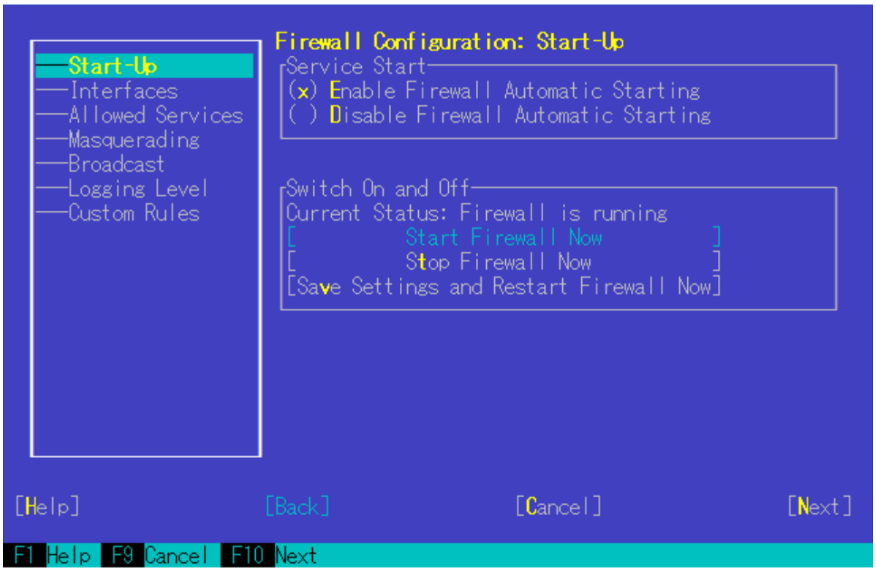
```
#yast
```

2. From [Security and Users] >, select [Firewall] and press the [Enter] key.



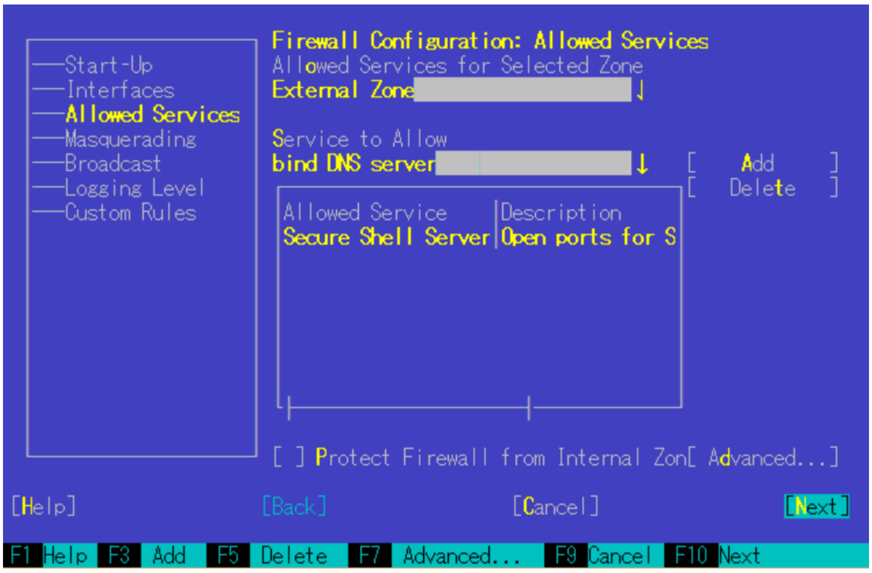
```
                     YaST Control Center

 Software          AppArmor Configuration
 Hardware          CA Management
 System            Common Server Certificate
 Network Devices   Firewall
 Network Services  Linux Audit Framework (LAF)
 Security and Users Security Center and Hardening
 Virtualization    Sudo
 Support           User and Group Management
 Miscellaneous

[Help]                                         [Run][Quit]
F1 Help  F9 Quit
```

3. From [Start-Up] screen, change the status of [Service Start] to “Enable Firewall Automatic Starting.”



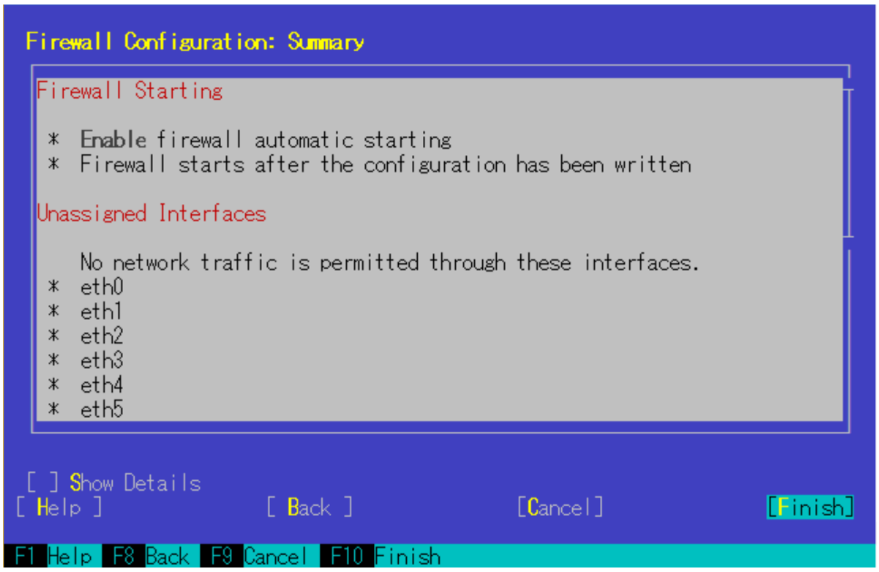
```
                    Firewall Configuration: Start-Up
──Start-Up          Service Start
──Interfaces        (x) Enable Firewall Automatic Starting
──Allowed Services  ( ) Disable Firewall Automatic Starting
──Masquerading
──Broadcast
──Logging Level     Switch On and Off
──Custom Rules      Current Status: Firewall is running
                    [       Start Firewall Now        ]
                    [       Stop Firewall Now         ]
                    [Save Settings and Restart Firewall Now]

[Help]           [Back]           [Cancel]           [Next]
F1 Help  F9 Cancel  F10 Next
```

4. From [Allowed Services] > [Service to Allow], select “Secure Shell Server” and select [Add] to press the [Enter] key.
5. Confirm if “Secure Shell Server” is added to [Allowed Service], and select [Next] to press the [Enter] key.



```
Firewall Configuration: Allowed Services
Allowed Services for Selected Zone
External Zone
Service to Allow
bind DNS server
Allowed Service     |Description
Secure Shell Server |Open ports for S
[ ] Protect Firewall from Internal Zon[ Advanced...]
```

6. After [Firewall Configuration: Summary] screen is displayed, select [Finish] and press the [Enter] key to finish the firewall settings.



```
Firewall Configuration: Summary
Firewall Starting

 *  Enable firewall automatic starting
 *  Firewall starts after the configuration has been written

Unassigned Interfaces

    No network traffic is permitted through these interfaces.
 *  eth0
 *  eth1
 *  eth2
 *  eth3
 *  eth4
 *  eth5

[ ] Show Details
```

[Note]

・Logging in as a root user is disabled by default in SUSE Linux Enterprise Server. To monitor target servers by using ISM 2.0, you need to allow login as a root user or you need to set up a user account comparable to the root user privilege. Change the settings as shown below for /etc/ssh/sshd_config to allow the root user to login with SSH.

```
PermitRootLogin    yes
```

2.3.3. Settings When Using Domain User Account

Monitoring by using a domain user account is the function supported in ISM2.0.0.a or later.

(1) Adding domain information to ISM-VA.

When carrying out monitoring using the domain user account, execute the procedures in “3.4.2 Initial Settings of ISM” (ISM 2.0 User’s Manual).

(2) Adding DNS information to ISM-VA

When carrying out monitoring using the domain user account, execute the procedures in “ISM2.0_ User’s Manual (4.9 Network Settings Add DNS server)” to register the DNS server on ISM-VA.

(3) Restriction when collecting Emulex card information

Use “hbacmd” to collect the card information for the devices on which the card provided by Avago/Emulex is mounted.

When collecting the card information with other than the root user authorization, give “hbacmd” an administrator privilege. For details, refer to "One Command Manager Command Line Interface User Manual".

(4) Restriction when collecting QLogic card information

You cannot get the information about the devices on which the card provided by QLogic is mounted, by using the domain user account. Register the root user from Edit OS Information screen to get the information.

(5) Restriction when collecting ServerView logs

You cannot collect ServerView logs by using the domain user account. Register the root user from Edit OS Information screen to collect the information.

(6) Restriction when updating firmware

You cannot execute online firmware update by using the domain user account. Register the root user from Edit OS Information screen to execute firmware update.

2.3.4 Setting Up the Account for Monitoring

(1) Setting “.bashrc”

Open the “.bashrc” file in the home directory of the appropriate account. Create a file if there is no “.bashrc” file.

```
#vi ~/.bashrc
```

Add the paths to “/sbin”, “/usr/sbin” and “/usr/loca/sbin” to “.bashrc” file.

```
PATH=$PATH:/sbin
PATH=$PATH:/usr/sbin
PATH=$PATH:/usr/local/sbin
```

(2) Setting Up the Environment Variable

To execute the Log Collection function of ServerView, log in to a monitoring target with SSH by using the OS account registered with an ISM 2.0 node, and confirm if the following conditions are satisfied (*).

・Directed to home directory upon login

・' ~' is included in the prompted strings upon login.

・' $' or ' #' is included after ' ~' in the prompted strings upon login.

Ex. 1) [root@hostname ~]#

Ex. 2) ADUSER¥ismuser@hostname ~ $

* You can change the prompted strings by changing the value of environment variable $PS1.

Example of parameter of environment variable $PS1)

```
[root@localhost ~]# echo $PS1
[¥u@¥h ¥W]¥$
```

2.4. Settings Procedure for VMware ESXi

ISM 2.0 communicates with target servers with VMware ESXi installed, by using vSphere API/CIM protocol. The following are the required settings.

・Enabling support for SSLv3 in VMware ESXi

2.4.1. Enabling Support for SSLv3 in Mware ESXi 5.5 and VMware ESXi 6.0

(1) Starting SSH Service

These settings are not required if SSH service is already running.

1. Log in to VMware ESXi on the target server with vSphere Client.
2. Select [Security Profile] of [Configuration] tab, and click on [Properties] of Services.
3. Select "SSH" and click on [Options].
4. Select [Start] of "Service Commands" to start SSH service, and click on [OK].

[Note]

When enabling SSH for VMware ESXi, the following message to be displayed on vSphere Client.

```
Configuration Issues
SSH for the host has been enabled.
```

(2) Enabling SSLv3 for CIM server

The support for SSLv3 is disabled for CIM server (port 5989). Edit the sfcb.cfgfile to enable SSLv3.

1. Log in to the target server with VMware ESXi installed, as administrator, via SSH.
2. Use challenge-response authentication to log in.
3. Edit the /etc/sfcb/sfcb.cfg file to add this statement to enable SSLv3.

```
enableSSLv3: true
```

Restart sfcbd-watchdog. Execute the following command.

```
#/etc/init.d/sfcbd-watchdog restart
```

[Note]

If the security patch (ESXi550-201501101-SG) is not applied to the releases previous to vSphere ESXi 5.5 Update 2, POODLE security vulnerability may occur. Be sure to apply the security patch before you enable SSLv3.

・VMware Security Patching Guidelines for ESXi and ESX (2020972)
(https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2020972)
・VMware ESXi 5.5, Patch ESXi550-201501101-SG: Updates esx-base (2099273)
(https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2099273)

(3) Stopping SSH Service

1. Log in to VMware ESXi on the target server with vSphere Client.
2. Select [Security Profile] of the [Configuration] tab, and click on [Properties] of Services.
3. Select [SSH] and click on [Options].
4. Select [Stop] of [Service Commands] to stop SSH service, and click on [OK].

2.4.2. Enabling Support for SSLv3 in VMware ESXi 6.5

(1) Starting SSH Service

These settings are not required if SSH service is already running.

1. Log in to VMware ESXi on the target server with vSphere Client.
   Use a Web browser to access https://<IP address of ESXi>/ui/.
2. Select [Host] - [Management] to open ESxi management screen.
3. Select [Service] – [SSH] from the list.
4. Select [Start].

[Note]

When enabling SSH for VMware ESXi, the following message to be displayed on VMware Host Client.

```
SSH is enabled on this host.   You should disable SSH unless it is necessary for administrative purposes.
```

(2) Enabling SSLv3 for CIM server

The support for SSLv3 is disabled for CIM server (port 5989). Edit the sfcb.cfg file to enable SSLv3.

1. Log in to the target server with administrator privilege which installed SSH of VMware ESXi.
2. Use challenge-response authentication to log in.
3. Edit the /etc/sfcb/sfcb.cfg file to add this statement to enable SSLv3.

```
enableSSLv3: true
```

Restart sfcbd-watchdog. Execute the following command.

```
#/etc/init.d/sfcbd-watchdog restart
```

(3) Stopping SSH Service

1. Log in to VMware ESXi on the target server with VMware Host Client.

Use a Web browser to access https://<IP address of ESXi>/ui/.

2. Select [Host] - [Management] to open ESxi management screen.
3. Select [Service] tab – [SSH] from the list.
4. Select [Start].

2.4.3. Settings When Using Domain User Account

Monitoring by using a domain user account is the function supported in ISM2.0.0.a or later.

(1) Adding domain information to ISM-VA

When carrying out monitoring using a domain user account, execute the procedures in "3.4.2 Initial Settings of ISM" (ISM 2.0 User's Manual).

(2) Adding DNS information to ISM-VA

When carrying out monitoring using the domain user account, execute the procedures in "ISM2.0_ User's Manual (4.9 Network Settings Add DNS server)" to register the DNS server on ISM-VA.

3. Settings Procedure for Monitoring Target (Cloud Management Software)

3.1. Settings Procedure for vCenter Server

3.1.1. Adding DNS information to ISM-VA

When carrying out monitoring under the condition where an ESXi host with FQDN is registered on vCenter, execute the procedures in "ISM2.0_ User's Manual (4.9 Network Settings Add DNS server)" to register the DNS server on ISM-VA.

3.1.2. Settings When Using Domain User Account

Monitoring by using a domain user account is the function supported in ISM2.0.0.a or later.

(1) Settings for Respective Hosts Registered on vCenter Server

To get information from vCenter Server, it is required that the settings for respective hosts registered on vCenter Server are already completed. Refer to "2.4. Settings Procedure for VMware ESXi" to perform the settings for respective hosts.

(2) Adding domain information to ISM-VA

When carrying out monitoring using the domain user account, execute the procedures in "3.4.2 Initial Settings of ISM" (ISM 2.0 User's Manual).

(3) Adding DNS information to ISM-VA

When carrying out monitoring using the domain user account, execute the procedures in "ISM2.0_ User's Manual (4.9 Network Settings Add DNS server)" to register the DNS server on ISM-VA.

3.2 Settings Procedure for Microsoft Failover Cluster

Monitoring Microsoft Failover Cluster is the function supported in ISM2.0.0.a or later.

3.2.1 Settings When Using Domain User Account

Monitoring by using a domain user account is the function supported in ISM2.0.0.a or later.

(1) Settings up WinRM for Respective Hosts Configuring Cluster

To get information from Microsoft Failover Cluster, it is required that the settings for respective hosts that configure a cluster are already completed. Refer to "2.1. Settings Procedure for Windows" to perform the settings for respective hosts.

(2) Adding SPN to Active Directory

It is required to correctly register the Service Principal Name (SPN) of a managed server on Active Directory when monitoring a Windows Server using the domain user account. Execute the following procedure to register the Service Principal Name of the managed server.

```
>setspn –A HOST/[monitoring target cluster IP] [monitoring target cluster name]
```

Checking Command

```
>setspn –L [monitoring target cluster name]
```

(3) Adding domain information to ISM-VA

When carrying out monitoring using the domain user account, execute the procedures in "3.4.2 Initial Settings of ISM" (ISM 2.0 User's Manual).

(4) Adding DNS information to ISM-VA

When carrying out monitoring using the domain user account, execute the procedures in "ISM2.0_ User's Manual (4.9 Network Settings Add DNS server)" to register the DNS server on ISM-VA.

(5) Kerberos delegation configuration for Active Directory

1. Log on to the Active Directory server.
2. Open Server Manager.
3. From [Tool] button, click on [Active Directory Users and Computers].
4. Expand the domain, then expand [Computers] folder.
5. Right-click the cluster node name on the right-side window, then click on [Properties].
6. On the [General] tab, confirm if [Trust computer for delegation to any service (Kerberos only)] checkbox is checked.
7. Click on [OK] and repeatedly perform the above steps 3 and 4 for all the cluster nodes.

3.3 Settings Procedure for Microsoft System Center

Monitoring Microsoft System Center is the function supported in ISM2.0.0.e or later.

Refer to "2.1 Settings Procedure for Windows" to perform the settings for the respective hosts and virtual machines with Microsoft System Center installed.