UNIVERGE SV9500

FP95-115 V5

Prepackaged Server Model
Installation and Operation Manual

NWD-170371-001
ISSUE 6.0

LIABILITY DISCLAIMER

NEC Corporation reserves the right to change the specifications, functions, or features, at any time, without notice.

NEC Corporation has prepared this document for use by its employees and customers. The information contained herein is the property of NEC Corporation, and shall not be reproduced without prior written approval from NEC Corporation.

All brand names and product names on this document are trademarks or registered trademarks of their respective companies.

NWD-170371-001
ISSUE 6.0
OCTOBER, 2017

UNIVERGE SV9500
Prepackaged Server Model
Installation and Operation Manual

TABLE OF CONTENTS

Page

TABLE OF CONTENTS (CONTINUED)

TABLE OF CONTENTS (CONTINUED)

CHAPTER 1
GENERAL

This chapter provides a function overview of SV9500 (Prepackaged Server Model).

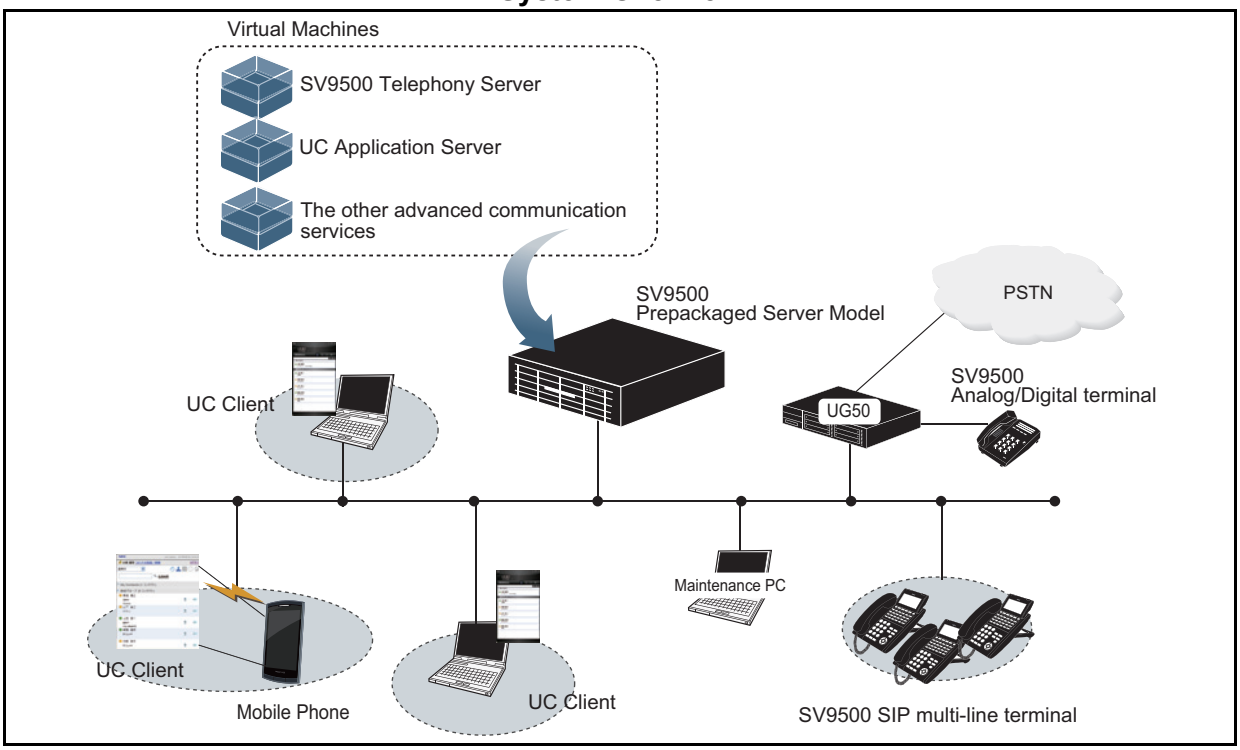
1. WHAT IS SV9500 Prepackaged Server Model?

1.1 General

SV9500 (Prepackaged Server Model) is a server-based communication platform that provides not only voice communication but also various advanced communication services, collaborating with NEC authorized UC (Unified Communications) applications installed in the same server.

There are two available types of SV9500 (Prepackaged Server Model): Prepackaged Server Model and Prepackaged FT Server Model. For more details on each model, see 2. Operating System Configurations.

System Overview

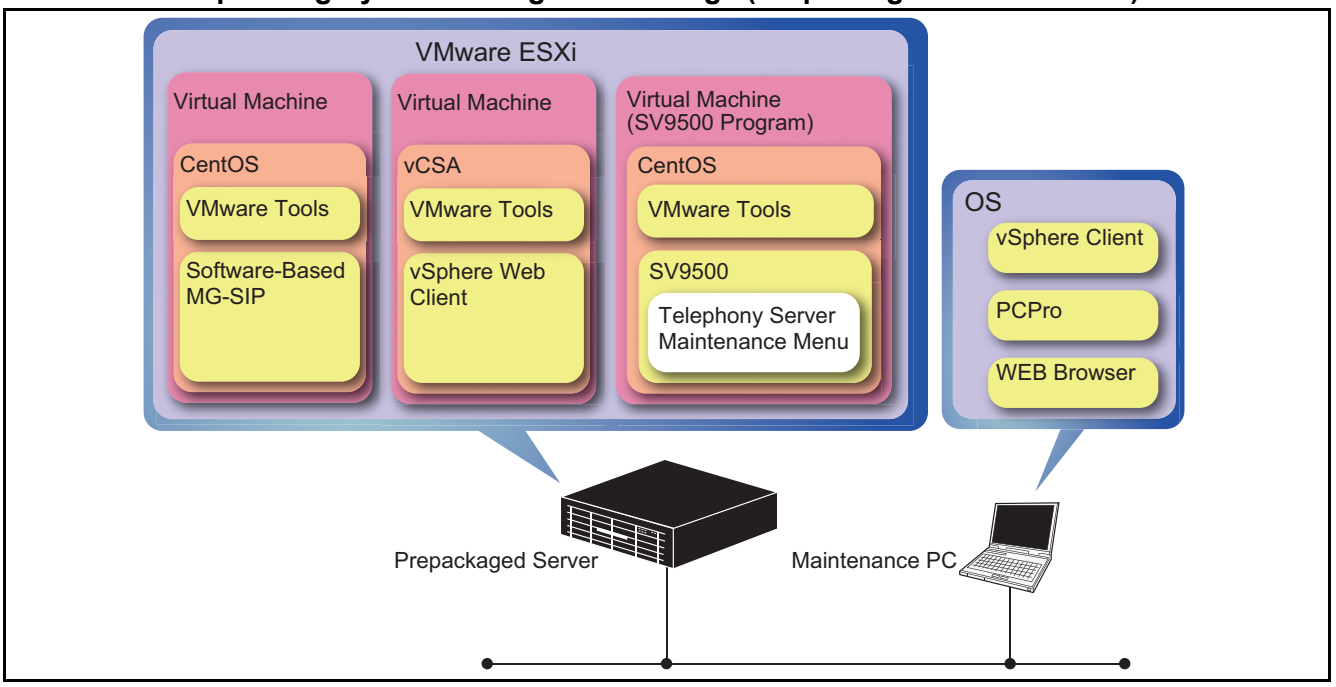


2. Operating System Configurations

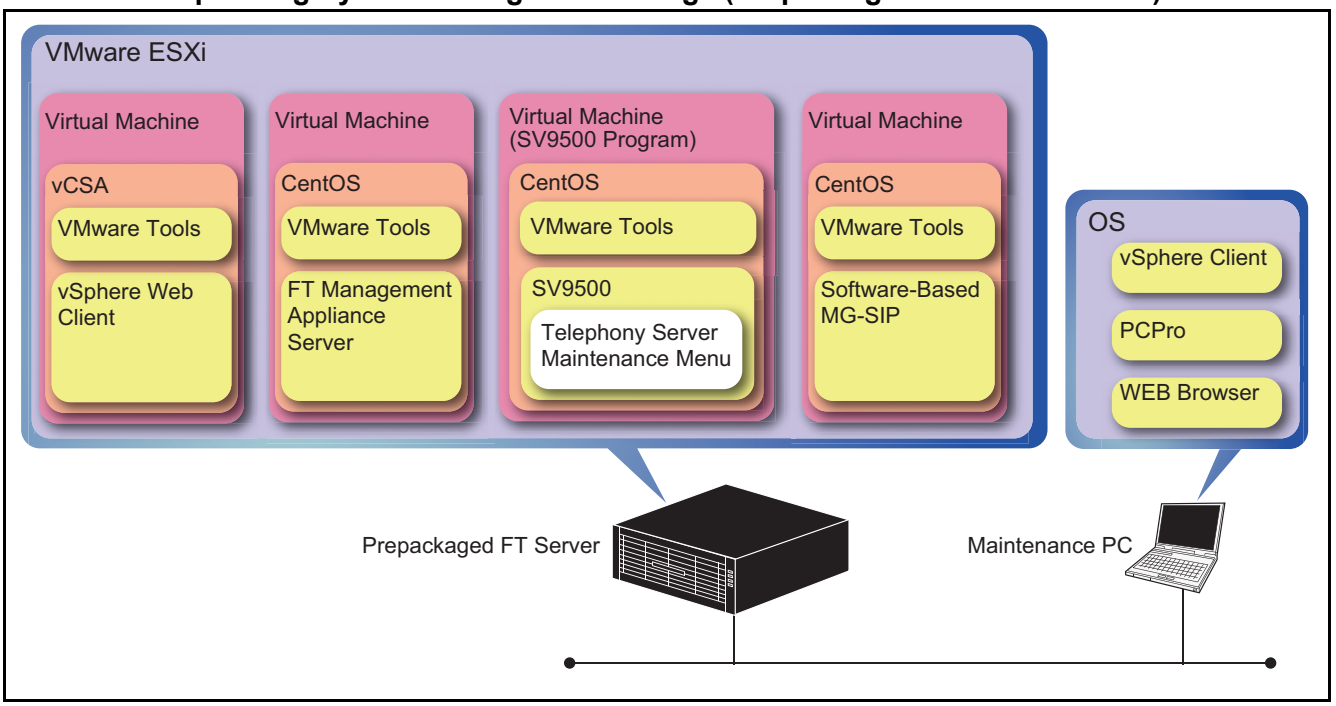
SV9500 (Prepackaged Server Model) operates multiple virtual machines on a Prepackaged Server/Prepackaged FT Server. A virtual machine is operated by a VMware vSphere Hypervisor (hereinafter, VMware ESXi).

The operating system that is installed on a virtual machine is called a guest operating system (OS).

Operating System Configuration Image (Prepackaged Server Model)



Operating System Configuration Image (Prepackaged FT Server Model)



The following must be installed on a virtual machine on a Prepackaged Server/Prepackaged FT Server:

Name	Description
vCenter Server Appliance (vCSA)	Manages the entire vSphere infrastructure (VMware ESXi, virtual machines, etc.)

The following must be installed on a guest OS on a Prepackaged Server/Prepackaged FT Server:

Name	Description
VMware Tools	• Operates on the virtual machines and receives instructions from VMware ESXi • Executes shutdown control of the guest OS and time synchronization between VMware ESXi and the guest OS
SV9500	SV9500 program
FT Management Appliance Server	• FT control software operates on this server for continuously monitoring and managing VMware ESXi • FT control software also used for changing system settings and providing commands for accessing system information • Only for the Prepackaged FT Server Model; for more details, see manuals for the Prepackaged FT Server Model **Note:** If the virtual machine on which FT Management Appliance Server is installed stops operation due to some problems, it automatically reboots approximately after 20 minutes.
Software-based MG-SIP **Note 1**	MG-SIP installed as a virtual machine in the server. For a detailed explanation, see SOFTWARE-BASED MG-SIP chapter in this manual.

Note 1: Software-based MG-SIP is available since FP95-112 V2.

The following must be installed on a maintenance PC:

Name	Description
vSphere Client	Manages vCenter Server and VMware ESXi
PCPro	• Used for data settings of SV9500 • For more details, refer to PCPro Setup Manual
Web Browser	Used for vSphere Web Client and Telephony Server Maintenance Menu **Note:** • vSphere Web Client: browser-based interface for configuring and managing virtual machines • Telephony Server Maintenance Menu: tool for managing SV9500

3. Hardware Configurations

There are two available types of SV9500 (Prepackaged Server Model):

- Prepackaged Server Model
- Prepackaged FT Server Model

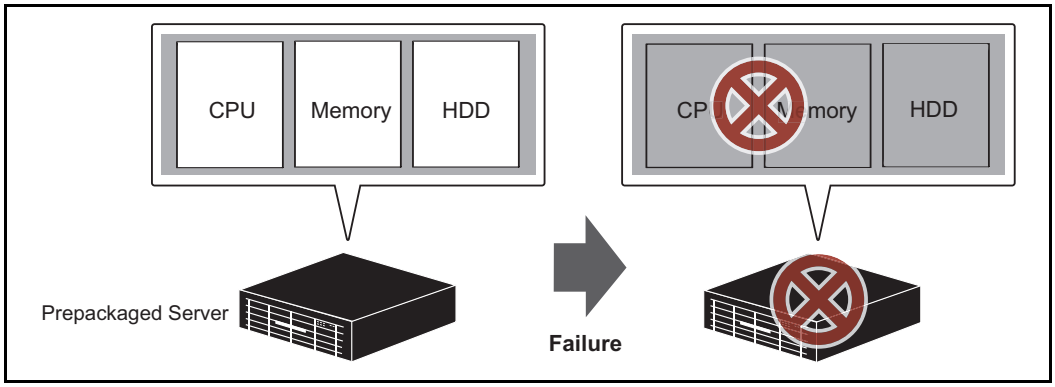
For more details on usage environment and conditions of a Prepackaged Server/Prepackaged FT Server, see Management by LAN Port.

Also, for more details on names and features of each component of a Prepackaged Server/Prepackaged FT Server, see the manuals for each server.

3.1 Prepackaged Server Model

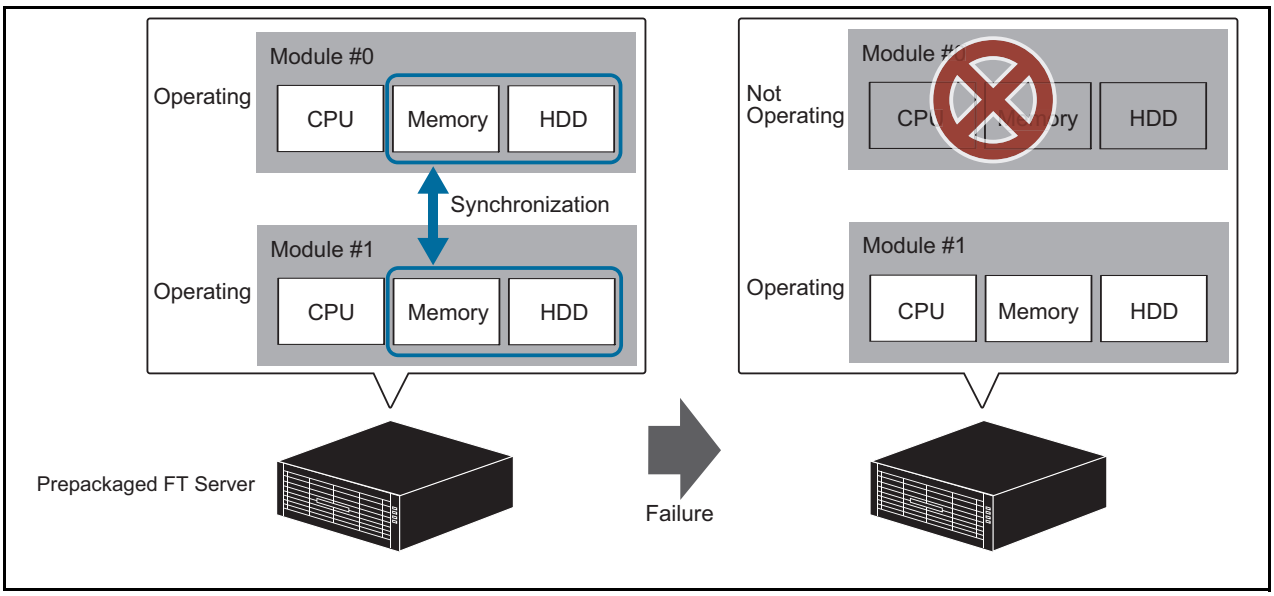
For increasing availability of HDD, a Prepackaged Server employs a redundant power supply unit and fan unit (hot-pluggable), and a RAID configuration.

However, hardware such as a CPU, memory and HDD is not redundant in a Prepackaged Server. If a failure occurs in these components, the operation of the system stops until its restoration is completed.



3.2 Prepackaged FT Server Model

A Prepackaged FT Server consists of two modules (Module #0 and Module #1). Each module has hardware such as a CPU, memory and HDD, and data in these modules is continuously synchronized. Even if a failure occurs in one module, the server can continue to operate with the other module and unexpected downtime of the system can be avoided.



4. Management by LAN Port

4.1 General

The number of physical NIC ports used for operating SV9500 (Prepackaged Server Model) are as follows:

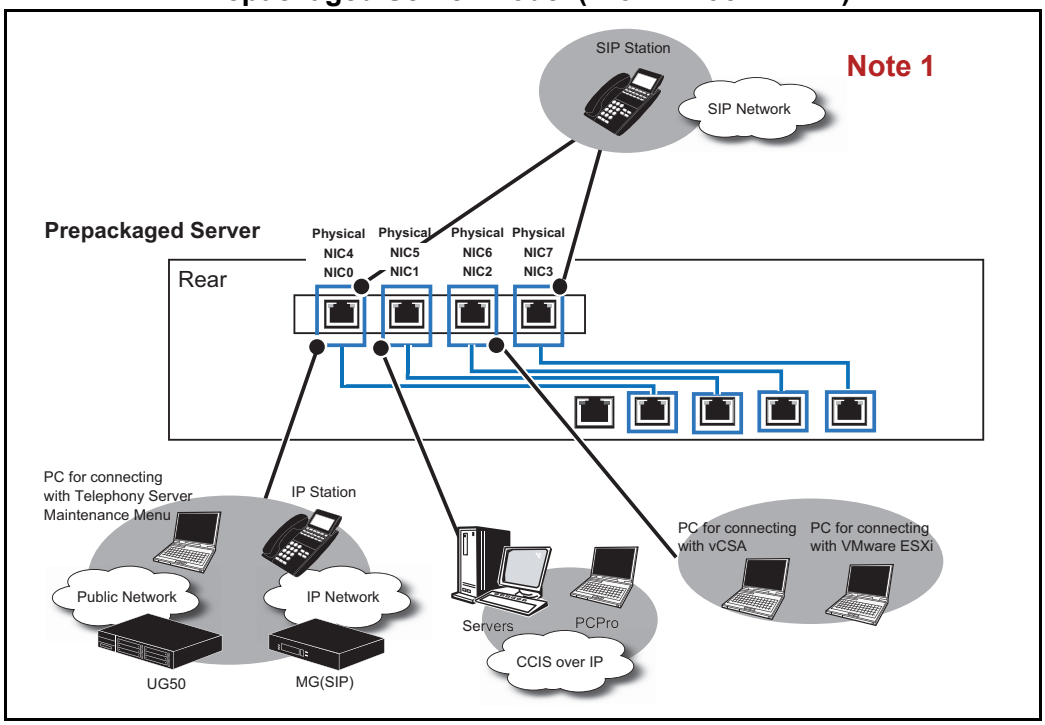
- Prepackaged Server Model: 8 or 10 physical NIC ports
- Prepackaged FT Server Model: 8 physical NIC ports

Physical NICs are teamed two by two for providing redundancy. When used in the LAN, a pair of teamed NICs must be respectively connected with a cable.

Note: In this section, NIC numbers are indicated on the ports used for operating SV9500 (Prepackaged Server Model) only. As for the NIC numbers of other ports, see the manuals for the manual attached to the server.

On Prepackaged Server Model (from FP95-112 V2), Physical NIC0 and NIC4 are used for call controlling and software-based MG-SIP, Physical NIC1 and NIC5 are used for maintenance and call controlling and Physical NIC3 and NIC7 are used for software-based MG-SIP.

Prepackaged Server Model (From FP95-112 V2)

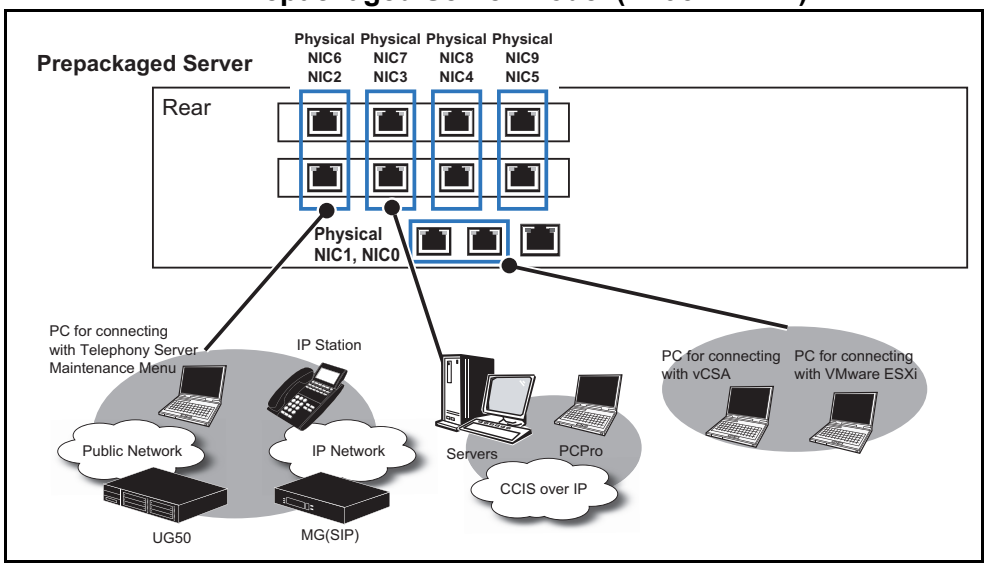


Note 1: Note the following:

- When Software-based MG-SIP is in one port configuration, Physical NIC0 and NIC4 connect to the SIP network but Physical NIC3 and NIC7 do not connect.
- Software-based MG-SIP is available from FP95-112 V2.

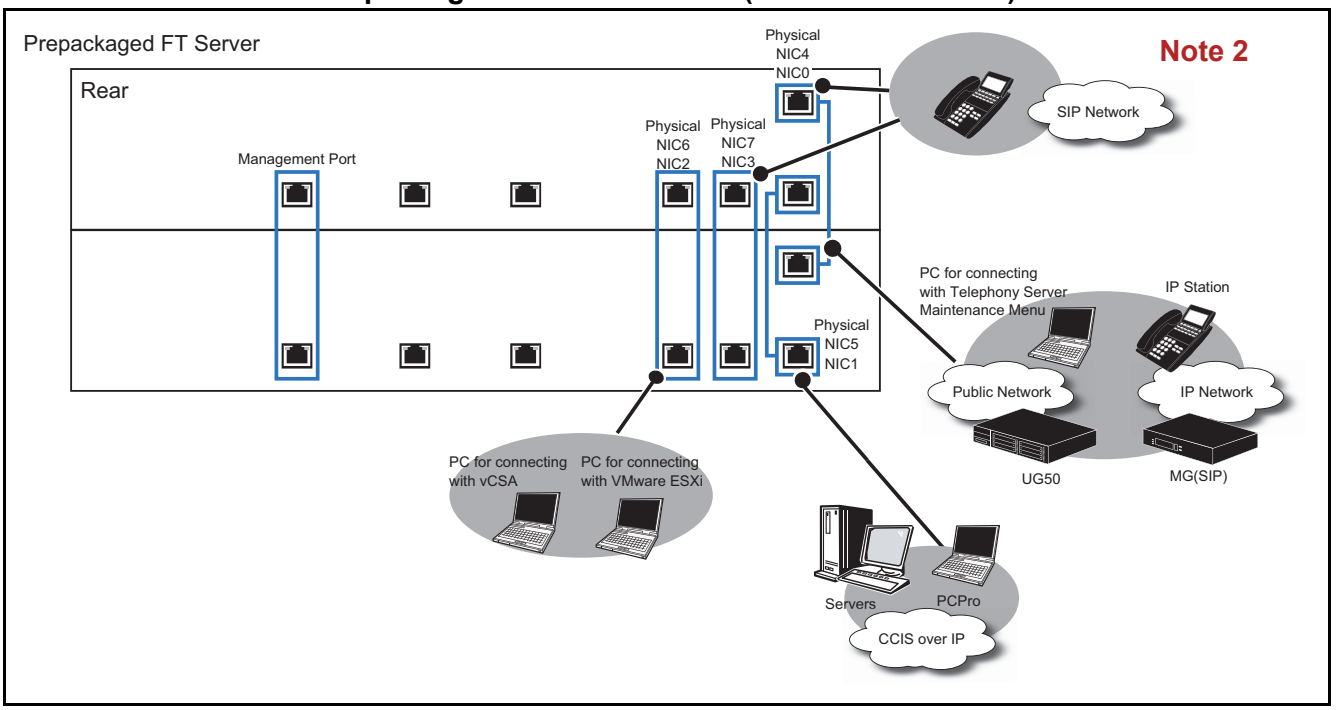
On Prepackaged Server Model (FP95-111 V1), Physical NIC2 and NIC6 are used for call controlling, and Physical NIC3 and NIC7 are used for maintenance and call controlling.

Prepackaged Server Model (FP95-111 V1)



On Prepackaged FT Server Model (from FP95-112 V2), Physical NIC0 and NIC4 are used for call controlling and Software-based MG-SIP, and Physical NIC1 and NIC5 are used for maintenance and call controlling, and Physical NIC3 and NIC7 are used for Software-based MG-SIP.

Prepackaged FT Server Model (From FP95-112 V2)

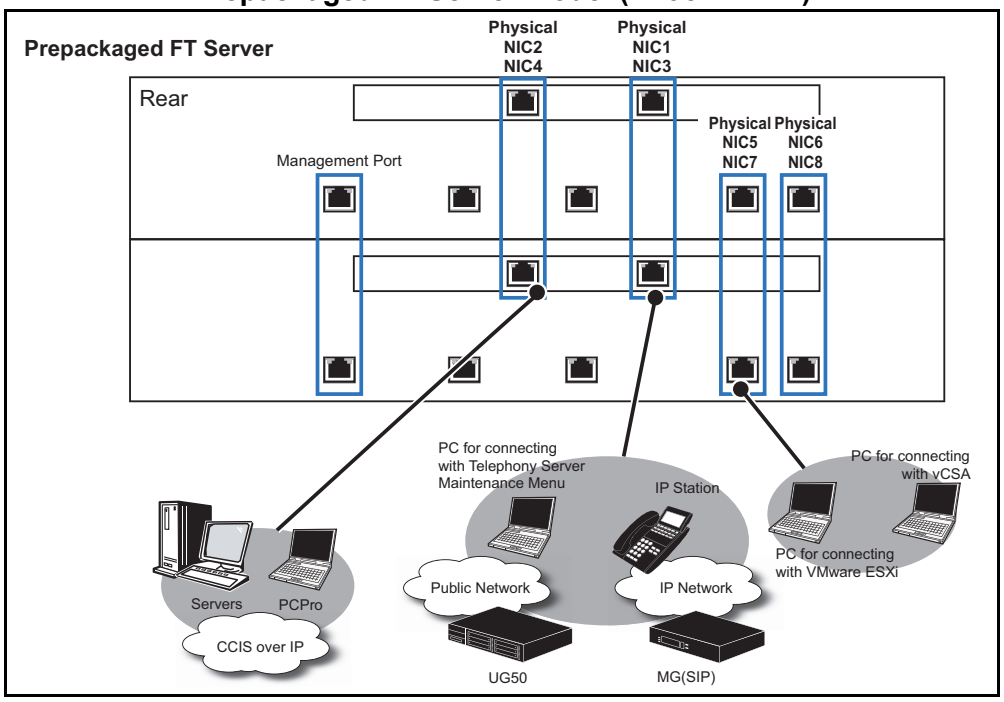


Note 2: Note the following:

- When Software-based MG-SIP is in one port configuration, Physical NIC0 and NIC4 connect to the SIP network but Physical NIC3 and NIC7 do not connect.
- Software-based MG-SIP is available from FP95-112 V2.

On Prepackaged FT Server Model (FP95-111 V1), Physical NIC1 and NIC3 are used for call controlling, and Physical NIC2 and NIC4 are used for maintenance and call controlling.

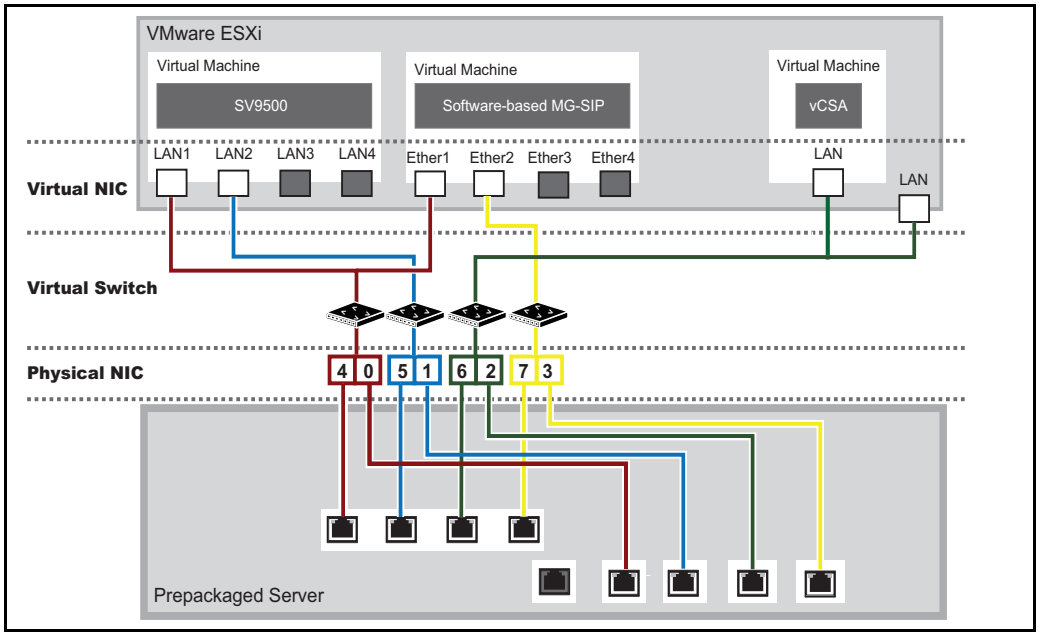
Prepackaged FT Server Model (FP95-111 V1)



4.2 Usage of LAN Ports

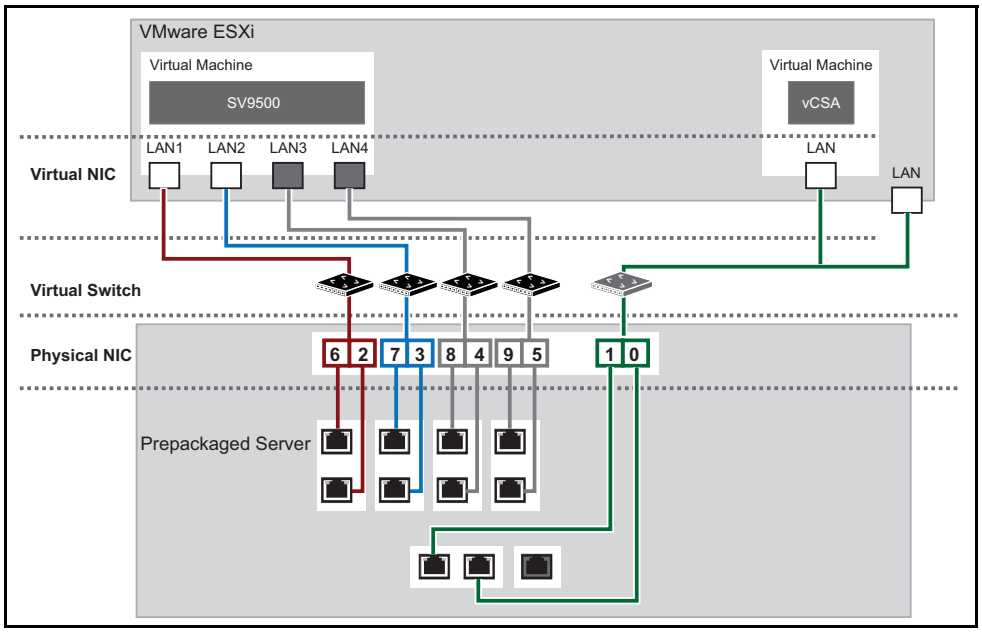
The following shows the usage of each LAN port.

- Prepackaged Server Model (from FP95-112 V2)



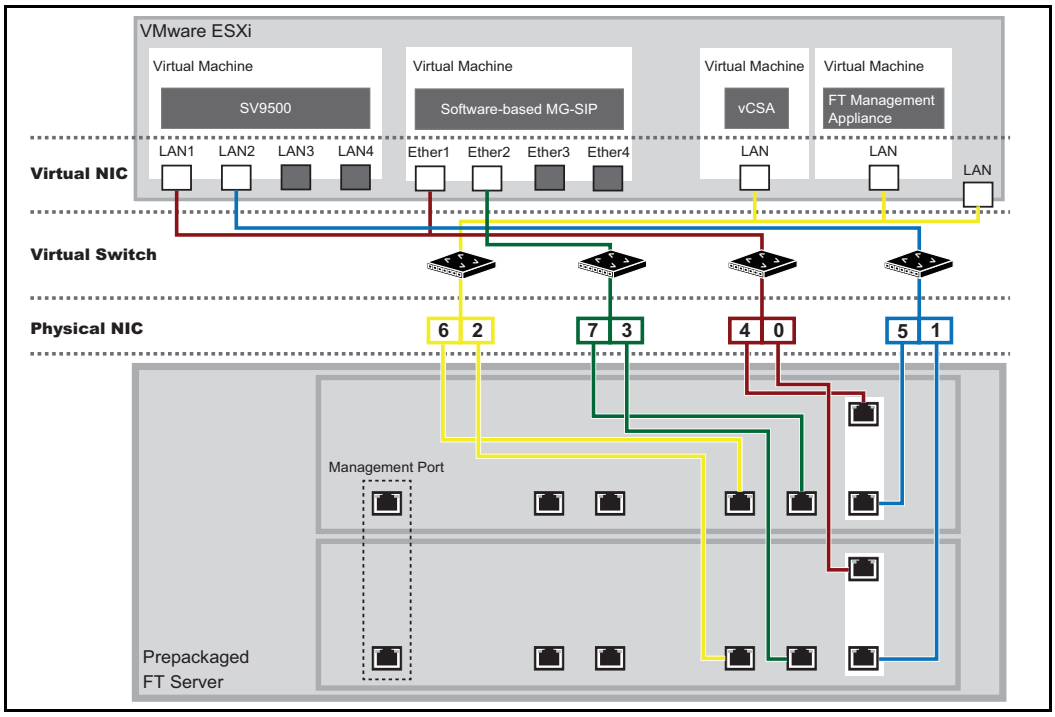
Port	Maximum Transmission Speed	Usage
Physical NIC0	1Gbps	Connected to LAN1 (virtual) of the SV9500 program and Ether1 (virtual) of Software-based MG-SIP
Physical NIC4		
Physical NIC1	1Gbps	Connected to LAN2 (virtual) of the SV9500 program
Physical NIC5		
Physical NIC2	1Gbps	Connected to VMware ESXi LAN and vCSA LAN
Physical NIC6		
Physical NIC3	1Gbps	Connected to Ether2 (virtual) of Software-based MG-SIP
Physical NIC7		

- Prepackaged Server Model (FP95-111 V1)



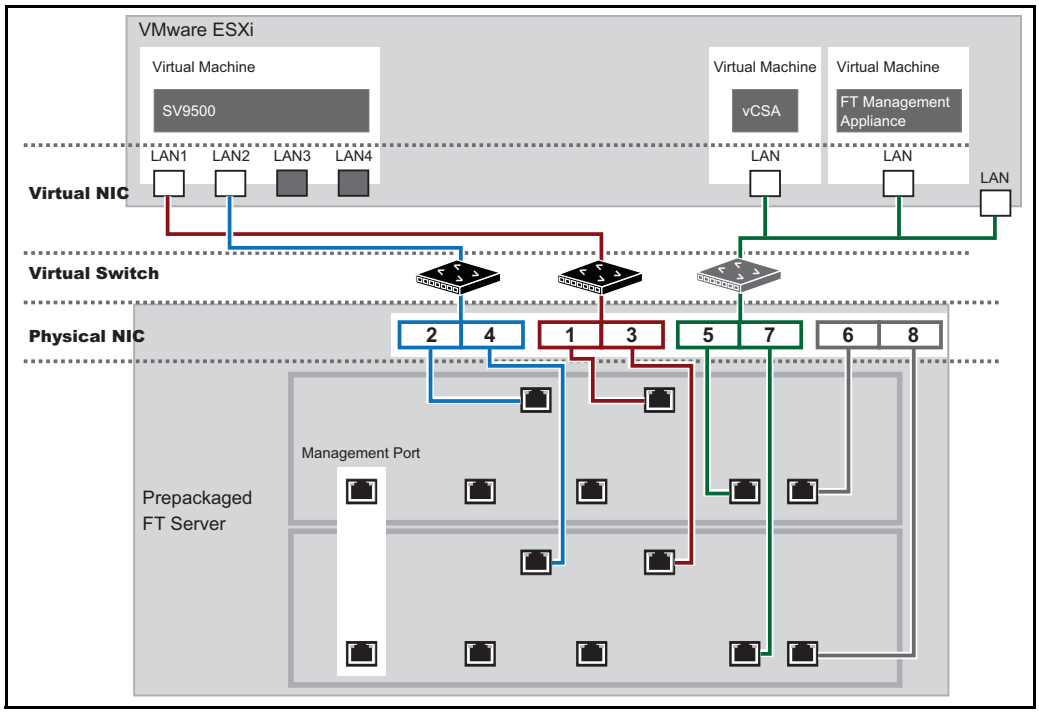
Port	Maximum Transmission Speed	Usage
Physical NIC0	1Gbps	Connected to LAN ports (virtual) of VMware ESXi and vCSA
Physical NIC1		
Physical NIC2	1Gbps	Connected to LAN1 (virtual) of the SV9500 program
Physical NIC6		
Physical NIC3	1Gbps	Connected to LAN2 (virtual) of the SV9500 program
Physical NIC7		
Physical NIC4	1Gbps	Unused (for being connected to LAN3 (virtual) of the SV9500 program)
Physical NIC8		
Physical NIC5	1Gbps	Unused (for being connected to LAN4 (virtual) of the SV9500 program)
Physical NIC9		

- Prepackaged FT Server Model (from FP95-112 V2)



Port	Maximum Transmission Speed	Features
Physical NIC0 Physical NIC4	1Gbps	Connected to LAN1 (virtual) of the SV9500 program and Ether1 (virtual) of Software-based MG-SIP
Physical NIC1 Physical NIC5	1Gbps	Connected to LAN2 (virtual) of the SV9500 program
Physical NIC2 Physical NIC6	1Gbps	Connected to LAN ports (virtual) of VMware ESXi, vCSA and FT Management Appliance
Physical NIC3 Physical NIC7	1Gbps	Connected to Ether2 (virtual) of Software-based MG-SIP
Management Port	100Mbps	Connects with the Baseboard Management Controller (BMC) Monitors hardware, performs power control and operates the Prepackaged FT Server by using BMC, without depending on the operation status or power on/off status of the guest OS

- Prepackaged FT Server Model (FP95-111 V1)



Port	Maximum Transmission Speed	Features
Physical NIC1 Physical NIC3	1Gbps	Connected to LAN1 (virtual) of the SV9500 program
Physical NIC2 Physical NIC4	1Gbps	Connected to LAN2 (virtual) of the SV9500 program
Physical NIC5 Physical NIC7	1Gbps	Connected to LAN ports (virtual) of VMware ESXi, vCSA and FT Management Appliance
Physical NIC6 Physical NIC8	1Gbps	Unused
Management Port	100Mbps	Connects with the Baseboard Management Controller (BMC) Monitors hardware, performs power control and operates the Pre-packaged FT Server by using BMC, without depending on the operation status or power on/off status of the guest OS

- Virtual Machine

LAN Port (Virtual)		Features
SV9500 program	LAN1	Communicates with devices/terminals including IP station, VS32, MGs and Telephony Server Maintenance Menu **Note 1**
	LAN2	Communicates with devices including PCPro (**Note 2**), OAI, SMDR, PMS, MCI, SNMP and CCIS over IP **Note 1**
	LAN3	Unused
	LAN4	Unused
Software-based MG-SIP **Note 3**	Ether1	Communicates with devices under SV9500 In one port configuration, connects with WAN (SIP network)
	Ether2	WAN connection (SIP network) In one port configuration, unused
	Ether3	Unused
	Ether4	

Note 1: Some devices/terminals/features listed above can be assigned to other LAN ports by using the ADTM command.

Note 2: Use LAN1 to make the connection with IPv6 addresses.

Note 3: Available from SP95-V112 V2.

4.2.1 NIC Setting of LAN Ports

The LAN ports of SV9500 are virtual ports. It is recommended to use the following operation mode settings:

LAN Port		Operation Mode Setting	
SV9500	LAN1	Transmission Speed	Auto Negotiation (10Mbps/100Mbps/1Gbps)
		Duplex Mode	Full duplex
	LAN2	Transmission Speed	Auto Negotiation (10Mbps/100Mbps/1Gbps)
		Duplex Mode	Full duplex

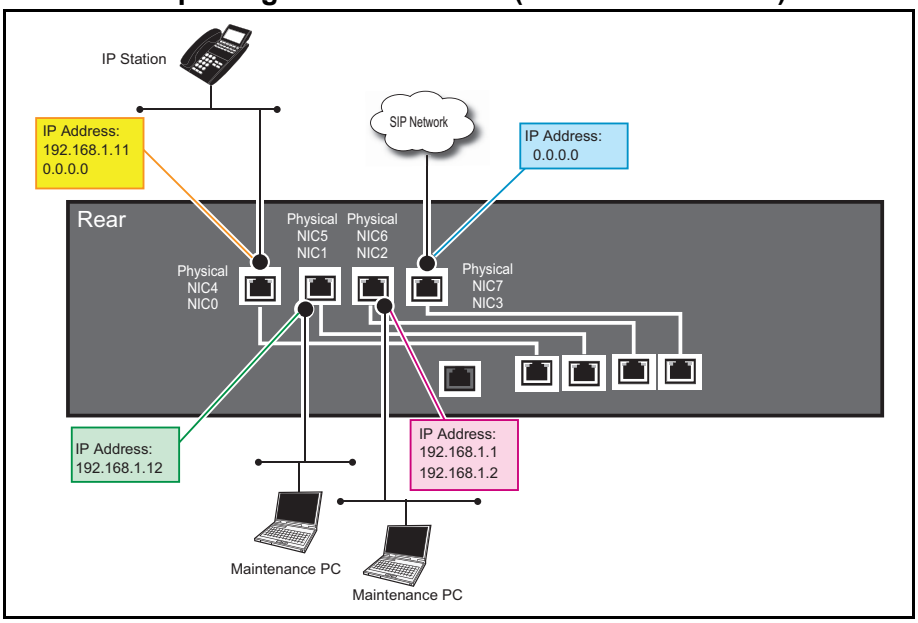
Note: A virtual port and a virtual switch always operate at 1 Gbps.

4.2.2 IP Address

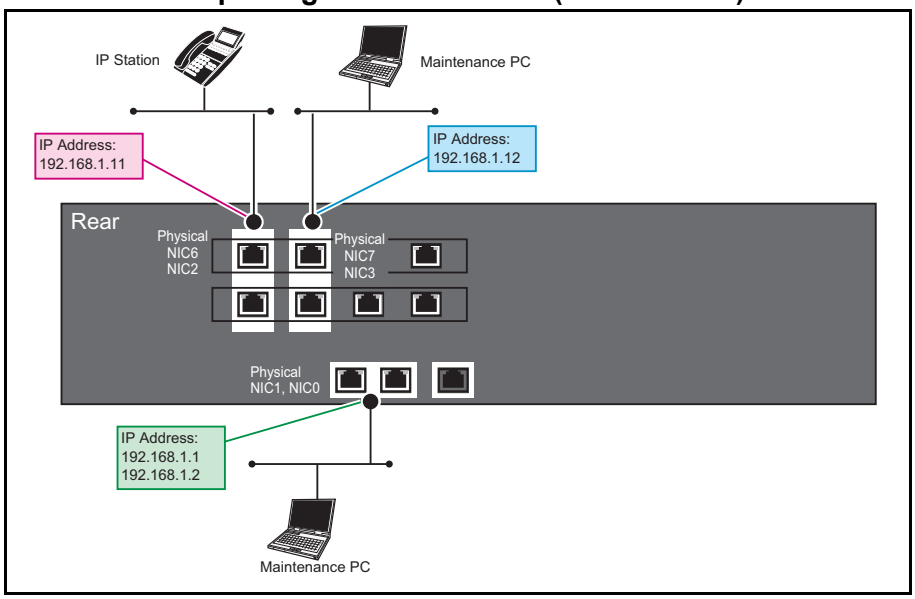
This section explains the IP addresses of the LAN ports of SV9500. IP addresses for LAN1 and LAN2 need to be assigned to LAN ports on a virtual machine. **Note 1**

Refer to the ADTM command in Command Manual for the data assignment of LAN1 and LAN2 of SV9500. The setting of LAN3 and LAN4 cannot be changed.

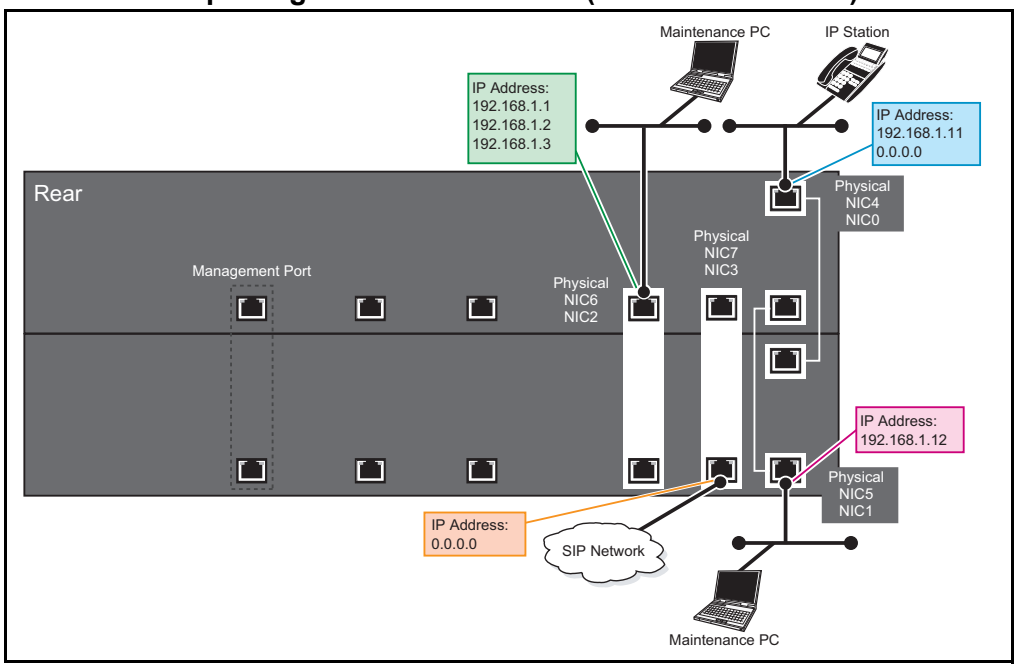
Prepackaged Server Model (From FP95-112 V2)



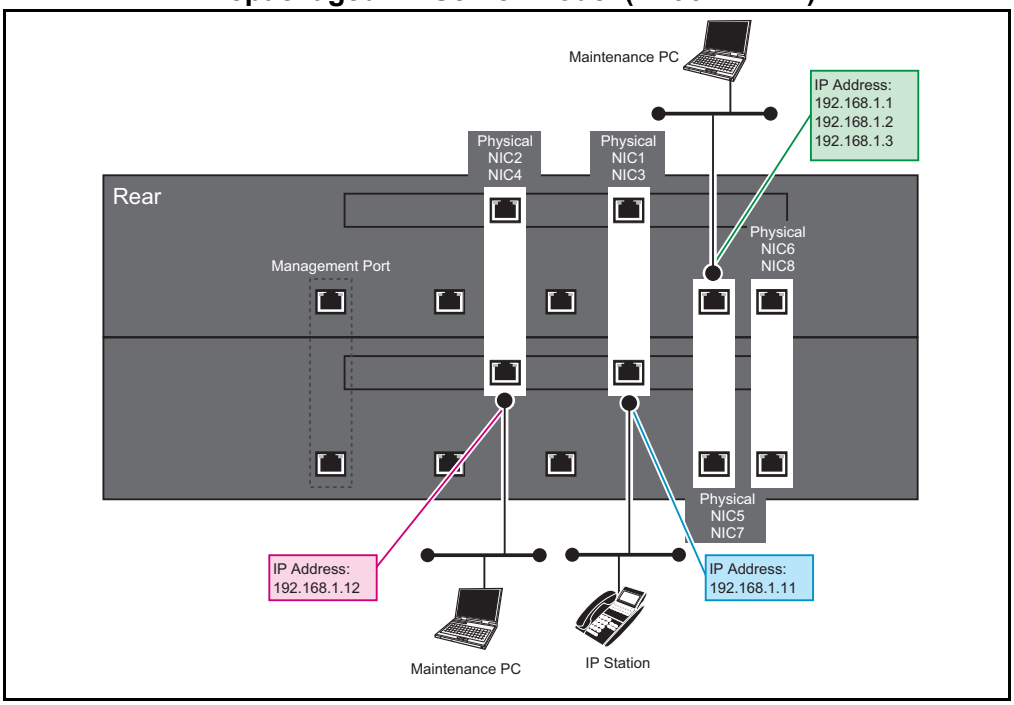
Prepackaged Server Model (FP95-111 V1)



Prepackaged FT Server Model (From FP95-112 V2)



Prepackaged FT Server Model (FP95-111 V1)



The following table shows the default IP address settings:

Kind of IP Address to be Assigned		Default IP Address
SV9500	IP address of LAN1	192.168.1.11/16
	IP address2 of LAN1 **Note 2**	None
	IP address of LAN2	192.168.1.12/16
Software-based MG-SIP	IP address of Ether1	0.0.0.0
	IP address of Ether2	0.0.0.0
VMware ESXi		192.168.1.1/16
vCSA		192.168.1.2/16
FT Management Appliance **Note 3**		192.168.1.3/16

Note 1: Note the following conditions when assigning IP addresses:
- The TCP/IP Module is initialized after the IP address of LAN1 of SV9500 is modified. (LAN1 and LAN2 ports of SV9500 are restarted. Then applications connecting to SV9500 through TCP/IP including PCPro are disconnected.)
- Initialize the system with the SINZ command (TYPE: System Initialize) after modifying the IP address of LAN1 of SV9500. In the case of LAN2 of SV9500, it is not necessary.
- The same or different subnet masks can be assigned to LAN1 and LAN2 of SV9500.
- Assign unique IP addresses to each LAN port.
- IP address 2 of LAN1 cannot use the same IP Address as LAN2 of SV9500.
- Assign the same Subnet Mask and routing data to both LAN1 IP address and LAN1 IP address 2 of SV9500.

Note 2: Note the following conditions when assigning IP address2:
- IP address2 can be assigned to LAN1 of SV9500 only.
- If a SIP Handler Controlled SIP terminal is not accommodated in the system, IP address2 is not required to be assigned.

Note 3: Provided only for the Prepackaged FT Server Model.

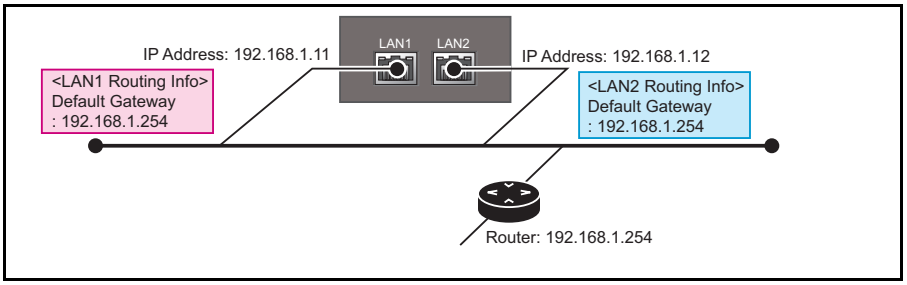
4.2.3 Routing Setting

The routing tables of LAN1 and LAN2 of SV9500 are independent of each other. So each needs routing data.

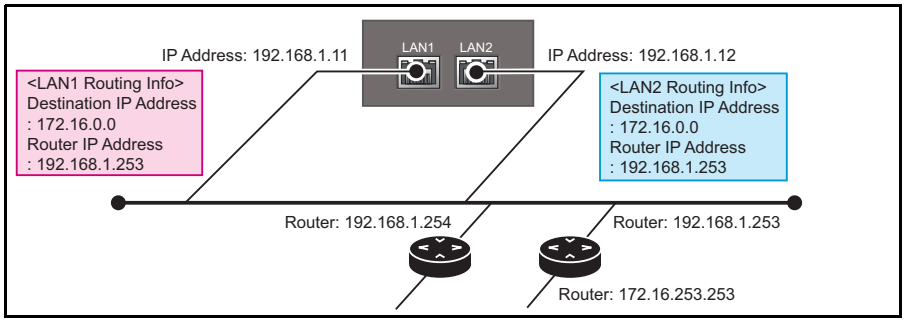
Note: Note the following conditions:
- Assign routing data (Default Gateway, static route) to each routing table of LAN 1 and LAN 2 respectively, with the ADTM command.
- A maximum of four destinations can be assigned as static routing information to each LAN1 and LAN2.

- **When LAN1 and LAN2 are in the same subnet:**

  Default Gateway information is assigned to each as in the example below.

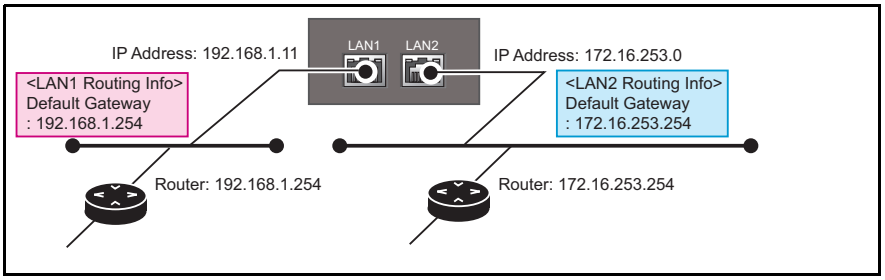


  Static Route information is assigned to each as in the example below.

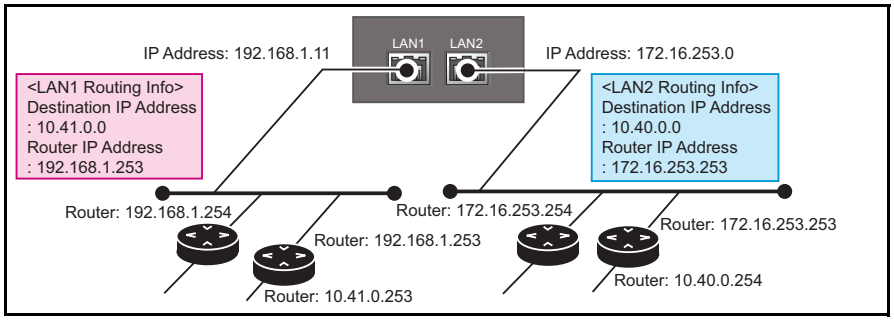


- **When LAN1 and LAN2 are in a different subnet:**

  Default Gateway information is assigned to each as in the example below.



  Static Route information is assigned to each as in the example below.



5. Specifications

5.1 Hardware

CPU, memory, HD and LAN interface data are given below. For other server specifications data, see the specific manual of the server.

[1] FP95-114 V4 Server

Item		Prepackaged Server Model	Prepackaged FT Server Model
CPU		2.2GHz, 10C/20T (2WAY)	2.3GHz,12C/24T (2WAY) ×2
Memory		64 GB	64 GB
HDD		2.5” SAS HDD 600 GB x 4 (RAID 6 configuration)	2.5” SAS HDD 600 GB x 4 (RAID 1 configuration)
LAN Interface	On Board	Management LAN connector x 1 • compatible with 1000BASE-T/100BASE-TX/10BASE-T • RJ-45 (1 port) • located on rear	Management LAN connector x 2 • compatible with 100BASE-TX/10BASE-T • RJ-45 (1 port x 2) • located on rear 10GBASE-T LAN connector x 4 • compatible with 10GBASE-T/1000BASE-T/100BASE-TX • RJ-45 (2 ports x 2) • located on rear 1000BASE-T LAN connector x 4 • compatible with 1000BASE-T/100BASE-TX/10BASE-T • RJ-45 (2 ports x 2) • located on rear
	On Expansion Card	1000BASE-T LAN connector x 8 • compatible with 1000BASE-T/100BASE-TX/10BASE-T • RJ-45 (4 ports on 2 Expansion Cards) • located on rear	1000BASE-T LAN connector x 4 • compatible with 1000BASE-T/100BASE-TX/10BASE-T • RJ-45 (2 ports on 1 Expansion Card x 2) • located on rear

[2] FP95-112 V2 Server

Item		Prepackaged Server Model	Prepackaged FT Server Model
CPU		2.40GHz, 6C/12T (2WAY)	2.50GHz,10C/20T (2WAY) ×2
Memory		64 GB	64 GB
HDD		2.5” SAS HDD 600 GB x 4 (RAID 6 configuration)	2.5” SAS HDD 600 GB x 4 (RAID 1 configuration)
LAN Interface	On Board	Management LAN connector x 1 • compatible with 1000BASE-T/100BASE-TX/10BASE-T • RJ-45 (1 port) • located on rear	Management LAN connector x 2 • compatible with 100BASE-TX/10BASE-T • RJ-45 (1 port x 2) • located on rear 10G/1000BASE-T LAN connector x 4 • compatible with 10GBASE-T/1000BASE-T/100BASE-TX • RJ-45 (2 ports x 2) • located on rear 1000BASE-T LAN connector x 4 • compatible with 1000BASE-T/100BASE-TX/10BASE-T • RJ-45 (2 ports x 2) • located on rear
	On Expansion Card	1000BASE-T LAN connector x 8 • compatible with 1000BASE-T/100BASE-TX/10BASE-T • RJ-45 (4 ports on 2 Expansion Cards) • located on rear	1000BASE-T LAN connector x 4 • compatible with 1000BASE-T/100BASE-TX/10BASE-T • RJ-45 (2 ports on 1 Expansion Card x 2) • located on rear

Note: These servers can be used from FP95-112 V2 to FP95-113 V3.

[3] FP95-111 V1 Server

Item		Prepackaged Server Model	Prepackaged FT Server Model
CPU		2.60 GHz, 12C/24T (2 way)	2.60 GHz, 16C/32T (2 way) x 2
Memory		64 GB	64 GB
HDD		2.5” SAS HDD 600 GB x 4 (RAID 6 configuration)	2.5” SAS HDD 600 GB x 4 (RAID 1 configuration)
LAN Interface	On Board	1000BASE-T LAN connector x 2 • compatible with 1000BASE-T/100BASE-TX/10BASE-T • RJ-45 (2 ports) • located on rear Management LAN connector x 1 • compatible with 100BASE-TX/10BASE-T • RJ-45 (1 port) • located on rear	1000BASE-T LAN connector x 4 • compatible with 1000BASE-T/100BASE-TX/10BASE-T • RJ-45 (2 ports x 2) • located on rear Management LAN connector x 2 • compatible with 100BASE-TX/10BASE-T • RJ-45 (1 port x 2) • located on rear 10GBASE-T LAN connector x 4 • compatible with 10GBASE-T/1000BASE-T/100BASE-TX • RJ-45 (2 ports x 2) • located on rear
	On Expansion Card	1000BASE-T LAN connector x 8 • compatible with 1000BASE-T/100BASE-TX/10BASE-T • RJ-45 (4 ports on 2 Expansion Cards) • located on rear	1000BASE-T LAN connector x 4 • compatible with 1000BASE-T/100BASE-TX/10BASE-T • RJ-45 (2 ports on 1 Expansion Card x 2) • located on rear

5.2 Software

Item	Prepackaged Server Model			Prepackaged FT Server Model		
	FP95-114 V4	FP95-112 V2 Note 2	FP95-111 V1	FP95-114 V4	FP95-112 V2 Note 2	FP95-111 V1
VMware ESXi	Version 6.0.1 (customized by NEC)	Version 5.5.2 (customized by NEC)	Version 5.1.1 (customized by NEC)	Version 6.0.1b	Version 5.5.1	Version 5.1.0
VMware Tools	Version 10.0.0	Version	Version 9.0.5	Version 10.0.0	Version 9.4.5	Version 9.0.0 Note 1
vCenter Server Appliance	Version 6.0.1	Version 5.5.2b	Version 5.1.0	Version 6.0.1	Version 5.5.2b	Version 5.1.0

Note 1: Version 9.0.5 is installed on the SV9500 virtual machine. VMware Tools is automatically installed when the SV9500 program is installed.

Note 2: This data is from FP95-112 V2 to FP95-113 V3.

6. Conditions and Limitations

6.1 Operating Environment

- vSphere Web Client:
  Check the required software in the VMware webpage manual for vSphere installation and set up.
- PCPro:
  For details on the operating environment of PCPro, see Operating Environments and Conditions in PCPro Setup Manual.
- Telephony Server Maintenance Menu:
  For details on the operating environment of Telephony Server Maintenance Menu, see Telephony Server Maintenance Menu.

6.2 Conditions and Limitations of SV9500 (Prepackaged Server Model)

Confirm the following conditions and limitations before installation of SV9500 (Prepackaged Server Model).

Note: For conditions of use of the Software-based MG-SIP, see SOFTWARE-BASED MG-SIP-chapter in this manual.

(1) VMware ESXi needs to be licensed before operating SV9500 (Prepackaged Server Model).

(2) SV9500 (Prepackaged Server Model) supports only a full IP configuration. UG50 is used for connection with analog and digital stations and external trunks.

(3) SV9500 cannot detect a failure that occurs in a Prepackaged Server/Prepackaged FT Server because SV9500 operates on a virtual machine.

(4) When a Prepackaged FT Server is used and a failure of the SV9500 program occurs, “0-ACT” is displayed in a system message output by the SV9500 program, regardless of which module (Module #0 or Module #1) the SV9500 program in question operates on.

(5) The following is available since FP95-112 V2:

- Hotel feature **Note 1**
- FCCS feature **Note 2**

Note 1: For Hotel features the following restrictions apply:
- Only the following terminals are available:
  - SIP Multiple Line terminal (DT700/DT800 series)
  - Standard SIP terminal
  - Digital terminal (DT300/400 series) with UG50
  - Analogue terminal with UG50

- Features that use Attendant Console cannot be used.

Note 2: Prepackaged Server Model and Appliance Model can be used together but only with FCCS Networking via IP (Peer-to-Peer).

(6) Features related to announcement must use VS32 server.

(7) VS-32 server can be used only with single connection. Multiple connection is not supported.

(8) The following features are not available for SV9500 (Prepackaged Server Model):

- ACD features
- Attendant Console features
- ACT-Side Quick Restart feature by the OAI system
- AUTOMATED ATTENDANT [A-82] via MG(SIP), provided by the RST card
- LOCATION DIVERSITY [L-55]
- POWER FAILURE TRANSFER [P-3]

(9) The features provided by the IOC card, such as Remote Maintenance and STATION MESSAGE DETAIL RECORDING (SMDR) [S-10] features, are not available.

(10) The following devices cannot be connected with SV9500 (Prepackaged Server Model):

- External Alarm Indication Panel
- External Music-On-Hold source
- ATM Module

Note: Use the Internal Holding Tone of each IP terminal or VS32 External IP Music-On-Hold.

(11) PIRs cannot be connected to SV9500 (Prepackaged Server Model). Note the following limitations:

(a) External Music-On-Hold provided by the EMA card is not available.

(b) CCIS networking is available only via IP (Peer-to-Peer connection). Also, when using CCIS networking, assign the system data ASYDL, SYS 1, Index 810, bit 0=1 (MOH from the Self Office).

(c) Attendant Console features are not supported.

(d) Cell Station (CS) cannot be used with SV9500 (Prepackaged Server Model).

(12) CPU/TSW changeover does not executed during a diagnostic of SV9500 (Prepackaged Server Model).

(13) Upgrading and switching back of the program version must be performed only through Telephony Server Maintenance Menu. Do not use PCPro commands.

(14) Note the following conditions regarding VMware:

(a) Failures are monitored by using the alarm feature of vCSA. This feature is not available when vCSA is down.

(b) When vCSA is down, reboot vCSA manually by using vSphere Client.

(c) VMware Tools is installed on a virtual machine that is managed by VMware ESXi. Do not upgrade or uninstall VMware Tools.

(d) When monitoring a startup status of the system via vSphere Web Client, there may be differences between the displayed status and the actual system status.

(15) Note the following when using a snapshot feature of VMware ESXi:

(a) Before using a snapshot feature, back up the office data to HDD with the MEM_HDD command.

(b) Before using a snapshot feature, ensure that the MEM_HDD command is not running on the SV9500 program and stop a diagnostic of the SV9500 program. If a backup operation (by the MEM_HDD command or a periodic backup) is in progress, do not use a snapshot feature.

(c) Clear the following check boxes when using a snapshot feature:

- Snapshot the virtual machine's memory
- Quiesce guest file system (Needs VMware Tools installed)

(16) Note the following conditions regarding time synchronization:

(a) The ATIM command cannot be used for time setting.

Note: A time zone and Daylight Savings time setting can be performed by the ATIM command.

(b) Time synchronization with an NTP server is executed only for VMware ESXi. Time synchronization between a guest OS and VMware ESXi is executed by VMware Tools.

Note: It takes up to two minutes from when the time is set in VMware ESXi by synchronizing with an NTP server to when the time set is reflected in the ATIM command.

Note: Do not use the ANTPL command.

(c) If the time of VMware ESXi is set to a later time than that of a guest OS, automatic time synchronization by VMware Tools is not executed. To do this, a time setting of VMware ESXi must be the same as that of a guest OS.

(d) When the time of VMware ESXi is changed while a guest OS is in operation, time synchronization between VMware ESXi and a guest OS is executed every one minute.

(e) In time synchronization with VMware Tools, the clocks of IP/SIP terminals are synchronized at the following times:

- at the startup of a guest OS
- approximately one minute after setting change

(17) Use the Internet for downloading vSphere Client installer.

(18) Use the Internet for downloading the installer for vCSA version 6 (from FP95-114 V4).

CHAPTER 2 SETUP

This chapter explains the setup procedures.

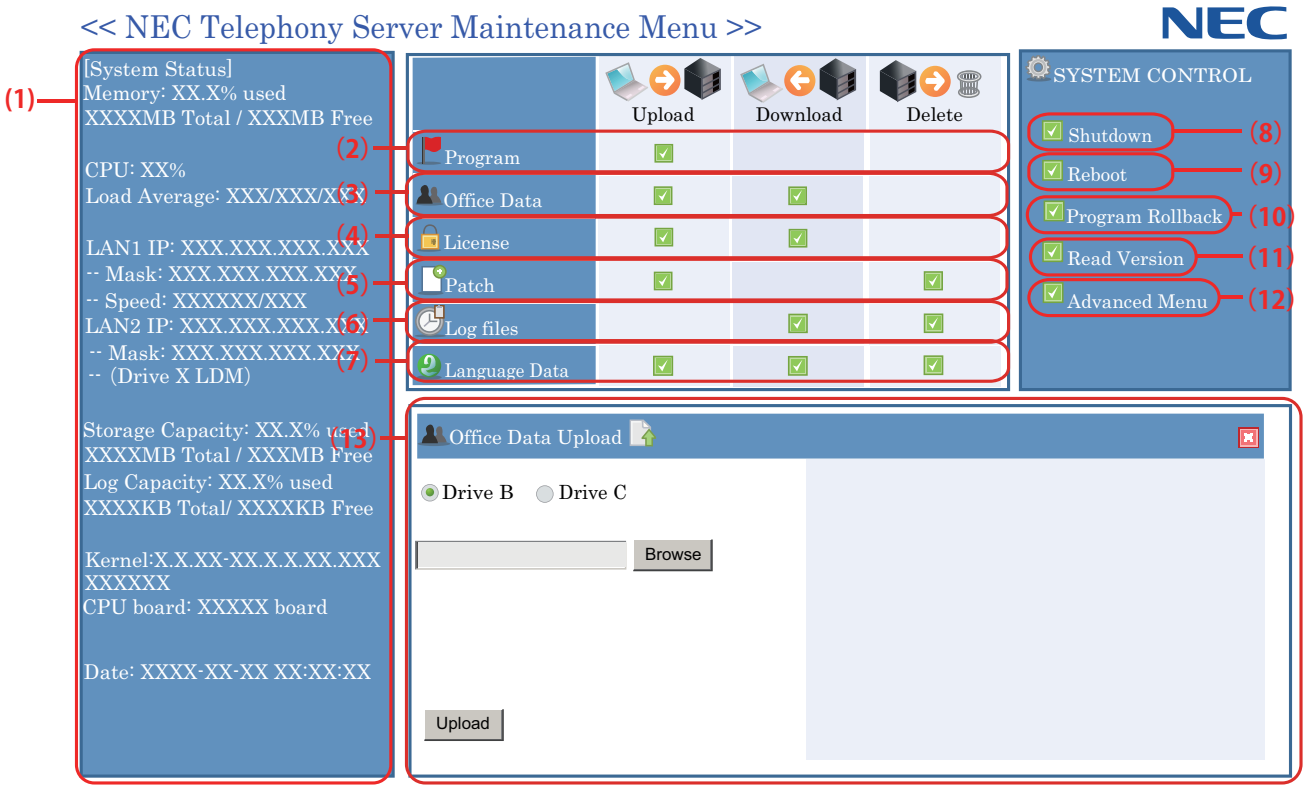
1. Telephony Server Maintenance Menu

This section gives an explanation on Telephony Server Maintenance Menu which is used as a tool to upload, download or delete the data to/from the CF card of the Telephony Server.

This tool can be accessed and operated from the maintenance PC to the Telephony Server via Web browser.

1.1 Screen Layout and Functions of Each Component

The following is the screen layout of Telephony Server Maintenance Menu and functional descriptions of each component.



No.	Item	Description
(1)	System Status Display Area	Displays the current status of the connecting Telephony Server. This information will be updated in real-time while Telephony Server Maintenance Menu is executed. Refer to "1.2 System Status Indication" for details on each parameter.

No.	Item	Description
(2)	Program Menu	Uploads the program including upgrading versions.**Note 1** **Note 2** The Program Upload dialog box appears in (13) Configuration Dialog Box Display Area by clicking the Upload button.
(3)	Office Data Menu	Uploads or downloads the Office Data. The Office Data Upload dialog box appears in (13) Configuration Dialog Box Display Area by clicking the Upload button and the Office Data Download dialog box for the Download button.
(4)	License Menu	Uploads or downloads the license. The License Upload dialog box appears in (13) Configuration Dialog Box Display Area by clicking the Upload button and the License Download dialog box for the Download button.
(5)	Patch Menu	Uploads or deletes the patch. The Patch Upload dialog box appears in (13) Configuration Dialog Box Display Area by clicking the Upload button and the Patch Delete dialog box for the Delete button.
(6)	Log files Menu	Downloads or deletes the log files. The Log files Download dialog box appears in (13) Configuration Dialog Box Display Area by clicking the Download button and the Log files Delete dialog box for the Delete button.
(7)	Language Data Menu	Uploads, downloads or deletes the language data. The Language Data Upload dialog box appears in (13) Configuration Dialog Box Display Area by clicking the Upload button, Language Data Download dialog box for the Download button, and the Language Data Delete dialog box for the Delete button.
(8)	Shutdown Menu	Shuts down the Telephony Server. The Shutdown dialog box appears in (13) Configuration Dialog Box Display Area.
(9)	Reboot Menu	Reboots the Telephony Server. The Reboot dialog box appears in (13) Configuration Dialog Box Display Area.
(10)	Program Rollback Menu	If there is a problem after performing a version upgrade, it allows to go back to the previous version. **Note 2** The Switch image dialog box appears in (13) Configuration Dialog Box Display Area.
(11)	Read Version Menu	Reads out the program version of the currently connecting Telephony Server. The Read Version dialog box appears in (13) Configuration Dialog Box Display Area. • Show results in new window: Place a checkmark to display the information of the program version in a new window. • Auto copy to clipboard: Place a checkmark to automatically copy the information of the program version to a clipboard. **Note 5**

No.	Item		Description
(12)	Advanced Menu	Change Maintenance Menu's Password	You can change user name and password for login. **Note 3 Note 4**
		Show Memory Details	Displays how much of the Telephony Server's memory is currently being used.
		Lock release of Maintenance Menu	Release the lock state when the Telephony Server Maintenance Menu is locked due to an unexpected event.
		Change root password	Changes Linux administrator (root) password. **Note 3**
		Remove host keys	Delete the host keys of the Telephone Server.
(13)	Configuration Dialog Box Display Area		Displays the dialog box for processes of each function according to the menu you have selected.

Note 1: Do not operate the Telephony Server Maintenance Menu while the upload is still being processed. Wait until the message “Operation successfully completed.” appears. If any operation is performed before the uploading process is completed, the Telephony Server Maintenance Menu turns to a locked status with a message “Process is busy now” indication and operations will all be denied. In this case, release the lock state from “Lock release of Maintenance Menu” under “Advanced Menu”.

Note 2: The Telephony Server is forced to restart when this process is executed.

Note 3: Contact NEC maintenance personnel if you need to confirm your User Name and Password.

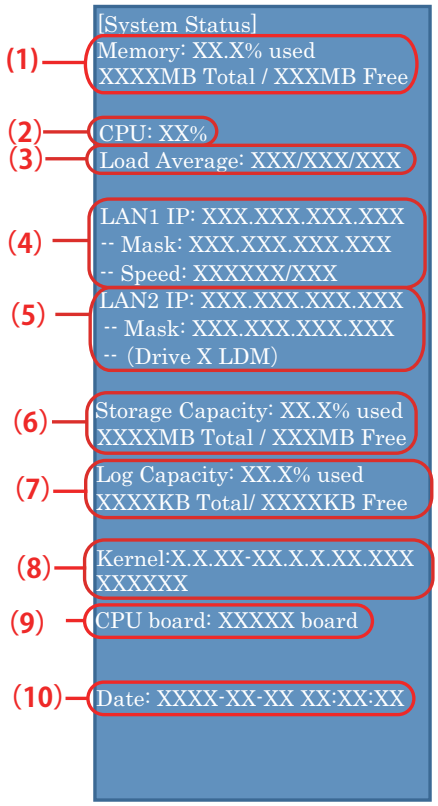
Note 4: See How to Change User Name and Password for changing user name or password.

Note 5: Telephony Server Maintenance Menu will not be displayed when Internet Explorer 10 or later is used. For copying the displayed result, check the “Show results in new window” box under Read Version. Then copy and paste the desired information.

1.2 System Status Indication

The current status of the connecting Telephony Server is displayed in the System Status area.

This section explains the details on each status displayed in the System Status area.



No.	Item		Description
(1)	Memory		Displays the capacity and an amount of free space of the memory mounted in the Telephony Server.
(2)	CPU		Displays the usage rate of the CPU.
(3)	Load Average		Displays the load factor of the CPU. **Note:** Load Average: the three numbers represent averages over progressively longer periods of time (one, five, and fifteen minute averages).
(4)	LAN1	IP	Displays the IP address of LAN1.
		Mask	Displays the Subnet Mask of LAN1.
		Speed	Displays the communication mode of LAN1.
(5)	LAN2	IP	Displays the IP address of LAN2.
		Mask	Displays the Subnet Mask of LAN2.
		Drive	Displays the drive retrieving the IP address of LAN2.

No.	Item	Description
(6)	Storage Capacity	Displays the usage rate, the capacity, and an amount of free space for the virtual machines under operation.
(7)	Log Capacity	Displays the usage rate, the capacity, and an amount of free space for the log storage area.
(8)	Kernel	Displays the version of the current Linux kernel.
(9)	CPU board	Displays the type of a CPU board (fix to Virtual Machine).
(10)	Date	Displays the date time information of the Telephony Server.

1.2.1 Operating Environment

This section explains the specifications on operating environment for the Telephony Server Maintenance Menu.

1.2.1.1 Specification on Operating Environment

Common Operating Environment

Item	Specification
Hard Disk	2.0GB of free disk space minimum
Monitor	1,024 x 768 dots or more, 16-bit colors (65,536) at least. **Note 1**
OS	**Note 2**
CPU	
Memory	
DVD-ROM drive	Required to install the program.
Mouse	Mouse, or equivalent pointing device
Serial Port	9-pin D-SUB (male) **Note 3**
LAN Port	10BASE-T/100BASE-TX/1000BASE-T (Depending on an intermediate device such as HUB) **Note 4**
PCMCIA Card Slot	Type II (Required for writing a program for CF card.)
Browser	Internet Explorer 7 or higher **Note 5**, **Note 6**
Number of Concurrent Access	Only one at a time

Note 1: When using desktop, 1,280 x 1,024 dots or more are recommended.

Note 2: For details of OS and specific operating environments, refer to “OS-Specific Operating Environments” in Chapter 2 PCPro Overview of PCPro Setup Manual.

Note 3: Required for the serial connection with the Telephony Server (via the IOC card).

Note 4: Required for LAN/WAN connection with the Telephony Server.

Note 5: Internet Explorer 8 or higher is recommended. Internet Explorer 7 is supported but the processing may take longer time. A warning message will appear when using Internet Explorer 6 or lower. Note that this is not available for Modern UI on Internet Explorer 10 or higher.

Note 6: Microsoft Edge is not supported. When operating Windows 10, use Internet Explorer.

1.2.2 Operating Conditions

An internet environment is required to access the License Management Server (LMS).

1.3 How to Change User Name and Password

This section explains how to change User Name and Password.

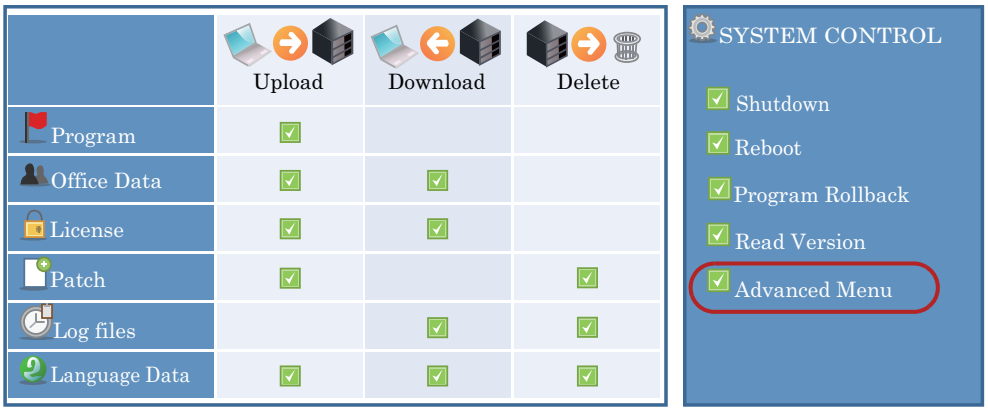
Note: When you change the user name and password, note the following points.
- Before you change a user name and password, you need to log into Telephony Server Maintenance Menu.
- After logging into Telephony Server Maintenance Menu, do not use Back button on browser.

Step1: Start Internet Explorer and type “http://xxx.xxx.xxx.xxx:9801/” into the address bar to access Telephony Server Maintenance Menu. (xxx.xxx.xxx.xxx represents the LAN1 IP address.)

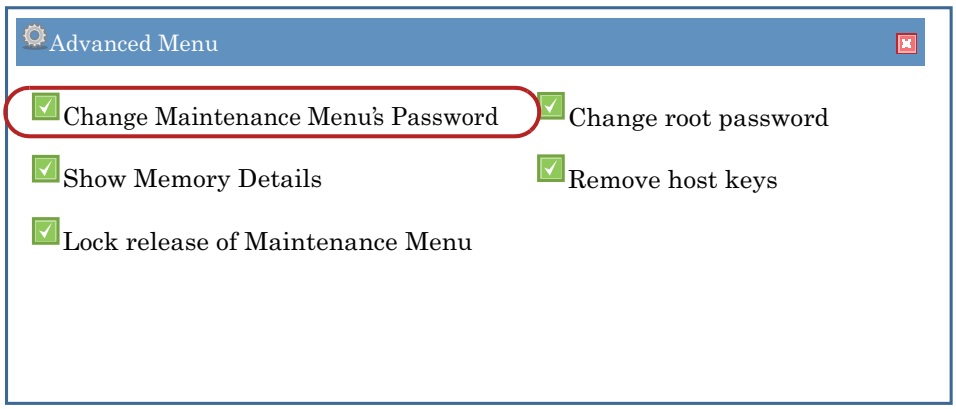
Step2: **Telephony Server Maintenance Menu Login** screen appears. Type a user name and password.

Note: When you type a user name and password, note the following points.
- The default for both user name and password is “admin”.
- Contact NEC maintenance personnel if you need to confirm your user Name and password.

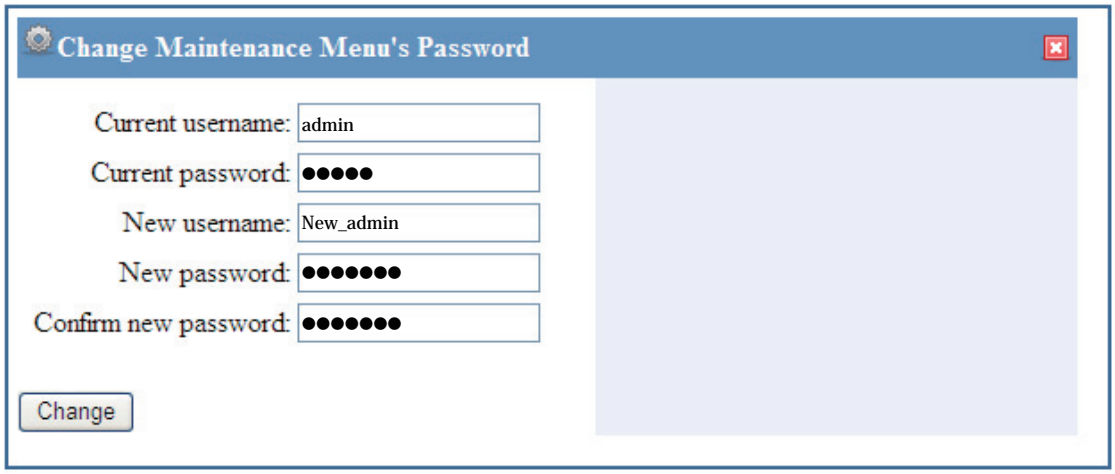
Step3: After the login, **Telephony Server Maintenance Menu** screen appears. Click the **Advanced Menu** button in the **SYSTEM CONTROL** area (in the upper right-hand part of the screen).



Step4: The **Advanced Menu** dialog box appears. Click the **Change Maintenance Menu's Password** button on the dialog box.



Step5: The **Change Password** dialog box appears. Configure each setting.



Screen Item	Type Item
Current username:	Type your current user name. **Note 1**
Current password:	Type your current password. **Note 1**
New username:	Type a new user name. **Note 2**
New password:	Type a new password. **Note 2**
Confirm new password:	Type a new password again to confirm the new password.

Note 1: The default for both user name and password is “admin”.

Note 2: Up to 64 alphanumeric characters including "-", "_" and "." can be included in a user name and password (case-sensitive).

Step6: Click the **Change** button.

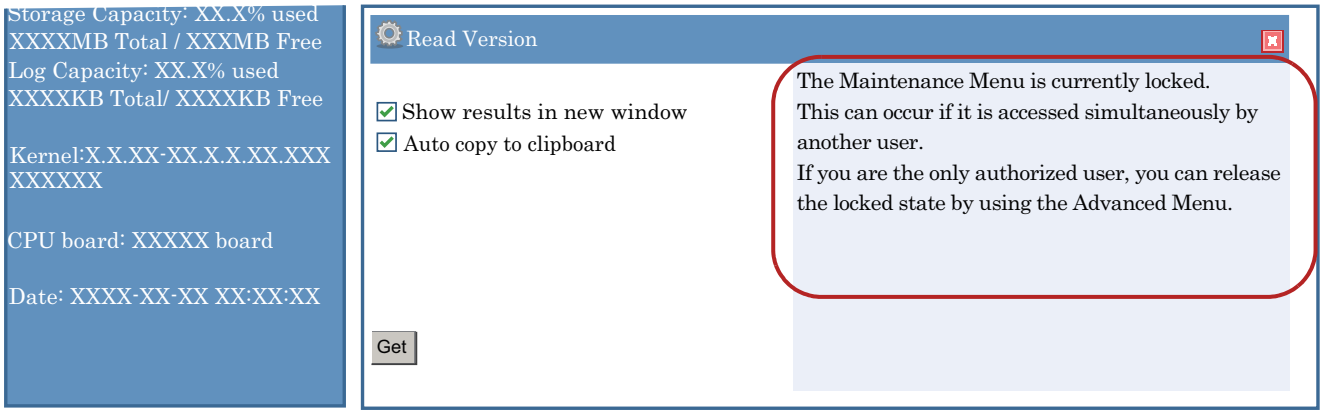
Note: The password in the **Confirm new password** field must match the password you entered in the **New password** field above.

Step7: Check that a message “Username and Password change success.” is displayed.

The change of the user name and password is complete.

1.3.1 How to Unlock the Locked Telephony Server Maintenance Menu

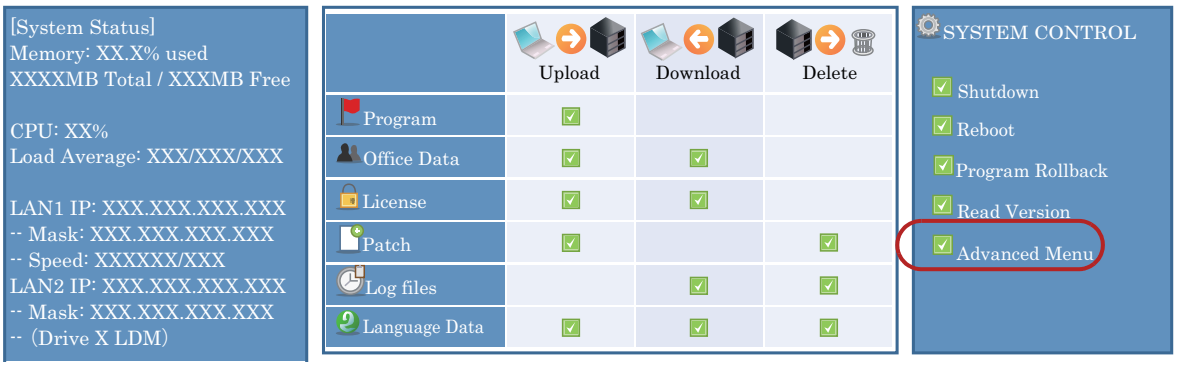
If you attempt to perform another action on the Telephony Server Maintenance Menu before program upload is completed (the message “Operation successfully completed.” appears), the menu may be locked and you will get the error message “Process is busy now. Please access later.” Once the menu is locked, only the unlock function is available



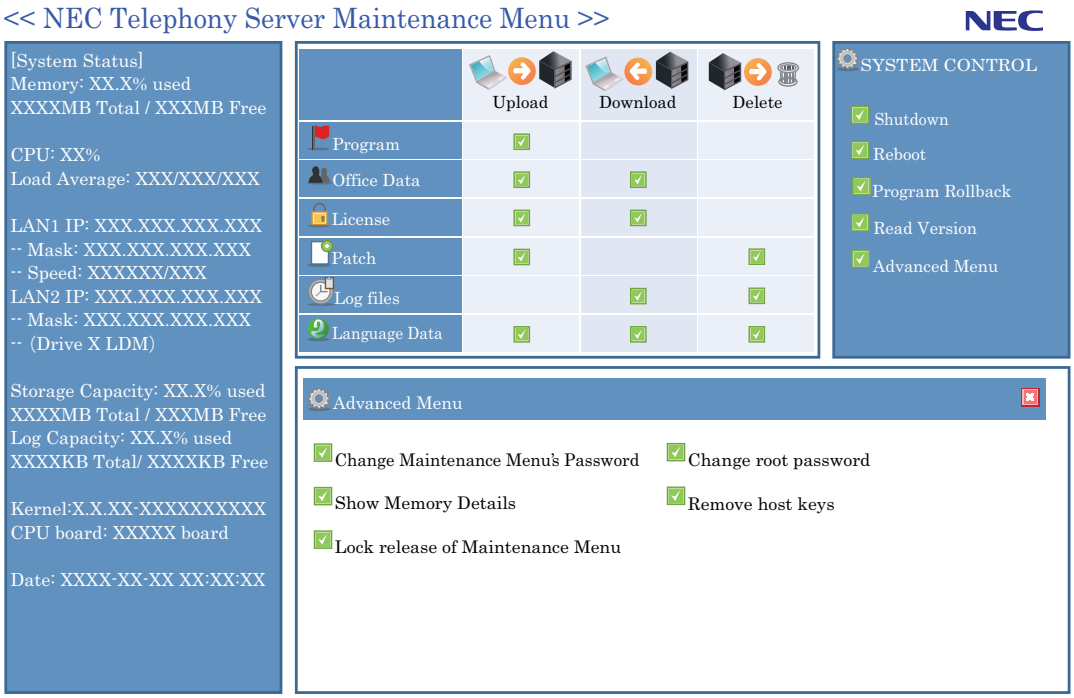
This section explains how to unlock the locked Telephony Server Maintenance Menu.

Note: When the message “Process is busy now. Please access later.” appears, first ensure that no other PC users are accessing the same Telephony Server, and then unlock the menu by following the steps below:

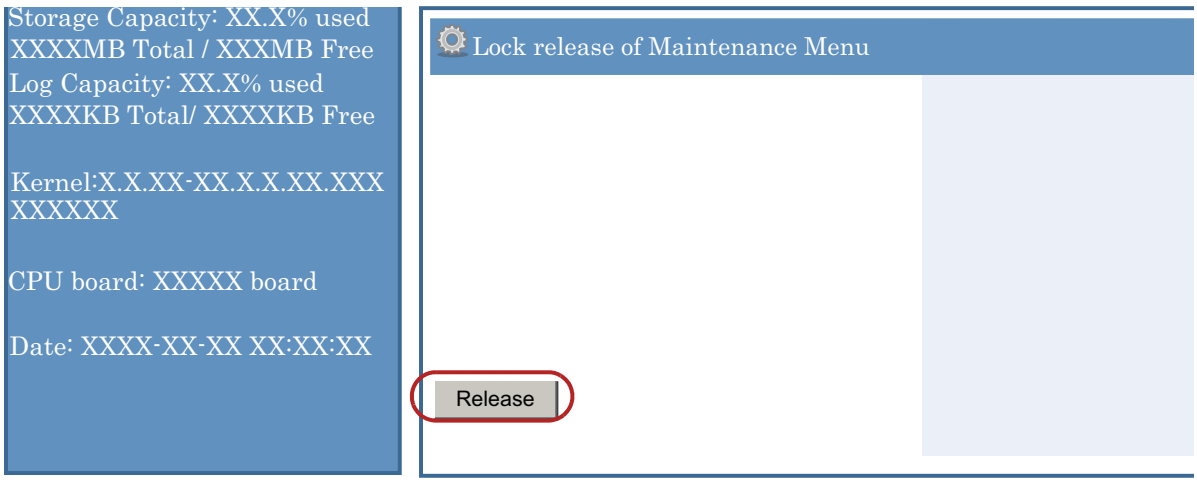
Step1: Click the **Advanced Menu** button in the **SYSTEM CONTROL** area.



Step2: The **Advanced Menu** dialog box appears. Click the **Lock release of Webconfig** button on the dialog box.



Step3: The **Lock release of Webconfig** dialog box appears. Click the **Release** button on the dialog box.



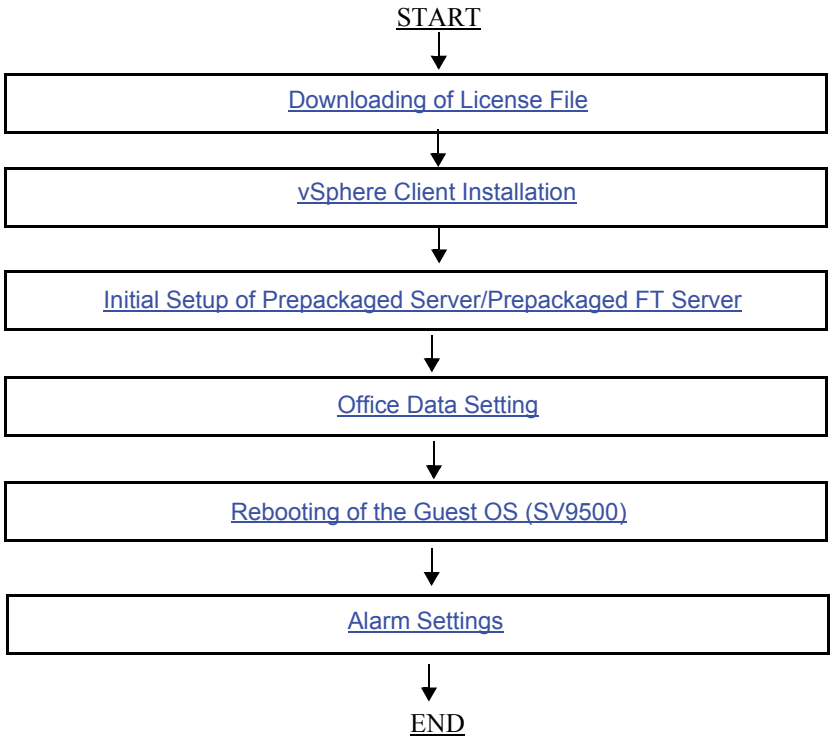
Step4: A confirmation message appears. Ensure that no other PC users are accessing the same Telephony Server, and click **OK**.

Step5: A message appears, saying “Operation successfully completed.” Click **OK** to close the message box.

2. Initial Startup Procedure

This section explains the initial startup procedure of SV9500 (Prepackaged Server Model). Follow the flow chart below to configure the initial startup.Take notice that some parts of the procedure may differ between the Prepackaged Server Model and the Prepackaged FT Server Model.

Note: Connect the Prepackaged Server/Prepackaged FT Server Model to your actual network only after completing the entire setup process and the alarm settings.



3. Downloading of License File

Access the License Management Server (LMS) to download a license file (svi.zip) and obtain Activation Code.

Note: Be sure to note the following conditions.

- A new Registration Activation code is necessary when the license is upgraded.
- The SVI file is downloaded in a zip format. Do not unzip the SVI file since this file is used as it is.
- You can rename the saved SVI file, but do not change the extension of the file.

4. vSphere Client Installation

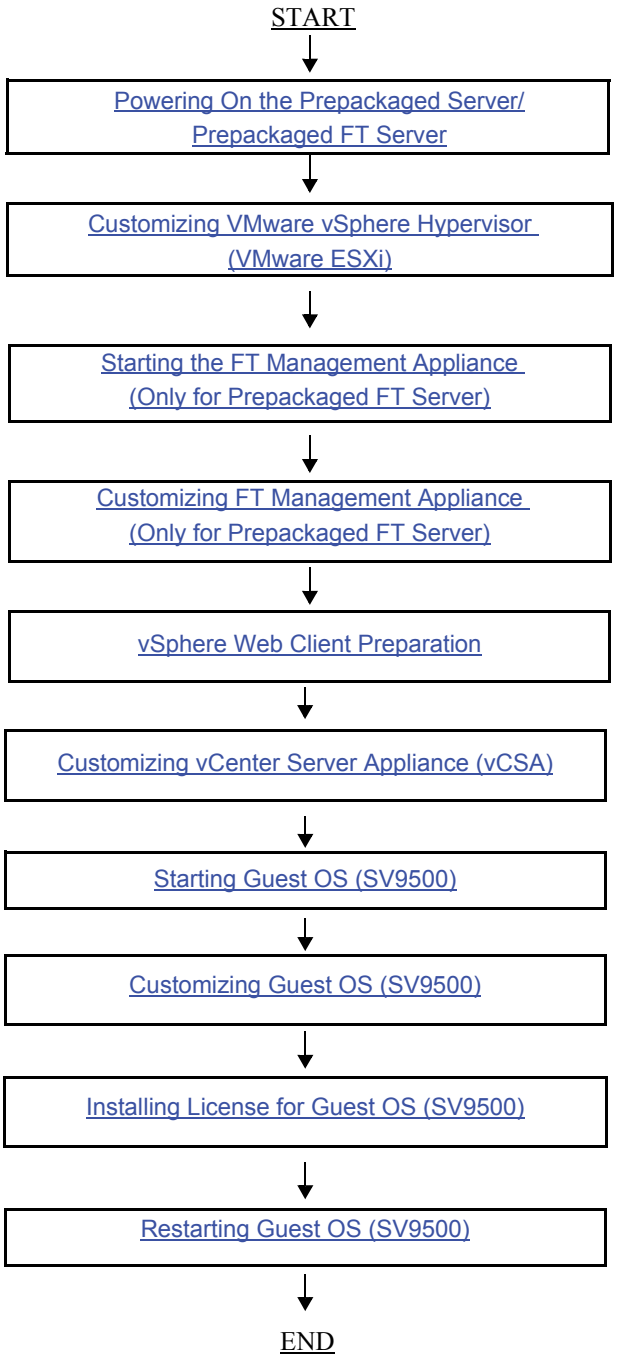
Follow the instructions below to install vSphere Client on the maintenance PC.

1. Connect to the VMware website and download the setup file for vSphere Client.
2. Open the setup file.
3. Follow the instructions for installation.

The process for the vSphere Client installation is finished.

5. Initial Setup of Prepackaged Server/Prepackaged FT Server

The initial setup procedure of the Prepackaged Server/Prepackaged FT Server is outlined in the flow chart below.



5.1 Powering On the Prepackaged Server/Prepackaged FT Server

Follow the instructions below to power on the Prepackaged Server/Prepackaged FT Server.

1 Plug the power cable into the Prepackaged Server/Prepackaged FT Server.
For the Prepackaged FT Server, follow the order as below.
(1) Plug the power cable for module #0 (upper part)
(2) Plug the power cable for module #1 (lower part)

Note:
Any time you unplug the power cable, wait at least 30 seconds before plugging it back in.

Point:
For the Prepackaged FT Server, the first module that has the cable connected becomes the primary.

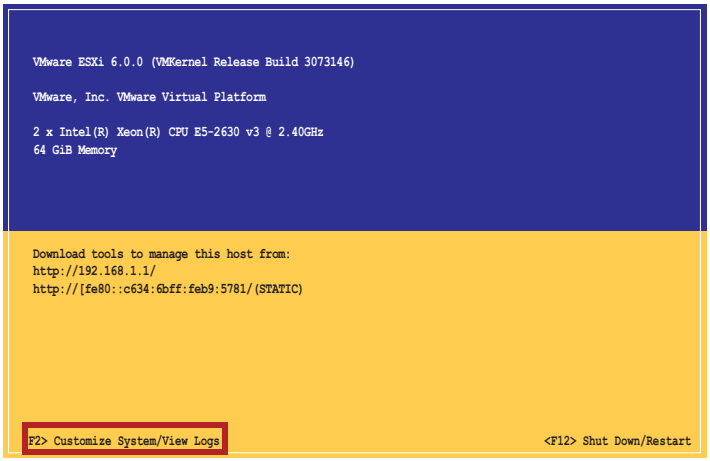
2 Perform all the LAN cable connections as explained in the Management by LAN Port section in this manual.Connect only the Prepackaged Server/Prepackaged FT Server LAN cable and the maintenance PC LAN cable to the same network.

Note:
Connect the Prepackaged Server/Prepackaged FT server to your actual network only after completing the entire setup process and the alarm settings.

3 Power on the monitor and other peripherals of the Prepackaged Server/Prepackaged FT Server.

Point:
Use a monitor designed for Prepackaged Server/ Prepackaged FT Server use.

4 Remove the front bezel and press the Prepackaged Server/Prepackaged FT Server front power switch.
The power lamp lights green and the **console screen** (the screen with [F2 (Customize System/View Logs)] on its lower left part) is shown on the monitor.



Note:
Build number and other data can be different from the screen shown on the left for a Prepackaged FT server.

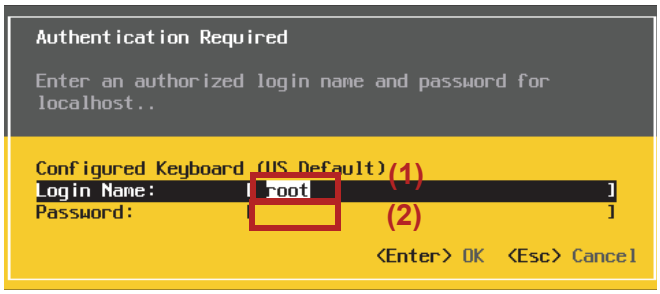
5.2 Customizing VMware vSphere Hypervisor (VMware ESXi)

The root password and the IP address on VMware ESXi must be changed.

1 With the Prepackaged Server/Prepackaged FT Server console screen displayed, press [F2] on the keyboard.

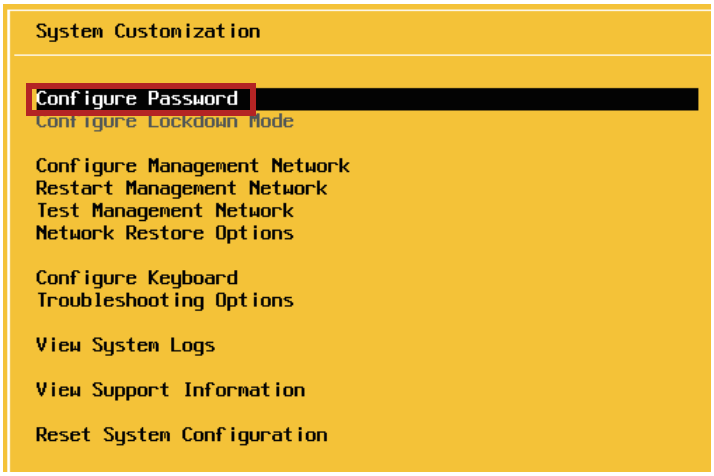
2 Enter the default user ID and password below. Press the Enter key to log in to the VMware ESXi.

(1) Login Name: root
(2) Password: sv9500type2



The **System Customization** screen appears.

3 Select **Configure Password** from the menu, and press the Enter key.

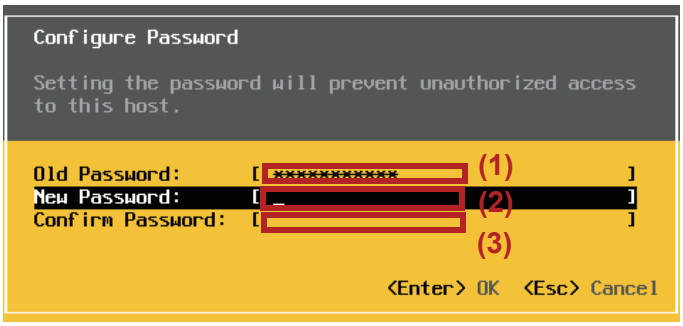


The **Configure Password** screen appears.

4 The root password needs to be changed.
In the **Configure Password** screen,

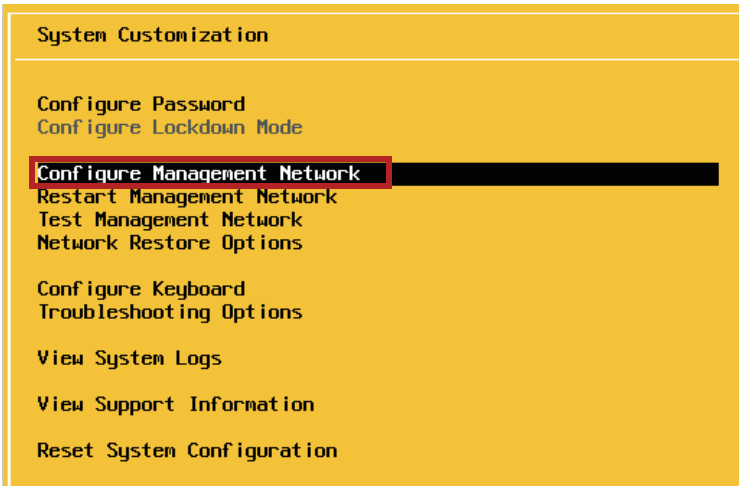
(1) Enter the old password (sv9500type2).
(2) Enter the new password.
(3) Enter the new password a second time to confirm it.

Press the Enter key to return to the **System Customization** screen.

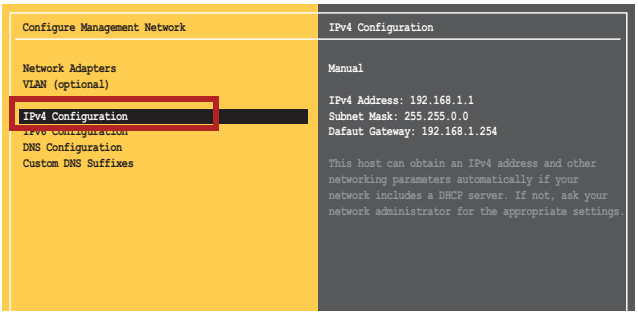


Note:
Use more than 8 characters for the password. Create a password that is difficult to guess and periodically change it.

5 The IP address for the management network interface (port for the access to vSphere Client) needs to be changed.
Select **Configure Management Network** from the menu, and press the Enter key.



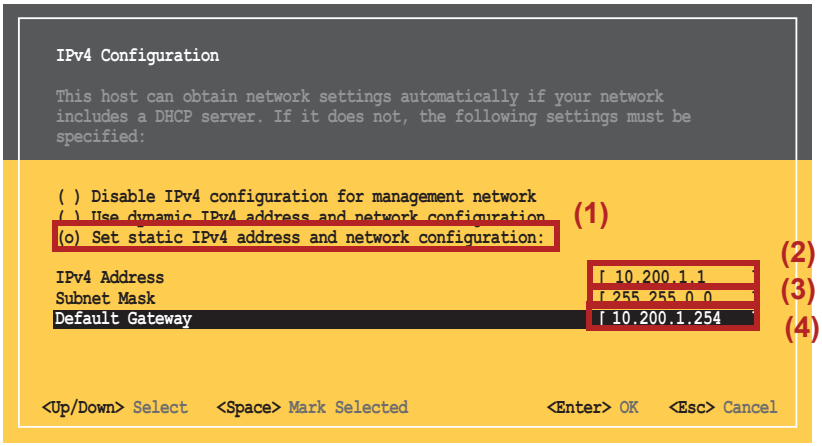
6 Select **IPv4 Configuration**, and press the Enter key.



IPv4 Configuration screen is displayed.

7

(1) Use the arrow keys to choose **Set static IPv4 address and network configuration**, and press the space bar to enable the option.
(2) Enter an IP address for the management network interface.
(3) Enter a subnet mask IP address.
(4) Enter a default gateway address and press the Enter key.



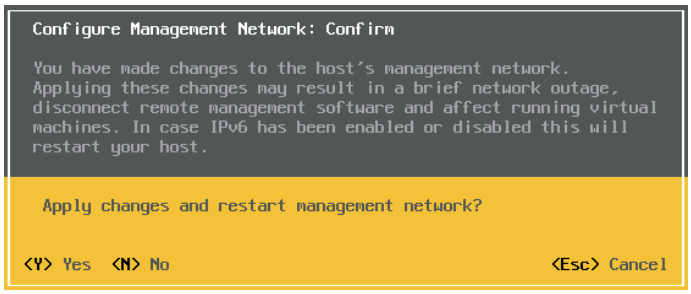
8

Verify the changes made are correct.

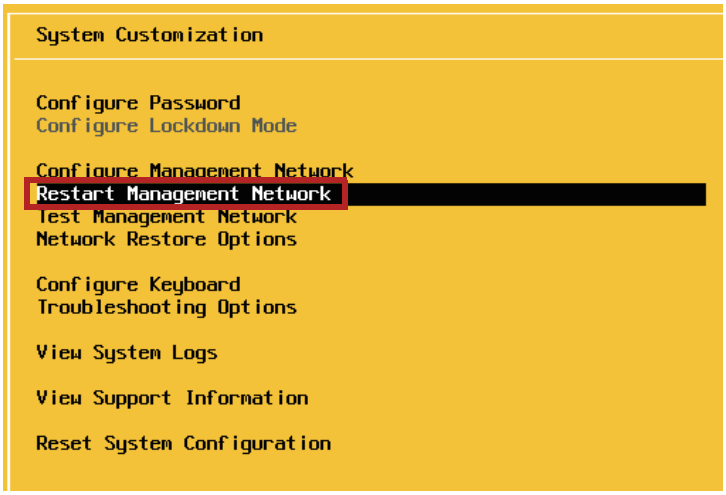
9

Press the ESC key.

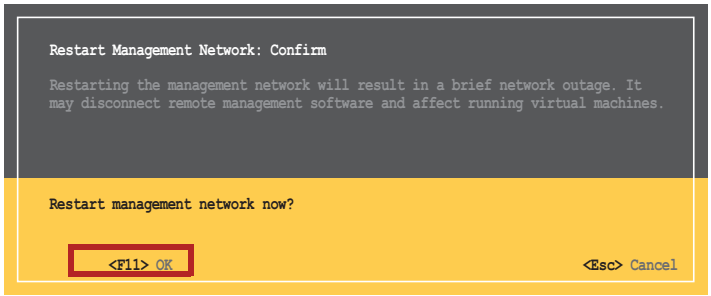
10 A confirmation message is displayed. Enter Y for Yes.



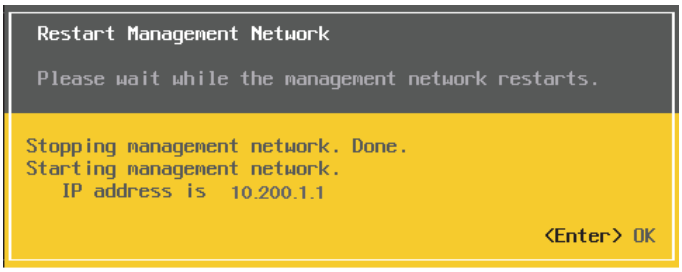
11 To apply the change to the IP address it is necessary to restart the management network. Select **Restart Management Network**.



12 Press the F11 key.



13 Press the Enter key.



14 Press the ESC key and logout.

5.3 Starting the FT Management Appliance (Only for Prepackaged FT Server)

This section explains the procedure for starting the FT Server management appliance for the Prepackaged FT Server. If a Prepackaged Server is used, skip this section. Usually the start of this appliance is automatically done, but if it does not start automatically, use this procedural to start it.

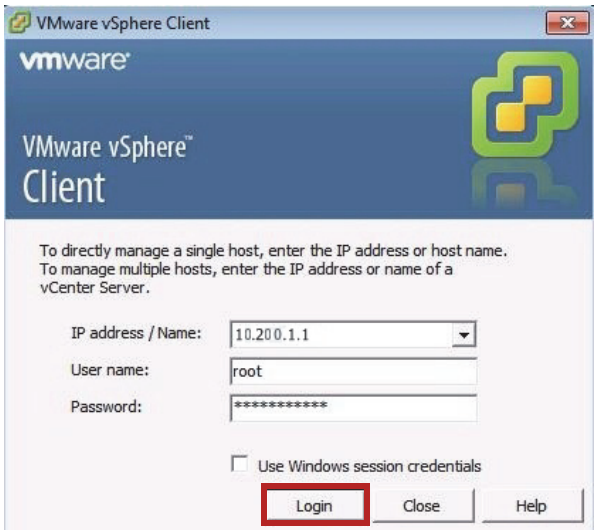
1 Assign an IP address to your maintenance PC that it is in the same network as the IP address of ESXi (which you have configured in Step 7 of Customizing VMware vSphere Hypervisor (VMware ESXi)).

2 Use the PING command from the maintenance PC and verify that there is a response from the IP address of VMware ESXi.

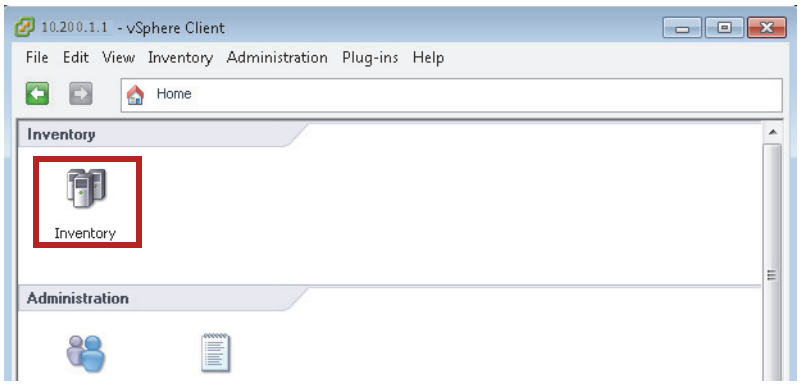
3 Launch vSphere Client from the maintenance PC. In the login window, enter the IP address of VMware ESXi and then enter the following user ID and password.

User name: root
Password: (The root password from Step 4 of Customizing VMware vSphere Hypervisor (VMware ESXi))

Press the **Login** button.



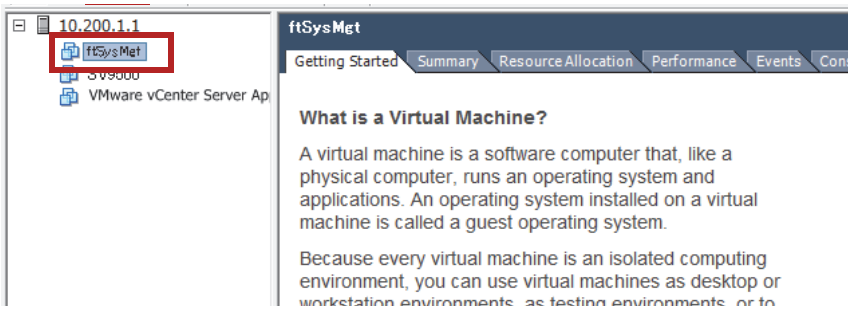
4 Click on **Inventory**.



5 Power on the virtual machine for the FT management appliance.

(1) Click first on VMware ESXi IP address and then click on the FT management appliance.

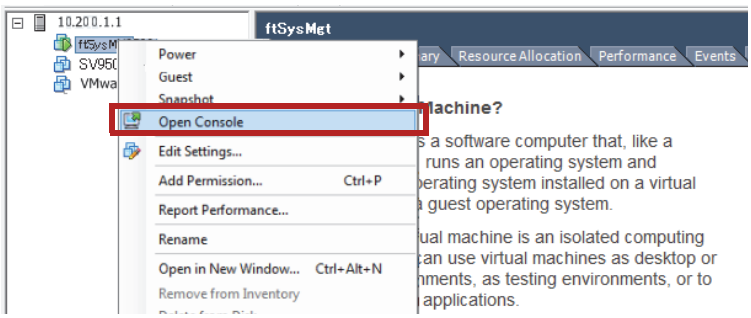
(2) Right-click the icon for the machine and select **Power** -> **Power On** to power on the virtual machine.



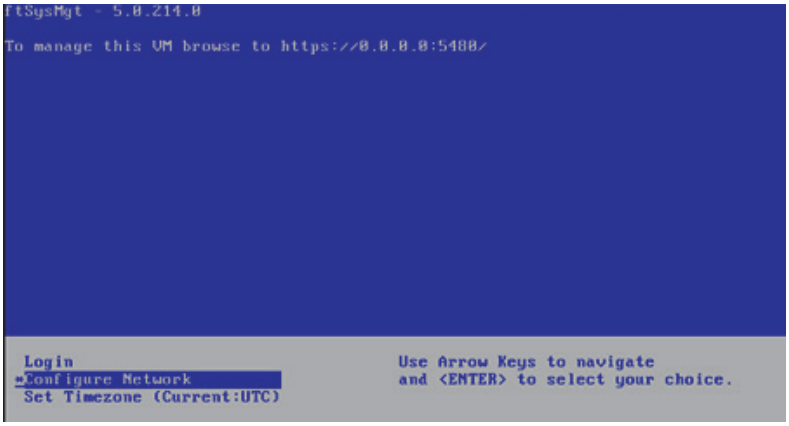
6 Assign an IP address to your maintenance PC that it is in the same network as the IP address of the FT management appliance (192.168.1.3/16).

7 Use the PING command from the maintenance PC and verify there is a response from the IP address of the FT management appliance.

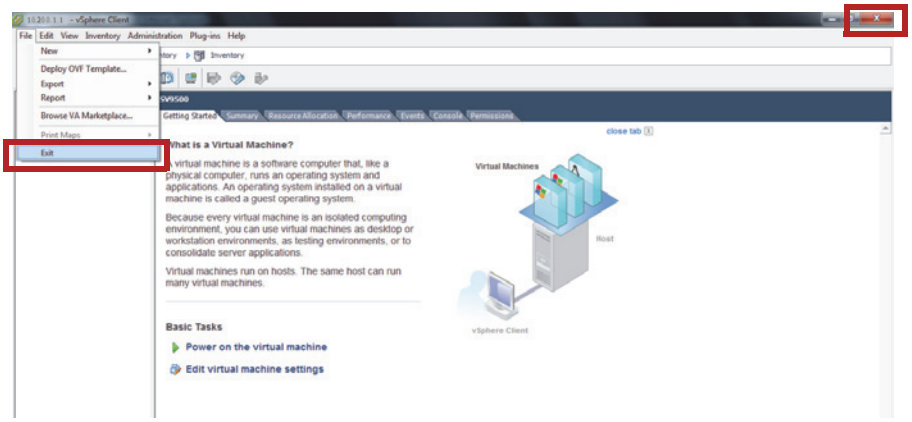
8 Click on the FT management appliance and select **Open Console** from the right-click menu.



9 Verify that the console screen is displayed.



10 Logout by clicking **Exit** on the **File** menu or **[x]** in the upper right hand corner.



Note:
In some cases, every five minutes the message “init: Id “osm” respawning too fast: disabled for 5minutes” is displayed.

5.4 Customizing FT Management Appliance (Only for Prepackaged FT Server)

This section explains the procedure for setup the FT management appliance IP address and root password. If a Prepackaged Server is used, skip this section.

1 Assign an IP address to your maintenance PC that it is in the same network as the address of ESXi (which you have configured in Step 7 of Customizing VMware vSphere Hypervisor (VMware ESXi)).

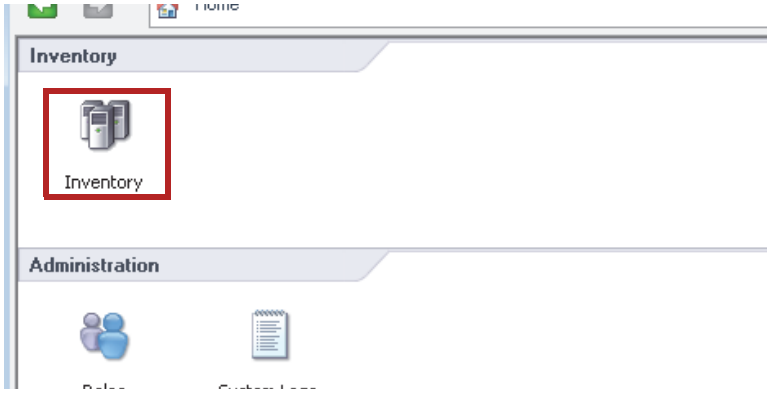
2 Use the PING command from the maintenance PC and verify there is a response from the IP address of VMware ESXi.

3 Launch vSphere Client from the maintenance PC and in the login window, enter the IP address of VMware ESXi and then enter the following user ID and password.

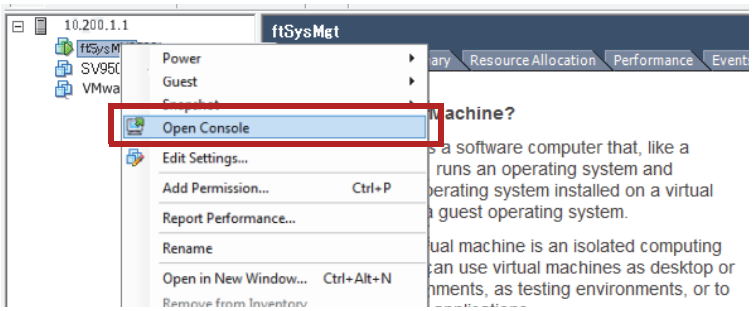
User name: root
Password: (The root password from Step 4 of Customizing VMware vSphere Hypervisor (VMware ESXi))

Press the **Login** button.

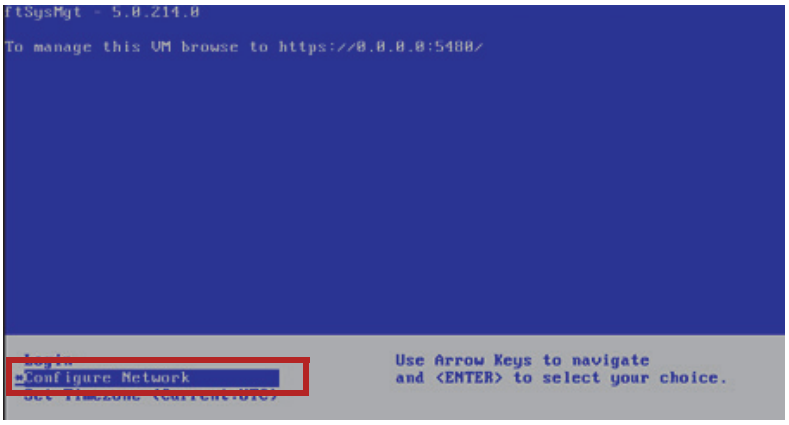
4 Click on **Inventory**.



5 Click on the FT management appliance and select **Open Console** from the right-click menu.



6 Select **Configure Network** and press the Enter key.



7 Enter [**6**] on [**Enter a menu number**].

```
Main Menu

0)      Show Current Configuration (scroll with
Shift-PgUp/PgDown)
1)      Exit this program
2)      Default Gateway
3)      Hostname
4)      DNS
5)      Proxy Server
6)      IP Address Allocation for eth0
Enter a menu number [0]: 6
```

8 Set the IP address as shown below.

(1) Enter [**y**].

```
Configure an IPv4 address for eth0? y/n [n]: y
```

(2) Enter [**n**].

```
Use a DHCPv4 Server instead of a static IPv4
address? y/n [n]: n
```

(3) Enter a new IP address.

```
IPv4 Address []: 10.200.1.3
```

(4) Enter a new subnet mask.

```
Netmask []: 255.255.0.0
```

9 Enter [**y**] if the displayed data is correct.

```
IPv4 Address:  10.200.1.3
Netmask:       255.255.0.0

Is this correct? y/n [y]: y
```

10 Enter [**2**] on [**Enter a menu number**].

```
Main Menu

0)      Show Current Configuration (scroll with
Shift-PgUp/PgDown)
1)      Exit this program
2)      Default Gateway
3)      Hostname
4)      DNS
5)      Proxy Server
6)      IP Address Allocation for eth0
Enter a menu number [0]: 2
```

11 To select eth0, enter [**0**].

```
0)      eth0
Choose the interface to associate with default
gateway [0]: 0
```

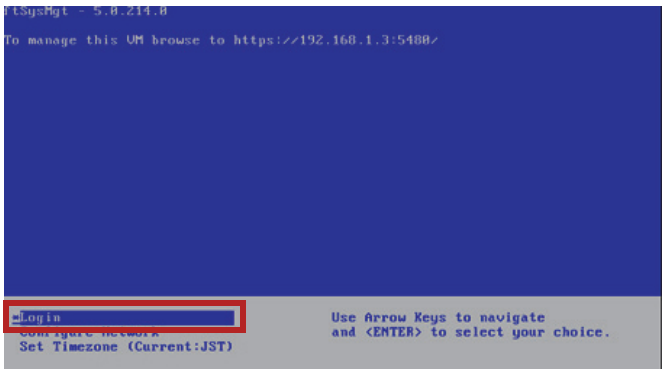
12 Enter the new default gateway.

```
IPv4 Default Gateway []: 10.200.1.254
```

13 IPv6 default gateway is displayed. Press the Enter key without enter any data.

```
IPv6 Default Gateway []:
```

14 Select [**Login**] and press the Enter key.



15 Log in with the data as shown in the screen below.

```
localhost login: root
Password: ftServer
```

16 Set a new password.

```
# passwd root
```

17 Customized data is implemented.

```
# /opt/ft/sbin/configure-appliance
# shutdown -r now
```

FT management appliance is rebooted.

18 Log in again from the console menu as root user.

19 Enter FT management appliance IP address. (In the screen below [xxx.xxx.xxx.xxx] represents the IP address.
Enter the FT Server management appliance IP address after "-l".

```
# /opt/ft/sbin/build-loghost update -l 10.200.1.1
```

20 Access the ESMPRO/Server Agent guide at:
http://www.58support.nec.co.jp/global/download/index.html
and proceed as below.

(1) Start Control Panel (ESMamsadm).
(2) Setup the trap information addressee IP address from SNMP Settings.

21 See NEC ESMPRO Server Management Guide and perform an automatic registration of the server.

5.5 vSphere Web Client Preparation

Proceed as follows to install the plug-in required for vSphere Web Client use.

1. On Internet Explorer, open [Tool] - [Internet options] - [Connections] - [LAN settings] - [Local Area Network (Lan) Settings] and make sure that there is not a check mark placed in any of the the check boxes.
2. Connect the maintenance PC to the server.
3. Insert the DVD for VMware vCenter installation in the maintenance PC and click on the file for plug-in installation. When the screen for starting the installation is displayed, press [Next].
4. When an Software License Agreement screen is displayed, place a check mark accepting the agreement and click [Next].
5. Select the folder to place the software and click [Next].
6. Click [Install] to start the installation.
7. When a screen notifying the completion of the installation is displayed, click [Finish].

Plug-in installation is finished.

5.6 Customizing vCenter Server Appliance (vCSA)

This section explains the procedure for changing vCSA password and IP address.

1 Assign an IP address to your maintenance PC that it is in the same network as the address of ESXi (which was configured in Step 7 of Customizing VMware vSphere Hypervisor (VMware ESXi)).

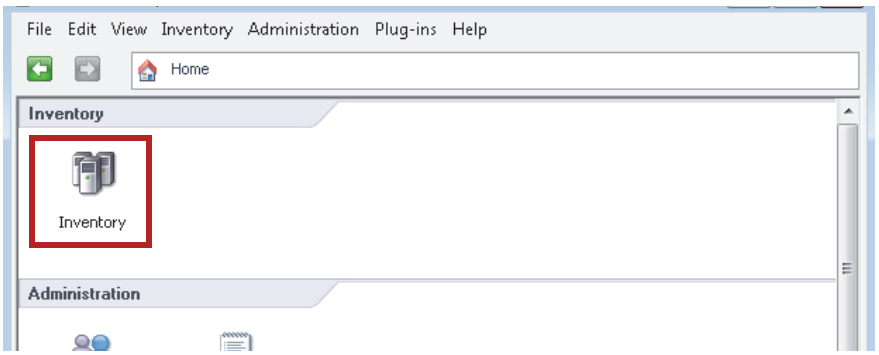
2 Use the PING command from the maintenance PC and verify there is a response from the IP address of VMware ESXi.

3 Launch vSphere Client from the maintenance PC. In the login window, enter the IP address of VMware ESXi and then enter the following user ID and password.

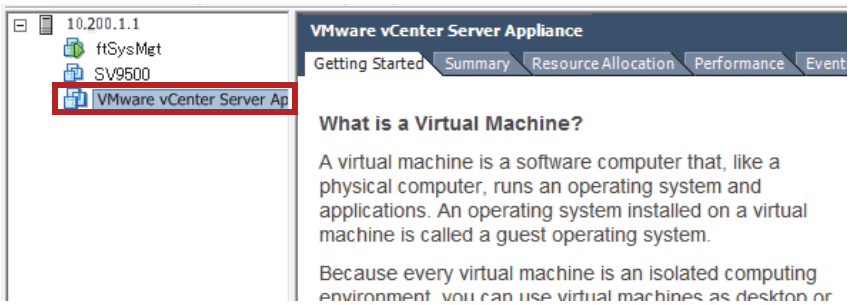
User name: root
Password: (The root password from Step 4 of Customizing VMware vSphere Hypervisor (VMware ESXi))

Press the **Login** button.

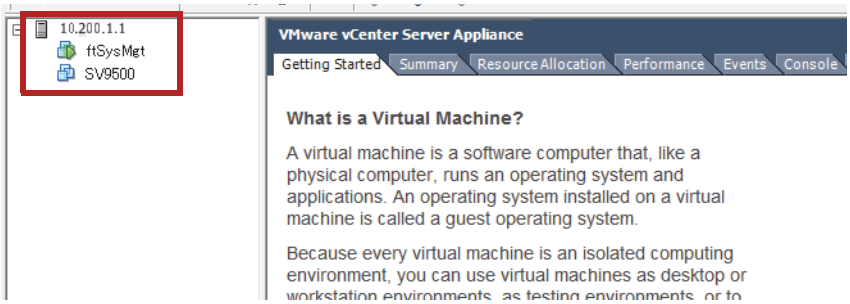
4 Click on **Inventory**.



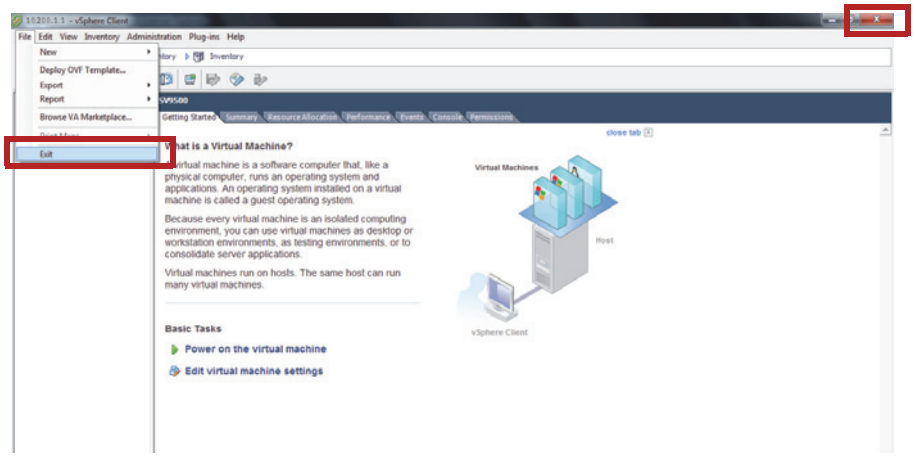
5 From vSphere Client, erase the virtual machine for the vCSA by right clicking the icon and selecting Power -> Delete from Disk (accept for the warning screen that will be displayed).



6 Verify that the vCSA icon is not displayed.



7 Logout by clicking **Exit** on the **File** menu or **[x]** in the upper right hand corner.



8 Install the DVD for vCSA installation in the client PC and click the [vcsa-setup.html] file of the DVD.

9 When the vCenter Server Appliance screen is displayed, click **Install**.

Note: If a screen asking for permission to opening the software is displayed, give such permission.

10 In the screen for Software License Agreement, place a check mark in the Software License Agreement box and click **Next**.

11 Give the following information for target server:

FQDN or IP address: **100.200.1.1** (the VMware ESXi IP address)
User: **root**
Password: (the VMware ESXi password)

12 When the security alert message is displayed, click **Yes.**

13 Choose an appliance name, set a password and click **Next**.

Note: Password must be eight characters or more. It must contain at least one capital letter and one lowercase letter, one number, and one special character.

14 For the deployment type place a check mark on the **Install vCenter with an Embedded Platform Services Controller** box and click **Next**.

15 Place a check mark in the box for new SSO domain. Set the data as follows (the following are examples, choose the names that you want):
vCenter SSO password:**SV9500@soo**
SSO domain: **vsphere.soo**
SSO site name:**SV9500-Site**
Click [**Next**].

16 Set the appliance size to [**Tiny (up to 10 hosts, 100 VMs)**] and click **Next**.

17 When selecting datastore, place a check mark on [**Enable Thin Disk Mode**] and click **Next**.

18 For the database, place a check mark on **Use an embedded database (vPostgres)** and click **Next**.

19 In the network settings screen enter the following data.

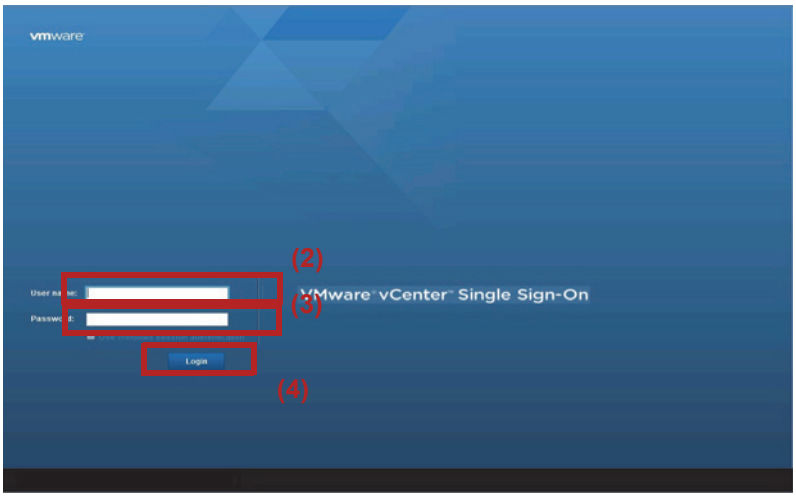
Choose a network: **VM Network**
IP address family: **IPv4**
Network type: **static**
Network address: (choose an IP address for vCSA (make sure is in the same network of VMware ESXi, for example 10.200.1.2).
System name [FQDN or IP address]: (Enter the same address entered above in Network address)
Subnet mask: (Enter the subnet mask that you want to use)
Network gateway: (Enter the gateway IP address that you want to use)
Network DNS Servers (separated by commas): (Enter an IP address for DNS server)
Configure time sync: Place a check mark in **Synchronize appliance time with ESXi host**.
Enable ssh: Place a check mark**.**

After all the data is entered, click **Next**.
Click **OK** for the message warning.

20 Verify that all the information is correct and click **Finish.**

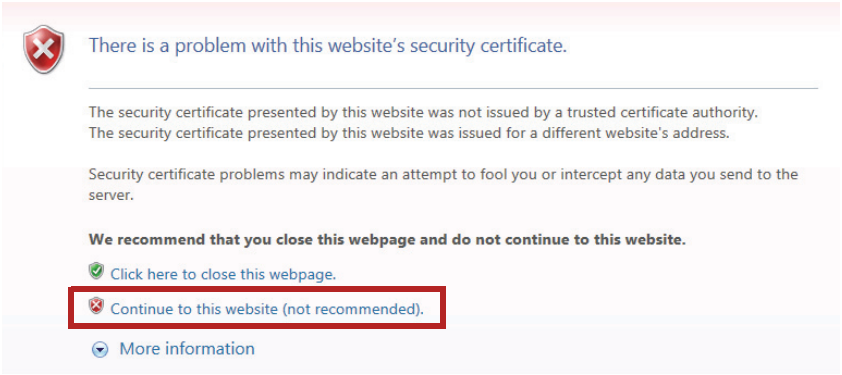
21 A screen is displayed during installation. After the installation is completed, the screen for notifying that it has been finished is displayed. Click the button for closing it.

22 (1) From the web browser of the maintenance PC, log in to vCSA (https://xx.xx.xx.xx:9433/) (xx.xx.xx.xx means the IP address that was set for vCSA).
Use the following user ID and password (below are given the examples used in step 15):
(2) User ID: **vsphere.sso**
(3) Password: **SV9500@sso**
(4) Press the **Login** button.

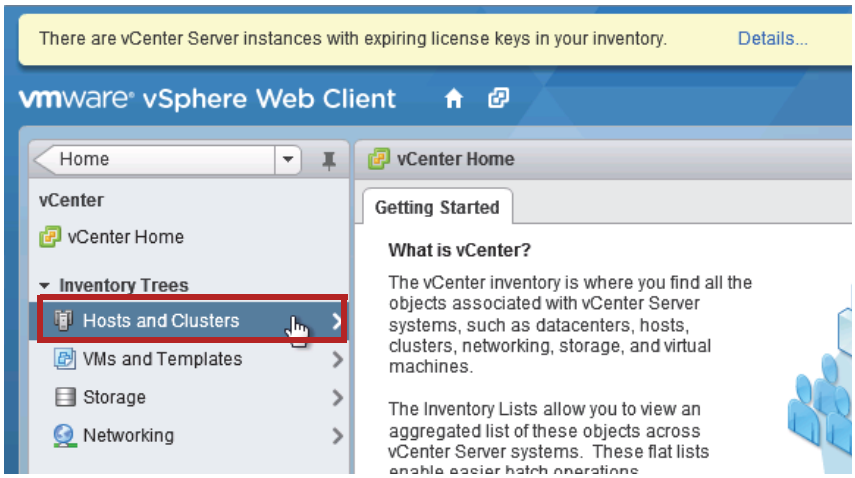


Note: Make sure that System name is set with the same IP address of vCSA, if there is a mistake vCSA needs to be reinstalled.
For reinstalling, use vSphere Client to erase the vCSA machine and start the process again.

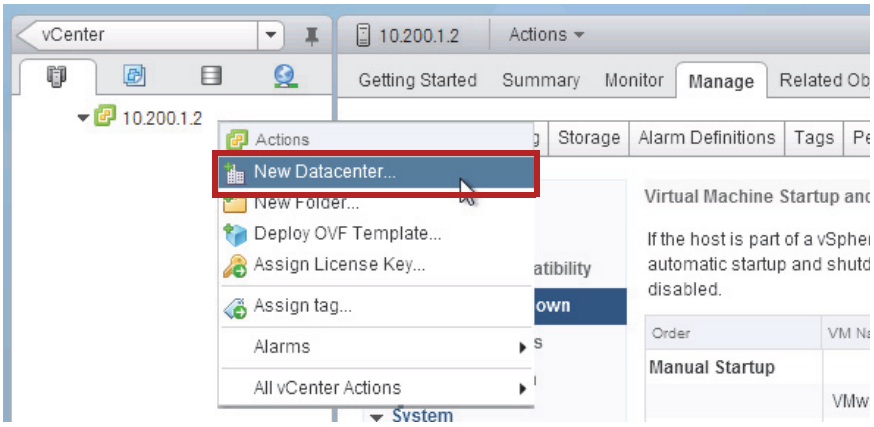
23 A warning message as shown below could appear. In that case, to continue, click on **Continue to this website (not recommended)**.



24 After accessing the page, from the menu on the left side of the screen, click **Hosts and Clusters**.

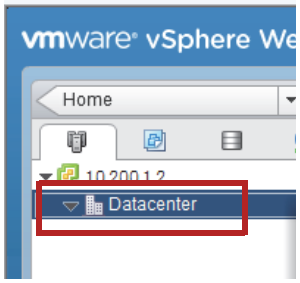


25 Select the IP address of vCSA (in this example 10.200.1.2) from the menu on the left side of the screen and click **New Datacenter**.

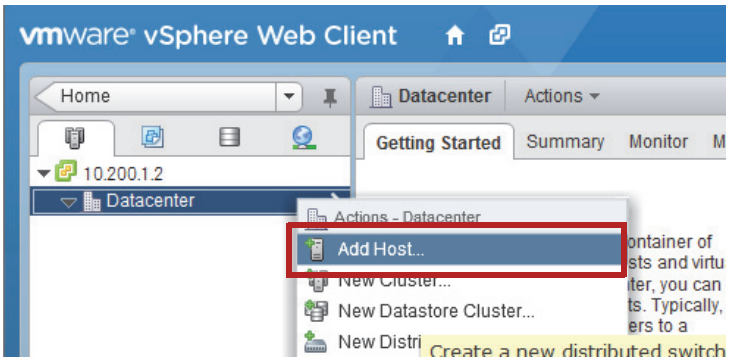


26 A dialog box is displayed. Leave the name for datacenter unchanged and click **OK**.

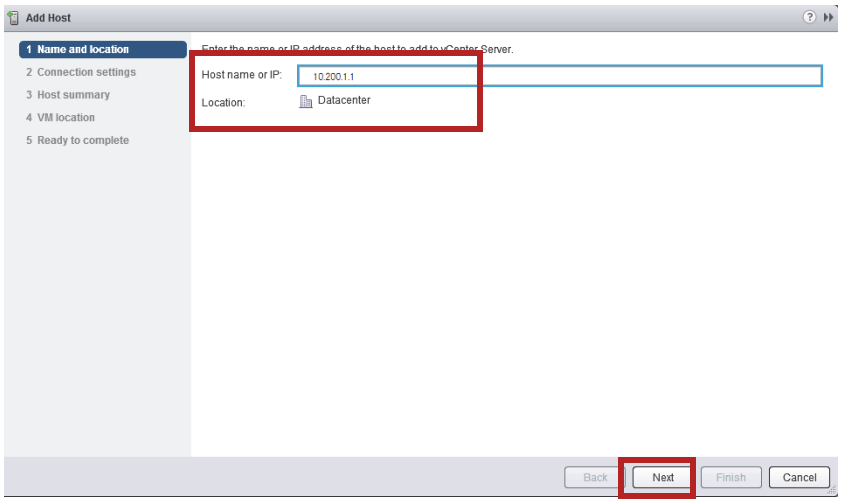
27 Verify that Datacenter icon is displayed.



28 Right-click the Datacenter icon and select **Add Host**.

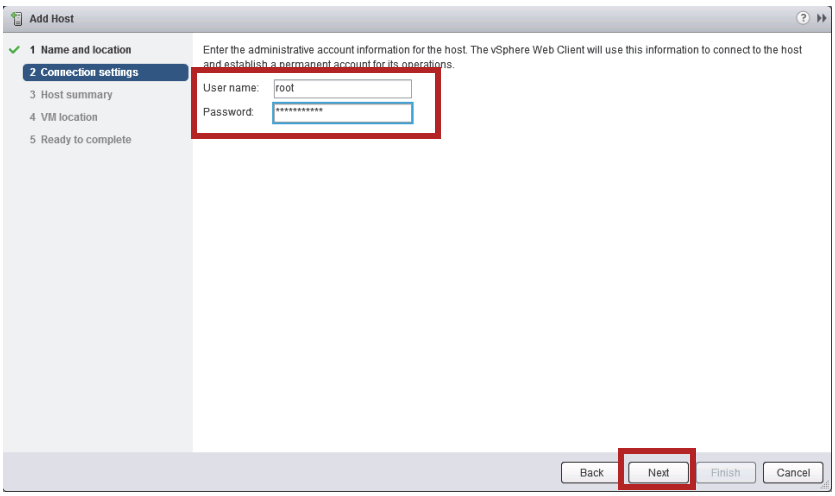


29 The Add Host wizard screen is displayed.
Enter IP address of VMware ESXi for **Host name or IP** and click **Next**.



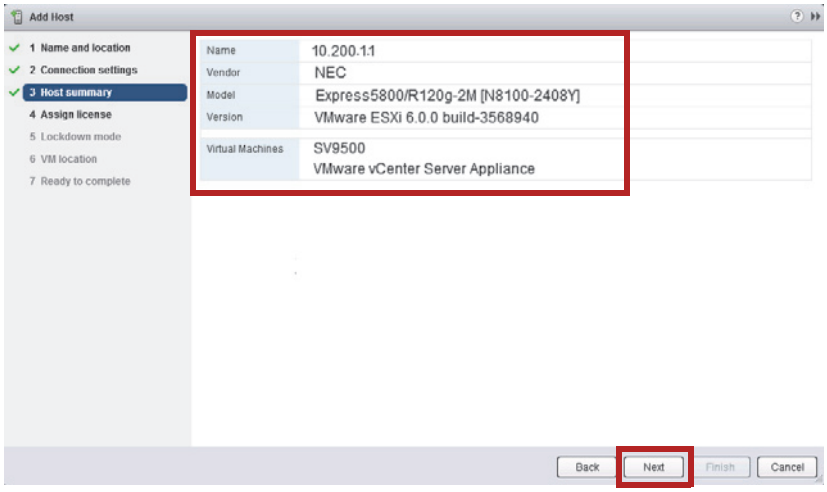
30 Enter the user name and password as below.
User name: **root**
Password: (the VMware ESXi password)

After Entering the data, click **Next**.

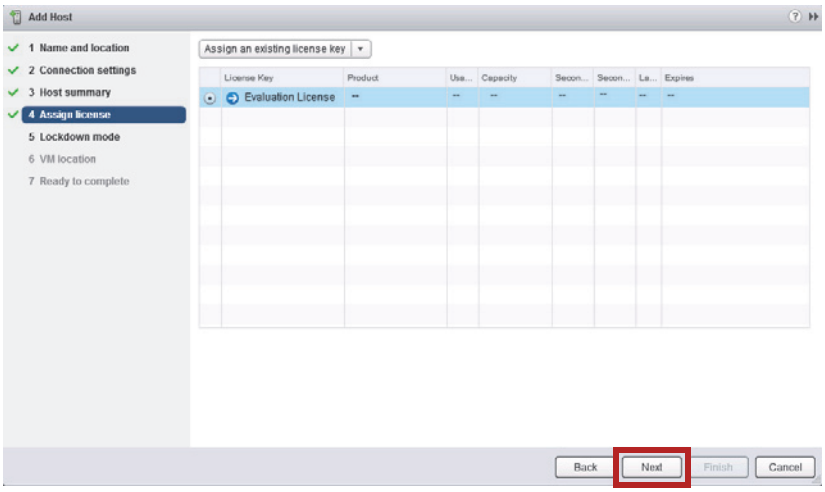


31 When the Security Alert message is displayed, click **Yes**.

32 Verify the added host settings information. If there are no problems on the displayed information, click **Next**.

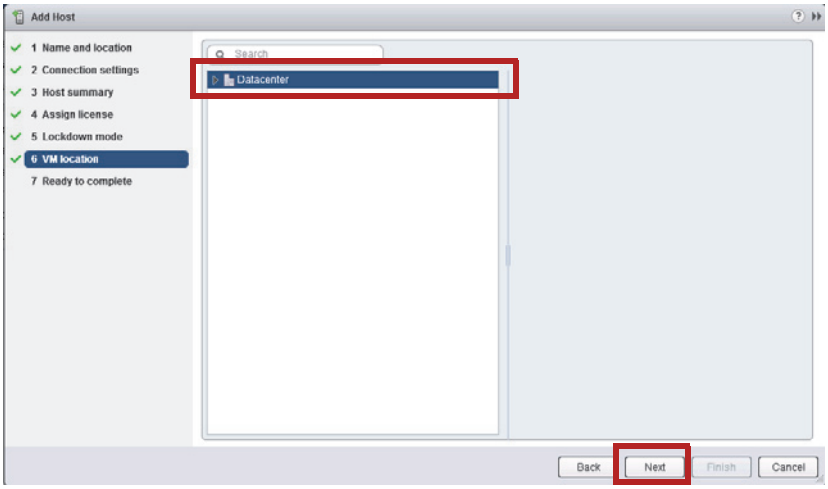


33 License information is displayed. Click **Next** without making any modification.

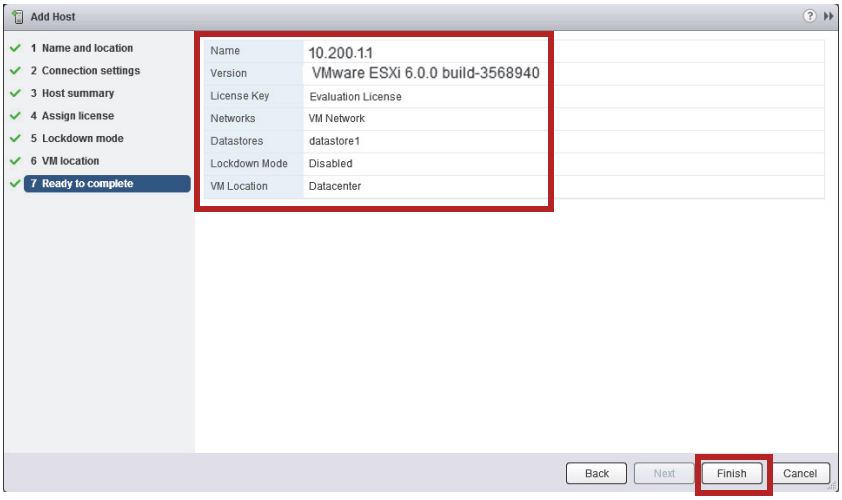


34 In the Lockdown mode screen place a mark on **Disabled** checkbox and click **Next**.

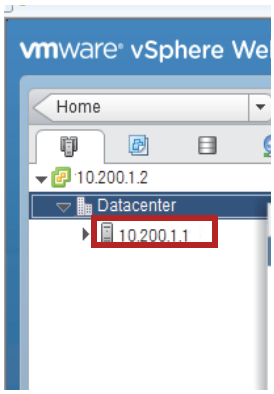
35 Select **Datacenter** and click **Next**.



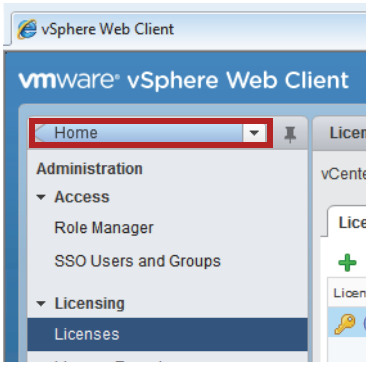
36 Verify that the settings are correct and if there are no problems click **Finish**.



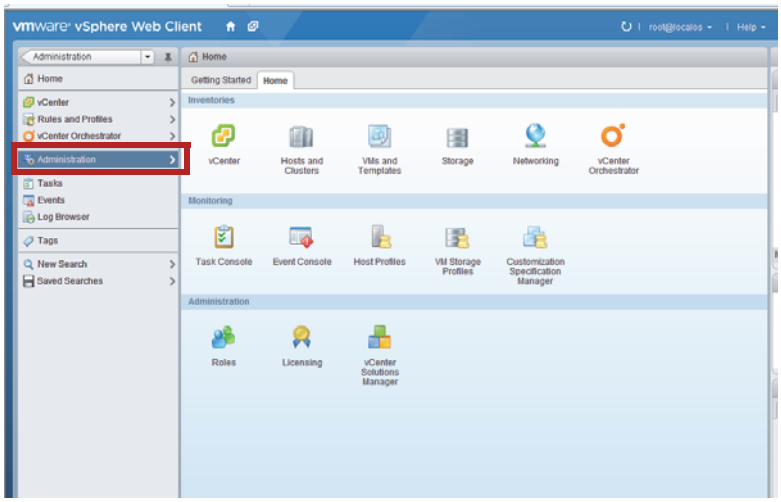
37 Verify that the host has been added.



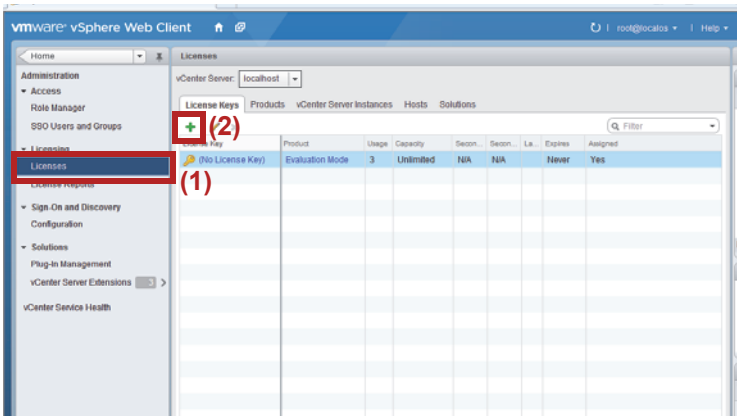
38 The next step is license registration.
Click **Home**.



39 Click **administration** on the home page.



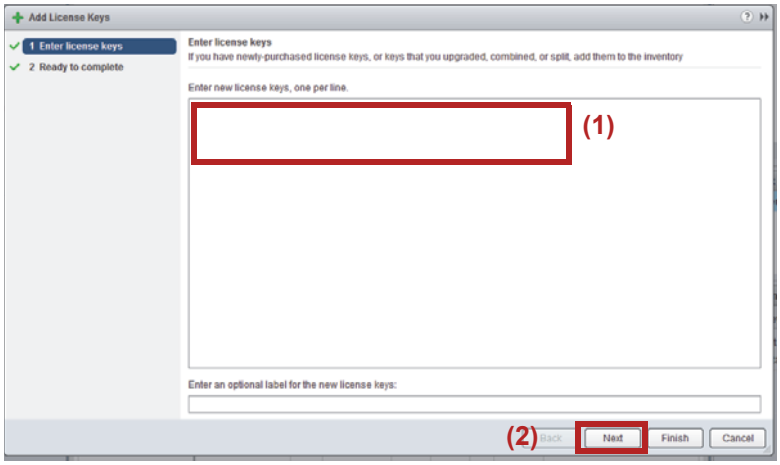
40 (1) Click the **Licenses** button.
(2) Click the **Add License** button.



Note:
License should be acquired in advance following the steps of vSphere license acquisition.

41

(1) Enter the license Key.
(2) Click the **Next** button.

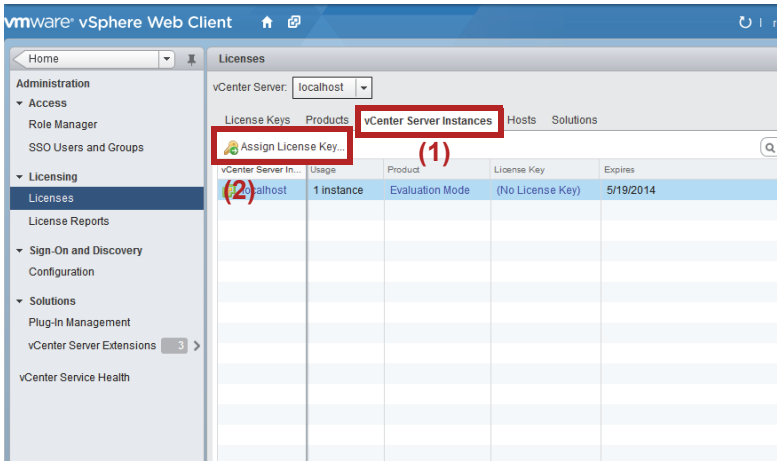


42

Register the license key following the indications of the displayed screen.

43

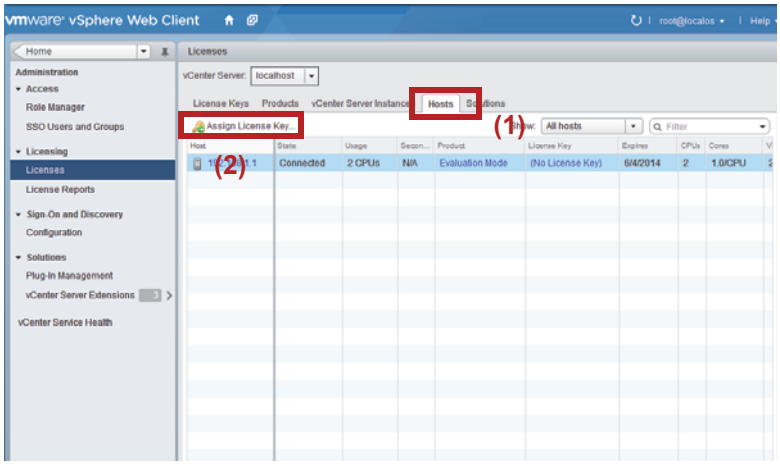
(1) Click the **vCenter Server Instances** tab.
(2) Click the **Assign License Key** button.



44

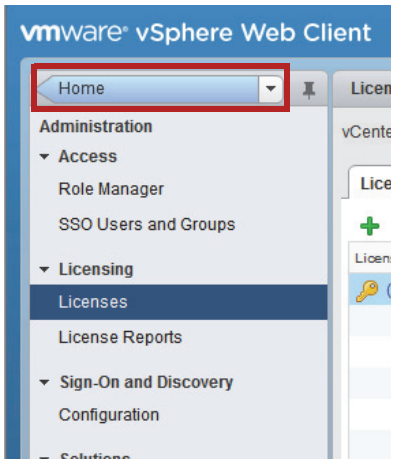
Split the license key following the screen guidance.

45 (1) Click the **Hosts** tab.
(2) Click the **Assign License Key** button.

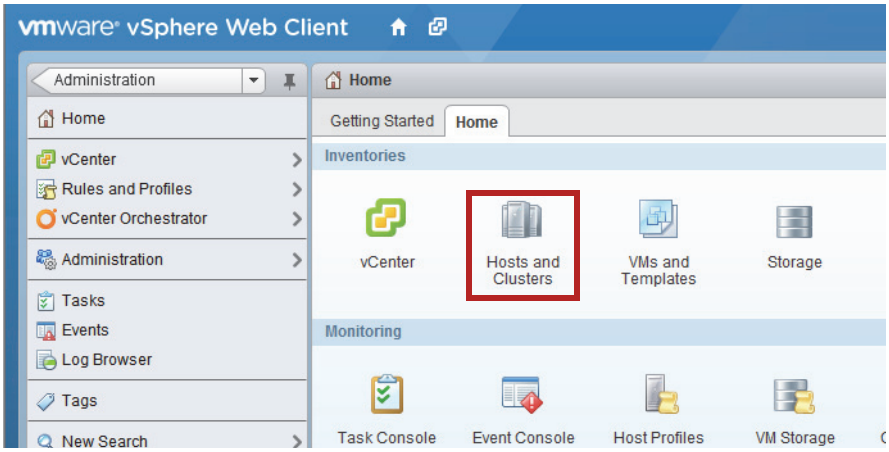


46 Split the license key following the screen guidance.

47 The next step is to startup the virtual machine.
Click **Home**.



48 Click **Host and Clusters**.



49

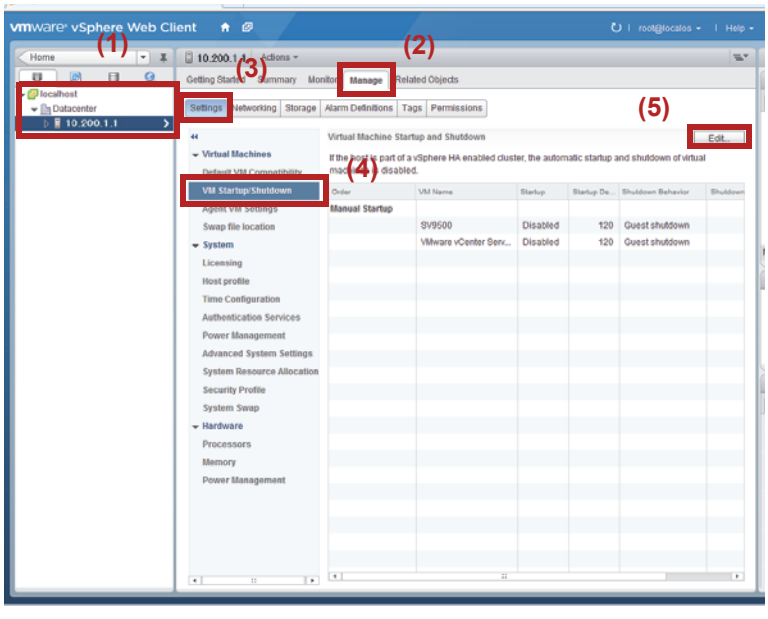
(1) Click **localhost->Datacenter->**xxx.xxx.xxx.xxx. (xxx.xxx.xxx.xxx is the ESXi IP address.)

(2) Click the **manage** button.

(3) Click on **settings**.

(4) Click **VM Startup/Shutdown**.

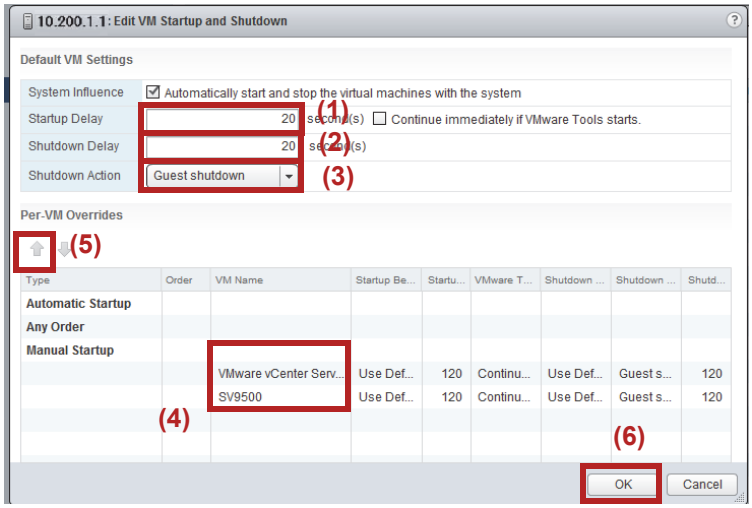
(5) Click the **Edit** button.



Note:
From this Step Prepackaged Server Model screens will be used (the FT management appliance machine is not displayed).

50

(1) Change the **Startup Delay** time from 120 seconds (default) to 20 seconds.
(2) Change the **Shutdown Delay** time from 120 seconds (default) to 20 seconds.
(3) On **Shutdown Action**, select **Guest Shutdown**.
(4) Select the virtual machines.
(5) Click on the arrow pointing up and go to **Automatic Startup**
(6) Click **OK**.



Set the order of the virtual machines as shown below.

Prepackaged Server Model

Order	Virtual Machine
1	vCSA
2	SV9500
3	Software-based MG-SIP

Prepackaged FT Server Model

Order	Virtual Machine
1	ftSysMgt
2	vCSA
3	SV9500
4	Software-based MG-SIP

Note:

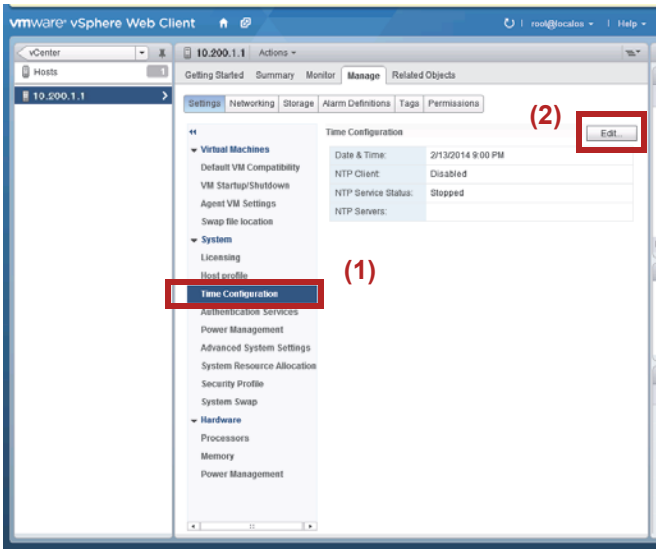
- Startup Delay and Shutdown Delay indicate the maximum time gap after being executed on a virtual machine till executing them again for the following one.
- Make sure that Automatic Startup is set.

51

Time Settings must be performed.

(1) Click **Time Configuration** from **Settings** on the **Manage** tab.

(2) On the upper right part of the displayed screen, click **Edit**.



If a NTP server is used go to STEP52.

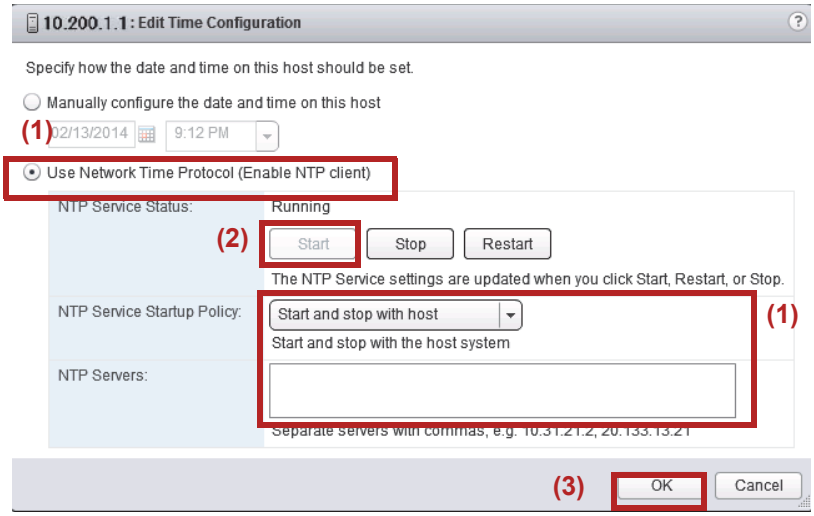
If a NTP server is not used go to STEP53.

52 Execute the settings of the NTP server as follows.

(1) Mark **Use Network Time Protocol (Enable NTP client)** and set the data in the following order.
NTP Service Startup Policy: Start and stop with host
NTP Servers: NTP server IP address

(2) Click the **Start** button.

(3) Click the **OK** button.

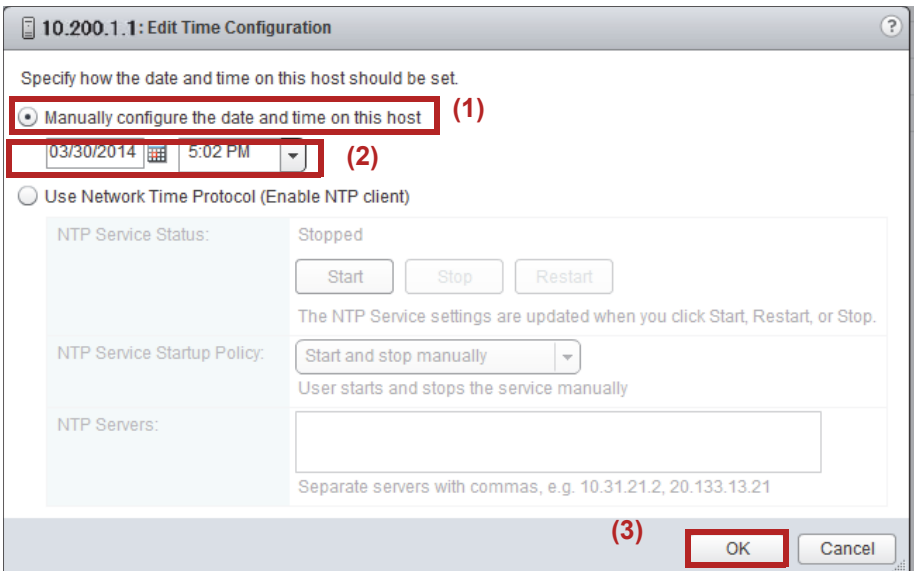


The NTP server setup is finished.

53 (1) Select **Manually configure the date and time on this host**

(2) Enter the day and hour.

(3) Click **OK**.



Time settings are finished.

5.7 Starting Guest OS (SV9500)

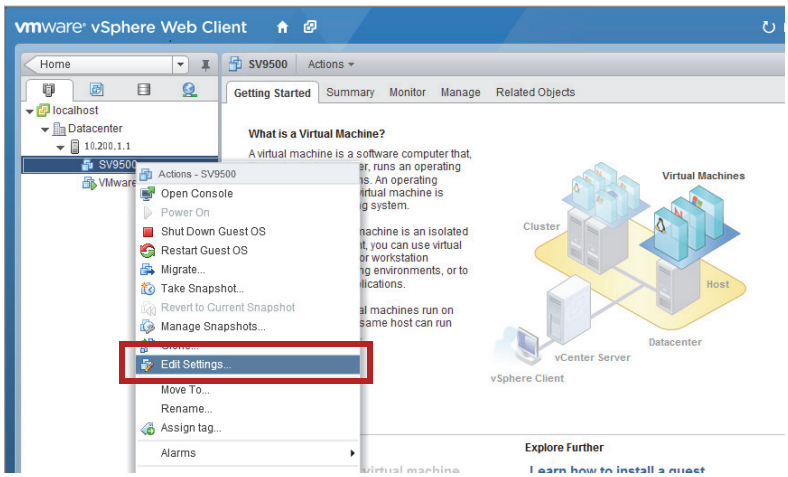
This section explains the procedure for starting the guest OS (SV9500).

1 From the web browser of the maintenance PC, log in as root user to vCSA(https://xxx.xxx.xxx:9443/). (xxx.xxx.xxx.xxx is the vCSA IP address).

2 To avoid and overlap, modify as follows the initial MAC address of each network adapter (LAN 1 to LAN 4) in the virtual machine for SV9500.

(1) Click **Hosts and Clusters (Inventories)** on **Home** tab.

(2) Right-click on the SV9500 virtual machine and select **Edit settings**.

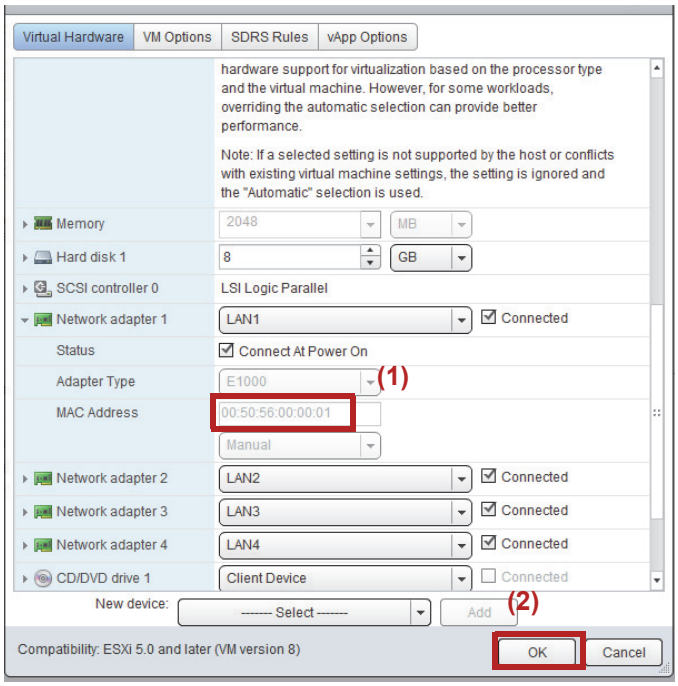


Note:
If there is not risk of overlapping, Steps 2 and 3 are not necessary.

3 Edit settings screen is displayed.

(1) Change **MAC addresses** for LAN1 to LAN4.

(2) Click the **OK** button.



Note:
When changing the MAC addresses, always do it in ascending order starting with the smallest number.

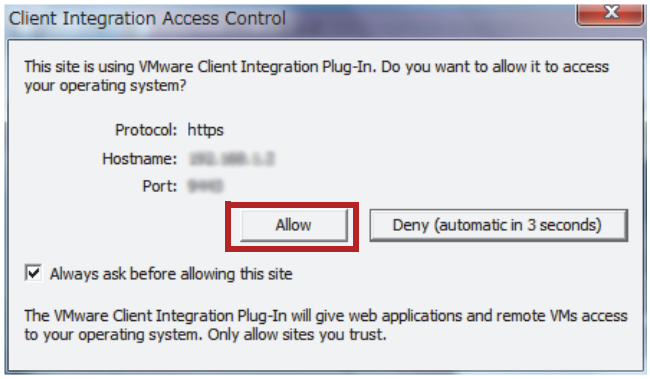
4 Save a copy of the OVF file in the maintenance PC.

(1) Right-click **SV9500** and select **Template**

(2) Select **Export OVF Template**.

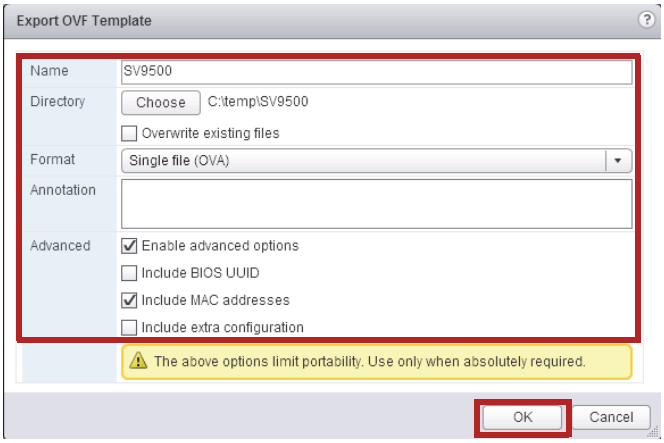
Note:
When restoring the virtual machine after a failure, not only the data included in this backup but other data as license and office data are necessary. Periodically make a backup for this data using the Telephony Server Maintenance Menu.

5 If a screen as the one below is displayed, click **Allow**. If not, go to the next step.



6 On the [Export OVF Template] screen, set the data as shown below and click [OK].

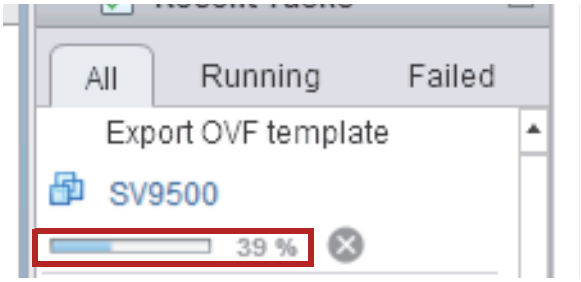
Name: Arbitrary (For example **SV9500**)
Directory: Click the **Choose** button for the place of your selection (it points to the export destination for the OVF template)
Format: **Single file (OVA)**
Annotation: Use this space if you need to left any note (it can be left blank)
Advanced:
Enable advance options: **checked**
Include MAC address: **checked**



Note:
The virtual machine usually requires around 2GB.

Note:
Consult NEC maintenance personnel or your local NEC dealer in case of using a backup file because of a failure.

7 When **Export OVF template** reaches 100% in the **Recent Tasks** column, the exporting is concluded.



8 Next step requires the virtual machine to be started. Right-click on the SV9500 virtual machine and select **Power** -> **Power On**.

9 Use the PING command from the maintenance PC and verify there is a response from the IP address of SV9500 LAN1 (192.168.1.11/16) and LAN2 (192.168.1.12/16).

10 Launch the web browser from the maintenance PC, connect to Telephone Server Maintenance Menu (http://192.168.1.11:9801/) and verify that the login screen is displayed.

Note:
The OVF template is exported to the client PC of vSphere Web Client. Make sure that the PC has enough storage capacity. Also, the exporting process may require some time, therefore make sure that the PC can be used as long as needed.

5.8 Customizing Guest OS (SV9500)

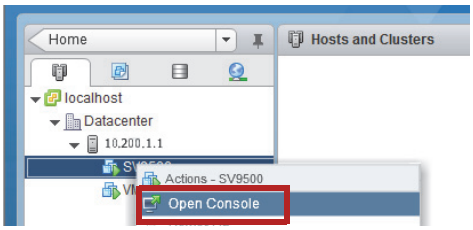
This section explains the procedure for configuring network settings for SV9500 (guest OS), such as the password and IP address information.

1 From the web browser of the maintenance PC, log in as root user to vCSA(https://xxx.xxx.xxx:9443/). (xxx.xxx.xxx.xxx is the vCSA IP address).

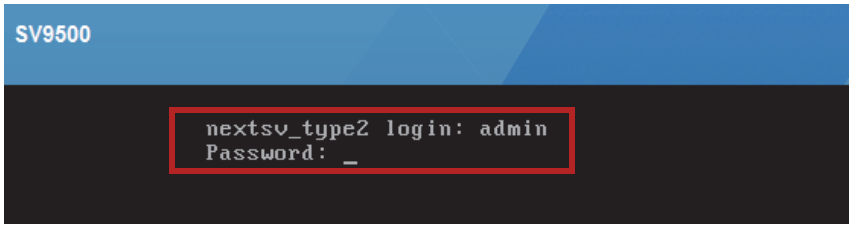
2 Open the console of the SV9500 virtual machine.

(1) Select **Hosts and Clusters (Inventories)** from **Home** tab.

(2) Right-click on SV9500 and select **Open Console**.

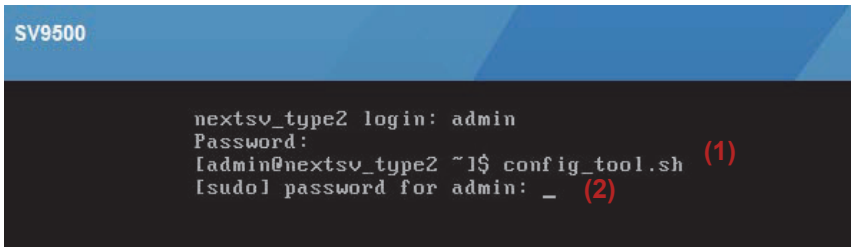


3 Log in to SV9500 from the login prompt as **admin** user.



4 (1) Execute **config_tool.sh**.

(2) Enter the password for admin again.

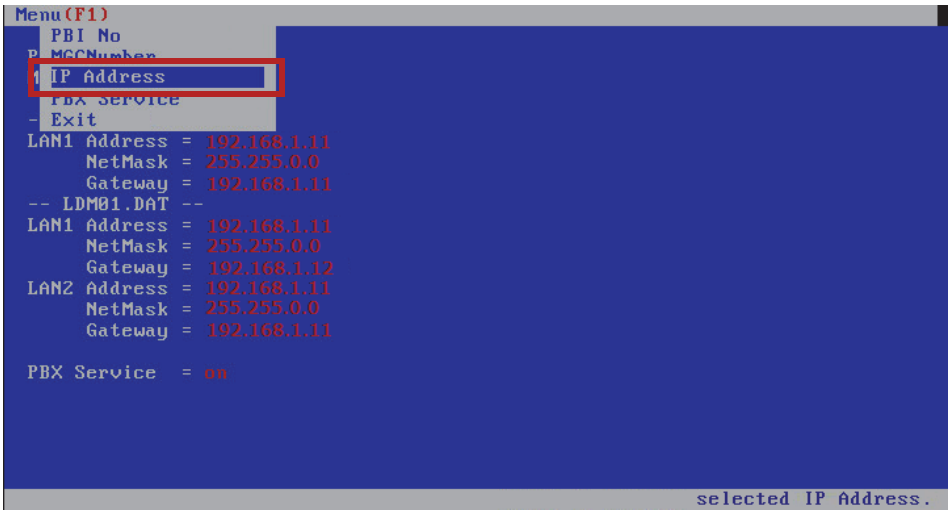


Note:
Ask your supplier for the password.

5 To modify the IP address of LAN 1 and LAN 2 respectively, proceed as follows.

(1) Press the F1 key.

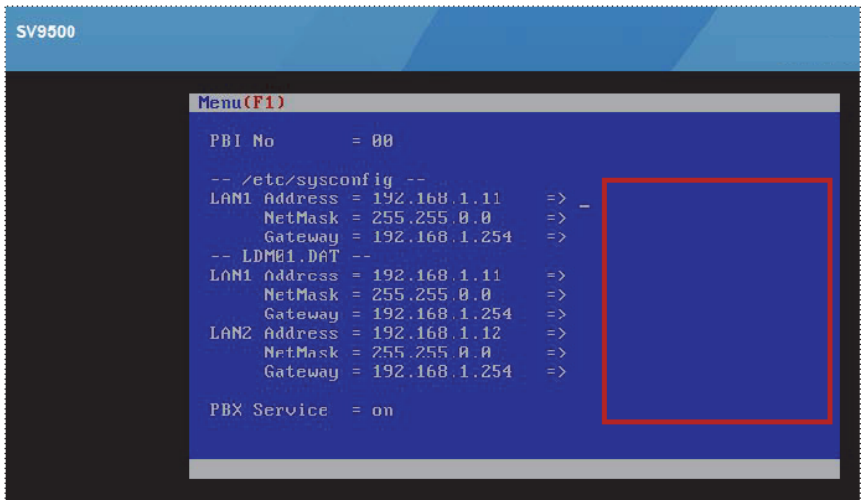
(2) Select **IP Address**.



6 (1) Modify the IP address of LAN 1 and LAN 2.

(2) After entering the **Gateway** data, press the Enter key.

Note:
The first highway counting from above cannot be left blank.



The monitor returns back to the previous screen.

7 (1) Press the F1 key.

(2) Select Exit

Close the **Console** screen.

8 Restart SV9500 virtual machine.

(1) Select the SV9500 virtual machine.

(2) Right-click and select **Power** -> **Restart GuestOS**.

9 Change the IP address of the maintenance PC to connect to the network of the LAN1 IP address from Step 6.

10 Use the PING command from the maintenance PC and verify there is a response from the IP address of LAN1.

11 Log in to the Telephony Server Maintenance Menu from the maintenance PC web browser.

(1) Launch the web browser from the maintenance PC, connect to Telephony Server Maintenance Menu (http://xxx.xxx.xxx.xxx:9801/). (xxx.xxx.xxx.xxx is the LAN1 IP address (ACT) of SV9500.)

(2) Enter **admin** as user name.

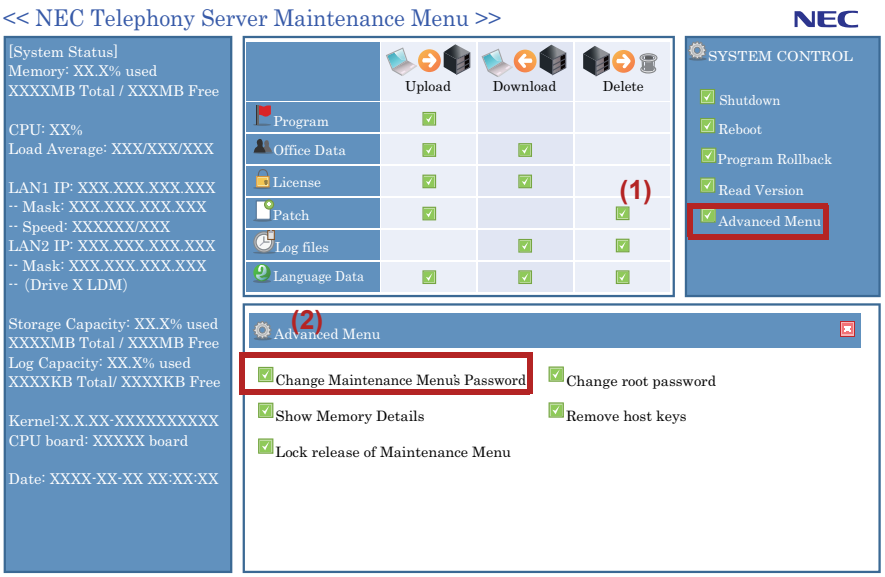
(3) Enter **admin** as password and press the **OK** button.

Note:

- Microsoft Internet Explorer 7.0 or higher is required to access Telephony Server Maintenance Menu.
- After logging into Telephony Server Maintenance Menu, do not use Back button on browser.

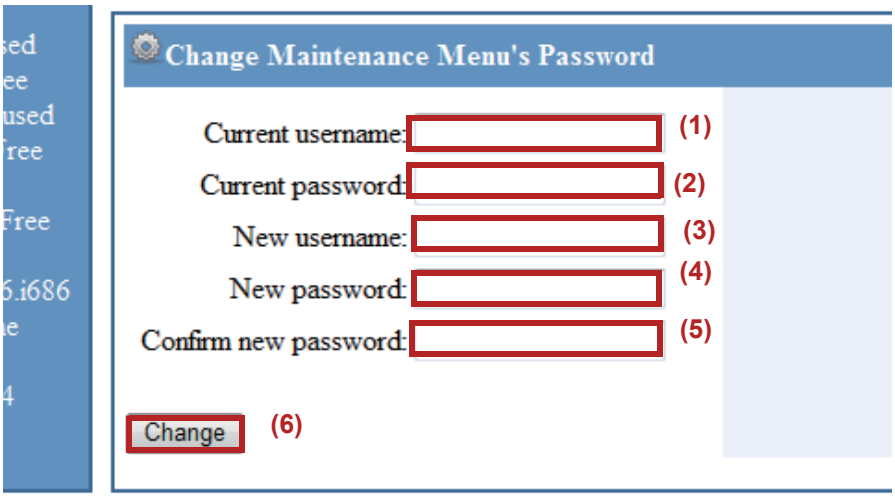
12 (1) Select Advanced Menu from SYSTEM CONTROL.

(2) Click **Change Maintenance Menu 's Password**.



13

(1) Enter admin on **Current username**.
(2) Enter admin on **Current password**.
(3) Enter a new user name on **New Username**.
(4) Enter a new password on **New Password**.
(5) Enter again the new password on **Confirm new password**.
(6) Click the **Change** button.



Note:
Use more than 8 characters for the password. Create a password that is difficult to guess and periodically change it.

5.9 Installing License for Guest OS (SV9500)

License has to be installed on SV9500.

1 Log in to the Telephony Server Maintenance Menu from the maintenance PC web browser.

(1) Launch the web browser from the maintenance PC, connect to Telephony Server Maintenance Menu (http://xxx.xxx.xxx.xxx:9801/). (xxx.xxx.xxx.xxx is the LAN1 IP address (ACT) from step 6 of Customizing Guest OS (SV9500).)

(2) Enter user name from step 13 of Customizing Guest OS (SV9500).

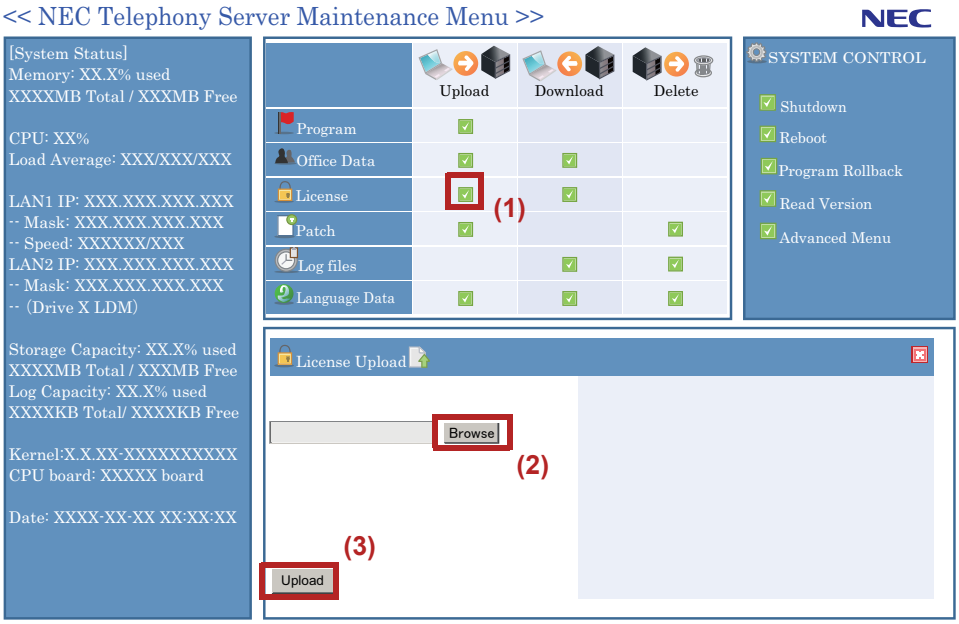
(3) Enter password from step 13 of Customizing Guest OS (SV9500). Press the **OK** button.

2

(1) Click the **Upload** button for **License**. The **License Upload** dialog box appears in the lower right portion of the screen.

(2) Click the **Browse** button on the dialog box and locate the License file downloaded in 3. Downloading of License File.

(3) Click the **Upload** button. When the uploading is complete, "Operation successfully completed" will be displayed. Click **OK**.



Note:
When the writing of license file ends in failure, "An error occurred! Please check the logs." is displayed and the details are displayed in the lower right portion of the screen.

Point:
The Language Data button needs to be clicked only when Optional Language Pack Loading [O-42] is used. For more details on Optional Language Pack Loading [O-42], see Data Programming Manual - Business.

5.10 Restarting Guest OS (SV9500)

To activate the settings of the guest OS (SV9500) it must be restarted.

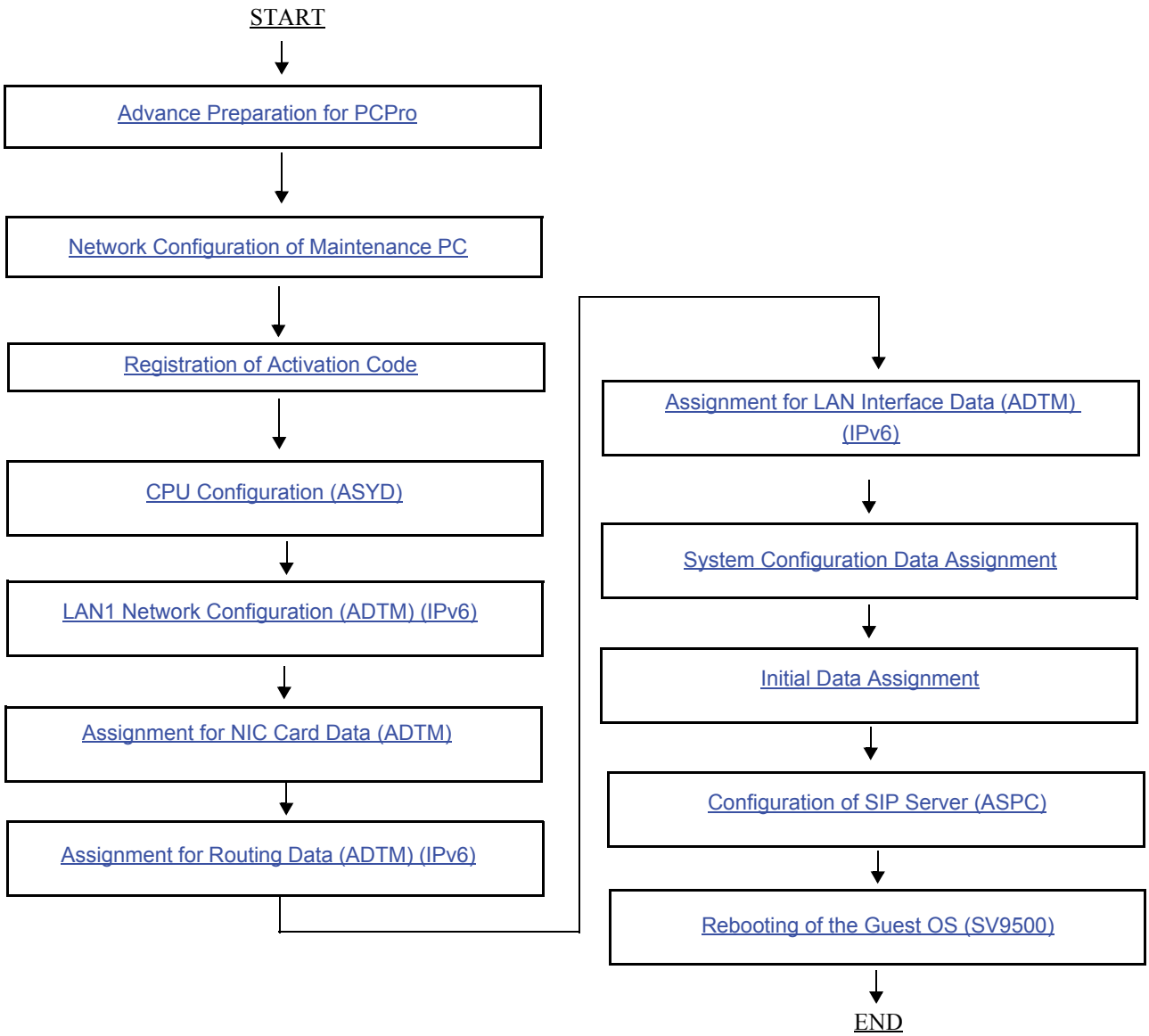
1. Launch the web browser from the maintenance PC, connect to vCSA (https://xxx.xxx.xxx.xxx:9443/) . (xxx.xxx.xxx.xxx is the vCSA IP address)
2. (1) Click **Hosts and Clusters (Inventories)** on **Home** tab.
   (2) Right-click in the SV9500 virtual machine and select from the appeared menu **Power** -> **Restart GuestOS.**
3. Use the PING command from the maintenance PC and verify there is a response from the IP addresses of SV9500 LAN1 and LAN2.
4. Launch the web browser from the maintenance PC, connect to Telephone Server Maintenance Menu (http://xxx.xxx.xxx.xxx:9801/) and verify that the Login screen is displayed. (xxx.xxx.xxx.xxx is the LAN1 IP address (ACT).)

With this the setup of the Prepackaged Server/Prepackaged FT Server is finished.

6. Office Data Setting

This section explains the procedure to set the Office Data used to operate the Telephony Server.

Follow the flow chart below to set the Office Data.



Note: The following settings are only for the IPv6 connection. If you use only IPv4 addresses, these settings are not required.

6.5 LAN1 Network Configuration (ADTM) (IPv6)
6.7 Assignment for Routing Data (ADTM) (IPv6)
6.8 Assignment for LAN Interface Data (ADTM) (IPv6)

6.1 Advance Preparation for PCPro

This section explains the procedure required to establish a communication link between PCPro and the Telephony Server.

1 Launch PCPro.

2 Create an account to connect for the IP address of LAN2 using the following steps.

Note: Make the account shown in the table "Account Setting Items (for IPv6)" only when you need to use the IPv6 connection with PCPro.

Note: Account settings shown in the table "Account Setting Items (for IPv4)" is also required even for the IPv6 connection.

Point:
For detailed procedure, refer to "Connection Account Setting" in Chapter 5 Various Settings of PCPro in PCPro Setup Manual.

Account Setting Items (for IPv4)

Setting Items	IP address of LAN2
Account Name	Arbitrary (e.g. NewOffice#1)
FUG	0
FPC	0
Connection Type	TCP/IPv4
IP address	IP address of LAN2 (e.g. 10.100.1.12)
Port Number	60000

Account Setting Items (for IPv6)

Setting Items	IPv6 Address
Account Name	Arbitrary (e.g. LAN1_IPv6)
FUG	0
FPC	0
Connection Type	TCP/IPv6
IP address	IPv6 Address (e.g. 2001:db8::c)
Port Number	60000

6.2 Network Configuration of Maintenance PC

This section explains the procedure to set the network configuration of the maintenance PC to connect to the Telephony Server.

1. Set the maintenance PC IP address to connect to the network of the LAN2 IP address.

2. Execute the ping command from the maintenance PC to the IP address of LAN2 and verify that a response is sent back.
If no response is received, verify the settings including the network configuration and cable connection.

Note:
The IE proxy server settings must be disabled in the maintenance PC.

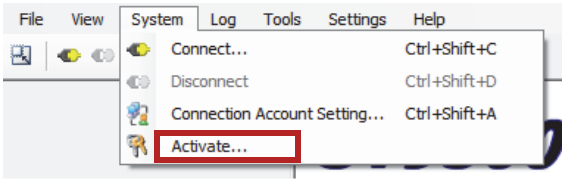
6.3 Registration of Activation Code

The following section explains how to register the activation code.

Note: You cannot be logged into the PCPro to use these steps.

Note: Register the Activation Code after you set the IP address of LAN1 (ACT). If you change the IP address of LAN1 (ACT) after the Certify Status was “Certify OK”, the status will change to “Certify NG (HKC)” (only for IPv4). In that case, see “APPENDIX A LICENSE FOR SV9500 (PREPACKAGED SERVER MODEL)”.

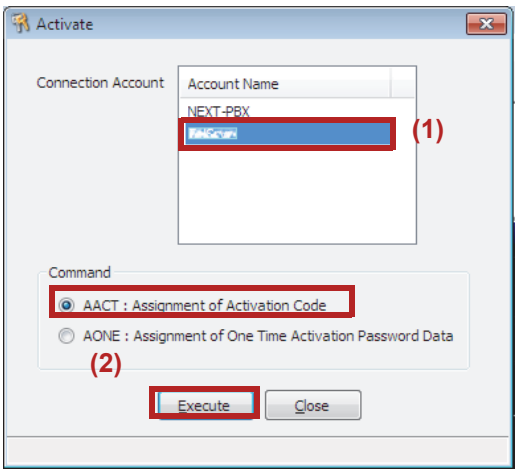
1 Launch PCPro and select **System** -> **Activate** on the menu bar.



2 The **Activate** screen will launch.

(1) Highlight the **Connection Account** configured for the IP address of LAN2

(2) Select the **AACT: Assignment of Activation Code** radio button and click **Execute**.



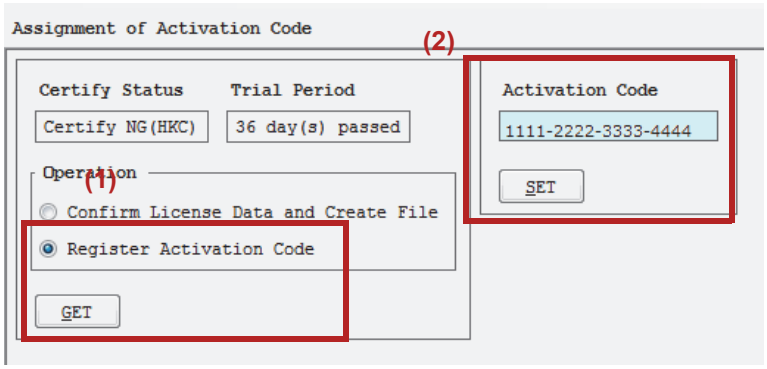
3 The AACT command will launch.

(1) Select the **Register Activation Code** radio button and press Get.

(2) Enter the **Activation Code** you have received from the LMS server, into the **Activation Code** field and press **Set**.

(3) Verify you receive the **Certify OK** confirmation message.

(4) Close the **AACT** command and the **Activate** screen.



4 You can now log into PCPro; remember to backup the Activation Code using the **MEM_HDD** command.

Note: If the Activation Code is not available, the SV9500 may be unlocked by selecting the **AONE** option instead of the **AACT** option. Once unlocked using the AONE option, the PCPro connection will be valid for 7 days. After 7 days, PCPro access will be denied until the SV9500 is registered. Please note that the AONE option can only be used once.

6.4 CPU Configuration (ASYD)

This section explains the procedure to configure the CPU for single configuration.

1 Connect to PCPro using the connection account assigned to the IP address of LAN2. The user ID and the password shown below need to be entered.

User ID: maintenance

Password:ty8*#02F

Note:
- If the user ID and the password are not entered, login is unavailable.
- After the first time login is performed, it is recommendable to change the password.

2 (1) Execute the ASYD command.

(2) Set the following data.

SYS1 INDEX58 bit0=0 (configuration of CPU=Single)

(3) Exit the ASYD command.

Note:
In case of a Prepackaged FT Server, make sure that the configuration of CPU is Single.

Point:
No modification is required since the default value is set for this data in normal cases.
If a different value is set, modify the data to the value as given.

6.5 LAN1 Network Configuration (ADTM) (IPv6)

This section explains how to set IPv6 addresses (e.g. 2001:db8::c) for LAN1.

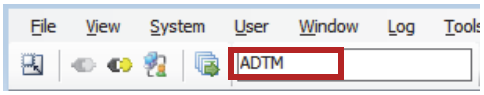
Note: Note the following conditions for this setting.

- This data setting is for the IPv6 connection with PCPro. If you use only IPv4 addresses, this setting is not required.
- Do not delete the setting of IPv4 addresses, because it is required when you use IPv6 addresses.
- For detailed conditions of IPv6 addresses, refer to"IPv6 Connection with PCPro" in the System Description.

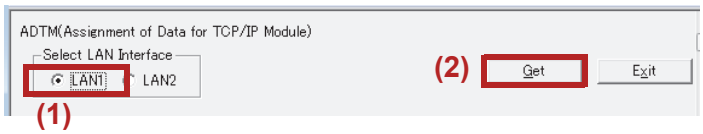
1 Launch PCPro and connect it to the Telephony Server by using the connection account assigned to the IP address of LAN2 connector.
To connect, use the previously set user name and password.

Note:
If the user ID and the password are not entered, login is unavailable.

2 Execute the ADTM command.

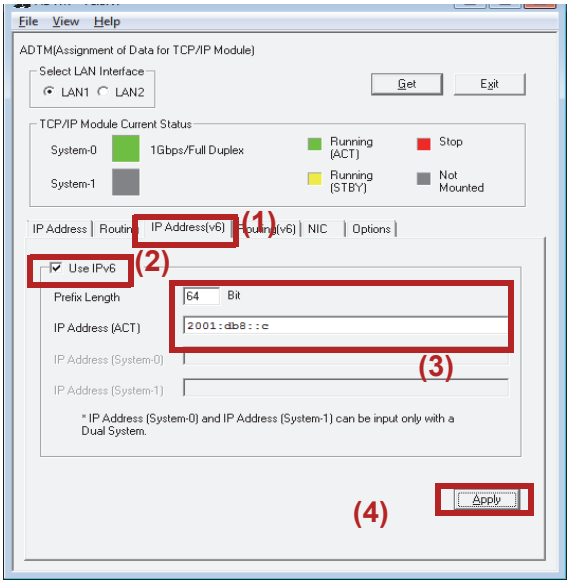


3 (1) Select **LAN1** under **Select LAN Interface**.
(2) Click the **Get** button.



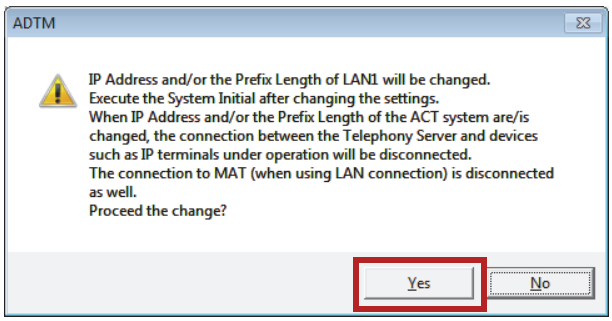
4

(1) Click the **IP Address (v6)** tab.
(2) Select the **Use IPv6** check box.
(3) Set the values corresponding to your actual network environment for **Prefix Length** and **IP Address (ACT)**.
(4) Click the **Apply** button.



5

The following confirmation message is displayed.
Click the **Yes** button to apply the new setting.



Note:

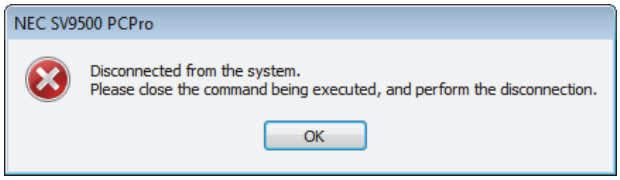
- Do not execute a system initialization even though the message recommends you to initialize the system.
- The data setting for the IPv6 address becomes valid after the change is applied.

Point:

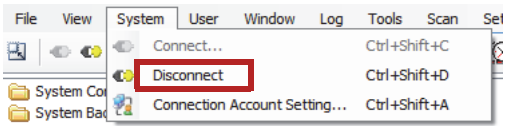
The connection to PC-Pro is disconnected when the data is modified.

6 Click the **Exit** button to exit the ADTM command.

7 The following message is displayed on PCPro.
Click **OK** to close the message.



8 Select **Disconnect** on the **System** menu on PCPro.



Point:
For detailed disconnecting procedure, refer to “Disconnecting the Communication Link” in Chapter 3 Setting Up PCPro in PCPro Setup Manual.

6.6 Assignment for NIC Card Data (ADTM)

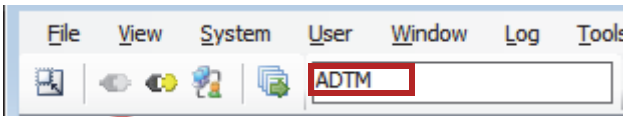
This section explains the procedure for configuring the network of the Telephony Server to conform with the actual network environment.

1 Connect to PCPro using the connection account assigned for the IP address of LAN2. Enter the user ID and the password that have been previously assigned to connect with PCPro.

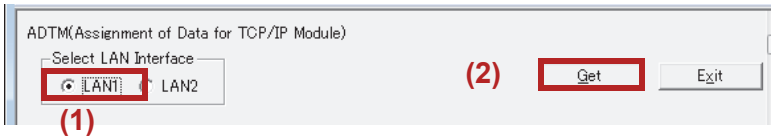
Note:
If the user ID and password are not entered, login is unavailable.

Point:
For detailed procedure to connect to PCPro, refer to "Communication Link with the Telephony Server" in Chapter 3 Setting Up PCPro in PCPro Setup Manual.

2 Execute the ADTM command.

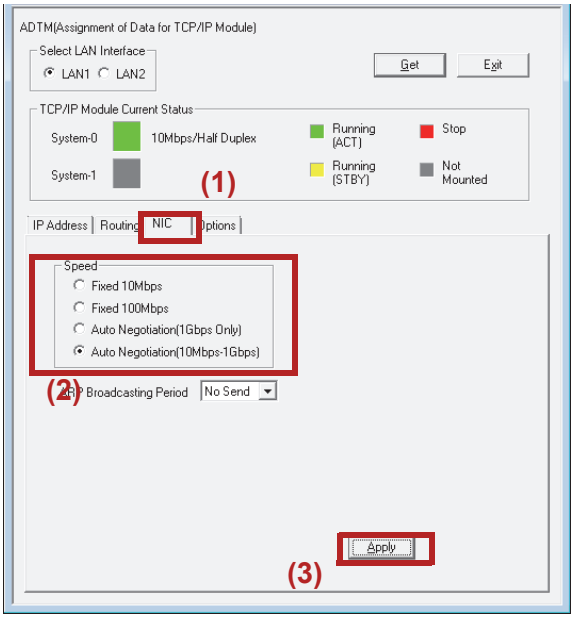


3 (1) Select **LAN1** for **Select LAN Interface**.
(2) Click the **Get** button.



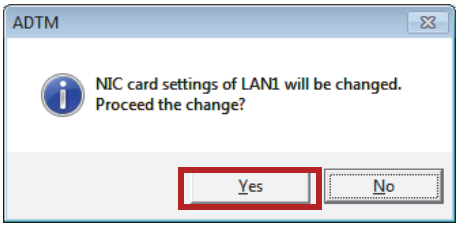
4

(1) Click the **NIC** tab.
(2) Select **Auto Negotiation (10MBps-1Gbps)** for **Speed**.
(3) Click the **Apply** button.



5

The confirmation message is displayed. Click the **Yes** button to apply the change.



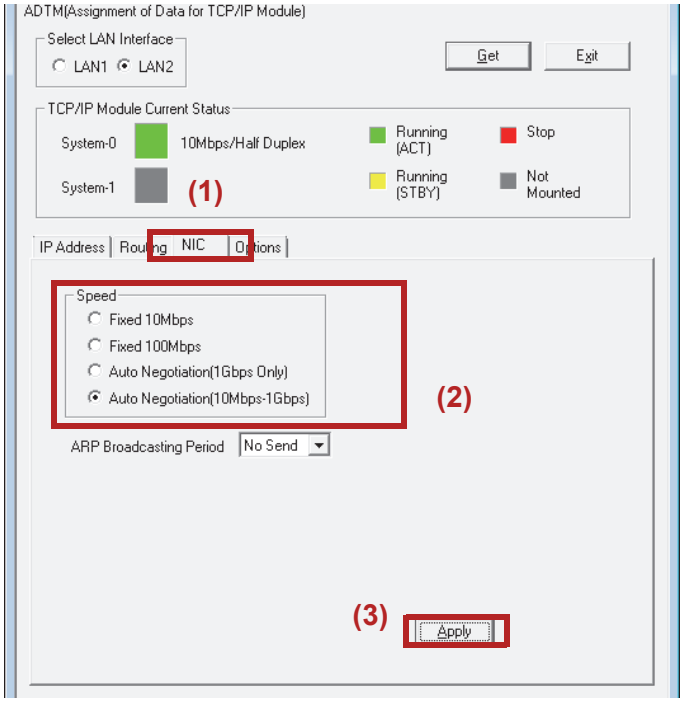
6

(1) Select **LAN2** for **Select LAN Interface**.
(2) Click the **Get** button.

Note:
Do not change the setting [Auto Negotiation (10MBps-1Gbps)].

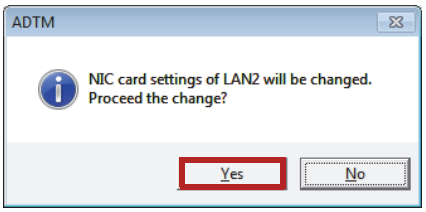
7

(1) Click the **NIC** tab.
(2) Select **Auto Negotiation (10MBps-1Gbps)** for **Speed**.
(3) Click the **Apply** button.



8

The confirmation message is displayed. Click the **Yes** button to apply the change.



9

Click the **Exit** button to exit the ADTM command.

Note:
Do not change the setting [Auto Negotiation (10MBps-1Gbps)].

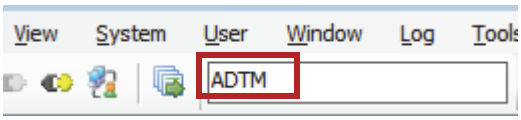
6.7 Assignment for Routing Data (ADTM) (IPv6)

This section explains the procedure for configuring the network of the Telephony Server to conform with the actual network environment.

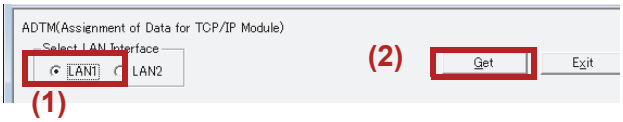
Note: Programming for IPv4 must be done before programming in this section can be done.

Note: This data setting is for the IPv6 connection with PCPro. If you use only IPv4 addresses, this setting is not required.

1 Execute the ADTM command.

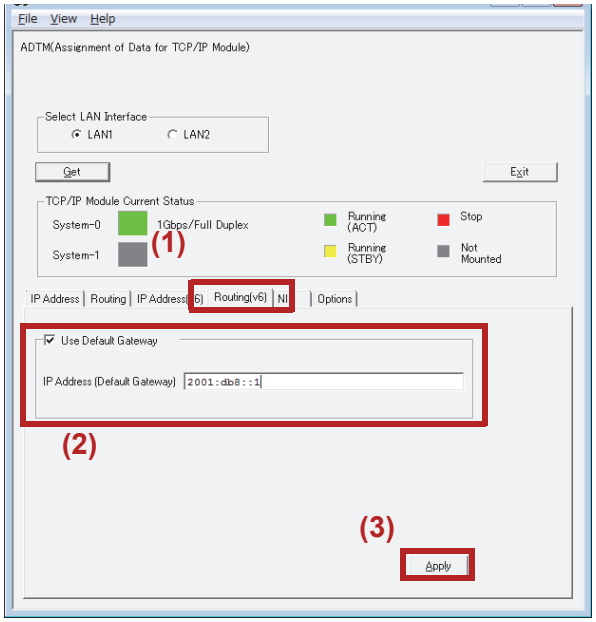


2 (1) Select **LAN1** under **Select LAN Interface**.
(2) Click the **Get** button.



3

(1) Click the **Routing (v6)** tab.
(2) Set the value corresponding to your actual network environment.
(3) Click the **Apply** button.



4

Click the **Exit** button to exit the ADTM command.

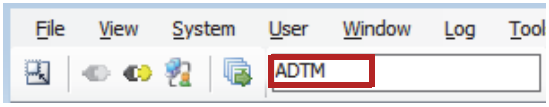
6.8 Assignment for LAN Interface Data (ADTM) (IPv6)

This section explains the procedure for configuring the LAN interface to connect to PCPro with IPv6 addresses.

Note: Programming for IPv4 must be done before programming in this section can be done.

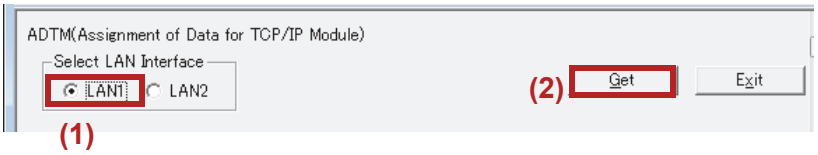
Note: This data setting is for the IPv6 connection with PCPro. If you use only IPv4 addresses, this setting is not required.

1 Execute the ADTM command.



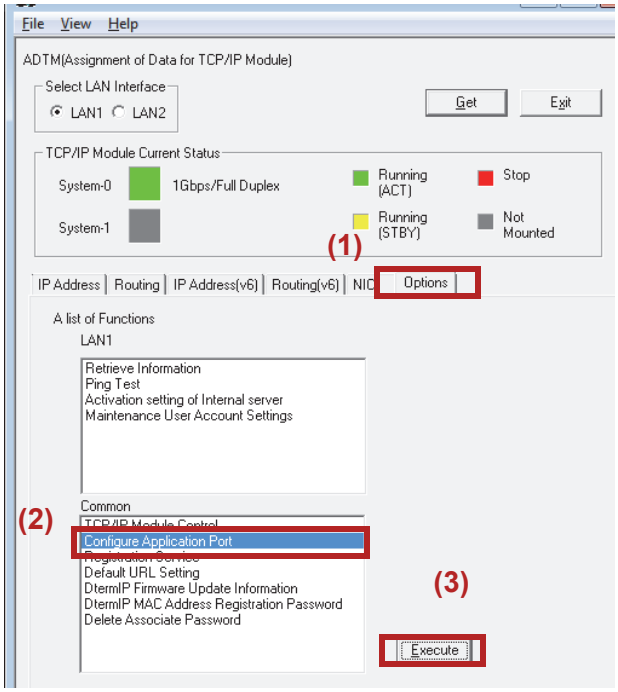
2

(1) Select **LAN1** under **Select LAN Interface**.
(2) Click the **Get** button.



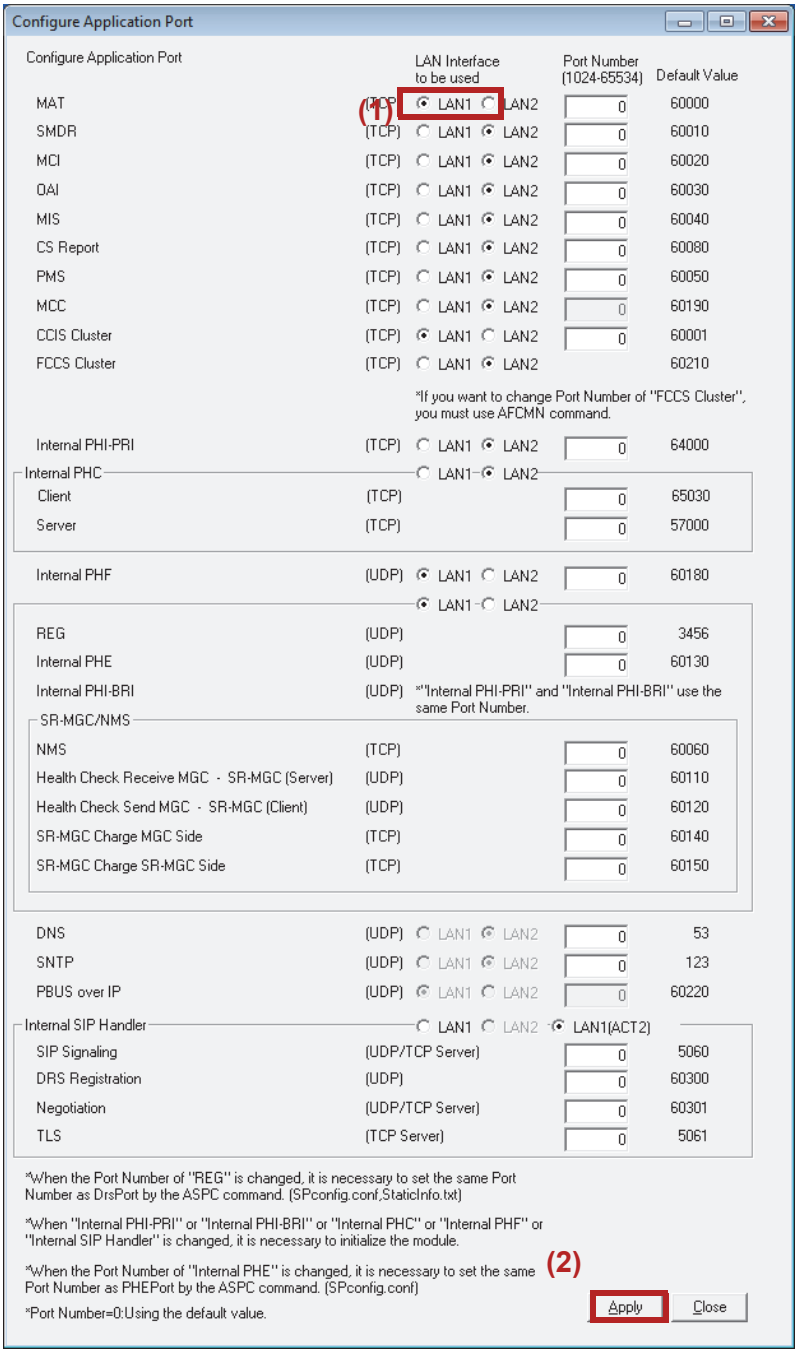
3

(1) Click the **Options** tab.
(2) In the **Common** list, select **Configure Application Port**.
(3) Click the **Execute** button.

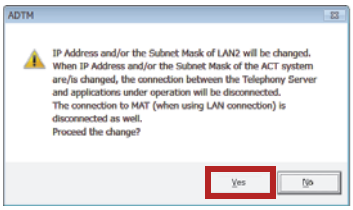


4

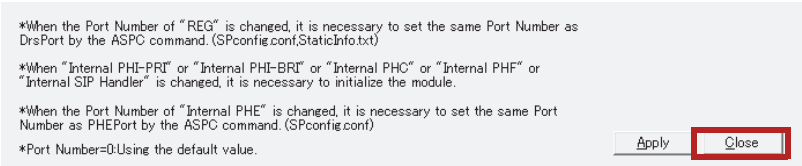
(1) Select **LAN1** under **LAN Interface to be used** in **MAT**.
(2) Click the **Apply** button.



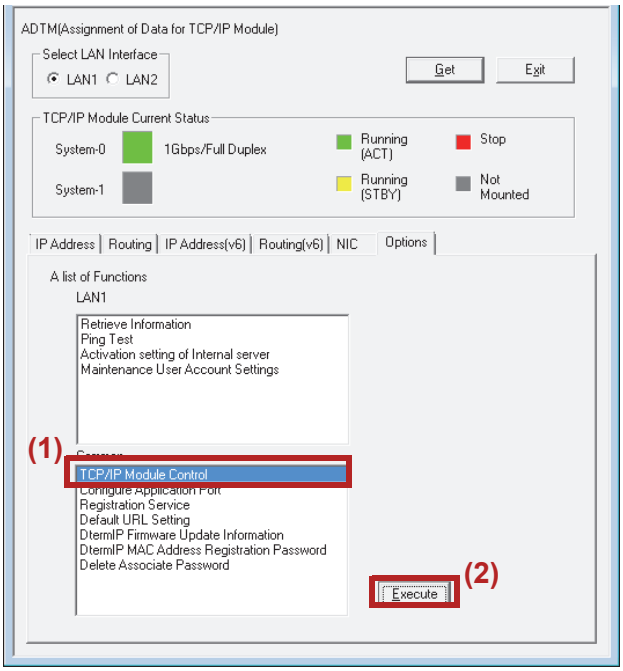
5 The confirmation message is displayed. Click the **Yes** button to apply the change.



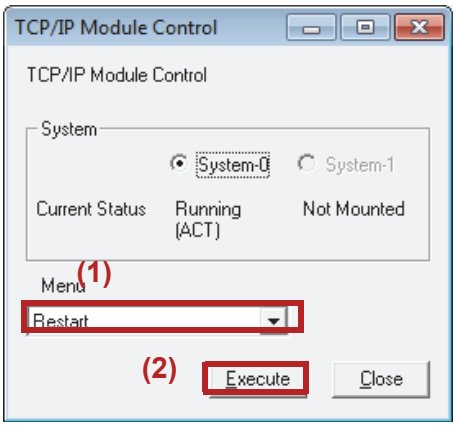
6 Click the **Close** button to close the **Configure Application Port** dialog box.



7 (1) Select **TCP/IP Module Control** in the **Common** list.
(2) Click the **Execute** button.

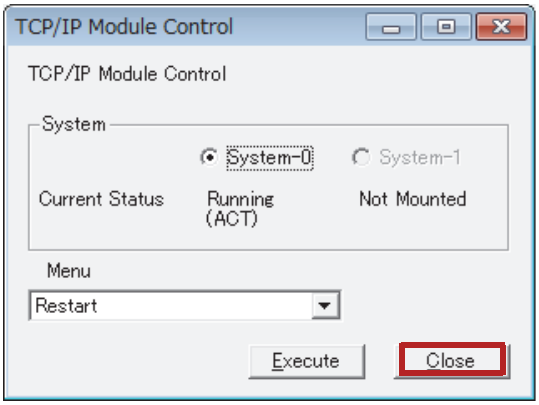


8 (1) Select **Restart** in the **Menu** box.
(2) Click the **Execute** button.



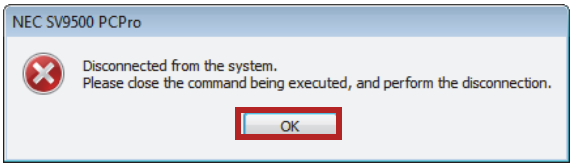
9 The following message is displayed. Click **OK** to close the message.

10 Click the **Close** button to close the **TCP/IP Module Control** dialog box.

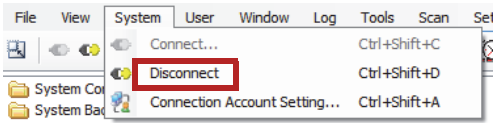


11 Click the **Exit** button to exit the ADTM command.

12 The following message is displayed on PCPro. Click **OK** to close the message.



13 Select **Disconnect** on the **System** menu on PCPro.



Point:
For detailed disconnecting procedure, refer to “Disconnecting the Communication Link” in Chapter 3 Setting Up PCPro in PCPro Setup Manual.

6.9 System Configuration Data Assignment

Basic data assignment of the Office Data must be set to start up the system.

Refer to 8. System Configuration Data Assignment for instructions on data assignment.

6.10 Initial Data Assignment

Initial data assignment is required to be set on the Telephony Server by PCPro.

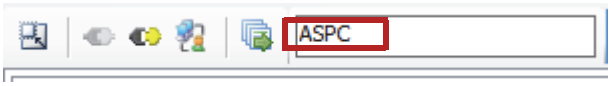
Refer to 9. Initial Data Assignment for instructions on data assignment.

6.11 Configuration of SIP Server (ASPC)

This section explains the procedure to configure the SP part of the system.

Note: The configuration of SIP Server must be set when using IP equipment (IP stations) within the system.

1 Execute the ASPC command.

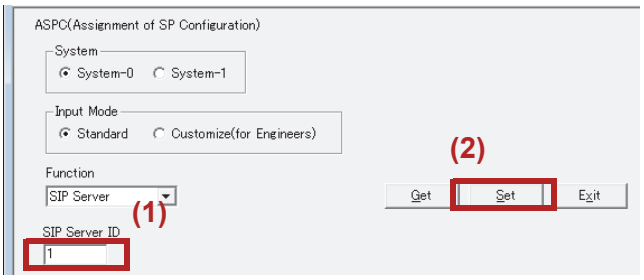


2 (1) Click **System-0** for **System**, **Standard** for **Input Mode** and **SIP Server** from the **Function** list.
(2) Click the **Get** button.

Note:
- System which does not exist cannot be selected for [System].
- Customize mode is for engineers only.

3

(1) Type the SIP Server Identifier for **SIP Server ID**.
(2) Click the **Set** button.



4

Disconnect PCPro from the system.

Note:

- Unique SIP-Server Identifier must be assigned in the network within the range from 1 to 127.
- Always assign SIP-Server Identifier when initializing the Telephony Server regardless of whether the SP Controlled SIP terminals are used or not. The number set for SIP-Server Identifier by ASSDL/ASSDN command must be assigned for ASPC command as well.

Point:

For detailed disconnecting procedure, refer to “Disconnecting the Communication Link” in Chapter 3 Setting Up PCPro in PCPro Setup Manual.

The basic office data assignment is completed.

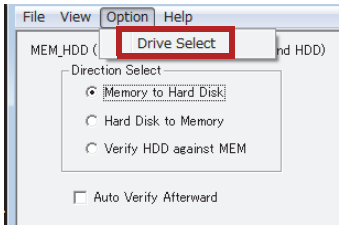
6.12 Rebooting of the Guest OS (SV9500)

This section explains the procedure to backup the Office Data using MEM_HDD command and to reboot the Telephony Server to activate the set data.

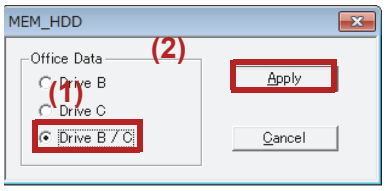
Point: The Office Data backed up in the guest OS can be stored on a maintenance PC by using Telephony Server Maintenance Menu.

1 Execute the **MEM_HDD** command.

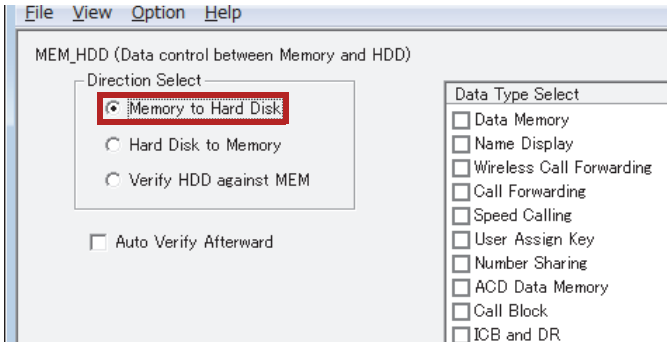
2 Select **Drive Select** from the **Option** menu.



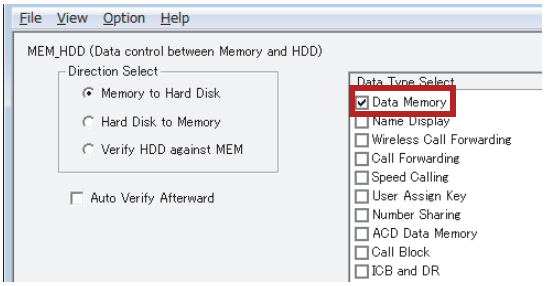
3 (1) Select **Drive B / C** for **Office Data**.
(2) Click the **Apply** button.



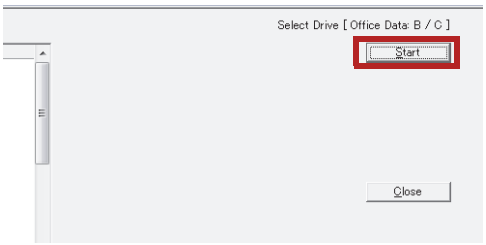
4 Select **Memory to Hard Disk** for **Direction Select**.



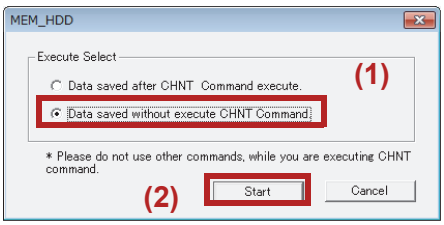
5 Select **Data Memory** for **Data Type Select**.



6 Click the **Start** button.



7 (1) Select **Data saved without execute CHNT Command** for **Execute Select**.
(2) Click the **Start** button.
The data backup begins.



8 After the backup is completed, click the **Close** button to exit the MEM_HDD command.

9 Launch the web browser from the maintenance PC, connect to vCSA(https://xxx.xxx.xxx.xxx:9443/) as root user. (xxx.xxx.xxx.xxx is the vCSA IP address.)

10 (1) Click **Hosts and Clusters (Inventories)** on **Home** tab.
(2) Right-Click the SV9500 virtual machine and click **Power** -> **Restart Guest OS**.

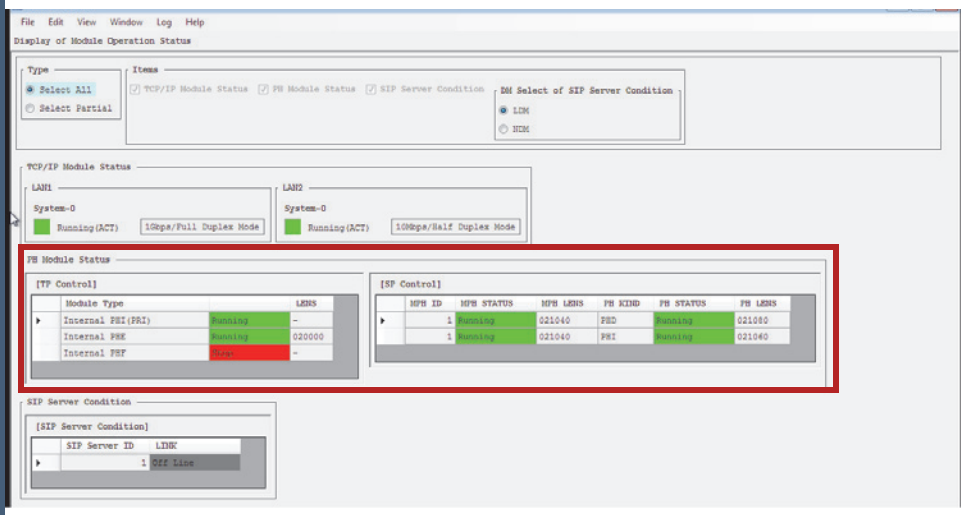
11 Use the PING command from the maintenance PC and verify there is a response from the IP address of SV9500 LAN1 and LAN 2.

12 Launch the web browser from the maintenance PC, connect to Telephone Server Maintenance Menu (http:// xxx.xxx.xxx.xxx:9801/) and verify that the login screen is displayed. (xxx.xxx.xxx.xxx is the SV9500 LAN1 IP address (ACT).)

13 Connect to PCPro and log in.

14 Start the DMOS command.

15 Confirm on **Module Operation Status** screen that TP Control and SP Control are operating normally.



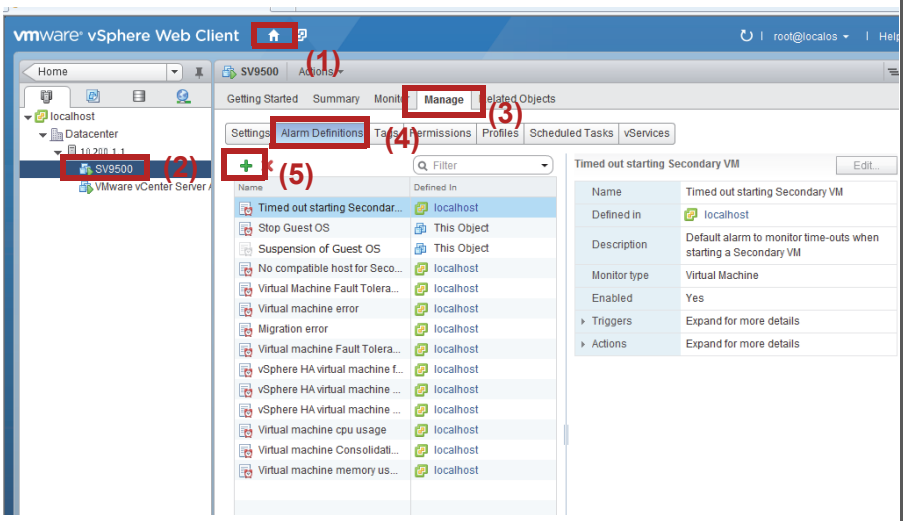
The rebooting of the guest OS is completed.

7. Alarm Settings

The last needed process is to setup an alarm for the virtual machine.

1 Launch the browser from the maintenance PC, connect as root user to vCSA (https://xxx.xxx.xxx.xxx:9443/). (xxx.xxx.xxx.xxx is the vCSA IP address.)

2
(1) Click **Hosts and Clusters (Inventories)** on **Home** tab.
(2) Click the SV9500 virtual machine.
(3) Click **Manage** tab.
(4) Click **Alarm Definitions**.
(5) Click [+].



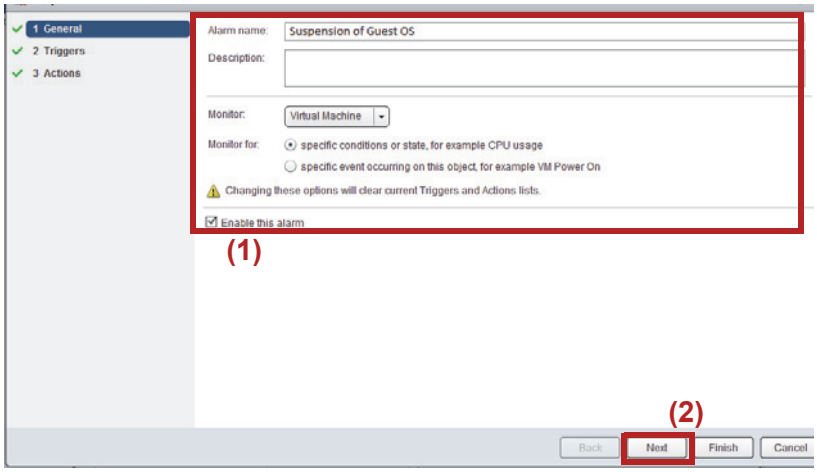
Note:
For this section Pre-packaged Server Model screens will be used (the FT management appliance machine is not displayed).

3

(1) The **New Alarm Definition** screen is displayed. Set the data for each field as shown below.

Alarm name: **Suspension of Guest OS**
Description: (blank)
Monitor: **Virtual Machine**
Monitor for: **specific conditions or state, for example CPU usage**
Enable this alarm: **checked**

(2) Click the **Next** button.



4

(1) In the **Trigger** screen select **ALL.**

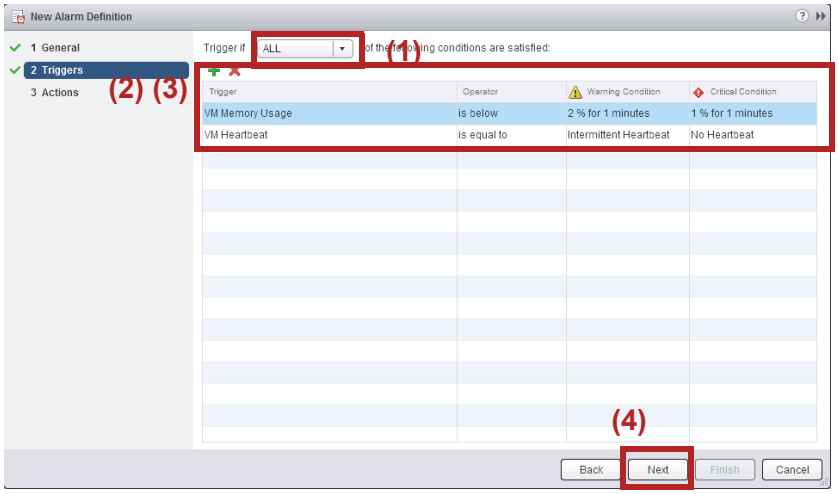
(2) Click [+] and set the following:

Trigger: **VM Memory Usage**
Operator: **is below**
Warning Condition: **2% for 1 minutes**
Critical Condition: **1% for 1 minutes**

(3) Click [+] and set the following:

Trigger: **VM Heartbeat**
Operator: **is equal to**
Warning Condition: **Intermittent Heartbeat**
Critical Condition: **No Heartbeat**

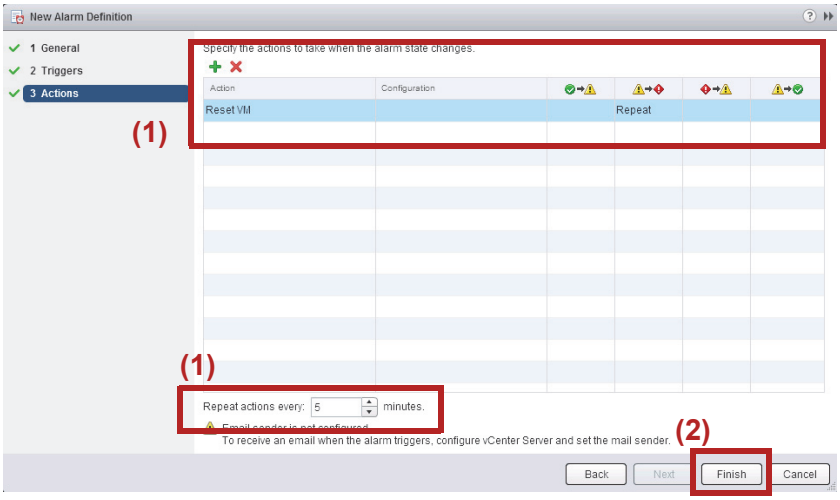
(4) After finishing, click **Next**.



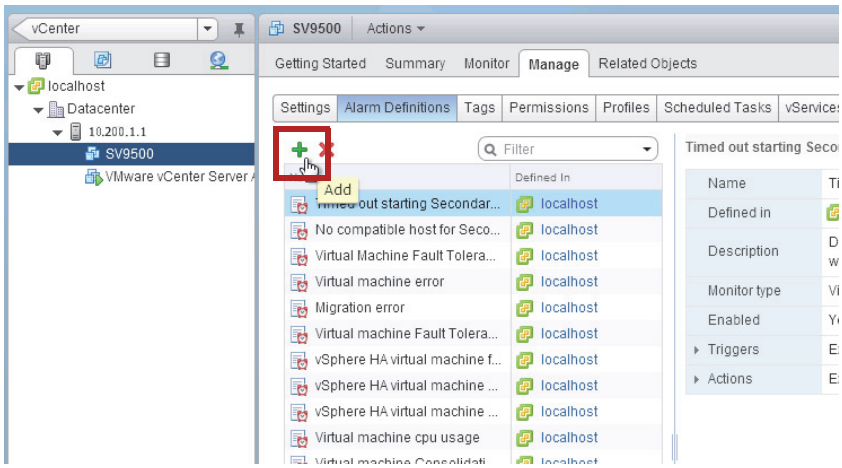
5 (1) In the **Actions** screen, click [+] and set as follows:

Action: **Reset VM**
Configuration: (blank)
: (blank)
: **Repeat**
: (blank)
: (blank)
Repeat actions every: **5** minutes.

(2) After finishing, click **Finish**.



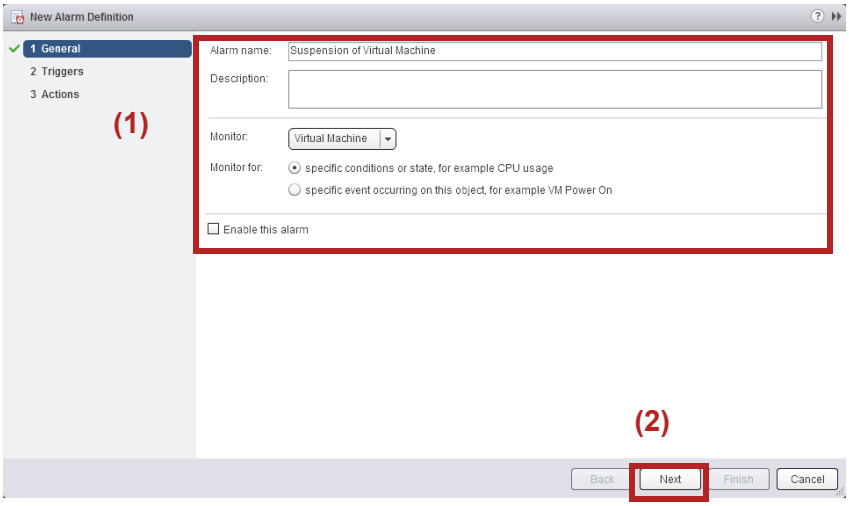
6 Click the [Add] (+) icon again as shown in the screen on the right. The **New Alarm Definition** will be displayed.



7 (1) On the **New Alarm Definition** screen enter the settings as shown below.

Alarm name: **Suspension of Virtual Machine**
Description: (blank)
Monitor: **Virtual Machine**
Monitor for: **specific conditions or state, for example CPU usage**
Enable this alarm: **checked**

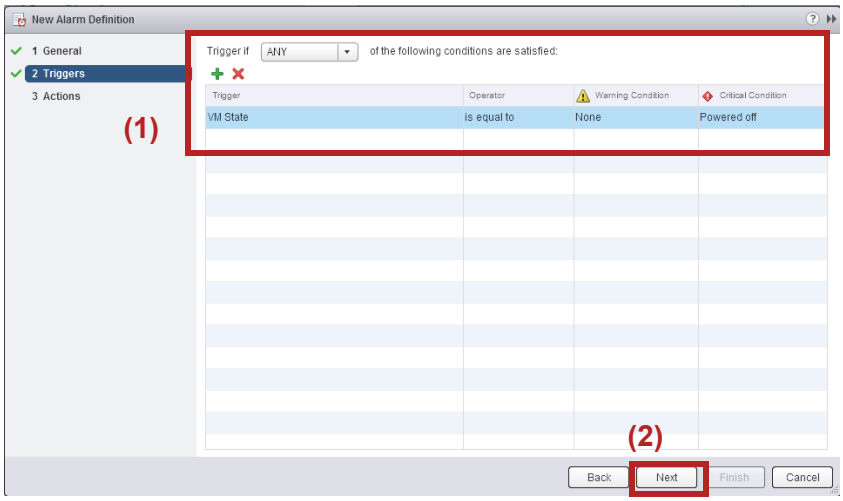
(2) After finishing, click **Next.**



8 (1) On the **Trigger** screen click [+] and enter the settings as shown below.

Trigger if: **ANY** of the following conditions are satisfied
Trigger: **VM State**
Operator: **is equal to**
Warning Condition: **None**
Critical Condition: **Powered off**

(2) After finishing, click **Next.**



9

(1) On the **Actions** screen click [+] and enter the settings as shown below.

Action: **Power on VM**

Configuration: (blank)

: (blank)

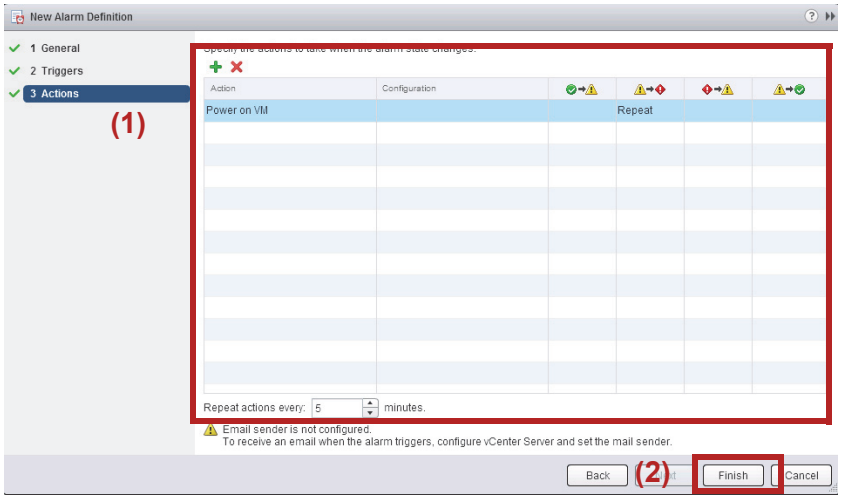
: **Repeat**

: (blank)

: (blank)

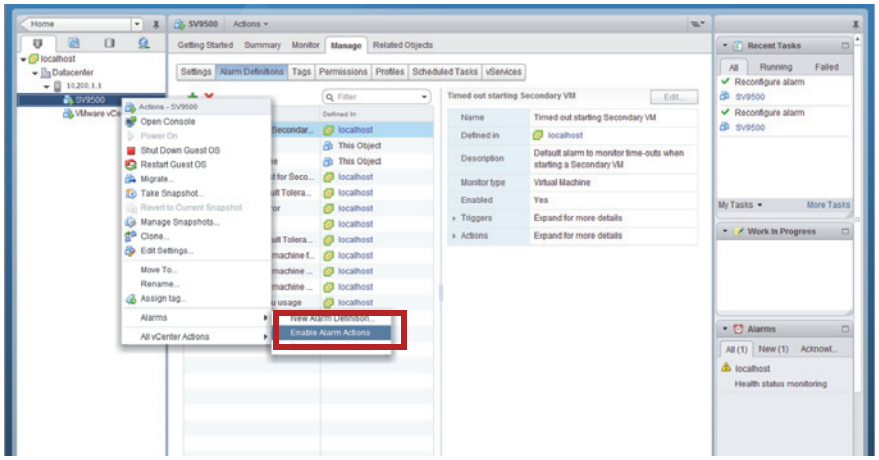
Repeat actions every: **5** minutes.

(2) After finishing, click **Finish**.



10

Right-Click the 9500 virtual machine and select **Alarm -> Enable Alarm Activations.**



Note: This step is not necessary if **Enable Alarm Activations** cannot be selected.

The alarm settings procedure has been completed and the initial startup process is finished. Connect the LAN cable of the server to your network.

Note: In the Prepackaged FT Server model, disable Ether Channel and TrunkPort connections. If they are enabled and there is a fail over in the CPU/IO module, network access could be down during one minute.

8. System Configuration Data Assignment

Basic data assignment for starting up the system is explained here. System configuration data such as system time, number of modules and units, #0/#1 configuration of controlling system, and data memory capacity are assigned.

8.1 System Time - ATIM

ATIM - Date and Time Setting

Only Time Zone and Daylight Savings Time are valid for the SV9500 (Prepackaged Server Model) using the ATIM command. The Date and Time are configured in VMware ESXi.

8.2 System Data - ASYD, ASYDL (LDM), and ASYDN (NDM)

System Data is assigned by ASYD consists of three major categories - SYS1 (Index 0 ~ 511), SYS2 (Index 0 ~ 15) and SYS3 (Index 0 ~31). The data of each index is entered in hexadecimal format (00 to FF). Each bit, 0 or 1 (in binary), has its meaning, such as “Use of Service A: 0=No, 1=Yes”.

- **ASYD SYS1:**

INDEX	SYSTEM CONFIGURATION	BIT	DATA
0	Number of Module Group (MG) **Note 1**	0-7	08 Hex
1	Number of Main Processor	0-7	01 Hex
3	Configuration of Time Division Switching (TSW) network	0-7	00 Hex
30	Capacity of Data Memory (DM) **Note 2**	0-7	06 Hex
31	Capacity of Common Memory (CM)	0-7	02 Hex
58	Configuration of CPU	0	Bit 0=0 (Fixed)
79	OAI/ACD Service	6	Bit 6=0 (In service) Bit 6=1 (Out of service)
194	MP (CPU) Mounting Status	0-7	01 Hex (Fixed)
198	IMG0, IMG1 Mounting Status	0-7	11 Hex (Fixed)
199	IMG2, IMG3 Mounting Status	0-7	11 Hex (Fixed)
256	Bit 2=1 (Fixed) Bit 3=0 (Fixed) Bit 4=1 (Fixed) Bit 5=0 (Fixed)	0-7	14 Hex

- **ASYDL SYS1:**

INDEX	SYSTEM CONFIGURATION	BIT	DATA
513	Capacity of Local Data Memory (LDM)	0-7	01 Hex
514	Capacity of Network Data Memory (NDM)	0-7	01 Hex
556	PIR0 ~ PIR3 mounting status on IMG0, IMG1	0-7	FF Hex **Note 3**
557	PIR0 ~ PIR3 mounting status on IMG2, IMG3	0-7	FF Hex **Note 3**
1026	UNIT use on MG00-MG03	0-7	FF Hex
1027	UNIT use on MG04-MG07	0-7	FF Hex

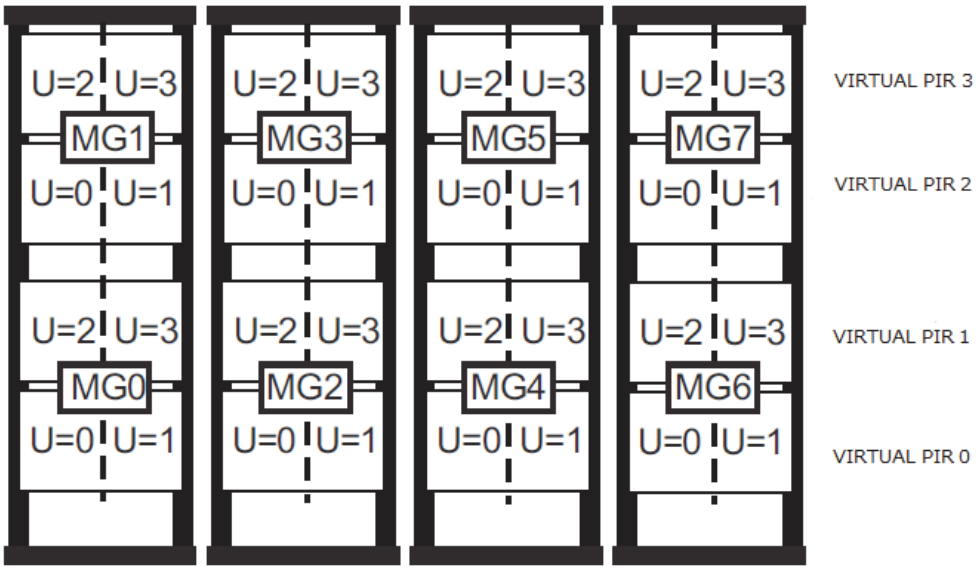
Note 1: As shown in the figure below, a Module Group (MG) consists of two virtual PIRs.

Note 2: Set to 06 Hex for systems that use PS or SIP terminals.

Note 3: SV9500 (Prepackaged Server Model) only uses virtual PIRs. For more information about virtual PIRs see ASSIGNMENT OF BASIC OFFICE DATA in the Data Programming Manual - Business.

8.3 Unit Data - AUNT

Assign the Unit (U) data by using AUNT.
The Unit (U) is the second element of the Line Equipment Numbers (LENS) that specifies the accommodated location of station/trunk, and is a minimum requirement to be assigned before the entry of station/trunk and other office data. The pattern of the Unit (U) allocation is shown below:



[Programming]

MG: Module Group Number
TYPE: 1 (Select 1 for Unit data assignment)
UNIT 0-3: 1 (Enter 2 for UNITS that are not mounted)

9. Initial Data Assignment

This section explains how to assign data with PCPro to enable terminal use. The procedures are the same for SV9500 (Prepackaged Server Model) and SV9500 (Appliance Model), therefore, see Initial Data assignment in Appliance Model Installation Manual.

CHAPTER 3
OPERATIONS AND MAINTENANCE

This chapter explains the procedures for Operations and Maintenance of the SV9500 (Prepackaged Server Model).

1. Maintenance of SV9500 (Prepackaged Server Model)

This section explains the maintenance services for SV9500 (Prepackaged Server Model).

1.1 Hard Disk Drive (HDD) Replacement Procedure

For failure detection and HDD replacement procedures, refer to the manual for the Prepackaged Server/Prepackaged FT Server product.

2. SNMP Setting

This section explains how to configure SNMP settings for VMware.

2.1 vCenter Server Setting Procedures

There are two procedures of configuration for vCenter Server.

(1) Via vSphere Client

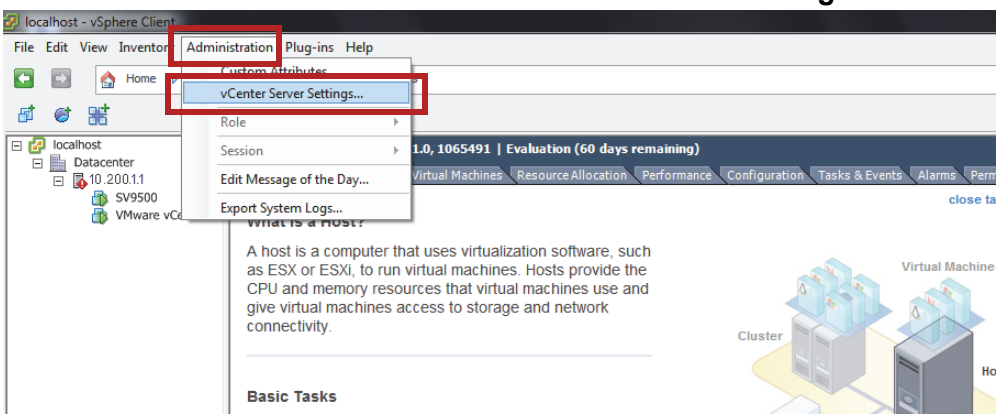
(2) Via vSphere Web Client

(1) Via vSphere Client

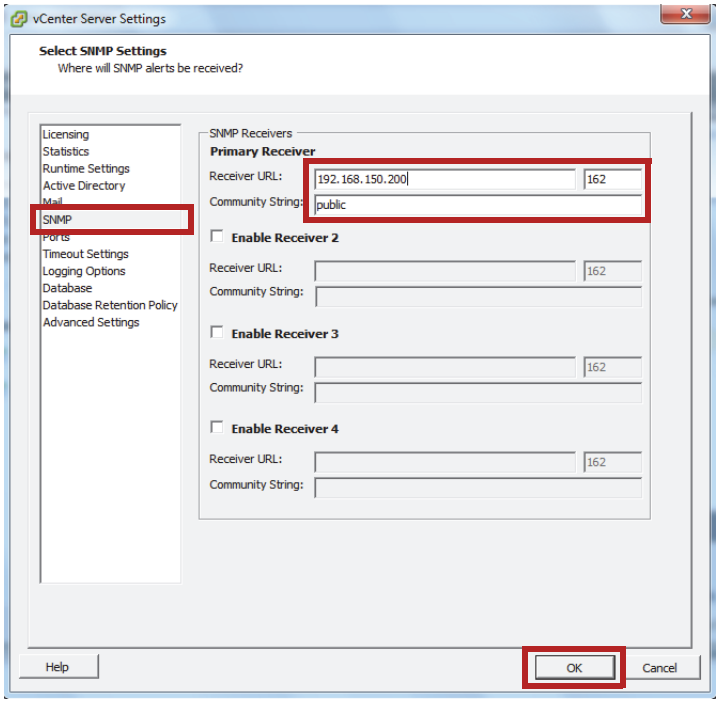
Step1: Launch vSphere Client from the maintenance PC and log in as root user to the IP address of vCenter Server.

Login with the password which is specified in "Initial Setup of Prepackaged Server/Prepackaged FT Server" of CHAPTER 2 SETUP.

Step2: Select the **Administration** menu -> **vCenter Server Settings**.



Step3: Click **SNMP** and enter URL of Primary Receiver (SNMP Manager's URL), Port number, and Community String and click **OK**. It can be set for multiple receivers.



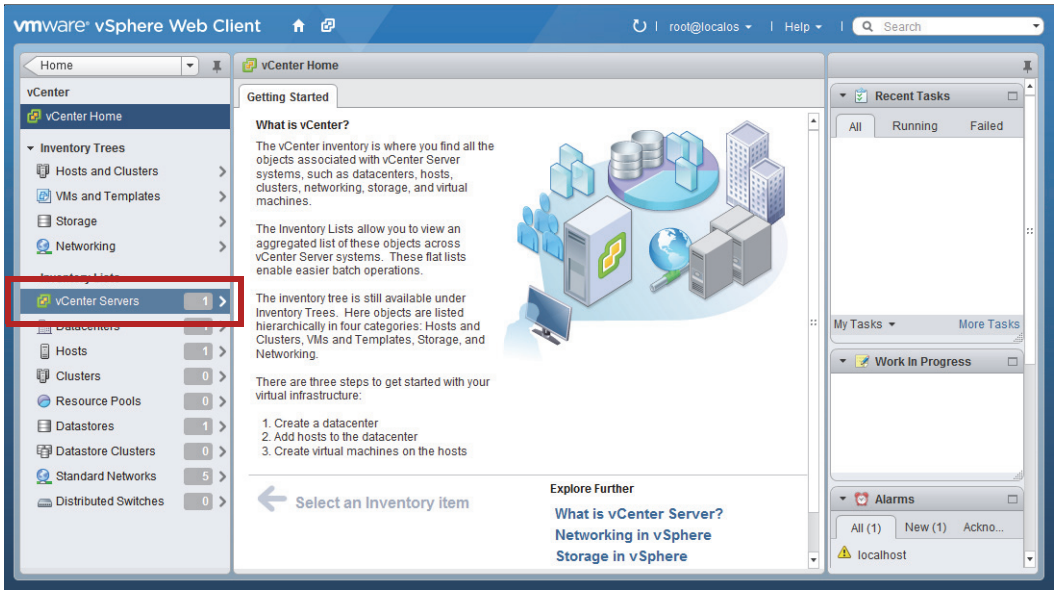
(2) Via vSphere Web Client

Step1: Launch vSphere Web Client from the maintenance PC and log in as root user to vCSA (https://xxx.xxx.xxx.xxx:9443/).

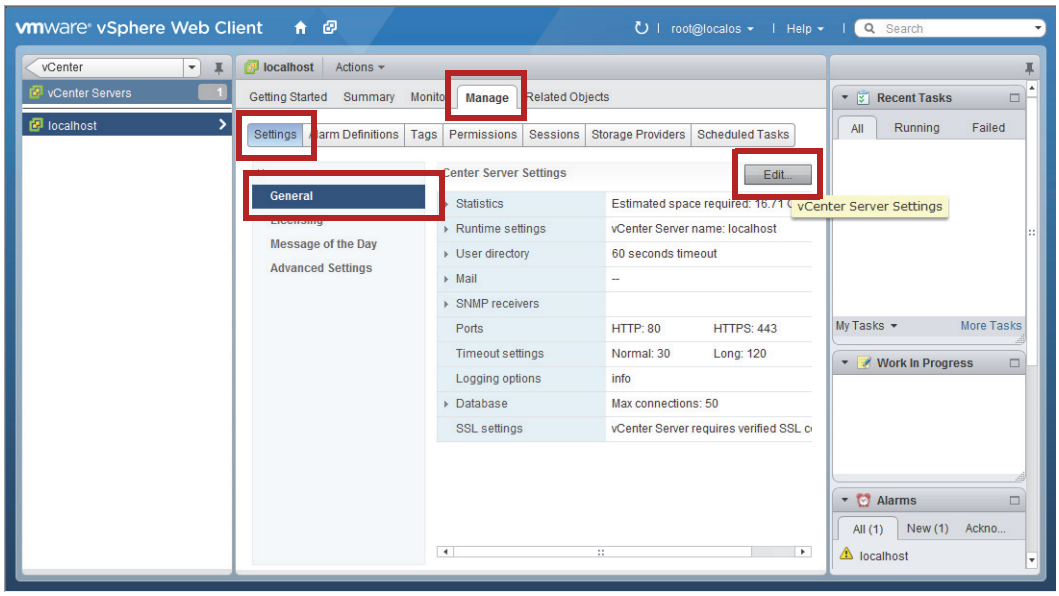
Replace "xxx.xxx.xxx.xxx" with the IP address of vCSA.

Login with the password which was configured in "5. Initial Setup of Prepackaged Server/Prepackaged FT Server" of CHAPTER 2 SETUP.

Step2: From the menu on the left side of the screen, click **vCenter** -> **vCenter Servers** in **Inventory Lists**.



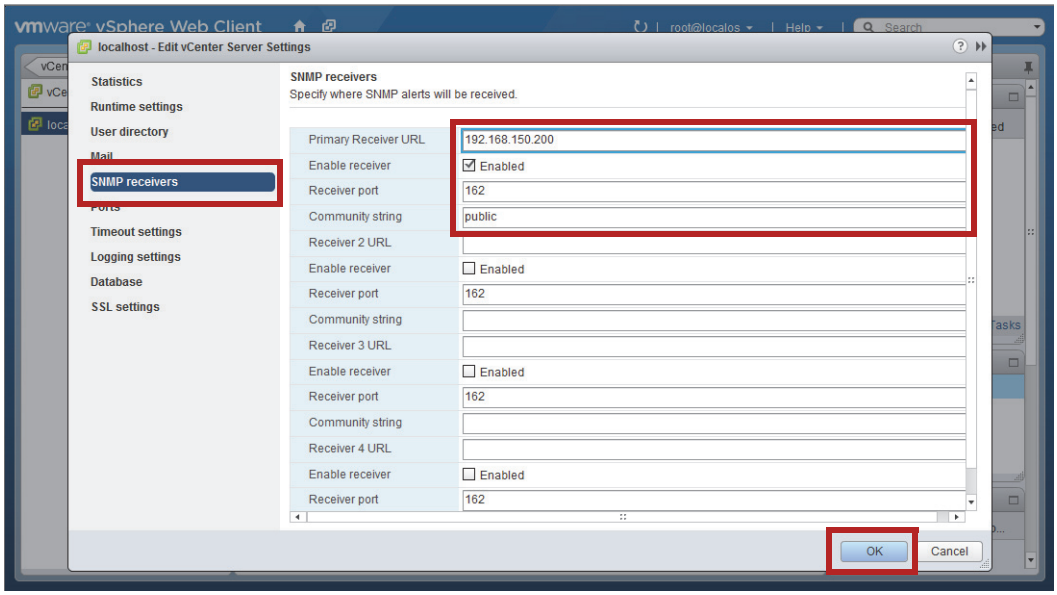
Step3: On the Manage tab, select **Settings** -> **General** and click the **Edit** button.



Step4: After selecting **SNMP receivers**, enter the following information and click **OK**. It can be set for multiple receivers.

- Primary Receiver URL (IP address of the SNMP manager)
- Enabled receiver: Enabled
- Receiver port

- Community string



2.2 VMware ESXi Setting

Set up VMware ESXi by using SSH or vSphere CLI. The following example describes how to connect the host with SSH.

(1) Enabling SSH **Note 1**

(2) Configuring VMware ESXi for SNMP v1 or v2c

(3) Configuring VMware ESXi for SNMP v3 or later

Note: When vSphere CLI is used for the setup, the following conditions must be met:
- You need to download the vSphere CLI package from the VMware Web site and install it on the maintenance PC. After installing, you can start it from the Windows Start menu, by selecting [Programs] - [VMware] - [VMware vSphere CLI] - [Command Prompt].
- The following option must be added the vSphere CLI.

```
-s <server>
```

`<server>` : Enter the IP address of VMware ESXi.

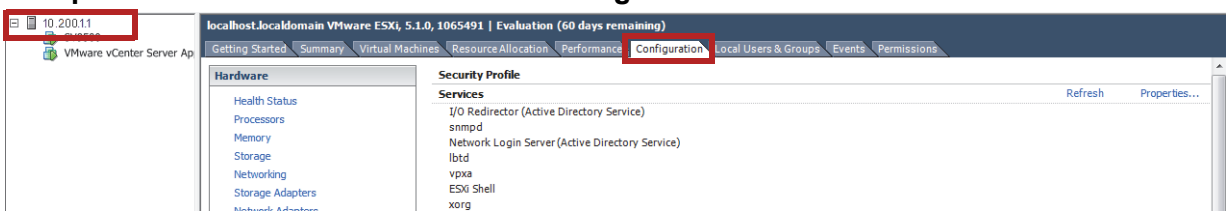
Note 1: Disable SSH after the VMware ESXi setting is completed. If you leave the SSH setting enabled, warning messages continues to appear on the VMware ESXi.

(1) Enabling SSH

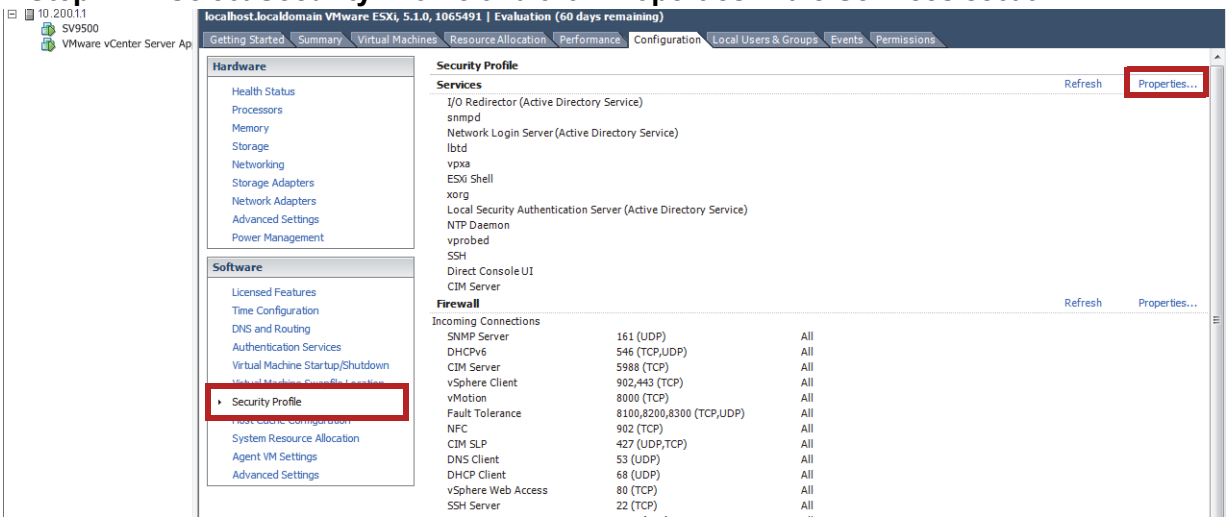
Enable SSH before configuring VMware ESXi for SNMP.

(a) Via vSphere Client

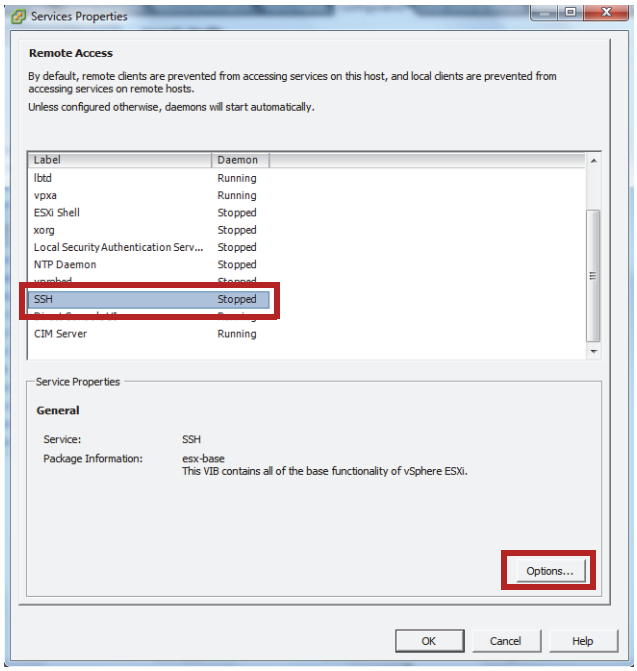
Step1: Select the host and click the **Configuration** tab.



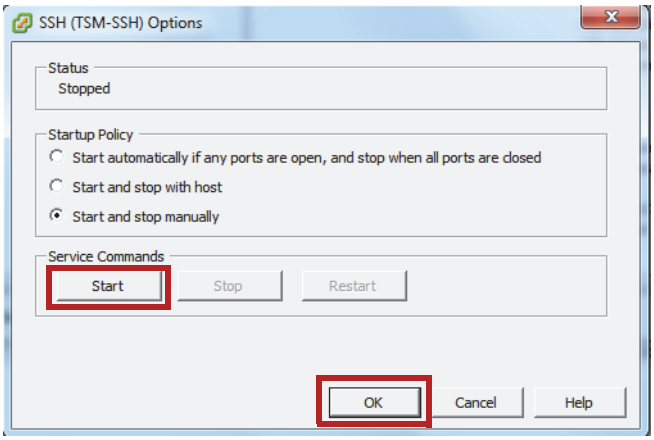
Step2: Select **Security Profile** and click **Properties** in the **Services** section.



Step3: Select **SSH** and click the **Options** button.



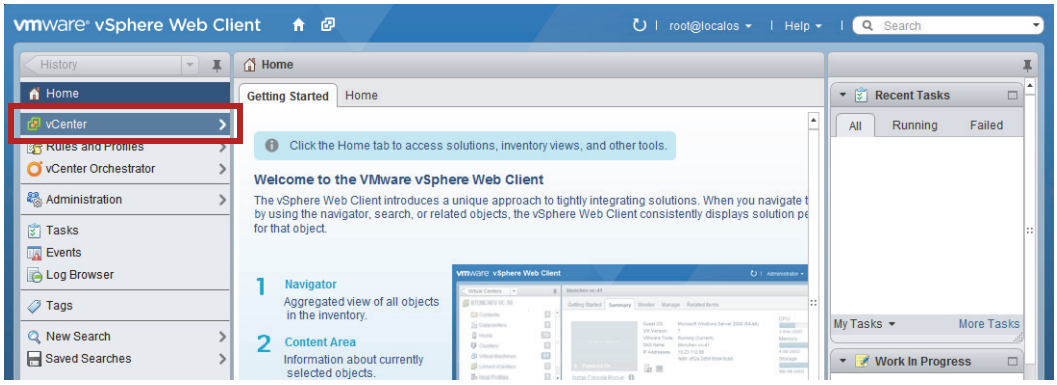
Step4: Click the **Start** button and **OK**.



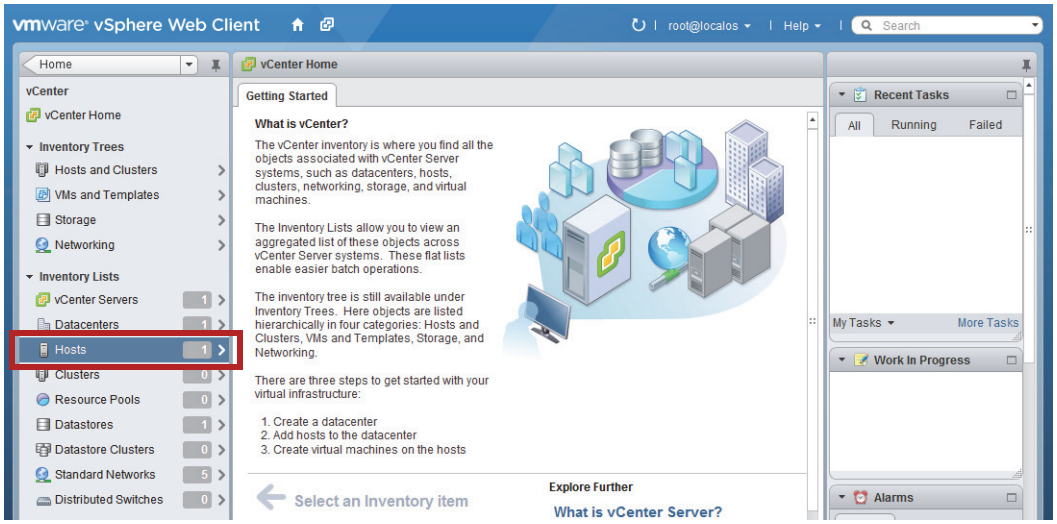
Step5: Click **OK** to finish.

(b) Via vSphere Web Client

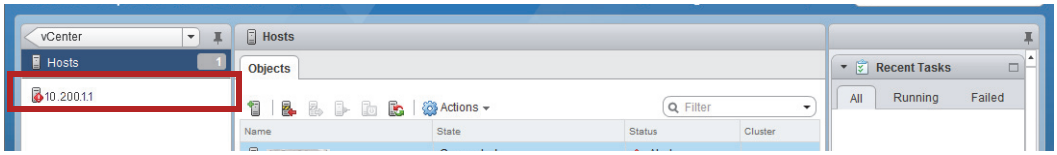
Step1: Click **vCenter** from the menu on the left side of the screen.



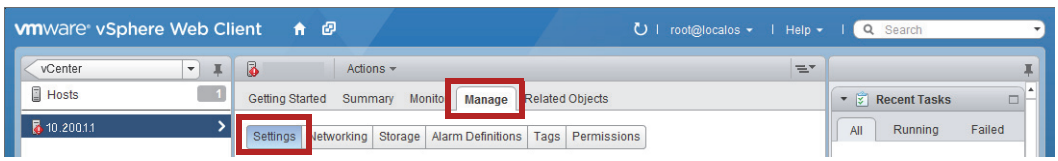
Step2: Click **Hosts** in **Inventory Lists**.



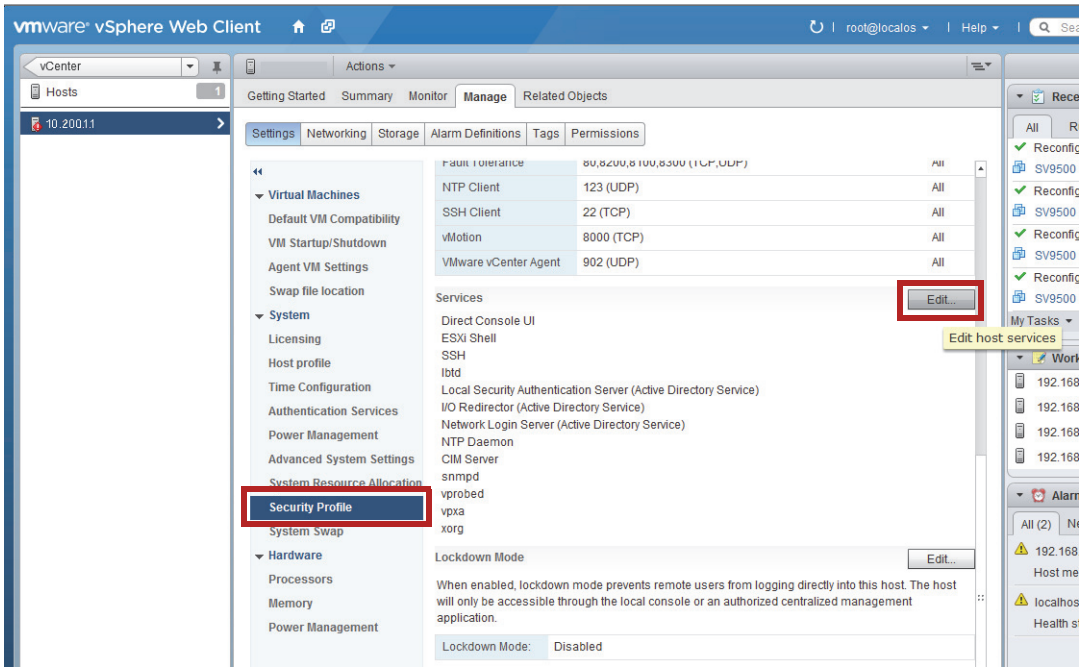
Step3: Select the IP address of the host.



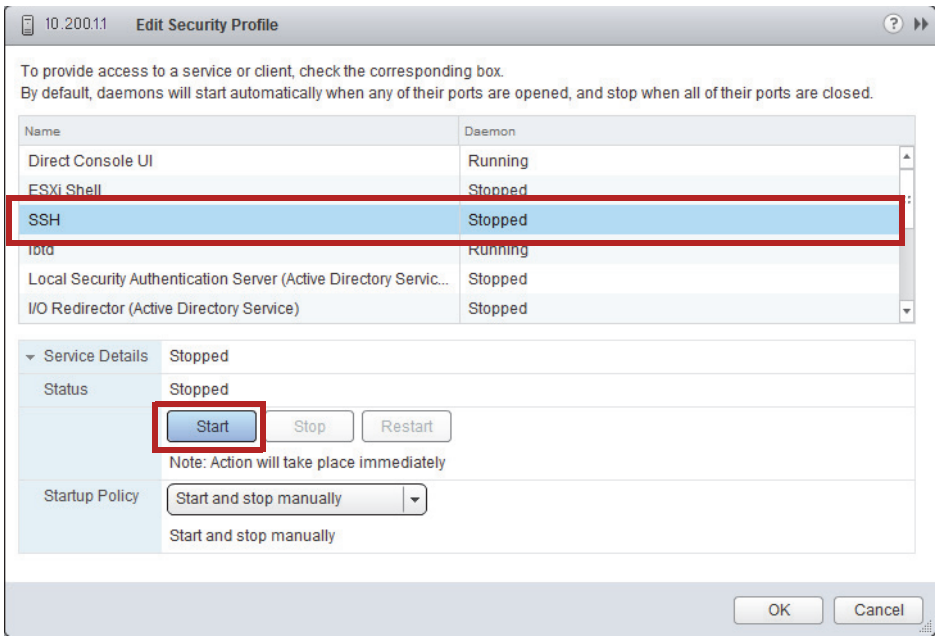
Step4: Select **Settings** on the **Manage** tab.



Step5: Select **Security Profile** and click the **Edit** button in the **Services** section.



Step6: Select **SSH** and click the **Start** button.



Step7: Confirm that **Service Details** is changed to running and click **OK** to finish.

(2) Configuring VMware ESXi for SNMP v1 or v2c

Step1: Access VMware ESXi with SSH.

Step2: Configure the community.

```
esxcli system snmp set --communities <community>
```

<community> : Enter the community name.

Step3: Configure the target (the receiver).

```
esxcli system snmp set --targets <target>@<port>/<community>
```

<target> : Enter FQDN or the IP address of the receiver.

<port> : Enter the port numbers of the receiver.

<community> : Enter the community name.

Step4: Configure the port number.

```
esxcli system snmp set --port <port>
```

<port> : Enter the port number of the sender.

Step5: Enable SNMP.

```
esxcli system snmp set --enable true
```

(3) Configuring VMware ESXi for SNMP v3 or later

Step1: Access VMware ESXi with SSH.

Step2: Configure the engine ID.

```
esxcli system snmp set --engineid <engine-id>
```

<engine-id> : Enter a character string (hexadecimal), ranging from 5 to 32 characters.

Step3: Set the authentication protocol.

```
esxcli system snmp set --authentication <auth-protocol>
```

<auth-protocol> : Enter none (for no security), SHA1 or MD5.

Step4: Set the privacy protocol.

```
esxcli system snmp set --privacy <priv-protocol>
```

<priv-protocol> : Enter none (for no privacy) or AES128.

Step5: Calculate the hash values.

(a) In case of designating the file.

```
esxcli system snmp hash --auth-hash <auth-file> --priv-hash <priv-file>
```

<auth-file> : Enter the path to the file that contains the user's authentication password.

<priv-file> : Enter the path to the file that contains the user's privacy password.

Note: "--priv-hash <priv-file>" does not need to be specified if you want to generate the hash value only from authentication password.

(b) In case of designating the password directly.

```
esxcli system snmp hash --auth-hash <auth-password> --priv-hash
 <priv-password> --raw-secret
```

<auth-password> : Enter user's authentication password.

<priv-password> : Enter user's privacy password.

Note: The following conditions must be met:
- The example command line is split in two lines because of space limitations. Type the command in one line without line breaks.
- "--priv-hash <priv-password>" does not need to be specified if you want to generate the hash value only from authentication password.

Step6: Configure the user.

```
esxcli system snmp set --users <username>/<auth-hash>/<priv-hash>/
<security>
```

<username> : Enter the user name.

<auth-hash> : Enter the authentication hash value which is generated by the hash function.

<priv-hash> : Enter the privacy hash value which is generated by the hash function.

<security> : Enter auth (for authentication only), priv (for authentication and privacy), or none (for no security).

Note: The example command line is split in two lines because of space limitations. Type the command in one line without line breaks.

Step7: If you configure SNMP Inform requests, type the following command line to configure the user.

```
esxcli system snmp set --remote-users <username>/<auth-protocol>/
<auth-hash>/<priv-protocol>/<priv-hash>/<engine-id>
```

<username> : Enter the user name.

<auth-protocol> : Enter none (for no security), SHA1 or MD5.

<auth-hash> : Enter the authentication hash value which is generated by the hash function. Specify "-" if authentication is none.

<priv-protocol> : Enter none (for no security) or AES128.

<priv-hash> : Enter the privacy hash value which is generated by the hash function. Specify "-" if privacy is none.

<engine-id> : Enter the character string (hexadecimal), ranging from 5 to 32 characters.

Note: The example command line is split in two lines because of space limitations. Type the command in one line without line breaks.

Step8: Configure the target (the receiver).

```
esxcli system snmp set --v3targets <target>@<port>/<username>/<security>/
<message-type>
```

<target> : Enter FQDN or the IP address of the receiver.

<port> : Enter the port numbers of the receiver.

<username> : Enter the user name.

<security> : Enter auth (for authentication only), priv (for authentication and privacy), or none (for no security).

<message-type> : Enter trap or inform.

Note: The example command line is split in two lines because of space limitations. Type the command in one line without line breaks.

Step9: Enable SNMP.

```
esxcli system snmp set --enable true
```

2.3 SNMP Manager Setting

The following describes how to configure SNMP Manager settings for SV9500 (Prepackaged Server Model).

Step1: Download VMware ESXi SNMP MIB modules from the VMware Web site.

https://my.vmware.com/en/web/vmware/details?productId=285&downloadGroup=VSP510-SNMPMIBS-510.

Step2: In SNMP Manager, specify the vCenter Server or VMware ESXi (host) as an SNMP-based managed device.

Step3: If you are using SNMP v1 or v2c, set up appropriate community names in the SNMP Manager.

Step4: If you are using SNMP v3, configure users and authentication and privacy protocols to match those configured on the VMware ESXi (host).

Step5: If you have configured the SNMP agent to send traps to a port on the management system other than the default UDP port 162, configure SNMP Manager to listen on the port you configured.

Step6: Load the VMware ESXi SNMP MIB modules into the SNMP Manager.

To prevent lookup errors, load these MIB files in the following order before loading other MIB files:

(1) VMWARE-ROOT-MIB.mib

(2) VMWARE-TC-MIB.mib

(3) VMWARE-PRODUCTS-MIB.mib

3. Powering On/Off Procedures

3.1 Powering On

Follow the steps below to turn on the system.

1 Connect the power cables to the Prepackaged Server/Prepackaged FT Server.
For Prepackaged FT Server Model, connect the power cables in the following order.

(1) Connect the power cable to module #0 (upper).

(2) Connect the power cable to module #1 (lower).

Note: Any time you unplug the power cable, wait at least 30 seconds before reconnecting.

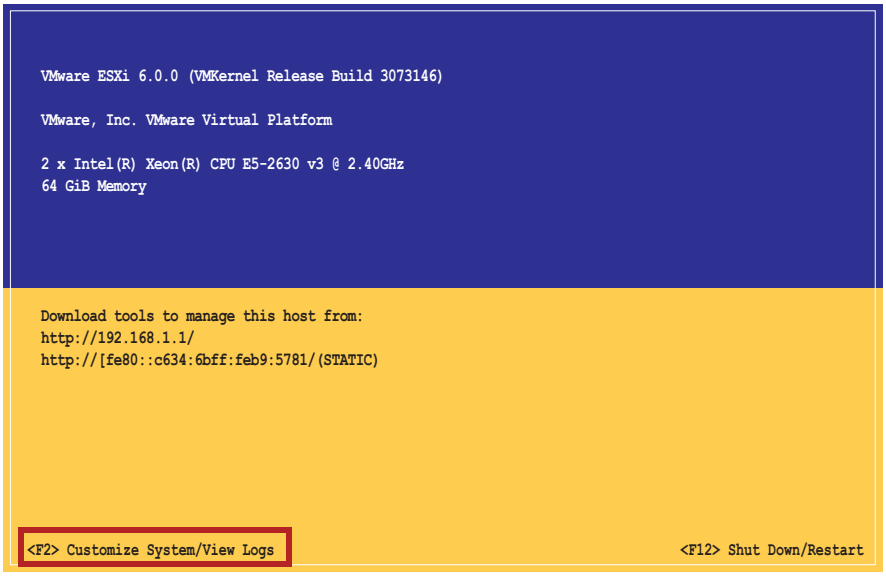
Note: For Prepackaged FT Server Model, the first module to be connected to a power cable becomes the primary.

2 Referring "Management by LAN Port" in CHAPTER 1 GENERAL, connect LAN cables to the Prepackaged Server/Prepackaged FT Server.

3 Turn on the monitor and the peripheral devices connected to the Prepackaged Server/Prepackaged FT Server.

4 Remove the front bezel, and press the power switch located on the front side of the server.

The POWER lamp lights up green, and the message “<F2> Customize System/View Logs” appears in the lower left corner of the direct console (hereinafter called “DCUI”).

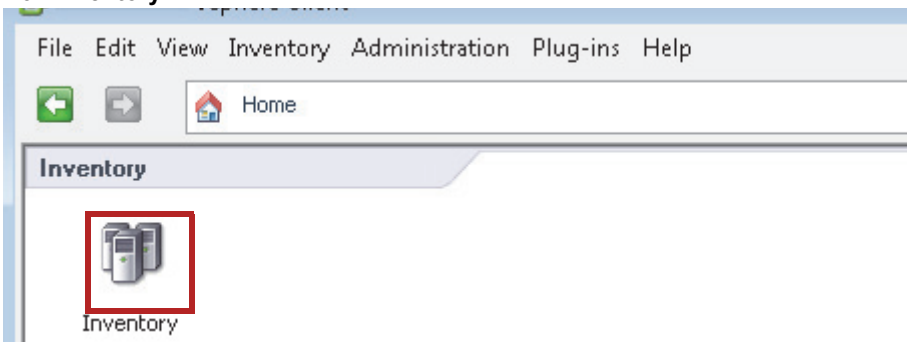


5 Assign an IP address to the maintenance PC so that it is in the same network segment as the server with VMware ESXi.

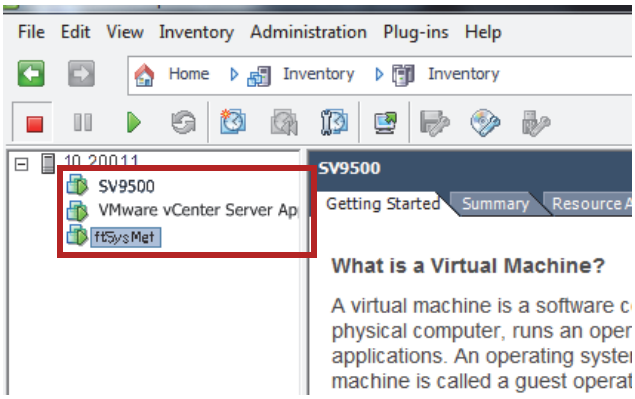
6 Send a ping request to the IP address of the VMware ESXi to verify connectivity.

7 From the maintenance PC, log in to VMware ESXi as root via vSphere Client.

8 Click on **Inventory**.



9 Confirm that all the virtual machines have been successfully started.

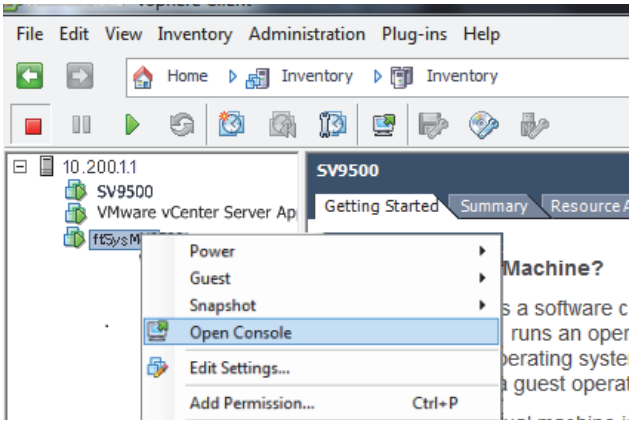


For Prepackaged Server Model, forward to STEP14.
For Prepackaged FT Server Model, forward to STEP10.

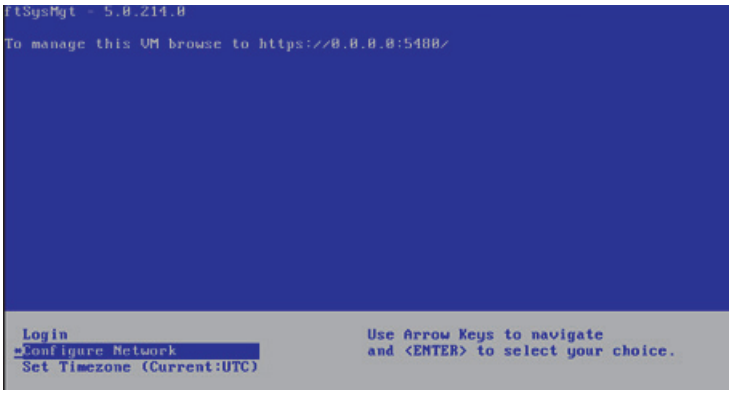
Note: It takes some time before all the virtual machines are started.

Note: FT management appliance is only for Prepackaged FT Server Model.

10 Click the virtual machine of FT management appliance, select **Open Console** from the right-click menu.



11 Confirm that the console menu is displayed.



12 Assign an IP address to the maintenance PC so that it is in the same network segment as FT management appliance.

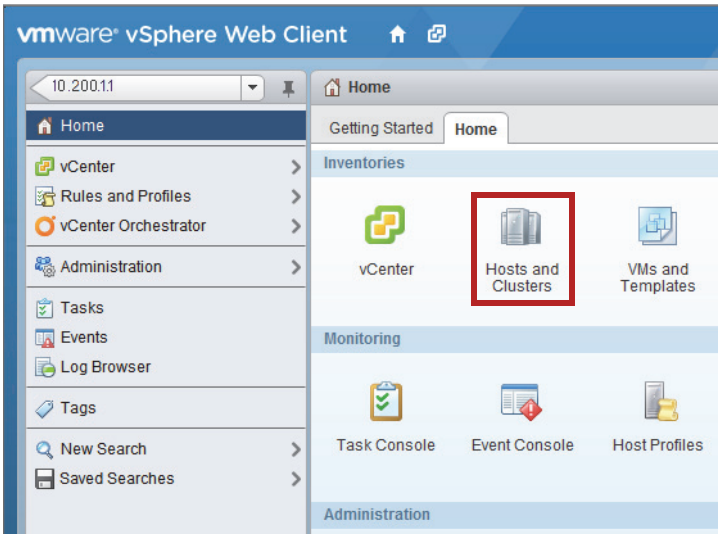
13 Send a ping request to the IP address of FT management appliance to verify connectivity.

14 Assign an IP address to the maintenance PC so that it is in the same network segment as vCSA.

15 Send a ping request to the IP address of vCSA to verify connectivity.

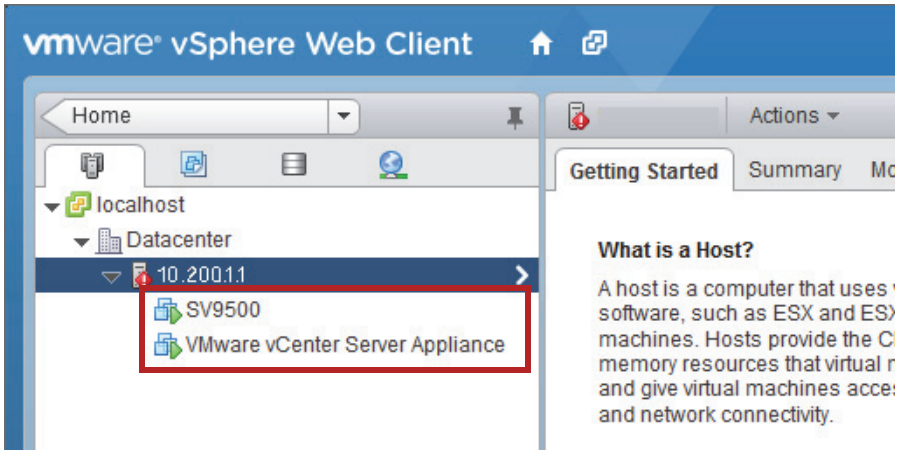
16 From the maintenance PC, log in to vCSA (https://xxx.xxx.xxx.xxx:9443/) as root via vSphere Web Client.
Replace “xxx.xxx.xxx.xxx” with the IP address of vCSA.

17 In the navigation area located in the left side of the **Home** screen, select **vCenter** - **Inventories** - **Hosts and Clusters**.



18 Confirm that all the virtual machines have been successfully started.

Note: It takes some time before all virtual machines are started.

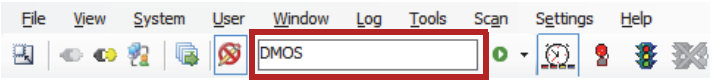


19 Send a ping request to the IP address of all the virtual machines to verify connectivity.

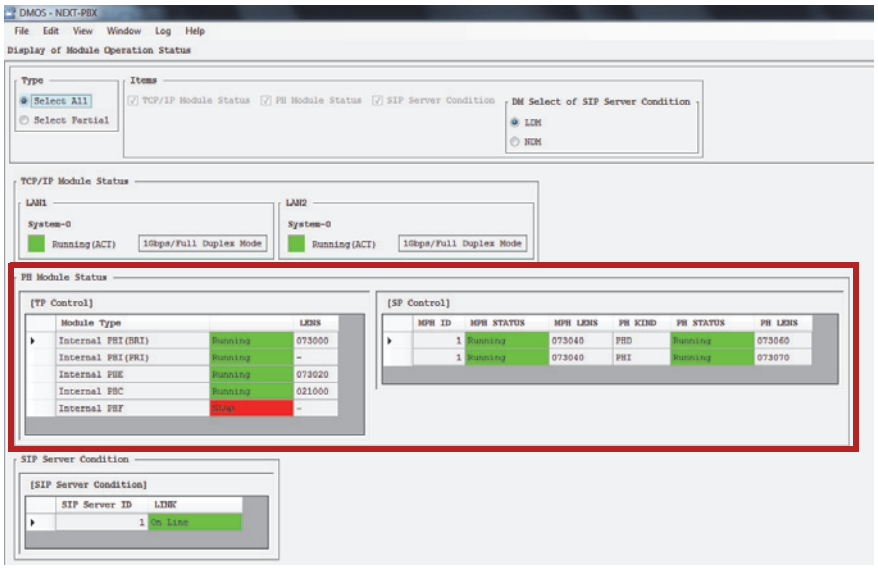
20 Confirm that SV9500 has been successfully started.
Launch the web browser from the maintenance PC and connect to Telephony Server Maintenance Menu at http://xxx.xxx.xxx.xxx:9801/. Confirm that the login screen is displayed.
Replace “xxx.xxx.xxx.xxx” with the IP address of LAN1 of SV9500.

21 Connect to PCPro and log in.

22 Start the DMOS command.



23 Confirm that the modules in **TP Control** and **SP Control** in the **PH Module Status** section are successfully running.



The power-on procedure has been completed.

3.2 Powering Off

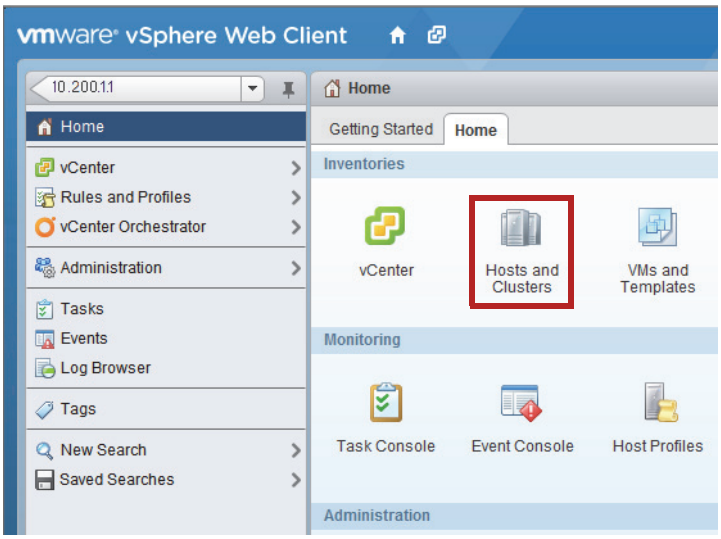
Follow the steps below to turn off the system.

1 Assign an IP address to the maintenance PC so that it is in the same network segment as the vCSA.

2 Send a ping request to the IP address of vCSA to verify connectivity.

3 From the maintenance PC, log in to vCSA (https://xxx.xxx.xxx.xxx:9443/) as root via vSphere Web Client.
Replace “xxx.xxx.xxx.xxx” with the IP address of vCSA.

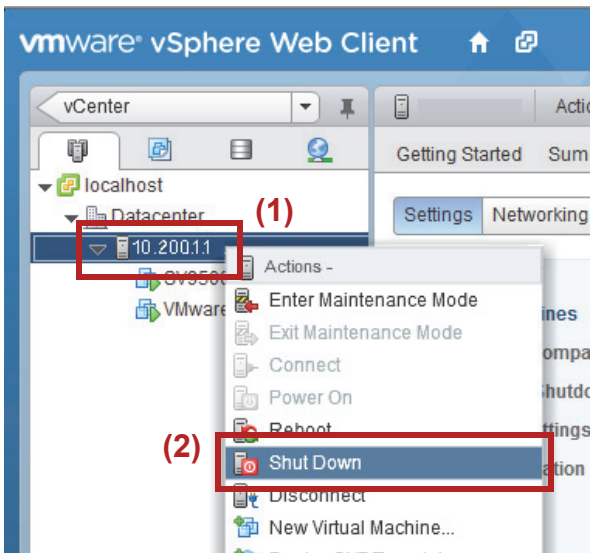
4 In the navigation area located in the left side of the **Home** screen, select **vCenter** - **Inventories** - **Hosts and Clusters**.



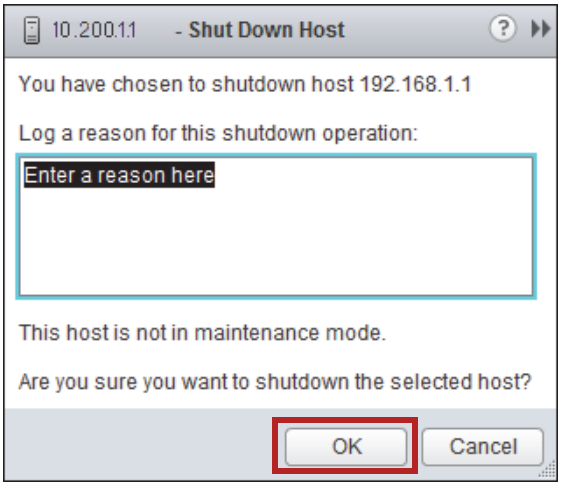
5 Shut down the VMware ESXi.

(1) Click the host machine (VMware ESXi).

(2) Right click and select **Shut Down**.



6 When a confirmation dialog box appears, click **OK**.



7 When the POWER lamp of the Prepackaged Server/Prepackaged FT Server goes out, turn off the peripheral devices connected to the server.

Note: It takes some time before the shut down is completed.

The shut down procedure has been completed.

4. Rebooting Guest OS (SV9500)

Follow the steps below to Reboot SV9500.

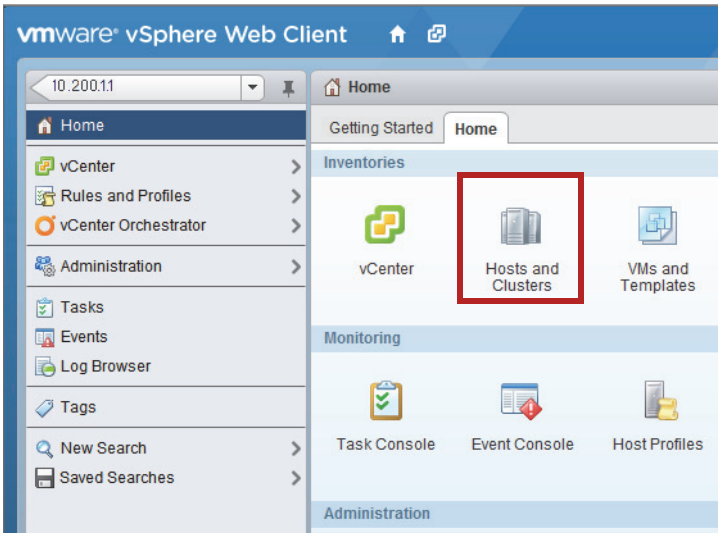
Note: SINZ command's **reboot** cannot be used. Follow the steps below to reboot.

1 Assign an IP address to the maintenance PC so that it is in the same network segment as vCSA.

2 Send a ping request to the IP address of vCSA to verify connectivity.

3 From the maintenance PC, log in to vCSA (https://xxx.xxx.xxx.xxx:9443/) as root via vSphere Web Client.
Replace “xxx.xxx.xxx.xxx” with the IP address of vCSA.

4 In the navigation area located in the left side of the **Home** screen, select **vCenter** - **Inventories** - **Hosts and Clusters**.



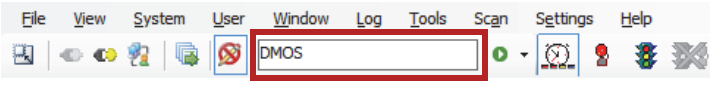
5 Restart SV9500.
(1) Right-click the SV9500 virtual machine from the menu on the left side of the screen.
(2) Select **Power** -> **Restart Guest OS**.

6 Send a ping request to the IP address of each LAN (LAN1 and LAN2) on SV9500 to verify connectivity.

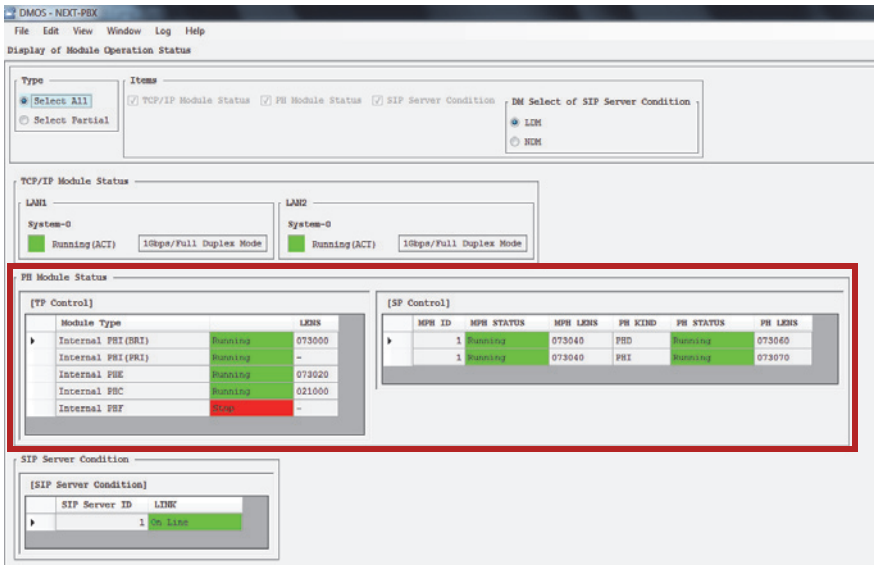
7 Confirm that SV9500 is successfully started.
From the maintenance PC, launch the web browser and connect to Telephony Server Maintenance Menu at http://xxx.xxx.xxx.xxx:9801/ and confirm that the login screen is displayed.
Replace “xxx.xxx.xxx.xxx” with the IP address of LAN1 of SV9500.

8 Connect to PCPro and log in.

9 Start the DMOS command.



10 Confirm that the modules in **TP Control** and **SP Control** in the **PH Module Status** section are successfully running.



The rebooting procedure has been completed.

5. Program Version Upgrade

This section explains the procedure to upgrade to a program version of the system program.

In the section, **Note** states the precautions required when performing each procedure. An error or failure may occur if these precautions are missed. Be sure to follow each precautions without exception. Point states tips and supplemental remarks to be considered when performing each procedure.

Note: For use by or as indicated by a certified technician.

5.1 Conditions of Use

(1) Minor program version upgrade for the SV9500 software is available from FP95-112 V2.

(2) Major program version upgrade for the SV9500 software is available from FP95-114 V4 Issue 4.0

(3) Downgrading is not available.

(4) If there is any problem with the upgraded version, it is possible to switch back to the previous version. It is only possible to switch back to the version from where the upgrading was performed but not to previous versions. Therefore, in the example below, it is possible to switch back to V2 (2.01) but not to V2 (2.00): V2 (2.00)-> (version up) - V2 (2.01)->(version up) - V2 (2.02).

(5) If an upgrading is performed after switching back, file uploading is required.
V2 (2.00) -> (first version up) V2 (2.01) -> (switch back) V2 (2.00) -> (second version up) V2 (2.01).
In the second version up above, file uploading is required.

(6) If an upgrading is performed right after switching back, one of the messages below may be displayed:

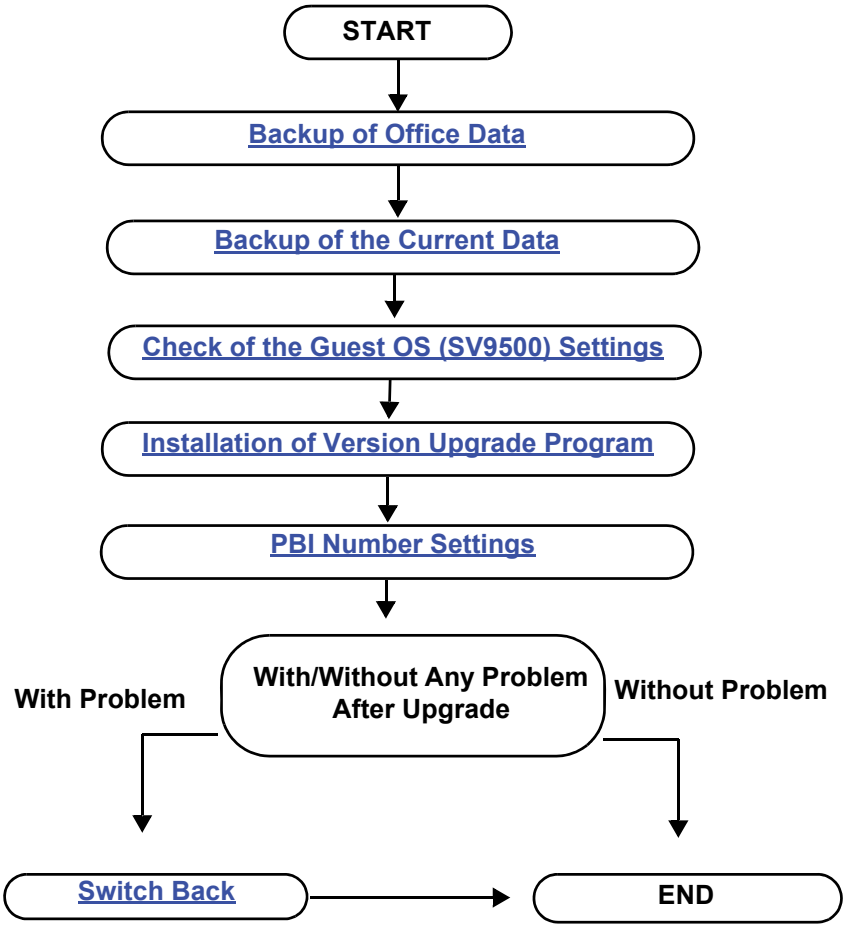
- It is currently running a merge.
- To exit because backup is not make.

In that case try the upgrading again after a few minutes (no more than 20 minutes may be necessary).

(7) License and data office are not lost during the upgrading.

(8) After switching back, data is restored to its settings before upgrading. Collect the logs before switching back.

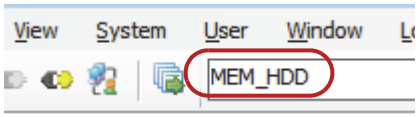
5.2 Procedure of Program Version Upgrade



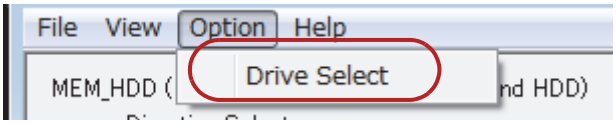
5.3 Backup of Office Data

This section explains the procedure to backup the Office Data using the MEM_HDD command.

1 Execute the MEM_HDD command.



2 Select “Drive Select” from [Option] menu.



3

(1) Select the drive which is currently used from [Office Data]. Which drive to select depends on your configuration. As an example, Office Data will be saved in Drive B in the figure below.

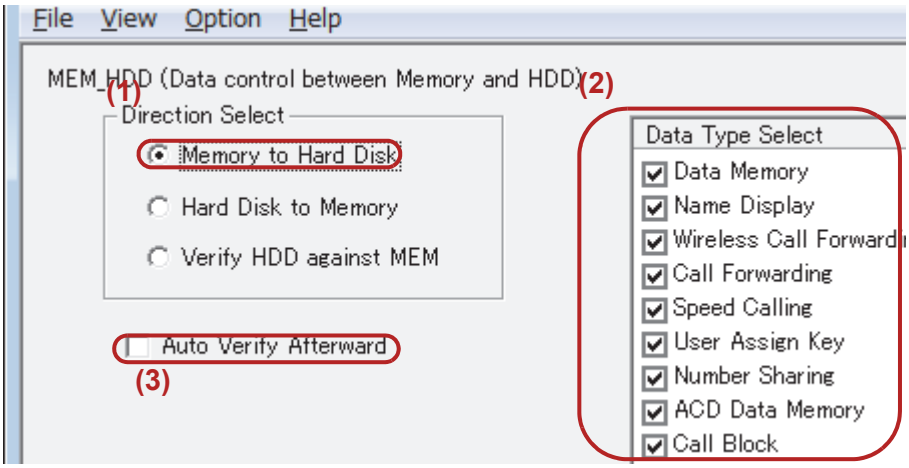
(2) Click the **Apply** button.

4

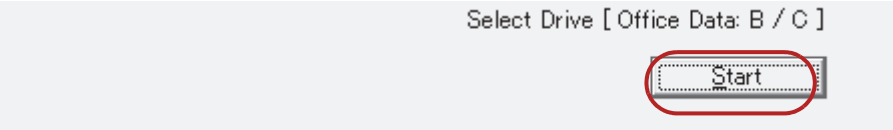
(1) Select “Memory to Hard Disk” for [Direction Select].

(2) Place a check mark for used data type on [Data Type Select].

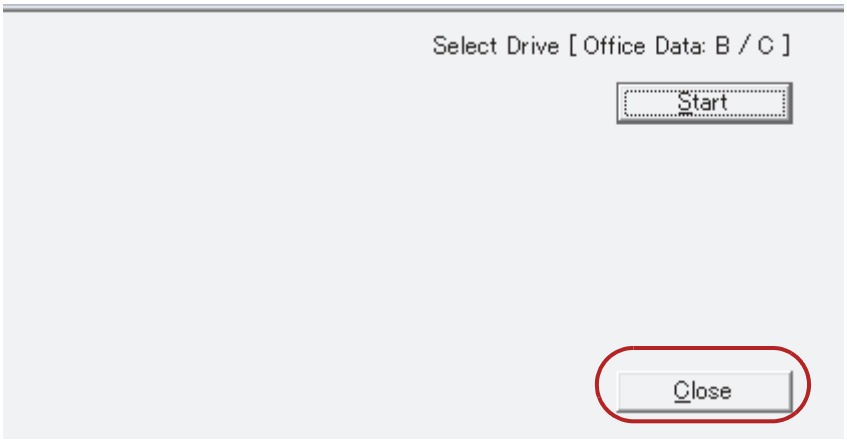
(3) Place a check mark on “Auto Verify Afterward”.



5 Click the **Start** button.



6 After the backup is completed, click the **Close** button to exit the MEM_HDD command.



The backup process of office data is completed

5.4 Backup of the Current Data

This section explains the procedure to back up the data (including the program, office data and license) currently used for operation to the maintenance PC in case of an emergency (such as when restoring the program).

1 Start Internet Explorer and type “http://xxx.xxx.xxx.xxx:9801/” into the address bar. “xxx.xxx.xxx.xxx” represents the LAN1 IP address (ex. 10.100.1.11).

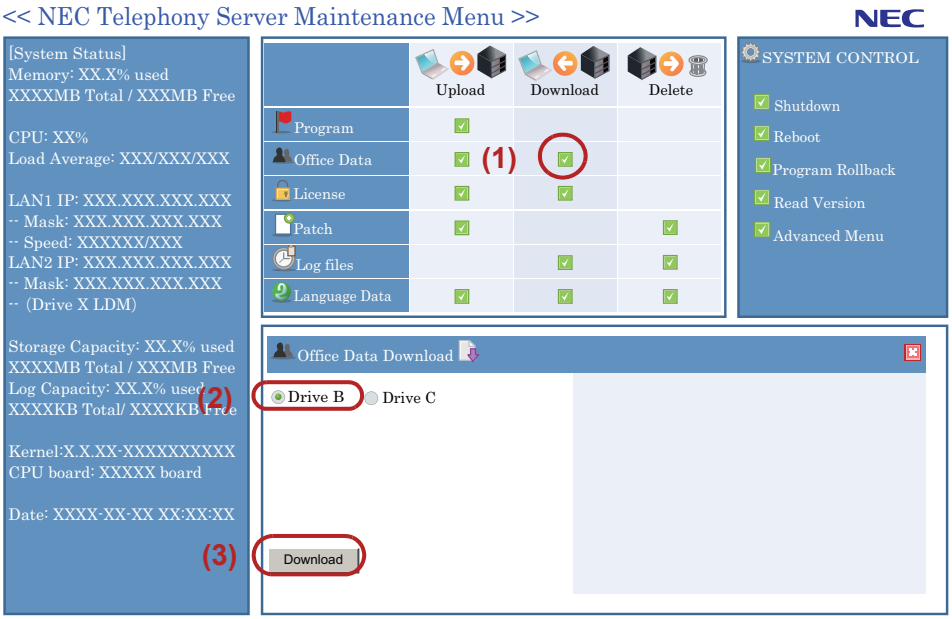
Note:
- Microsoft Internet Explorer 7.0 or higher is required to access Telephony Server Maintenance Menu.

2
(1) **Telephony Server Maintenance Menu Login** screen appears. Type a user name and password.
(2) Click the **OK** button to log in to **Telephony Server Maintenance Menu**.

Note:
- Contact NEC maintenance personnel if you need to confirm User Name and Password.
- After logging into Telephony Server Maintenance Menu, do not use **Back** button on browser.

3

(1) Click the **Download** button for **Office Data**. The **Office Data Download** dialog box appears in the lower right portion of the screen.
(2) Choose a drive (Drive B or Drive C) which you specified at STEP3 of 5.3 Backup of Office Data.
(3) Click the **Download** button on the dialog box and save the data in the desired folder.

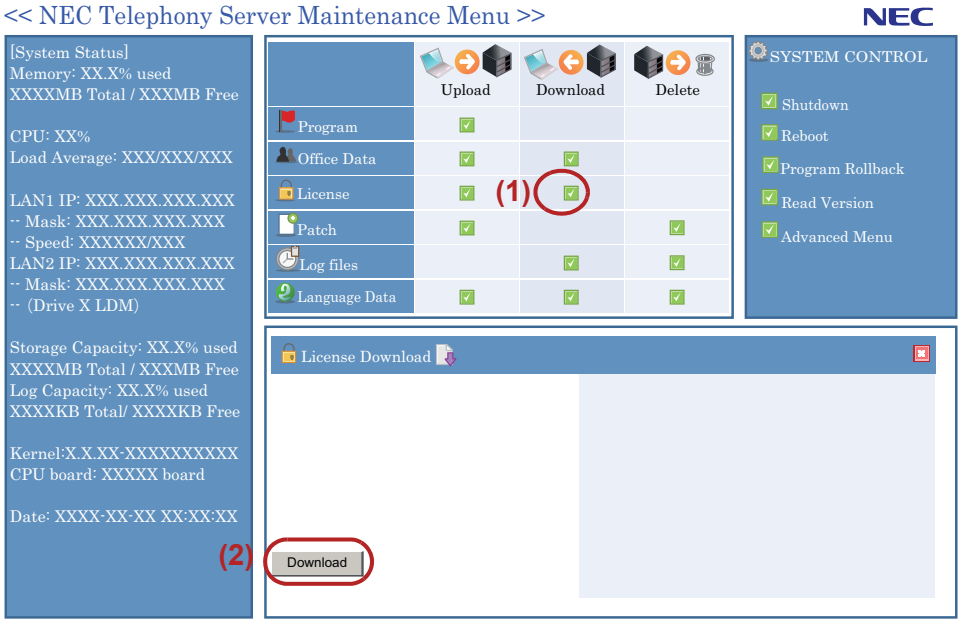


Note:
When the download of office data ends in failure, “An error occurred! Please check the logs.” is displayed and the details are displayed in the lower right portion of the screen.

4

(1) Click the **Download** button for **License**. The **License Download** dialog box appears in the lower right portion of the screen.

(2) Click **the Download** button on the dialog box and save the license file in the desired folder.



Note:
Telephony Server Maintenance Menu will not be displayed when Internet Explorer 10 is used.
For copying the displayed result, check the “Show results in new window” box under Read Version. Then copy and paste the desired information.

Note:
When the download ends in failure, “An error occurred! Please check the logs.” is displayed and the details are displayed in the lower right portion of the screen.

The backup process of the current data is completed.

However, if your system provides the OPTIONAL LANGUAGE PACK LOADING [O-42] service, backing up the following language data is also required:

<When customized language file is used for Extension Language>

- Extension Language file (for example, “English_0001.txt”)
- Information file of Extension Languages (exlang_info)

For further information, see “Updating Extension Language File (Customized Language File)” of OPTIONAL LANGUAGE PACK LOADING [O-42] in Data Programming Manual - Business.

<When Sample Language file is used for Extension Language>

- Information file of Extension Languages (exlang_info)

For further information, see “Updating Extension Language File (Sample Language File)” of OPTIONAL LANGUAGE PACK LOADING [O-42] in Data Programming Manual - Business.

5.5 Check of the Guest OS (SV9500) Settings

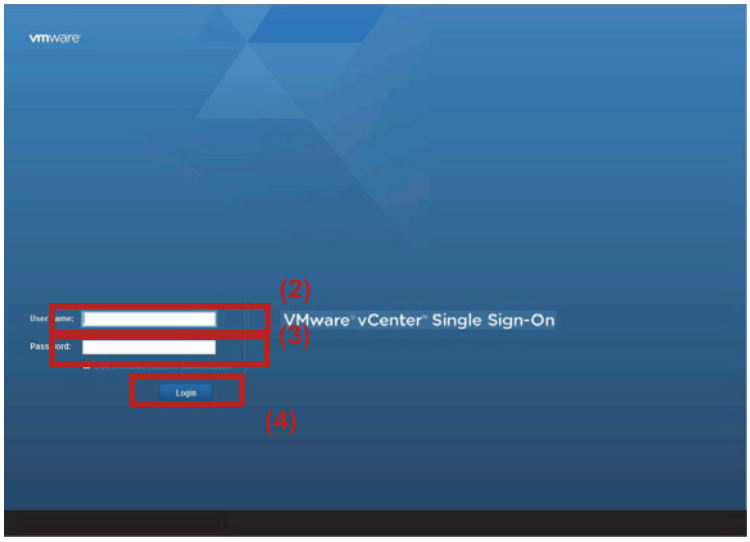
1

(1) From the web browser of the maintenance PC, log in to vCSA (https://xx.xx.xx.xx:9433/).
use the following user ID and password (below are given the examples used in 5.6 Customizing vCenter Server Appliance (vCSA) in CHAPTER 2 SETUP:

(2) User ID: **vsphere.sso**

(3) Password: **SV9500@sso**

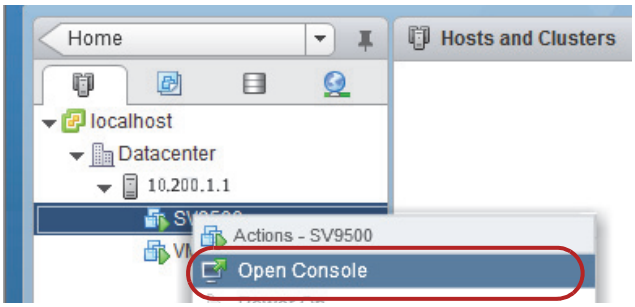
(4) Press the **Login** button.



2

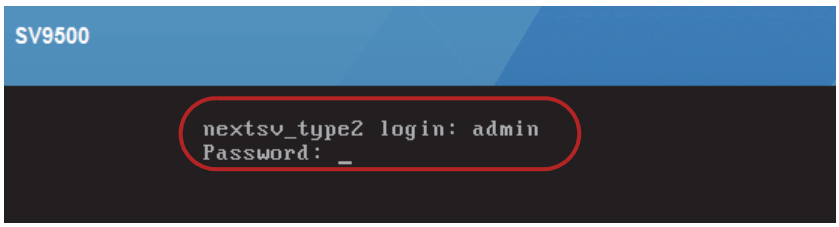
(1) Click [Hosts and Clusters] on [vCenter]-> [Inventory Trees] from the menu on the left side of the home screen.

(2) Right-click on SV9500 and select Open Console.



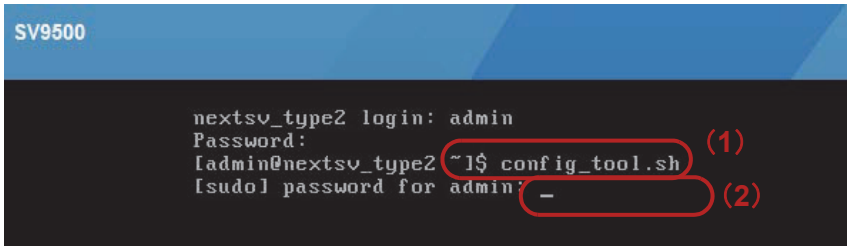
Note: From FP95-114 V4, Check of the Guest OS (SV9500) Settings is not necessary.

3 Log in as admin to sv9500.

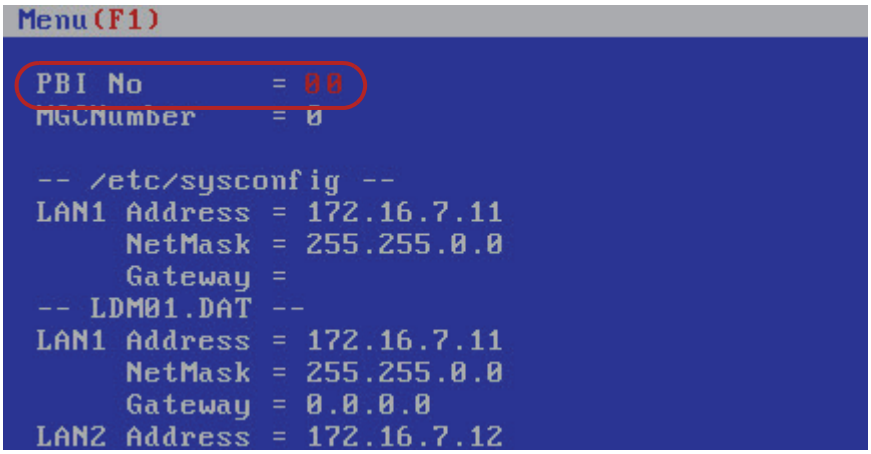


Note: Contact NEC maintenance personnel if you need to confirm your User Name and Password.

4 (1) Execute “config_tool.sh”.
(2) Enter the password for admin again.



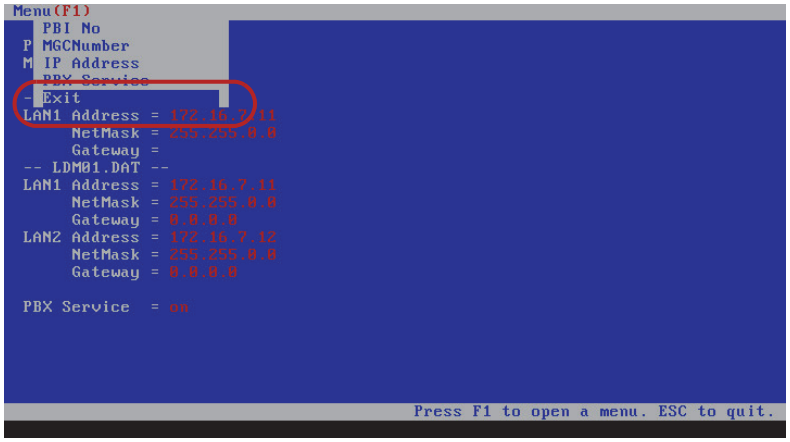
5 Check the PBI number.



Note:
Take a memo with the number.

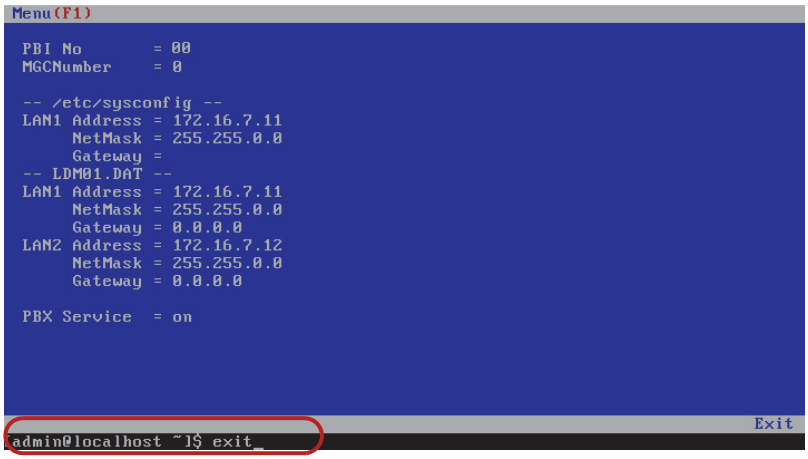
6

(1) Press **F1**.
(2) Select **Exit**.



7

(1) Verify that admin@localhost is displayed.
(2) Type “exit” and press **Enter**.



8 After being displayed again the log in screen, close the console screen.

5.6 Installation of Version Upgrade Program

This section explains the procedure to install a version upgrade program in the Telephony Server.

5.6.1 Checking the Version Information (Before Upgrading)

This section explains how to check the version in use.

1 Start Internet Explorer and type “http://xxx.xxx.xxx.xxx:9801/” into the address bar. “xxx.xxx.xxx.xxx” represents the LAN1 IP address (ex. 10.100.1.11).

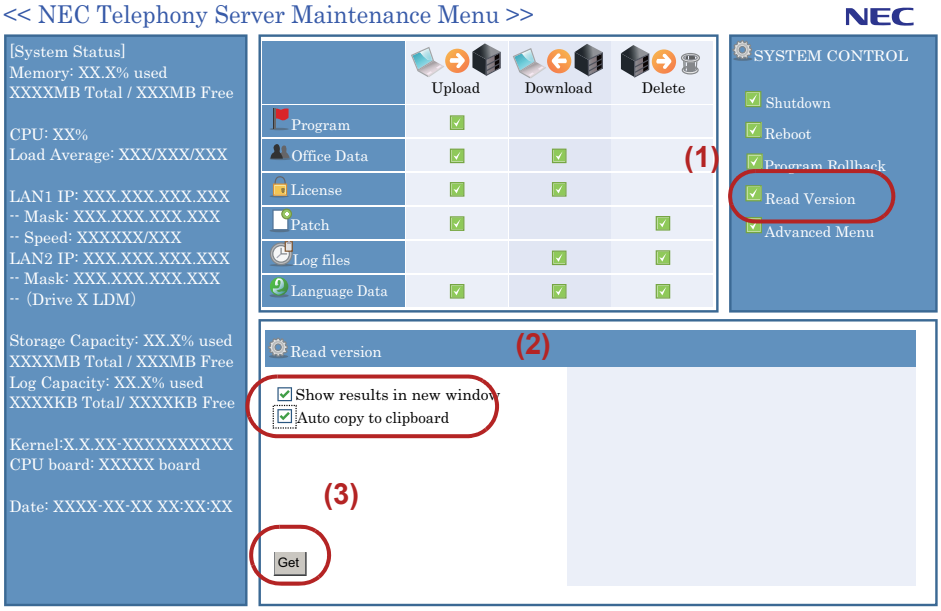
Note:
- Microsoft Internet Explorer 7.0 or higher is required to access Telephony Server Maintenance Menu.

2
(1) **Telephony Server Maintenance Menu Login** screen appears. Type a user name and password.
(2) Click the **OK** button to log into **Telephony Server Maintenance Menu**.

Note:
- Contact NEC maintenance personnel if you need to confirm your User Name and Password.
- After logging into SV9500 Maintenance Menu, do not use **Back** button on a browser.

3

(1) Click the **Read Version** button in the **SYSTEM CONTROL** area. The **Read Version** dialog box appears in the lower right portion of the screen.
(2) Select both the **Show results in new window** and the **Auto copy to clipboard** check boxes.
(3) Click the **Get** button to display the program version list.



A new screen is opened where the program version is displayed.

Note:
From Internet Explorer 10 and later “Auto copy to clipboard” is not displayed. If it is necessary to attach the results to a clipboard, copy them from the new window opened with “Show results in new window” using the mouse right button.

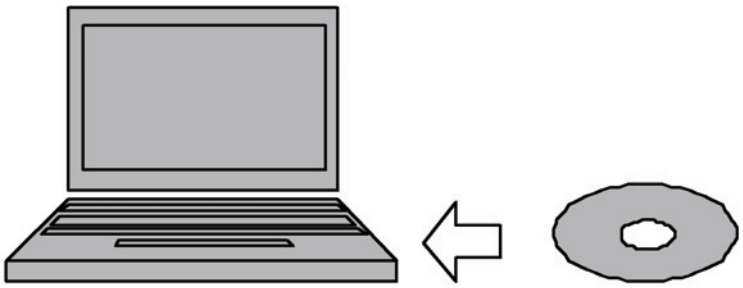
4 Check the software version (currently-operated program version) for MAIN.

```
## Date : 2015-03-04 10:00:00
## Read Version
------------------------------------------------------------
          MAIN   V02 02.00 000 20150212
          ACDP   V02 02.00 000 20150115
      MISCLIBS   V02 02.00 000 20150121
           MPH   V02 02.00 000 20141120
           PHD   V02 02.00 000 20141120
           PHI   V02 02.00 000 20141120
    B2BUA_MAIN   V02 02.00 000 20141120
       SP_BOOT   V02 02.00 000 20141120
      SIPSV_PHE  V02 02.00 000 20141120
      SIPSV_SIP  V02 02.00 000 20141120
         LIBCMN  V02 02.00 000 20141120
       LIBFSMTL  V02 02.00 000 20141120
        LIBOSIP  V02 02.00 000 20141120
         IP_DTG  V02 02.00 000 20140716
        SV_GATE  V02 02.00 000 20140717
      SV_TSKCTL  V02 02.00 000 20140717
         SV_EMA  V02 02.00 000 20140717
         SV_IOC  V02 02.00 000 20140717
        SV_CPLD  V02 02.00 000 20140717
     PBXWATCHD   V02 02.00 000 20140716
      SVSYSSUB   V02 02.00 000 20141009
      BASE_SYS   V02 02.00 000 20150128
    95SYS_First  V02 02.00 000 20141125
```

5.6.2 Data Copy from Install DVD

Copy the files in the install DVD to the maintenance PC.

1 Set the Install DVD “GENERIC SOFTWARE” with the new version in the disk drive.



2 Copy all the files in the Install DVD into a desired folder on the maintenance PC.

The data copy from the DVD is completed.

5.6.3 Performing the Version Upgrading

This section explains how perform the upgrading.

1 Start Internet Explorer and type “http://xxx.xxx.xxx.xxx:9801/” into the address bar. “xxx.xxx.xxx.xxx” represents the LAN 1 IP address (ex. 10.100.1.11).

Note:
Microsoft Internet Explorer 7.0 or higher is required to access Telephony Server Maintenance Menu.

2 (1) **Telephony Server Maintenance Menu Login** screen appears. Type a user name and password.
(2) Click the **OK** button to log into **Telephony Server Maintenance Menu**.

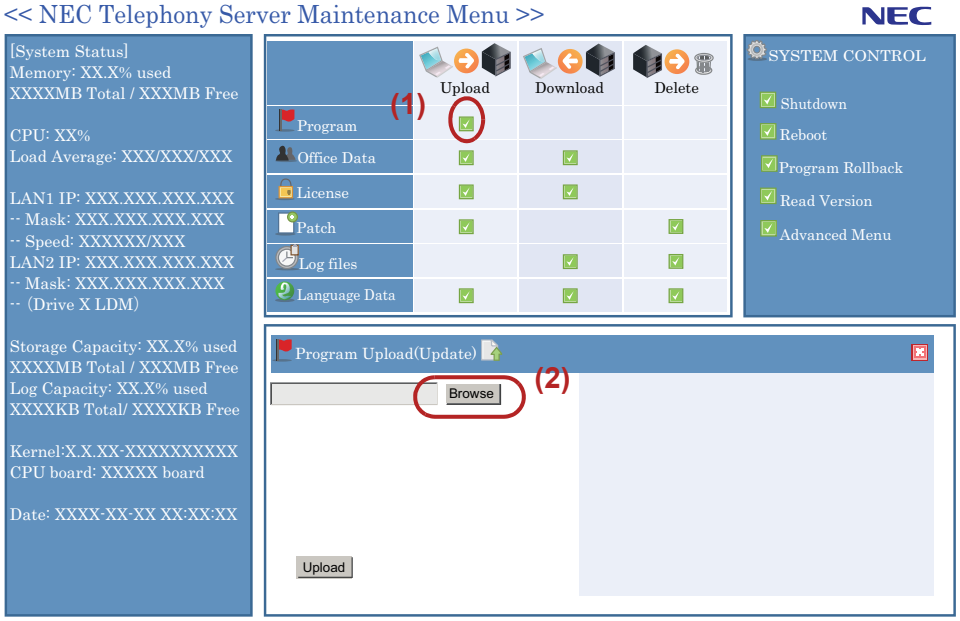
Note:
- Contact NEC maintenance personnel if you need to confirm your User Name and Password.
- After logging into SV9500 Maintenance Menu, do not use **Back** button on a browser.

3

(1) Click the **Upload** button for **Program**. The **Program Upload** dialog box appears in the lower right portion of the screen.

(2) Click the **Browse** button on the dialog box and then specify the following two files (located in the folder in which you copied the upgraded program as in Data Copy from Install DVD).

- SC Number_Major Version_Issue Number_the data on which the file is created (Ex: 4439_020_0182_150220.tgz)
- work.zip

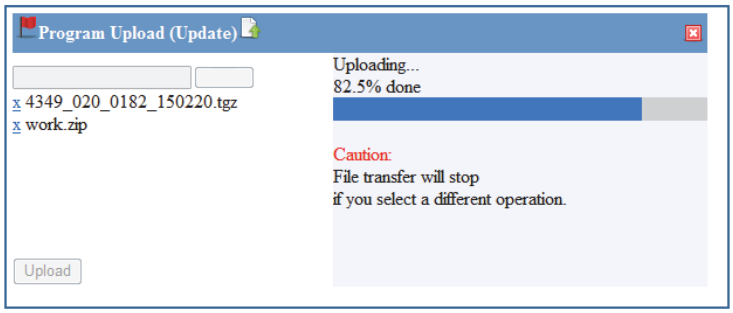


4

Check that the correct files are selected and click the **Upload** button.

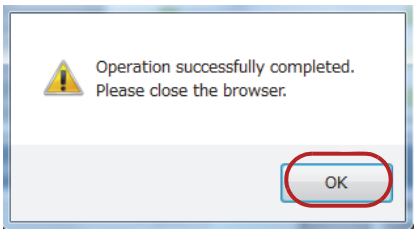
Note:
From Internet Explorer 10, you can select at once several files with control key and Shift key or drag and drop. However, if it is necessary to erase or add files, since you cannot do it one by one, select several files at once.

5 A screen is displayed to confirm the starting of the updating, click **OK** and the uploading starts**.**



Note:
By clicking OK, the files loading and the restarting are executed.
Do not perform any action until the confirmation screen is displayed.

6 A confirmation message appears.Click **OK**.



Note:
When the program upload ends in failure, “An error occurred! Please check the logs.” is displayed and the details are displayed in the lower right portion of the screen.

5.6.4 Checking the Version Information (After Upgrading)

This section explains how to check the version in use.

1 Start Internet Explorer and type “http://xxx.xxx.xxx.xxx:9801/” into the address bar. “xxx.xxx.xxx.xxx” represents the LAN1 IP address (ex. 10.100.1.11).

Note:
- Microsoft Internet Explorer 7.0 or higher is required to access Telephony Server Maintenance Menu.

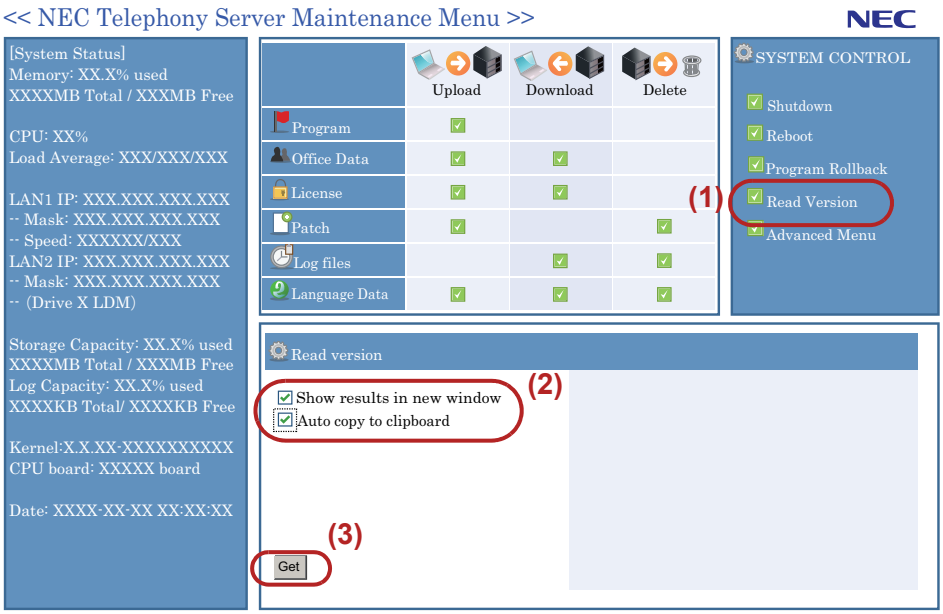
2

(1) **Telephony Server Maintenance Menu Login** screen appears. Type a user name and password.
(2) Click the **OK** button to log into **Telephony Server Maintenance Menu**.

Note:
- Contact NEC maintenance personnel if you need to confirm User Name and Password.
- After logging into SV9500 Maintenance Menu, do not use **Back** button on a browser.

3

(1) Click the **Read Version** button in the **SYSTEM CONTROL** area. The **Read Version** dialog box appears in the lower right portion of the screen.
(2) Select both the **Show results in new window** and the **Auto copy to clipboard** check boxes.
(3) Click the **Get** button to display the program version list.



A new screen is opened where the program version is displayed.

Note:
From Internet Explorer 10 “Auto copy to clipboard” is not displayed. If it is necessary to attach the results to a clipboard, copy them from the new window opened with “Show results in new window” using the mouse right button.

4 Check the software version (currently-operated program version) for MAIN.

```
## Date : 2015-03-04 11:30:00
## Read Version
-------------------------------------------------------
          MAIN    V02 02.01 000 20150304
          ACDP    V02 02.00 000 20150115
      MISCLIBS    V02 02.00 000 20150121
           MPH    V02 02.00 000 20141120
           PHD    V02 02.00 000 20141120
           PHI    V02 02.00 000 20141120
    B2BUA_MAIN    V02 02.00 000 20141120
       SP_BOOT    V02 02.00 000 20141120
      SIPSV_PHE    V02 02.00 000 20141120
      SIPSV_SIP    V02 02.00 000 20141120
         LIBCMN    V02 02.00 000 20141120
       LIBFSMTL    V02 02.00 000 20141120
        LIBOSIP    V02 02.00 000 20141120
         IP_DTG    V02 02.00 000 20140716
        SV_GATE    V02 02.00 000 20140717
      SV_TSKCTL    V02 02.00 000 20140717
         SV_EMA    V02 02.00 000 20140717
         SV_IOC    V02 02.00 000 20140717
        SV_CPLD    V02 02.00 000 20140717
     PBXWATCHD     V02 02.00 000 20140716
     SVSYSSUB      V02 02.00 000 20141009
     BASE_SYS      V02 02.00 000 20150304
    95SYS_First    V02 02.00 000 20141125
```

After checking the version proceed with the next section (Change of the Guest OS (SV9500) Settings).

5.7 PBI Number Settings

Note: From FP95-114 V4, PBI Number Settings is not necessary.

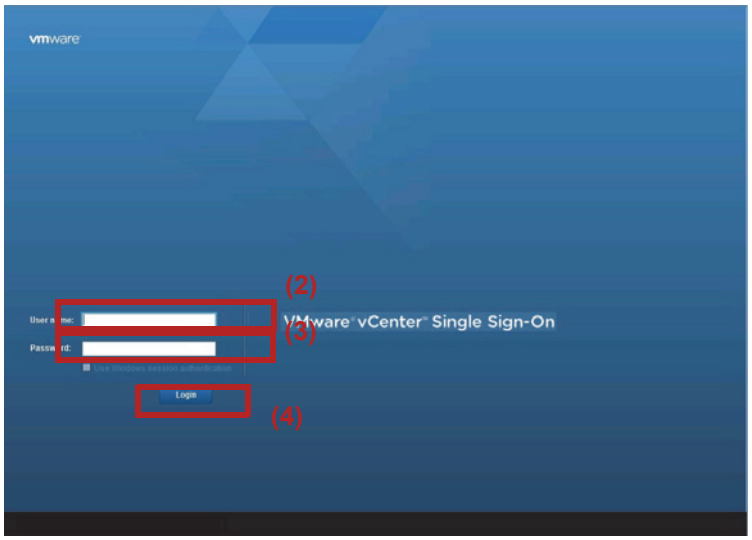
1

(1) From the web browser of the maintenance PC, log in to vCSA (https://xx.xx.xx.xx:9433/).
use the following user ID and password (below are given the examples used in 5.6 Customizing vCenter Server Appliance (vCSA) in CHAPTER 2 SETUP:

(2) User ID: **vsphere.sso**

(3) Password: **SV9500@sso**

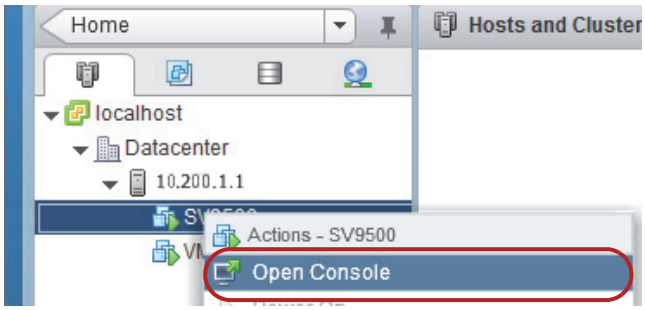
(4) Press the **Login** button.



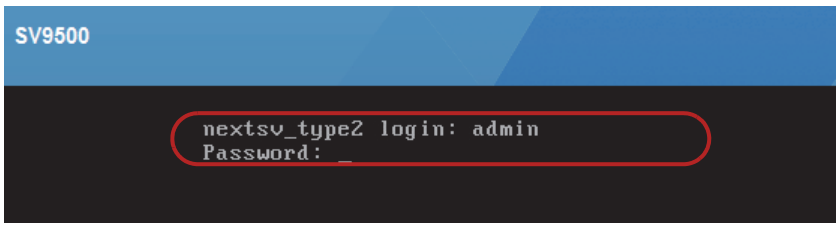
2

(1) Click [Hosts and Clusters] on [vCenter]-> [Inventory Trees] from the menu on the left side of the home screen.

(2) Right-click on SV9500 and select Open Console.

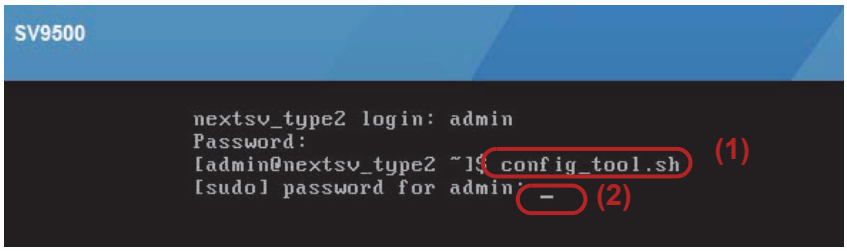


3 Log in as admin to sv9500.

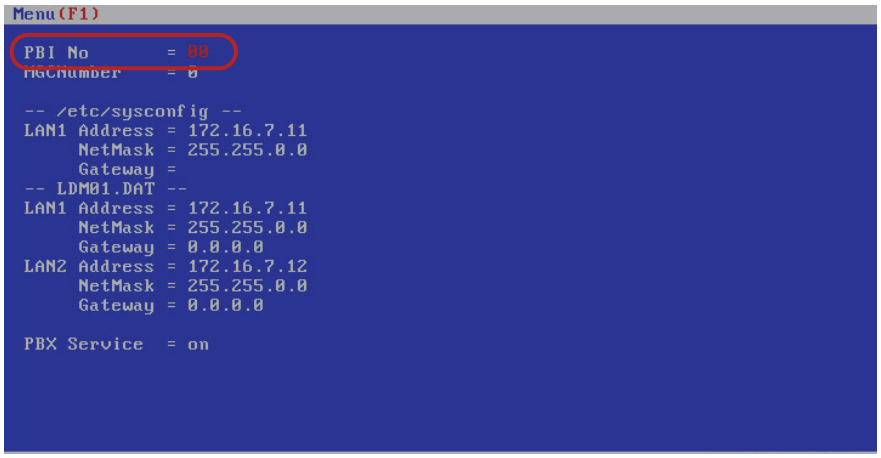


Note: Contact NEC maintenance personnel if you need to confirm your User Name and Password.

4 (1) Execute “config_tool.sh”.
(2) Enter the password for admin again.



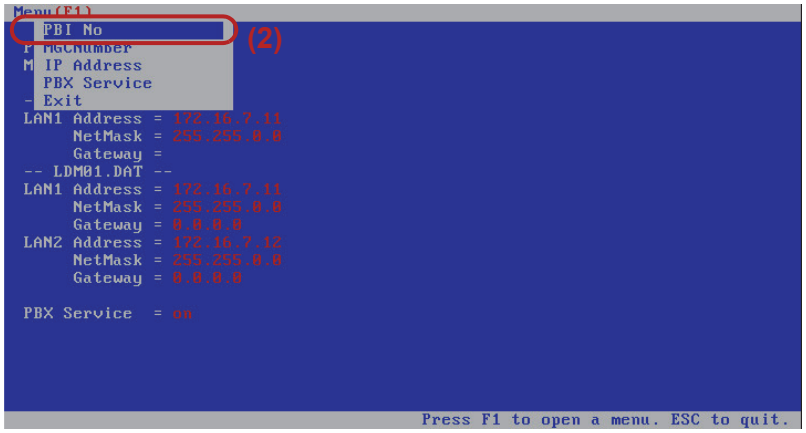
5 Check the PBX number and verify that is the same as Check of the Guest OS (SV9500) Settings. (in the example below, “00”.)



Note: If the PBI number is correct, go to step 11.

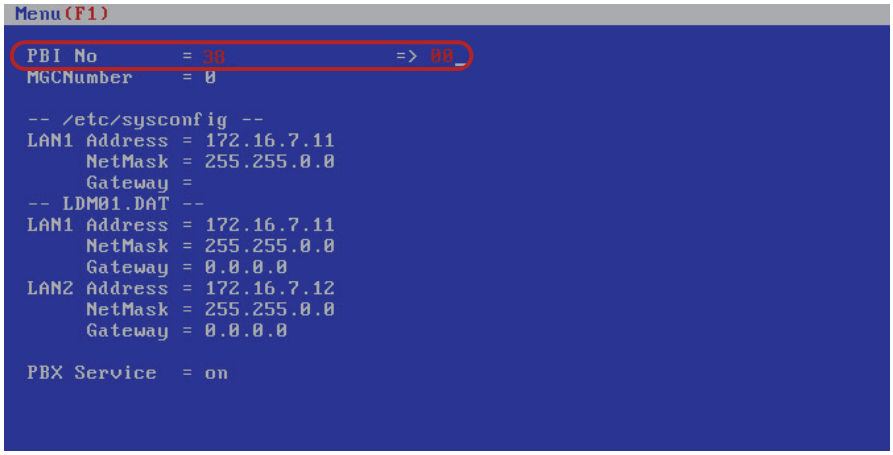
6

(1) Press **F1**.
(2) Select **PBI No**.



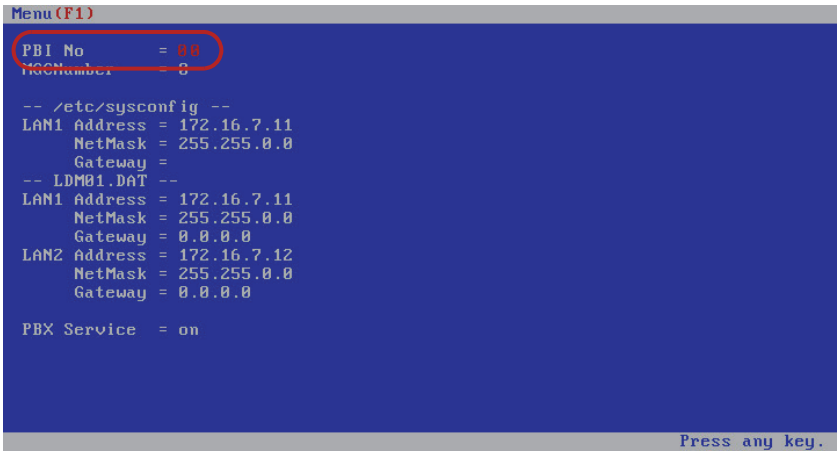
7

Enter the correct PBI number ("00").



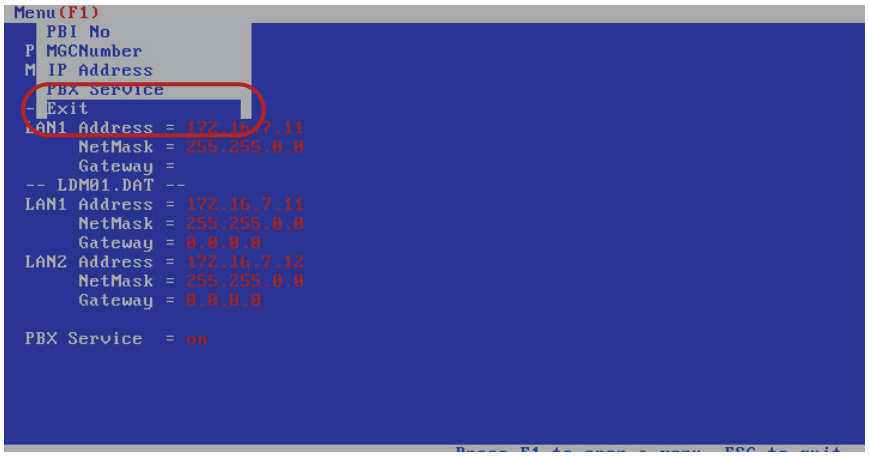
8

Check the PBI number.



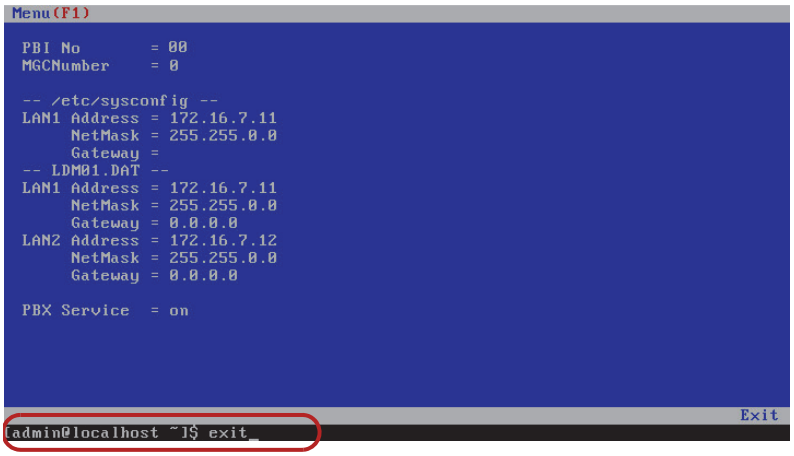
9

(1) Press **F1**.
(2) Select **Exit**.

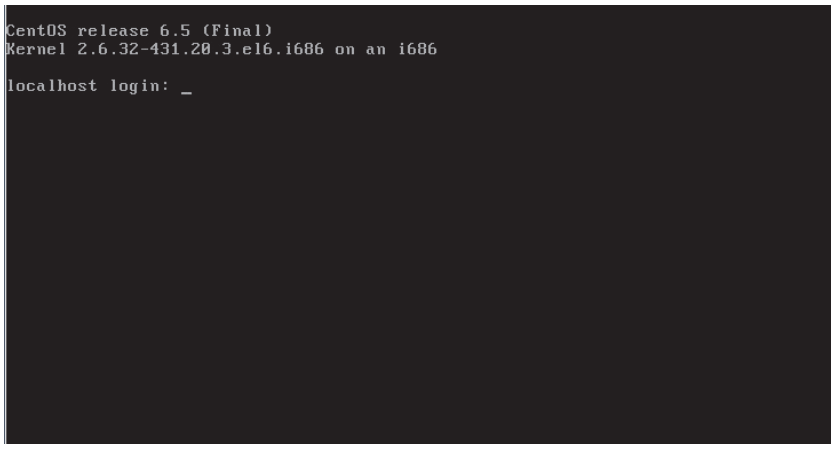


10

(1) Verify that admin@localhost is displayed.
(2) Type exit and press **Enter**.



11 After being displayed again the log in screen, close the console screen.



5.8 PBX Service Settings

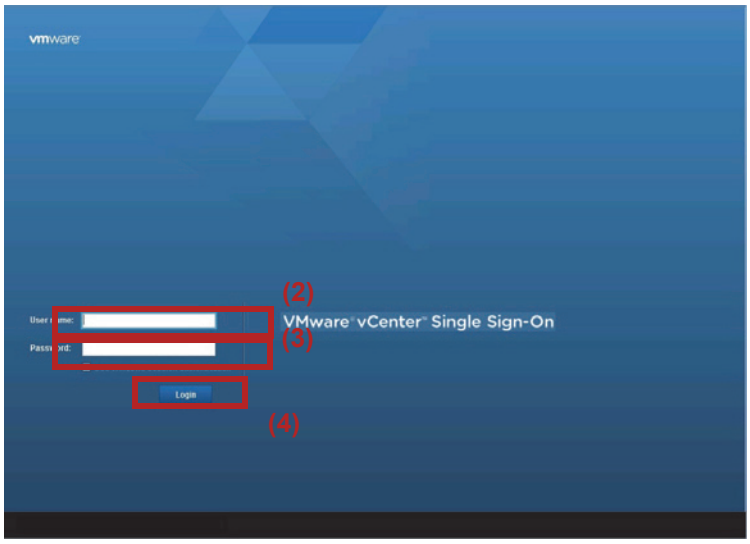
1

(1) From the web browser of the maintenance PC, log in to vCSA (https://xx.xx.xx.xx:9433/).
use the following user ID and password (below are given the examples used in 5.6 Customizing vCenter Server Appliance (vCSA) in CHAPTER 2 SETUP:

(2) User ID: **vsphere.sso**

(3) Password: **SV9500@sso**

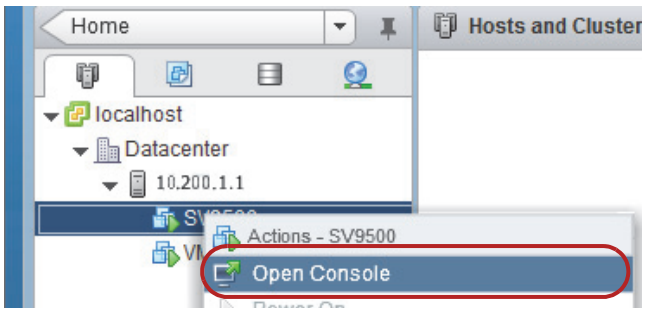
(4) Press the **Login** button.



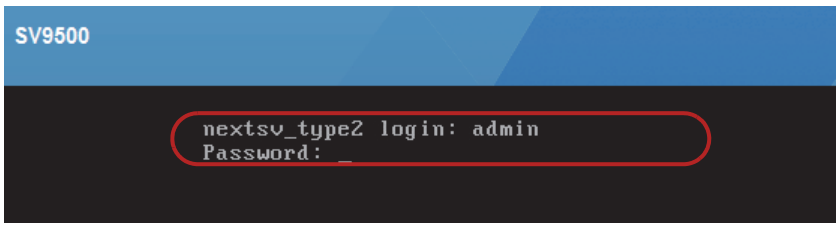
2

(1) Click [Hosts and Clusters] on [vCenter]-> [Inventory Trees] from the menu on the left side of the home screen.

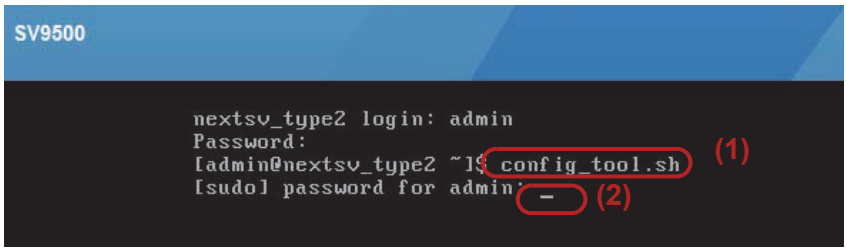
(2) Right-click on SV9500 and select Open Console.



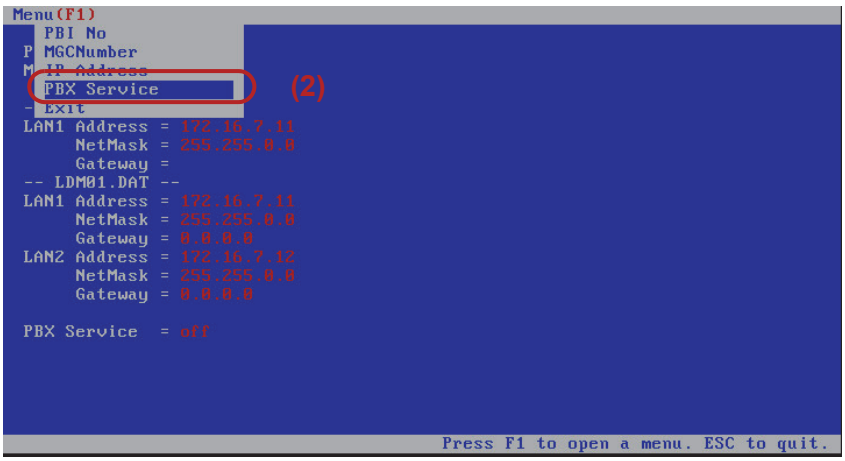
3 Log in as admin to sv9500.



4
(1) Execute “config_tool.sh”.
(2) Enter the password for admin again.

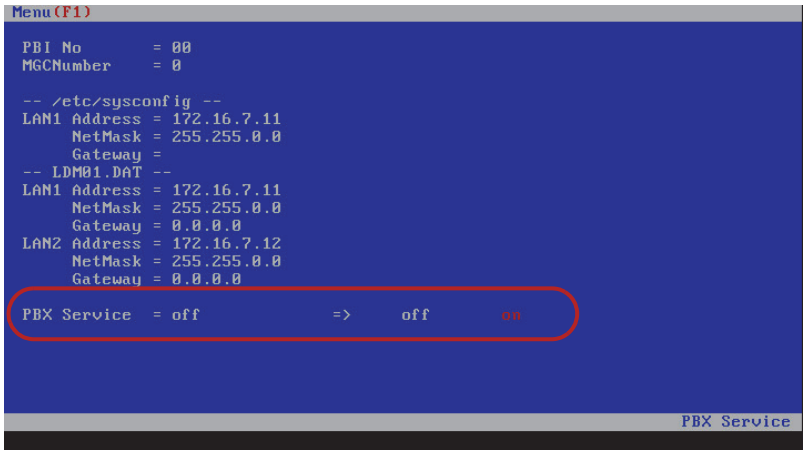


5
(1) Press **F1**.
(2) Select **PBX Service**.

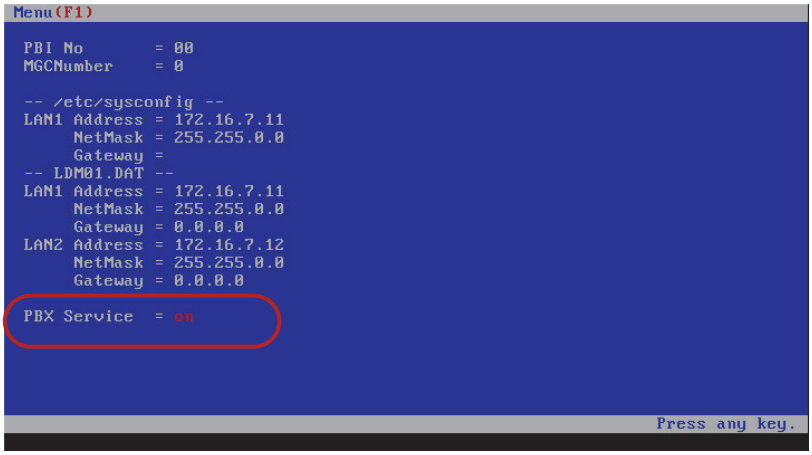


Note: Contact NEC maintenance personnel if you need to confirm your User Name and Password.

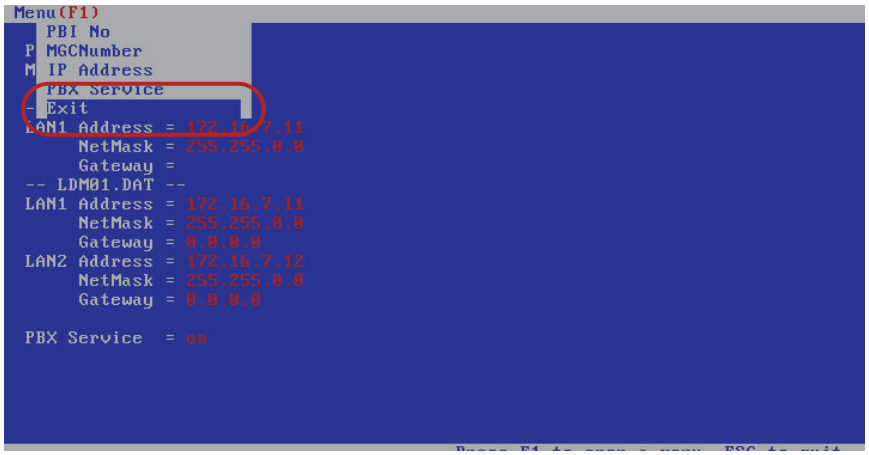
6 Select **ON** for **PBX Service**.



Verify **ON** for **PBX Service**.

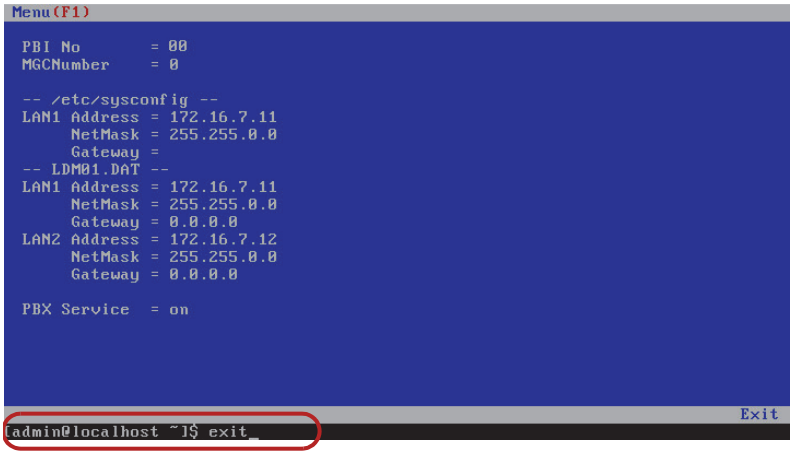


7 (1) Press **F1**.
(2) Select **Exit**.



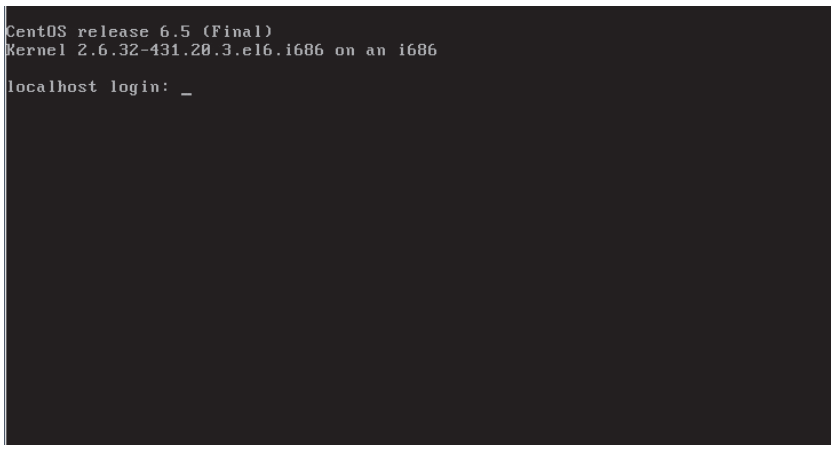
8

(1) Verify that admin@localhost is displayed.
(2) Type exit and press **Enter**.



9

After being displayed again the log in screen, close the console screen.



5.9 Switch Back

If you encounter any troubles, and you need to switch back the upgraded program to the original, follow the procedures below.

Note: After switching back, also the generated logs and the office data modified after the upgrading returns to the previous state. Before switching back, collect all the logs.

5.9.1 Switch Back

To switch back the version follow the steps below.

1 Start Internet Explorer and type “http://xxx.xxx.xxx.xxx:9801/” into the address bar.
“xxx.xxx.xxx.xxx” represents the LAN 1 IP address of the Telephony Server (ex. 10.100.1.11).

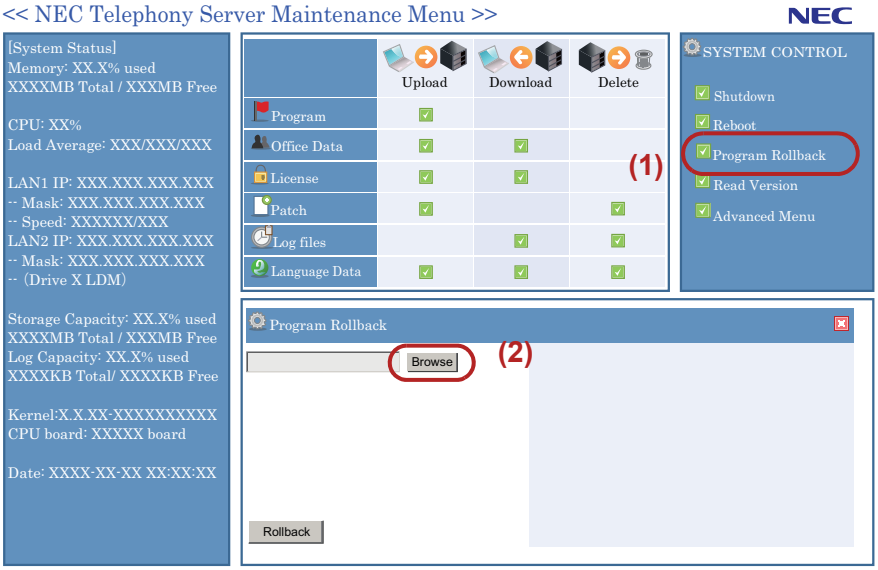
Note:
Microsoft Internet Explorer 7.0 or higher is required to access Telephony Server Maintenance Menu.

2
(1) **Telephony Server Maintenance Menu Login** screen appears. Type a user name and password.
(2) Click the **OK** button to log into **Telephony Server Maintenance Menu**.

Note:
- Contact NEC maintenance personnel if you need to confirm your User Name and Password.
- After logging into SV9500 Maintenance Menu, do not use **Back** button on a browser.

3

(1) Click the **Program Rollback** button in the **SYSTEM CONTROL** area. **Program Rollback** screen is displayed.
(2) Click the **Browse** button and select [work.zip].



4

Click **Rollback**.

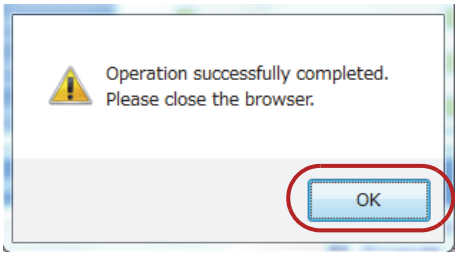
5

Click the **OK** button for the confirmation screen.

Note:
By clicking OK, the switching back and the restarting are executed.

Note: Do not perform any action until the confirmation screen is displayed.

6 Click the **OK** button for the screen reporting a successful completion.



7 Confirm that the version is correct with the same process of Checking the Version Information (Before Upgrading).

Switching back of the program is completed.

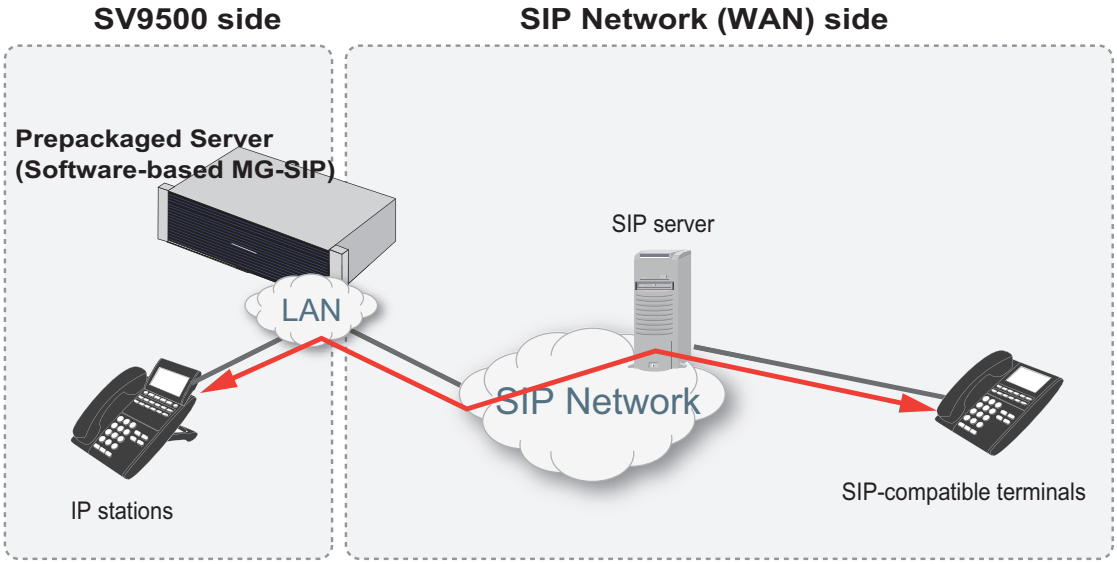
CHAPTER 4 SOFTWARE-BASED MG-SIP

This chapter describes an overview, conditions, setup procedure and operations and maintenance of Software-based MG-SIP.

1. Overview

This chapter describes an overview, conditions, setup procedures and maintenance procedures of a software-based MG-SIP. The software-based MG-SIP is application to be installed in a virtual machine on a Prepackaged Server/Prepackaged FT Server as a guest operating system (OS).

It is a software-based SIP-compatible media gateway to realize communication with service networks. MG-SIPs provides VoIP devices supporting SIP (Session Initiation Protocol, based on RFC3261) with peer-to-peer VoIP services. MG-SIPs also connects an IP station located on LAN with a SIP terminal (based on RFC3261) located on the WAN-side (SIP network) and maintain voice quality.



Note: When using video call feature (available from FP95-114 V4), refer to VIDEO CALL [V-31] in the Data Programming Manual - Business for MCU usage.

2. Conditions

Service conditions of the software-based MG-SIP are as follows:

Note: This section only describes conditions specific to the software-based MG-SIP. For general conditions on MG-SIP, see MEDIA GATEWAY SIP [M-111] in the Data Programming Manual - Business.

(1) Software-based MG-SIP is available since FP95-112 V2.

(2) Software-based MG-SIP can register to both the SV9500 Prepackaged Server Model that is installed in the same server as the MG-SIP and SV9500 Appliance Model.

Note: The registration destination SV9500 must be FP95-112 V2 or later version.

(3) The firmware version of Software-based MG-SIP is SP-4085 Issue 1.0 or later.

(4) As a tool for configuring the command data of the software-based MG-SIP, the virtual console of the guest OS (CentOS) is used instead of the conventional serial console. Though there are 6 virtual consoles (No.1 to No.6), the MG-SIP can only use a console No.1.

Note: To change the virtual console, press the Alt + F1-F6 key. For example, when the Alt + F2 key is pressed, the screen of the virtual console No.2 is displayed. This operation is used when you want to display a new screen while the original screen is being displayed. (virtual consoles No.2 to No.6 cannot be used)

(5) On a Prepackaged FT Server Model, when the primary sever fails and the secondary server becomes active during a call via the MG-SIP, a silent state for a few seconds may be generated due to the memory copy to the secondary server.

(6) SV9500 cannot detect an Ethernet link down because the software-based MG-SIP runs on the virtual machine. Alternate routing due to an Ethernet link down in the SIP network is not available.

(7) Available operation mode of the virtual console is auto negotiation only. Therefore, set “0=auto-negotiation” for the **set interface** command.

(8) Since software-based MG-SIP does not have any lamp, unlike the existing hardware-based MG-SIP, the state of the unit such as power-on/off cannot be indicated by a lamp. MG-SIP registration status can be checked with "1=IPX Status" of the **show status** command or ONLINE START/OFFLINE START message displayed on the virtual console.

(9) Software-based MG-SIP supports the firmware update only. When an update or recovery of a guest OS/other applications is required, contact the maintenance personnel.

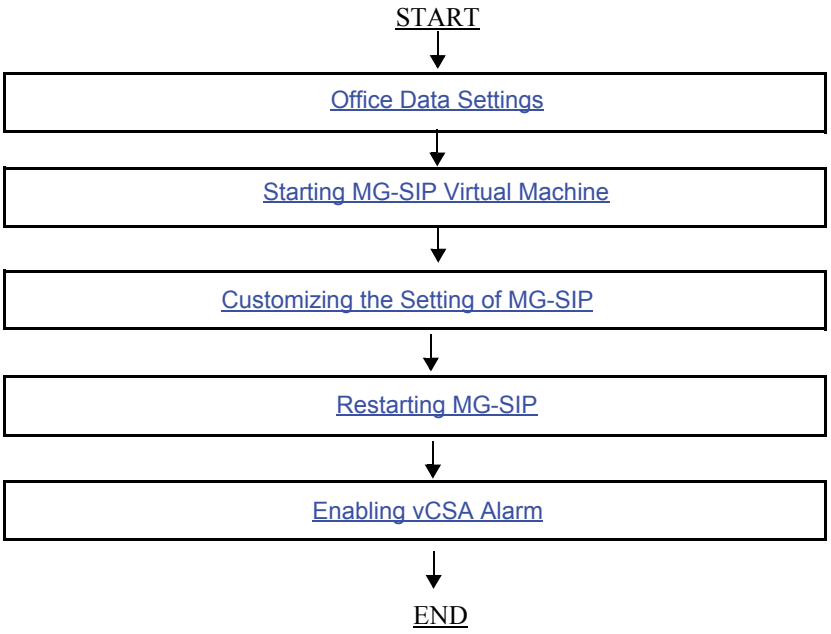
(10) An alarm can be output when a guest OS of software-based MG-SIP fails to start, stops, or is shut down. It is necessary to enable the alarm feature of vCSA (3.5 Enabling vCSA Alarm).

(11) Software-based MG-SIP acquires clock information from the SV9500 server when registering to the server. When the clock information is changed on the host (VMware ESXi), the MG-SIP needs to perform re-registration.

(12) When the SV9500 in the same server is initialized or reset, the MG-SIP will be rebooted by the health check timeout. After the rebooting, the MG-SIP can become operative.

3. Setup

This section describes the setup procedure of software-based MG-SIP. Follow the flow chart below.



3.1 Office Data Settings

Follow the steps below to turn on the system.

1 Connect to PCPro using the connection account (e.g. NewOffice#1) assigned for the IP address of LAN2 connector. Enter the user ID and the password that have been previously assigned to connect to PCPro.

2 Assign the Route Class Data for Virtual Speech Channel through the **ARTD/ARTDN** command.

(1) Enter a Route Number (1-255).
(2) Choose “MG-SIP” for Template Type.
(3) Assign the following data.

CDN	FUNC	DATA
66	DC	1-15

(4) Also, assign the following data to the dummy route.

CDN	FUNC	DATA
111	ADVPRA	1

Note: To change the data for existing route (RT), initialize or reboot the MG-SIP.

3 Assign the trunk application data for Virtual Speech Channel through the **ARTI/ARTIN** command.

(1) Assign the following data.

CDN	FUNC	DATA
47	INTD	2
68	VIR	2
77	RA_RT	0/1

(2) When using a FAX communication, assign the following data.

CDN	FUNC	DATA
71	FXD	0/1
72	FXJS	1-30
73	FXPT	0-6
74	FXPS	1-4

4 Assign a trunk data to the Virtual Speech Channel through the **ATRK** command.

RT: Specify Route Number (1-255).
PC: Specify Trunk Number (1-255).
LENS: Specify Accommodated Location (Six digits).

[Example]

RT (1-255)	TK (1-255)	LENS			
		MG 00-07	U 0-3	G 00-23	LV 0-7
10	1	01	0	00	0
:	:	:	:	:	:
10	192	01	0	23	7
10	193	01	1	00	0
:	:	:	:	:	:
10	254	01	1	07	5

Virtual Communication Channel

Note: The conditions when this command is assigned are as follows.

- Be sure to register the virtual communication channel per four groups.
- Other than MG-SIP virtual communication channel cannot be registered for HW (4 group) that is registered one or more MG-SIP virtual communication channels.
- The virtual communication channel is assigned by using the **AMGIL** command.
- Do not assign the LENS that belongs to even-numbered module group, Unit=0 and Group=0 to a trunk, because not supported by MG-SIP.

5 Assign a Point Code on the Virtual Speech Channel through the **ADPC** command.

RT: Specify Route Number (1-255).
PC: Specify unused Point Code, not Point Code used in SS7 (1-16383).

6 Assign the top number of 32-channel LENS through the **ACSC** command.
CSCG: Specify the CSC Group Number (an even number from 130 to 255)
GROUP: Specify the CIC Group Number.
CCH: Specify the lead LENS of a unit.

[Example]

CSCG	CICG	CCH		
		MG 00-07	U 0-3	G 00-23
130	0	01	0	00
	1	01	0	04
	2	01	0	08
	3	01	0	12
	4	01	0	16
	5	01	0	20
	6	01	1	00
	7	01	1	04

Note: Be sure to set the LENS of Virtual Signal Channel to the lead CIC Group Number (CICG) of each MG-SIP.

7 Activate the **ACIC1** command. Specify the accommodated location of Virtual Signal Channel on Point Code as follows:
PC: Enter Point Code specified by ADPC.
CSCG: Enter CSC group specified by ACSC.

8 Activate the **ACIC2** command. Specify the accommodated location of Virtual Control Channel on Point Code as follows:
PC: Enter Point Code specified by the **ADPC** command.
CIC: Enter CIC numbers in sequential number.
LENS: Enter accommodated locations of Speech Channel and B-Channel.

Note: Assign CIC numbers in order from “1.”

9 Execute the **MBTK** command to cancel Make Busy state of the Virtual Speech Channel.

10 Assign the necessary information data regarding to the Virtual MG-SIP through the **AMGIL** command.

MG-ID: Enter MAC Address (6 bytes)
FUNCTION = Setting
KIND = SIP-MG
LINE = 0 (fixed)
CH = 0 (fixed)
LENS: Enter Basic Accommodated Location (the first number of HW)
RETRY = 0
Service Type: Specify QoS settings of Signaling that is used when Internal PHI-BRI connects MG-SIP.
Usable CH Num: Enter the number of channels to be used per MG-SIP.
Service of Authentication exists: Select the check box if registration is required per number.
MG Group: Enter MG-SIP Group Number 1-15 to make an alternate route for redundancy configuration. **Note 1**
MG Number: Enter MG-SIP Number 1-15 belonging to the MG-SIP Group.**Note 1**

Note1: This parameter only appears if “Service of Authentication exists” check box is selected.

Note: Assign the MAC address of the Software-based MG-SIP server (LAN side) to the MG-ID parameter.

Note: Whether to use Service of Authentication is determined by the carrier’s selected services. For more information about this feature, refer to Multiple Number Service (MG-SIP) [M-113] in the Data Programming Manual.

The office data settings have been completed.

3.2 Starting MG-SIP Virtual Machine

Follow the steps below to start up the MG-SIP virtual machine.

1

(1) From the web browser of the maintenance PC, log in to vCSA (https://xx.xx.xx.xx:9433/). use the following user ID and password (below are given the examples used in 5.6 Customizing vCenter Server Appliance (vCSA) in CHAPTER 2 SETUP:

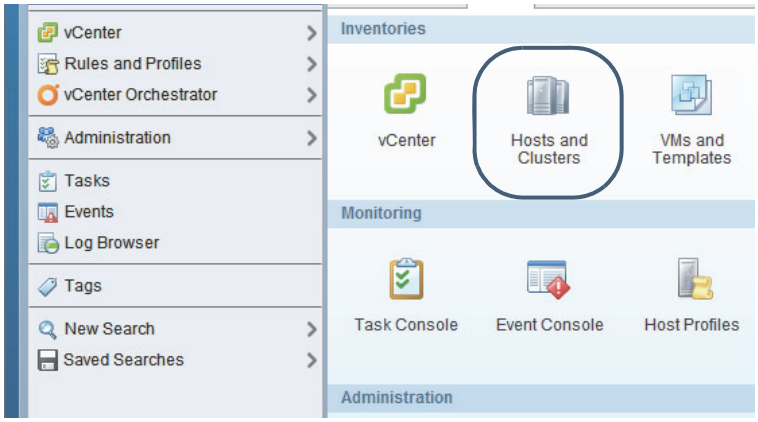
(2) User ID: **vsphere.sso**

(3) Password: **SV9500@sso**

(4) Press the **Login** button.

2

Click **Hosts and Clusters**.



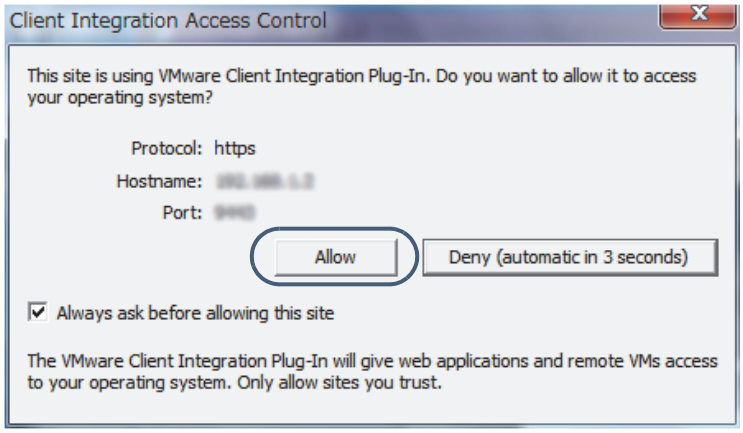
3 Save a copy of the OVF file in the maintenance PC.

(1) Right-click **SV9500** and select **Template**

(2) Select **Export OVF Template**.

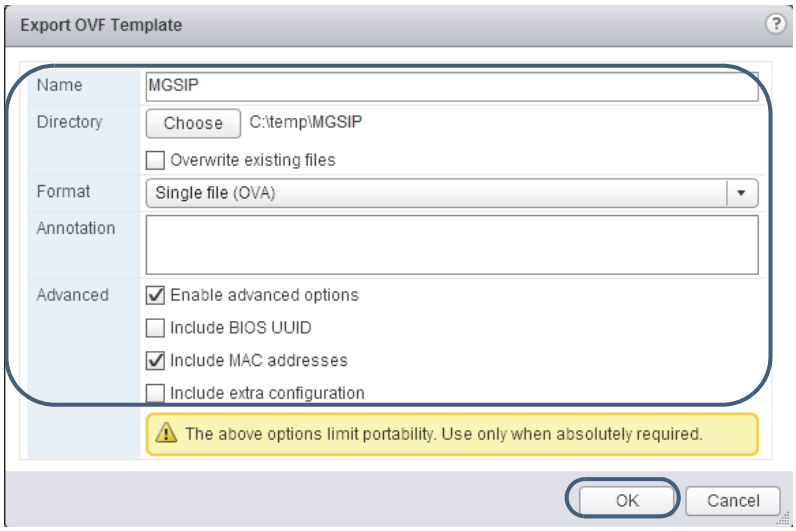
Note: When restoring the virtual machine after a failure, not only the data included in this back-up but other data for MG-SIP configuration is necessary. Periodically make a backup for this data as a text file using the “show config” command.

4 If a screen as the one below is displayed, click **Allow**. If not, go to the next step.



5 On the [Export OVF Template] screen, set the data as shown below and click [OK].

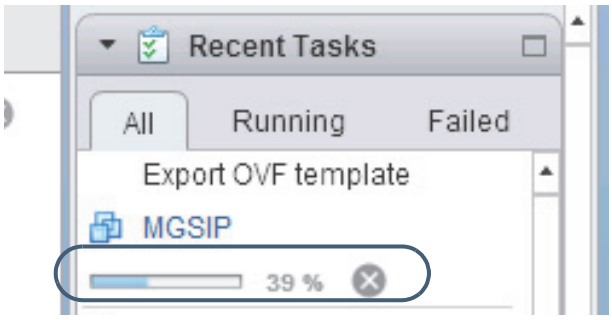
Name: Arbitrary (example: **MGSIP**)
Directory: Click the **Choose** button for the place of your selection (it points to the export destination for the OVF template)
Format: **Single file (OVA)**
Annotation: Use this space if you need to left any note (it can be left blank)
Advanced:
Enable advance options: **checked**
Include MAC address: **checked**



Note: A virtual machine usually requires around 2GB.

Note: Consult NEC maintenance personnel or your local NEC dealer in case of using a backup file because of a failure.

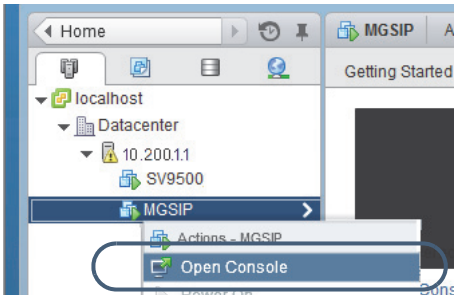
6 When **Export OVF template** reaches 100% in the **Recent Tasks** column, the exporting is concluded.



Note: The OVF template is exported to the client PC of vSphere Web Client. Make sure that the PC has enough storage capacity. Also, the exporting process may require some time, therefore make sure that the PC can be used as long as needed.

7 Right-click the MG-SIP virtual machine from the menu on the left side of the screen. Choose **Power** -> **Power On**.

8 Right-click the MG-SIP virtual machine from the menu on the left side of the screen. Choose **Open Console**.



9 “mgsip login:” appears on the console screen.

```
mgsip login:
```

The start-up of the MG-SIP virtual machine has been completed.

3.3 Customizing the Setting of MG-SIP

Follow the steps below to change the settings of MG-SIP virtual machine.

1 After starting the MG-SIP virtual machine, type “config” as login name and press Enter key.

```
mgsip login : config
```

2 The prompt “MG(SIP) > appears on the screen.

```
mgsip login : config
MG(SIP)>
```

3 Execute the **set default** command to initialize the settings. Type “y” for **Are you sure? Y/N=**.

```
MG(SIP)> set default
Are you sure? Y/N=y
Config data default set.
```

4 Execute the **set config _template** command to collectively set the standard data.

(1) Select the pattern of template for **Input template pattern. (0-255)**.

(2) Enter “y” for **Are you sure? Y/N=**.

```
MG(SIP)> set config_template
Input template pattern. (0-255)  : 1
Are you sure? Y/N=y
Selected template is set.
```

Note: When there is no template data for the entered number, “Not used” is displayed.

5 Execute the **set ipaddress** command to set an IP address of the MG-SIP.

(1) When using 2 ports, enter “n” for **Do you use one-port only? Y/N=**.

(2) Enter IP addresses and subnet masks of Ether1 and Ether2.

```
MG(SIP)> set ipaddress
Do you use one-port only? Y/N= n
Ether[1]
Input IP Address. (default=0.0.0.0)
          : 172. 16. 0. 1
Input Subnet mask. (default=0.0.0.0)
          : 255. 255. 255. 0
Ether[2]
Input IP Address. (default=0.0.0.0)
          : 172. 16. 1. 2
Input Subnet mask. (default=0.0.0.0)
          : 255. 255. 255. 0
```

Note:

- When using Ether1 (LAN side) only, enter "y" for **Do you use one-port only? Y/N=**.
- With **one-port only** enabled, Ethernet Port Redundancy function can be used. For an explanation of the Ethernet Port Redundancy function, see the ipaddress command in Set command section of Chapter 2 of Software Model Peripheral Equipment Description.
- When using PPPoE, be sure to use 2 ports. In this case, an IP address obtained from the PPPoE server is automatically set as Enter2 IP address.
- If you set a non-default port number, be careful not to choose the same number set in other port numbers (set by "set sip_rtp_port_no", "set ipx_rtp_port_no", "set sip_media_port_no", "set ipx_media_port_no", "set registration_port_no", "set signaling_port_no", "set pre_negotiation_port_no", "set sip_port_no" commands).
  When the same port number is set, a warning message is displayed.
  Set the routing information data through the **ipx_route** command as necessary.

6 Execute the set drsaddress command to set IP address of the SV9500 server LAN1.

(1) Enter an IP address of the SV9500 server LAN1 for "Input IP address. (default=0.0.0.0)".

(2) Enter a port number for "Input Port Number. (1024-65535 (default=3456)".

```
MG (SIP) > set drsaddress
[Primary DRS Setting]
Input IP address. (default=0.0.0.0)
          : 172.16.253.1
Input Port Number. (1024-65535 (default=3456)
          : 3456
[Secondary DRS Setting]
Input IP address. (default=0.0.0.0)
          : 0.0.0.0
Input Port Number. (1024-65535 (default=3456)
          : 3456
[Tertiary DRS Setting]
Input IP address.  (default=0.0.0.0)
          : 0.0.0.0
Input Port Number.  (1024-65535 (default=3456)
          : 3456
[Quaternary DRS Setting]
Input IP address.  (default=0.0.0.0)
          : 0.0.0.0
Input Port Nunber.  (1024-65535 (default=3456)
          : 3456
```

7 Execute the Select SIP server type. command to set an IP address of the SIP server or FQDN.

(1) When "0" is entered in the above step, enter IP address and port number.

(2) When "1" is entered in the above step, enter FQDN and port number.

```
MG(SIP) > set sip_server
Select SIP server type.
0=IPAddress(default)
1=FQDN
Input:0
Input SIP server IP Address.(default=0.0.0.0)
                          :192.168.100.100
Input SIP server Port Number.
(1024-65535(default=5060)):5060
```

(3) Enter "0" or "1" for **Select SIP server Router type**.
When proxy server is a strict router, enter 0. When using loose router, enter "1".

```
Select SIP server Router type.
0=Strict(default)
1=Loose
Input:0
```

(4) Input a string that specifies the service provider in maximum of 128 characters.

```
Input Domain Name.(default=0, MAX128(strings))
```

Note: If you have set a character string to specify the service provider, the character string is used as the SIP domain name.

Note: Be sure not to enter a blank character to the end of the FQDN (with the Copy and Paste features of your personal computer), and be careful not to mistype a character. (“0”(zero) or “O” (alphabetical O), for example.)

8 Execute the **set keynumber** command to set a pilot number of the MG-SIP.

```
MG(SIP)> set keynumber
Input Keynumber.(default=0, MAX32(strings))
              :0
```

3.4 Restarting MG-SIP

Follow the steps below to restart the MG-SIP virtual machine.

1 Execute the reboot command to restart the MG-SIP after saving the configuration data.

(1) Enter "y" for **Do you want to save Config data? Y/N=**.
(2) Enter "y" for **Do you want to reboot MG(SIP)? Y/N=**.

```
MG(SIP)> reboot
Do you want to save Config data? Y/N=y
Do you want to reboot MG(SIP)? Y/N=y
Config data File write start.
Config data File write end.
MG(SIP)reboot start...
```

Note: Before selecting "y" to save the running configuration data to the flash memory, be sure to execute the following commands:

- set ipaddress (Assign the IP addresses for LAN network side and SIP network side)
- set drsaddress (Assign the IP address of the SV9500 server)
- set sip_server (Assign the IP address of the SIP proxy server)
- set keynumber (Assign a pilot number.)

If any of these items have not been assigned when saving the running configuration data, the following message will be displayed to the unassigned item. When these messages are displayed, you can select if you want to set the default configuration data or not. If you select "y" here, the default values are applied to the configuration data.

```
The following setting commands are not perfect.
"set ipaddress" command.(IPX side)
"set ipaddress" command.(SIP side)
"set drsaddress" command.
"set sip_server" command.
"set keynumber" command.
So, Config data is made a default setup.
Is it all right? Y/N=y
```

2 After the MG-SIP is rebooted, the following message appears on the screen.

```
mgsip login:
```

3.5 Enabling vCSA Alarm

Follow the steps below to enable the vCSA alarm.

1

(1) From the web browser of the maintenance PC, log in to vCSA (https://xx.xx.xx.xx:9433/). use the following user ID and password (below are given the examples used in 5.6 Customizing vCenter Server Appliance (vCSA) in CHAPTER 2 SETUP:

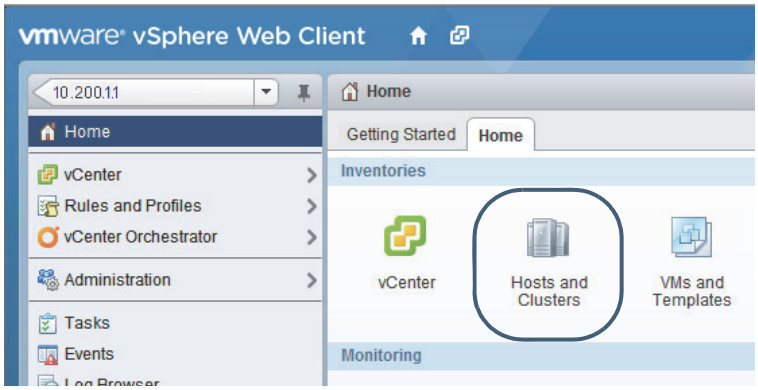
(2) User ID: **vsphere.sso**

(3) Password: **SV9500@sso**

(4) Press the **Login** button.

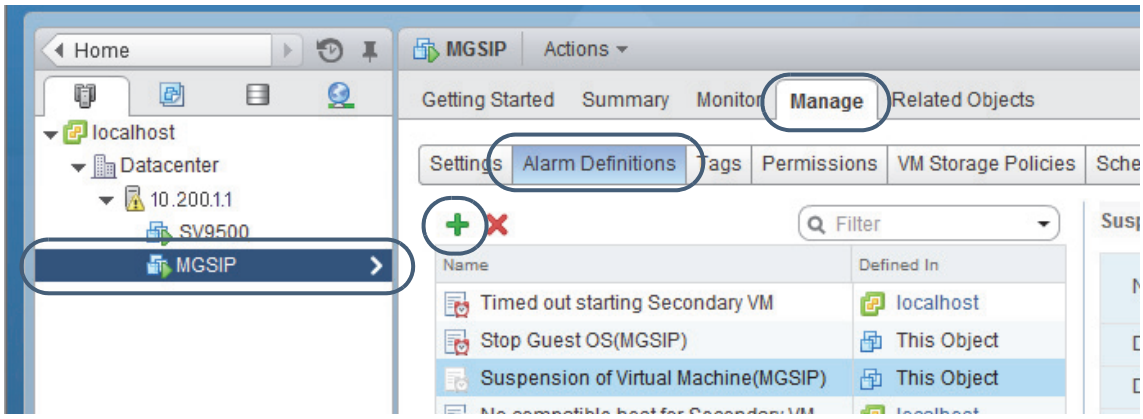
2

Click **Hosts and Clusters**.



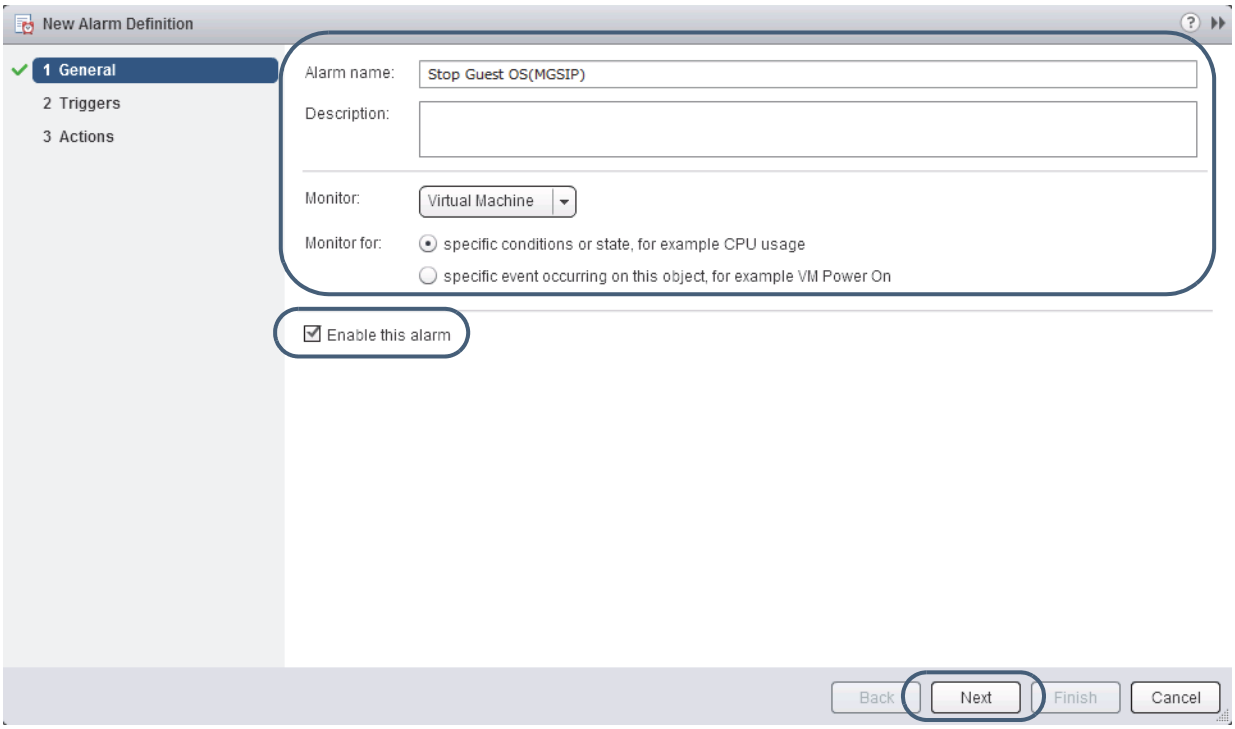
3

(1) Click the MG-SIP virtual machine.
(2) Click **Manage** tab.
(3) Click **Alarm Definitions**.
(4) Click [+] icon.



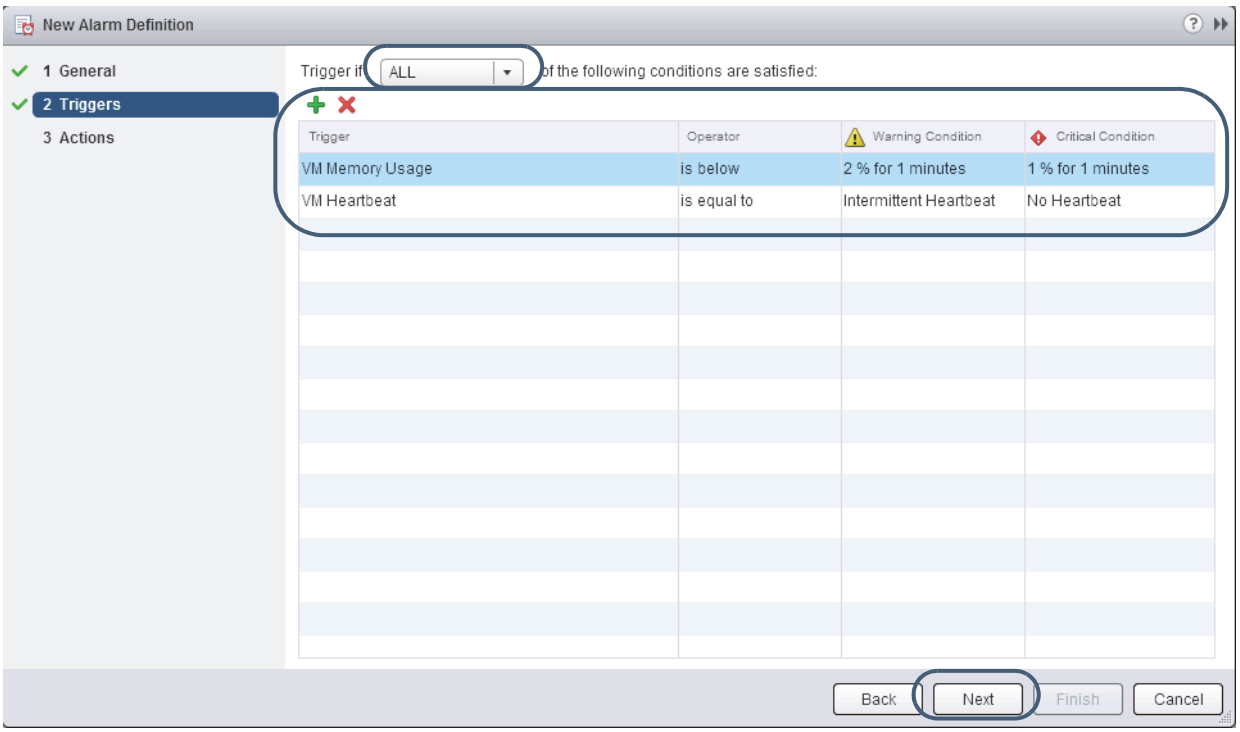
4

(1) The **New Alarm Definition** screen appears. Set the following:
Alarm Name: Stop Guest OS(MGSIP)
Description: blank
Monitor: Virtual Machine
Monitor for: specific conditions or state, for example CPU usage
(2) Click **Enable this alarm**.
(3) Click **Next** button.

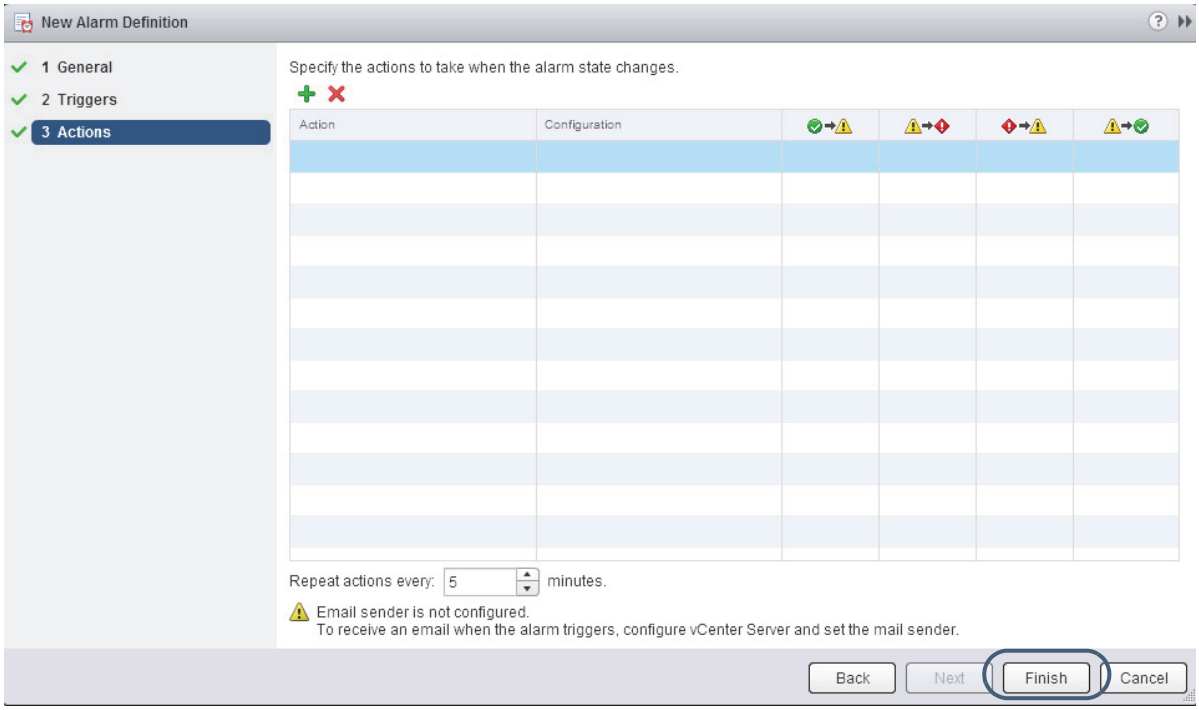


5

(1) The screen shown below appears. Select **ALL** (Trigger if **All** of the following conditions are satisfied:)
(2) Click [+] icon and set the following:
Trigger: VM Memory Usage
Operator: is below
Warning Condition: 2% for 1 minutes
Critical Condition: 1% for 1 minutes
(3) Click [+] icon again and set the following:
Trigger: VM Heartbeat
Operator: is equal to
Warning Condition: Intermittent Heartbeat
Critical Condition: No Heartbeat
(4) Click the **NEXT** button.



6 The screen changes as follows. Leave the default settings and click the **Finish** button.

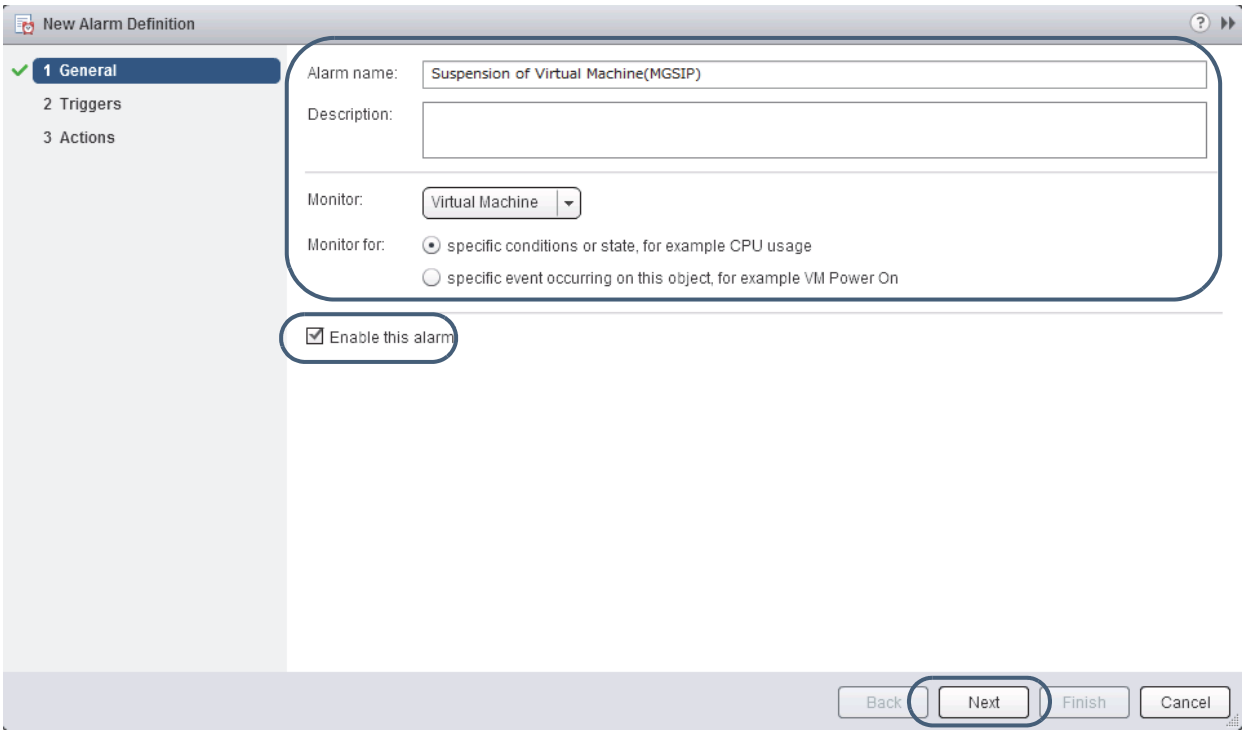


7 The screen returns to Alarm Definition. Click [+] icon again.

8 The screen shown below appears. Set the following:

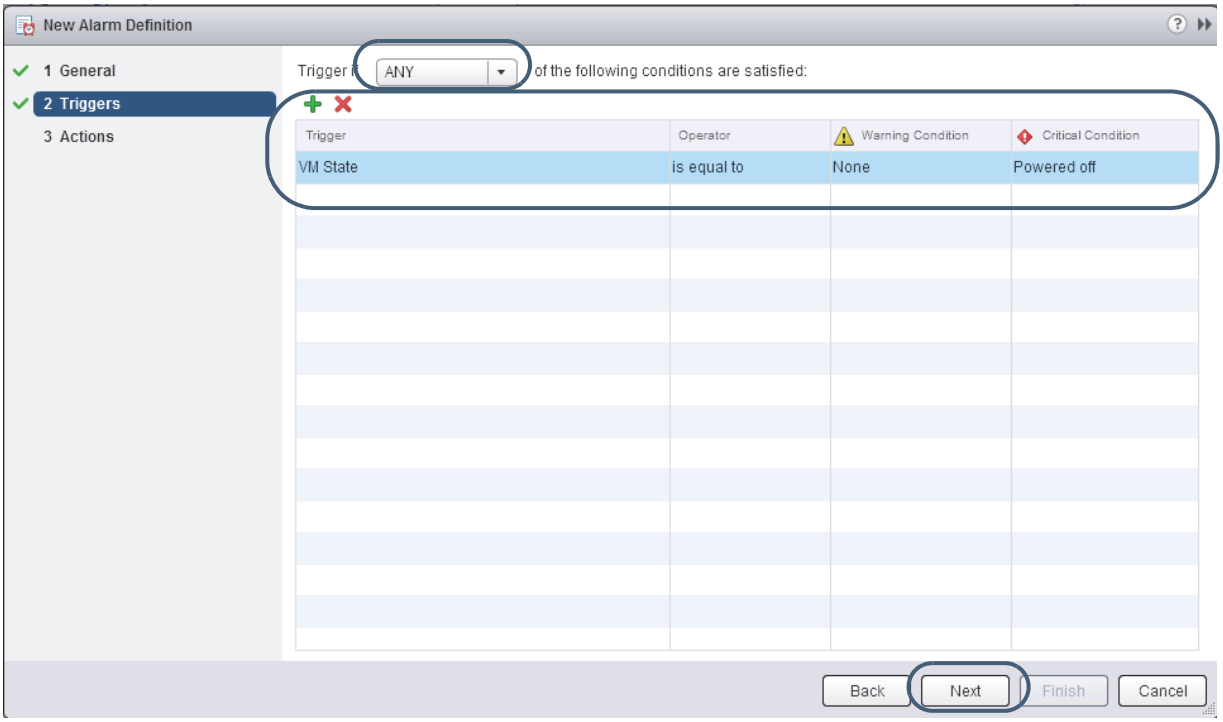
Alarm Name: Suspension of Virtual Machine (MGSIP)
Description: blank
Monitor: Virtual Machine
Monitor for: specific conditions or state, for example CPU usage

(5) Click **Enable this alarm**.
(6) Click **Next** button.



9

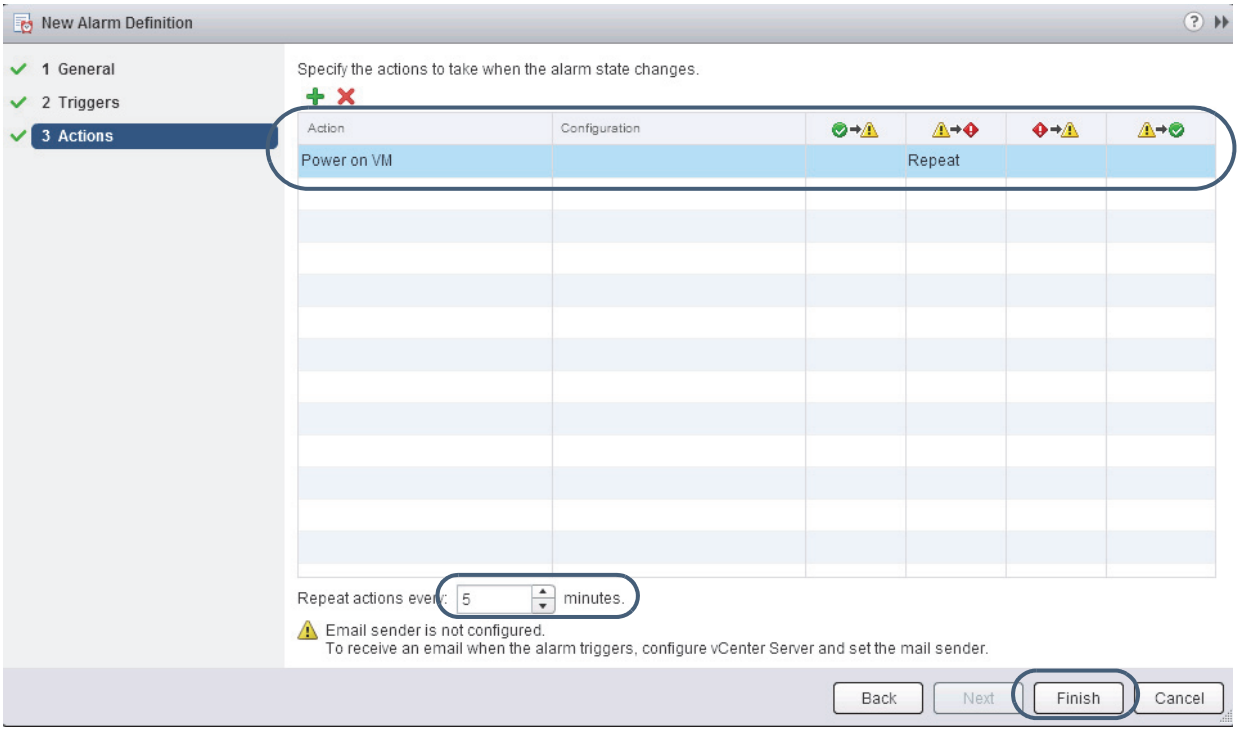
(1) The screen shown below appears. Select **ANY** (Trigger if **ANY** of the following conditions are satisfied:)
(2) Click [+] icon again and set the following:
Trigger: VM State
Operator: is equal to
Warning Condition: None
Critical Condition: Power off
(3) Click the **NEXT** button.



10

(1) The screen shown below appears. Click [+] icon and set the following:
Action: Power on VM
Configuration: (blank)
: (blank)
: **Repeat**
: (blank)
: (blank)
Repeat actions every: 5 minutes.

(2) Click the **Finish** button.



11

Right-click the MG-SIP virtual machine and select **Alarm** -> **Enable Alarm Activations**.

Note: This step is not necessary if Enable Alarm Activations cannot be selected.

4. Maintenance

4.1 Connecting to MG-SIP Virtual Console

Follow the steps below to connect to the MG-SIP virtual console.

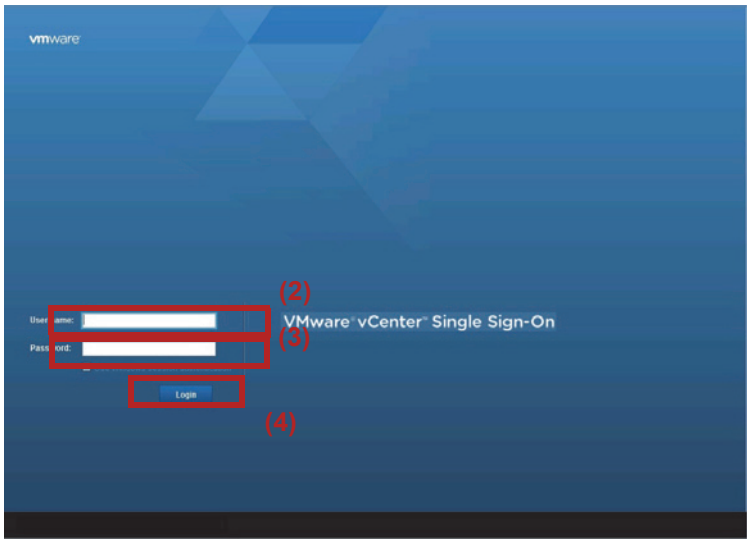
1

(1) From the web browser of the maintenance PC, log in to vCSA (https://xx.xx.xx.xx:9433/). use the following user ID and password (below are given the examples used in 5.6 Customizing vCenter Server Appliance (vCSA) in CHAPTER 2 SETUP:

(2) User ID: **vsphere.sso**

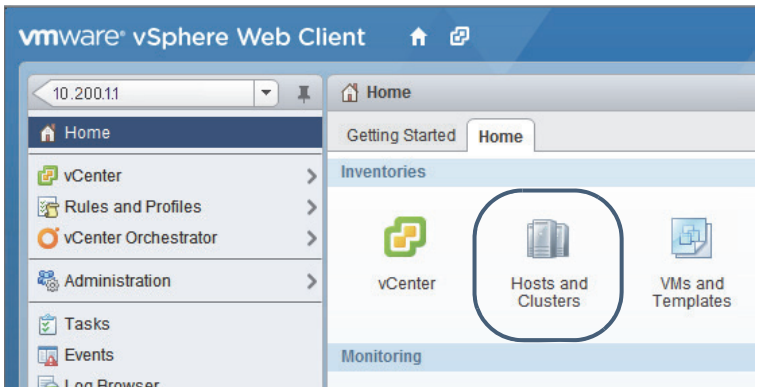
(3) Password: **SV9500@sso**

(4) Press the **Login** button.

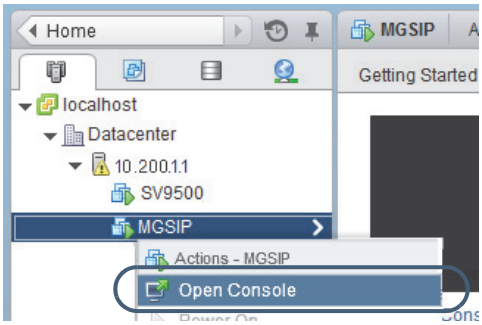


2

Click **Hosts and Clusters**.



3 Right-click the MG-SIP virtual machine from the menu on the left side of the screen. Choose **Open Console**.



4 "mgsip login:" appears on the console screen.

```
mgsip login:
```

5 After starting the MG-SIP virtual machine, type "config" as login name and press Enter key.

```
mgsip login : config
```

6 The prompt "MG(SIP) > appears on the screen.

```
mgsip login : config
MG(SIP)>
```

4.2 Rebooting MG-SIP

Basically, when rebooting the MG-SIP virtual machine, use virtual console. When virtual console cannot be used, reboot vSphere Web Client through the vSphere Web Client.

Note: When restarting the MG-SIP using vSphere Web Client, the configuration data will not be saved. When the data saving is necessary, be sure to use virtual console to save the data.

Note: During restarting of the MG-SIP, an alarm “Stop Guest OS(MGSIP)” may be detected. In that case, after an elapse of one minute of the restarting, update the display of vSphere Web Client and confirm that the alarm disappears.

4.2.1 Rebooting MG-SIP with Virtual Console

1 Log in with config user. (see 4.1 Connecting to MG-SIP Virtual Console.)

2 Execute the reboot command and save the configuration data.
Reboot the MG-SIP.
(1) Enter “y” for **Do you want to save Config data? Y/N=**.
(2) Enter “y” for **Do you want to reboot MG(SIP)? Y/N=**.

```
MG(SIP)> reboot
Do you want to save Config data? Y/N=y
Do you want to reboot MG(SIP)? Y/N=y
Config data File write start.
Config data File write end.
MG(SIP)reboot start...
```

3 After the reboot, the following prompt appears.

```
mgsip login:
```

4 Enter “config” as login name and press the Enter key.

```
mgsip login:config
```

Check that the prompt “MG(SIP) > appears on the screen.

```
mgsip login:config
MG(SIP)>
```

4.2.2 Rebooting MG-SIP with vSphere Web Client

1

(1) From the web browser of the maintenance PC, log in to vCSA (https://xx.xx.xx.xx:9433/). use the following user ID and password (below are given the examples used in 5.6 Customizing vCenter Server Appliance (vCSA) in CHAPTER 2 SETUP:

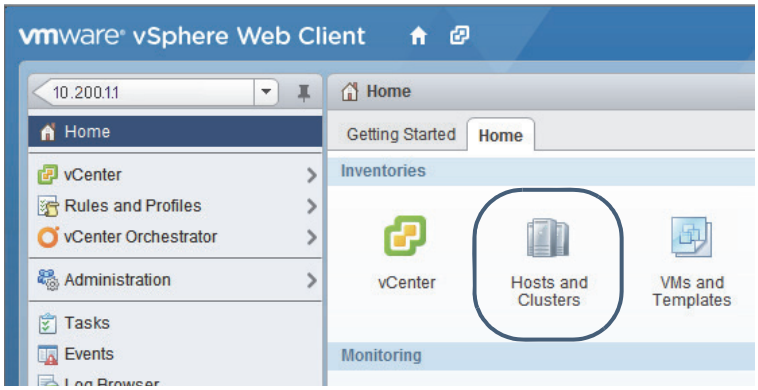
(2) User ID: **vsphere.sso**

(3) Password: **SV9500@sso**

(4) Press the **Login** button.

2

Click **Hosts and Clusters**.



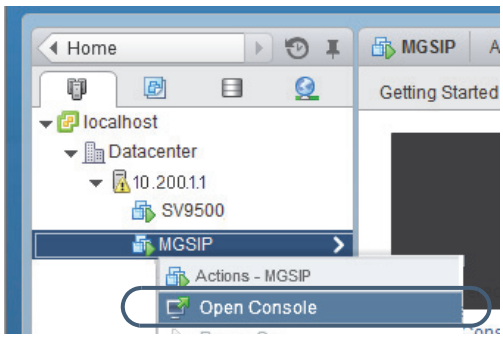
3

Right-click the MG-SIP virtual machine from the menu on the left side of the screen. Choose **Power** -> **Restart Guest OS**.

4

Transmit a Ping command from the maintenance console to IP addresses of Ether1 and Ether2 of the MG-SIP. Confirm its response.

5 Right-click the MG-SIP virtual machine from the menu on the left side of the screen. Choose **Open Console**.



6 After the reboot, the following prompt appears.

```
mgsip login:
```

7 Enter “config” as login name and press the Enter key.

```
mgsip login : config
```

Check that the prompt “MG(SIP) > appears on the screen.

```
mgsip login : config
MG(SIP)>
```

4.3 Configuration Commands

For an explanation of configuration commands, see the Configuration Commands section of Chapter 2 in Software Model Peripheral Equipment Description.

APPENDIX A
LICENSE FOR SV9500 (PREPACKAGED SERVER MODEL)

1. License File for SV9500 (Prepackaged Server Model)

An Activation Code for SV9500 (Prepackaged Server Model) is calculated based on the IP address (IPv4) of LAN1 (ACT). Keep the Certify Status in the AACT command at "Certify OK". When the Certify Status is "Certify NG", the PCPro connection restriction will be implemented (you will be locked out of the MAT). Certify Status of the license can be checked by using the AACT command.

[Conditions subject to PCPro connection restriction]

PCPro connection is restricted in the following cases:

(a) Initial Startup

When SV9500 (Prepackaged Server Model) is started up with factory default settings, PCPro connection is not in a restricted state. Certify Status becomes "Certify NG (A.C)" when SV9500 (Prepackaged Server Model) is started up with a license file that has been downloaded from the License Management Server (https://eip.necunified.com/login.aspx).

Solution: Register an Activation Code. For more information, see 4.3 Registration of Activation Code in Chapter 2.

(b) License Update

Certify Status becomes "Certify NG (A.C)" when the license information is updated (for example, due to an increase in number of clients).

Solution: Register an Activation Code. For more information, see 4.3 Registration of Activation Code in Chapter 2.

(c) Change of IP address (IPv4) of LAN1 (ACT)

Certify Status becomes "Certify NG (HKC)" when the IP address (IPv4) of LAN1 (ACT) is modified.

Solution: Visit the License Management Server (LMS) (https://eip.necunified.com/login.aspx) and update LMS with the new IP Address information and obtain a new Activation Code.

Note: Be sure that LMS has been updated with the current LAN1(ACT) IP Address.

(d) Loading office data

The Activation Code registered with the AACT command is stored in the office data. Certify Status may become "Certify NG (A.C)" when:

- the office data was saved before the AACT command was assigned, or
- the office data of another node has been loaded

Solution: Register an Activation Code. For more information, see 4.3 Registration of Activation Code in Chapter 2.

[Solutions when PCPro connection is restricted]

(a) Certify NG (HKC)

Before performing this procedure, ensure that the IP address (IPv4) of LAN1 (ACT) is modified to the one used for the actual environment. If the IP address (IPv4) of LAN1 (ACT) is modified after the Certify Status shows "Certify OK", a new Activation Code will be required.

Visit the License Management Server (LMS) (https://eip.necunified.com/login.aspx) and obtain a new Activation Code.

(b) Certify NG (A.C)

Before performing this procedure, ensure that the IP address (IPv4) of LAN1 (ACT) is modified to the one used for the actual environment. If the IP address (IPv4) of LAN1 (ACT) is changed after the Certify Status shows "Certify OK", an Activation Code is required to be registered again.

Step1: Select **Confirm License Data and Create File** in the AACT command and click the **GET** button. A list of Hardware Keycodes and Software Keycodes are displayed.

Step2: Click the **File Save** button and save the Keycode file "KEYCODE.ACT" on your PC.

Step3: Visit the License Management Server (LMS) (https://eip.necunified.com/login.aspx) and register the saved Keycode file. Also, update LMS with the new IP Address information, if needed and obtain a new Activation Code.

Note: Note: Be sure that LMS has been updated with the current LAN1(ACT) IP Address.

Step4: Select **Register Activation Code** in the AACT command and click the **GET** button. Enter the Activation Code and click the **SET** button. The registration is completed when Certify Status shows "Certify OK".

[Temporary measures when PCPro connection is restricted]

PCPro connection restriction due to "Certify NG" status can be temporarily released for seven days (168 hours). This cancellation is allowed only once. Seven days after this cancellation, PCPro connection restriction is in effect again until registration of the Activation Code has been completed.

Step1: In the PCPro tool bar, select System, then Activate.

Step2: Select the AACT command and press Execute.

Step3: Select Confirm License Data and Create File and then press Get.

Step4: Select File Save and save the KeyCode.act file to your PC.

Step5: Close the AACT command.

Step6: From the same Activate screen in Step 1, select the AONE command and press Execute.

Step7: Open the KeyCode.act file from Step 4.

Step8: Copy and paste the first Software Key Code from the file into the AONE command and press Set.

Step9: Verify you receive the Certify OK confirmation message.

Step10: Close the AONE command and the Activate screen.

Step11: SV9500 in now temporarily unlocked.

[Limitations]

If Certify Status changes from “Certify OK” to “Certify NG” due to the modification of the IP address (IPv4) of LAN1 (ACT) or a license file, PCPro connection will not be restricted immediately. PCPro connection restriction is applied at the following times:

- After power off and on or initialization of SV9500
- After entering an incorrect Activation Code with the AACT command
- At midnight (00:00 a.m.)

UNIVERGE SV9500
Prepackaged Server Model Installation and Operation Manual

NWD-170371-001

Revision Sheet

V5: DATE OCTOBER, 2017

Chapter 2
42,90

Chapter 3
146,147

V4: DATE MARCH, 2017

Chapter 1
26

V4: DATE OCTOBER, 2016

Chapter 1
21, 22, 23, 24, 25, 28

Chapter 2
34, 35, 42, 43, 48, 49, 52, 53, 54, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 76, 78, 79, 80, 82, 86, 87, 91, 96, 110, 111

Chapter 3
130, 135, 144, 146, 152, 155, 156, 167, 168, 169, 172, 175

Chapter 4
180, 181, 183, 185, 186, 187, 188, 189, 190, 191, 192, 193, 195, 196, 197, 204, 206, 207, 208, 209

V3: DATE JUNE, 2016

Chapter 1
11, 13, 21, 22, 23, 24

Chapter 2
33, 34, 41, 58, 64, 81, 82, 83, 124

Chapter 4
153, 154, 159, 162, 163, 164, 166

V2: DATE MARCH, 2015

REGULATORY NOTICE
2, 9, 10, 11, 12

Chapter 1
3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 22, 23, 24, 25, 26, 27

Chapter 2
31, 33, 35, 90, 91, 92, 99, 102, 110, 112, 113

Chapter 4
152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180

APPENDIX C
229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 290, 291, 292, 293, 300, 301, 302, 303, 304, 305, 306, 308, 309, 311, 313, 314, 316, 317, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330 331, 332, 333, 336, 337

APPENDIX D
338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365
366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 398, 399, 400, 401, 406, 408, 409, 410, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 425, 426, 428, 429, 430, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 445, 446, 448, 449, 450, 451, 452, 453, 454, 455

APPENDIX E
456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482