NSFOCUS RSAS
Installation Guide

Version: V6.0R04F04 (2024-06-30)

Confidentiality: RESTRICTED

■ Statement

The purchased products, services, or features are stipulated in the contract made between NSFOCUS and the customer. Part of products, services, and features described in this document may not be within the purchased scope or the usage scope.

All information in this document is provided "AS-IS" without guarantees of any kind, express or implied. The information in this document is subject to change without notice. It may slightly differ from the actual product due to version upgrade or other reasons.

■ Disclaimer

Please read the disclaimer carefully before using the product. Once you use the product, you acknowledge and agree to all the contents of this disclaimer. NSFOCUS shall not assume any responsibility for any loss or damage in the following circumstances:

- Data loss and system availability reduction caused by the negligence or misconduct of the system O&M or management personnel, for example, they do not handle alerts that affect system stability and availability in a timely manner.
- Data loss and system availability reduction caused by the fact that the traffic exceeds the planned hardware capacity.
- Data loss and system availability reduction or unavailability caused by natural disasters (including but not limited to floods, fires, and earthquakes) or environmental factors (including but not limited to network disconnection and power outage).

Contents

Preface

This document describes the installation procedure of NSFOCUS Remote Security Assessment System (RSAS), including its hardware edition and virtual edition (vRSAS).

The product information involved in this document may slightly differ from your product to be installed because of version upgrades or other reasons.

Organization

Chapter	Description
1 Product Overview	Provides basic information about RSAS.
2 Installation Procedure	Describes the installation procedures of the hardware edition and virtual edition of RSAS.
3 Initial Login	Provides instructions for initial configuration of RSAS.
ADefault Parameters	Provides default parameters of RSAS.

Change History

Version	Description
V6.0R04F04	First release.

Conventions

Convention	Description
Bold font	Keywords, names of screen elements like buttons, drop-down lists or fields, and user-entered text appear in bold font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in italic font.
Note	Reminds users to take note.
Tip	Indicates a tip to make your operations easier.

Convention	Description
Caution	Indicates a situation in which you might perform an action that could result in equipment damage or loss of data.
Warning	Indicates a situation in which you might perform an action that could result in bodily injury.
A > B	Indicates selection of menu options.

Technical Support

Hardware and Software Support

Email: support@nsfocusglobal.com

Cloud Mitigation Support

Email: cloud-support@nsfocusglobal.com

Phone:

- USA: +1-844-673-6287 or +1-844-NSFOCUS
- UK: +44 808 164 0673 or +44 808 164 0NSF
- Australia: +61 2 8599 0673 or +61 2 8599 0NSF
- Netherlands: +31 85 208 2673 or +31 85 208 2NSF
- Brazil: +55 13 4042 1673 or +55 13 4042 1NSF
- Japan: +81 3-4510-8673 or +81 3-4510-8NSF
- Singapore: +65 3158 3757
- Hong Kong: +852 5803 2673 or +852 5803 2NSF
- Middle East: +973 1619 7607

Documentation Feedback

For any query regarding the usage of the documentation, you can contact us:

Email: info-support@nsfocus.com

1 Product Overview

Based on years of practical experience in vulnerability discovery, configuration checking, and security services, NSFOCUS has developed RSAS, a next-generation vulnerability scanning and configuration management product.

This chapter provides basic information about RSAS. It contains the following sections:

Section	Description
Product Characteristics	Describes characteristics of RSAS.
Main Functions	Describes major functions of RSAS.
Typical Deployment	Describes deployment modes supported by RSAS.

1.1 Product Characteristics

As a next-generation vulnerability scanning and configuration management product, RSAS can fully detect vulnerabilities on the network, enabling users to quickly identify potential cyber risks.

All-Round Detection of Vulnerabilities

RASA can comprehensively detect vulnerabilities in IT systems. For example, it can detect security vulnerabilities in the target hosts, security configuration defects, web application vulnerabilities, weak passwords, and code defects and identify accounts, services, and ports that should not be opened in the system.

Graphic Display of Vulnerabilities

By means of NSFOCUS's proprietary security risk calculation method, RSAS analyzes various vulnerabilities on the network and evaluates the risks, provides an overall security status assessment, and comprehensively presents security risks in the information system, forming a complete security risk report. This helps the administrator to discover vulnerabilities earlier than attackers and fix the vulnerabilities timely.

The analysis result is displayed on the dashboard from perspectives of the risk area, type, and severity. As a result, you can comprehensively know the security risks, focus on critical areas and assets, and fix serious vulnerabilities first. Clicking the risk data on the dashboard helps you to locate vulnerabilities of an IP address.

Clear Asset Management

RSAS manages assets, which are uniquely identified with IP addresses, by using the risk view, in which the system and network security status is visualized in real time. When deploying RSAS, users could define a logical network structure in advance to manage risks by using either the asset view or the asset repository automatically generated from assessment tasks.

Asset management includes the following:

- When performing a scanning task, RSAS automatically detects IP addresses on the network and updates asset information to the asset repository.
- You can search the asset repository for the status of network assets.
- RSAS determines the risk level based on the risk score, which is calculated with the criticality of assets in the asset repository taken into account.
- When generating a report, RSAS locates the matched assets for each IP address. Then it reads and displays the node name and node administrator. In this manner, when a vulnerability is found in a node, the related node administrator can promptly identify the vulnerable asset and ask the asset owner to immediately fix the vulnerability.

Diversified Vulnerability and Configuration Databases

NSFOCUS boasts a professional security research team, NSFOCUS Security Team, with full-time researchers for vulnerability tracking and prospective study. The team has independently found over 40 vulnerabilities in common images, operating systems, databases, and network devices and been providing vulnerability-related rule support for world-famous network security vendors. NSFOCUS Security Team is responsible for maintaining the vulnerability database and detection rules and performing an upgrade every two weeks. In addition, for major vulnerabilities, the team can upgrade the vulnerability database and detection rules within two days after they are first detected.

Taking advantage of NSFOCUS Security Team's research accumulation, the RSAS knowledge base has over 270,000 vulnerabilities, covering all mainstream underlying systems, application systems, and network devices. It also provides the configuration checking base, professional suggestions for remediation, and security configuration checking standards for multiple industries. The configuration checking base is available for hundreds of systems, which are divided into seven categories and cover more than 30 products.

RSAS can discover security defects and noncompliant code practices by auditing mainstream code files.

Identification of Nonstandard Ports

With the advanced nonstandard port identification technology and protocol fingerprint base, RSAS can identify application service types on nonstandard ports quickly and accurately and conduct vulnerability checking, effectively avoiding false negatives and false positives during scanning.

1.2 Main Functions

Baseline security requirements consist of security vulnerability and security configuration checking items. The coverage and effectiveness of such checking items are crucial to baseline security.

Vulnerability Management

According to security management regulations, RSAS provides risk alerting, checking, management, remediation, and auditing and supervises the implementation of security management regulations in each phase of the risk management process. RSAS can effectively and comprehensively detect vulnerability risks on the network, provide professional and effective analysis and remediation suggestions, and audit remediation effects throughout the risk management process, as shown in Figure 1-1. RSAS can reduce attacks to the maximum extent possible and is a "vulnerability management expert".

Figure 1-1 Security management process

Configuration Management

With a complete security configuration database, RSAS helps security configuration and remediation for IT information systems.

- By means of machine languages and the combination of remote detection and local detection, RSAS can automatically check security configurations and provide detailed detection reports. Compared with the traditional manual check, this helps reduce the check time and avoid mistakes.
- RSAS integrates leading technologies (including NSFOCUS Intelligent Profile (NSIP)) to detect security configuration issues in network assets automatically, effectively, and accurately.
- With continuous updates and improvement, RSAS is capable of supporting emerging device types. Check rules are also continuously updated to provide the most comprehensive automatic configuration checks, reducing risk costs and protecting your assets.

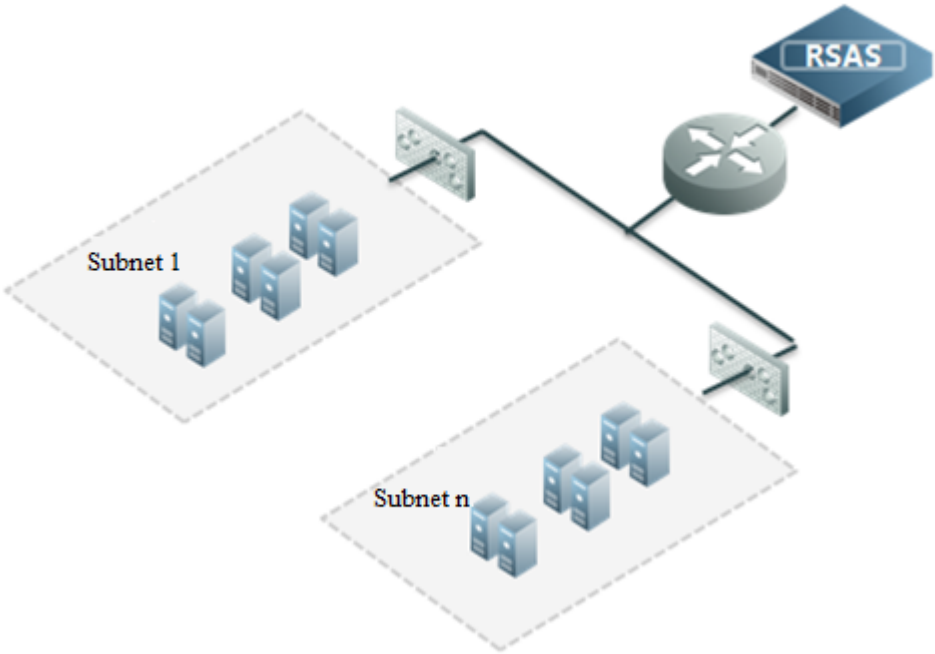
1.3 Typical Deployment

Standalone deployment is recommended for small and medium-sized enterprises, e-commerce, e-government, educational institutions, and independent Internet Data Centers (IDCs), which have more centralized data and simpler network topologies (mostly bus or star).

1.3.1 Deployment in a Small-Scale Network

RSAS can be easily deployed in the security maintenance environment of small-scale networks to detect various security vulnerabilities in business systems.

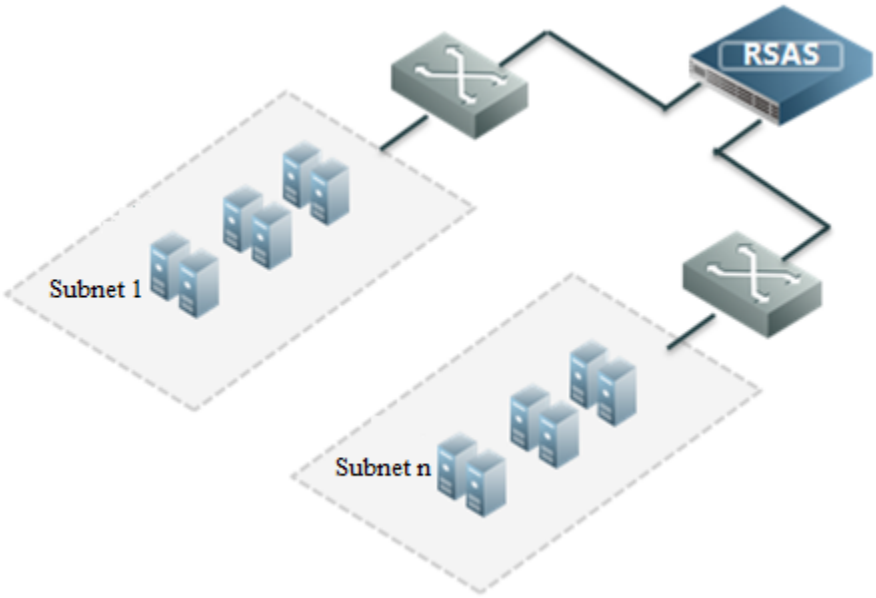
Figure 1-2 Deployment of RSAS in a small-scale network



1.3.2 Deployment in a Small and Medium-Scale Network

For small and medium-sized enterprises, their business networks may be divided into multiple subnets. It is costly to deploy a vulnerability management system on each subnet and also dangerous to open access permissions for vulnerability management on subnet firewalls. To cater to this situation, RSAS provides multiple scanning links and ports, each of which can connect to a subnet without extra firewall rule, as shown in Figure 1-3. This effectively reduces costs and avoids risks.

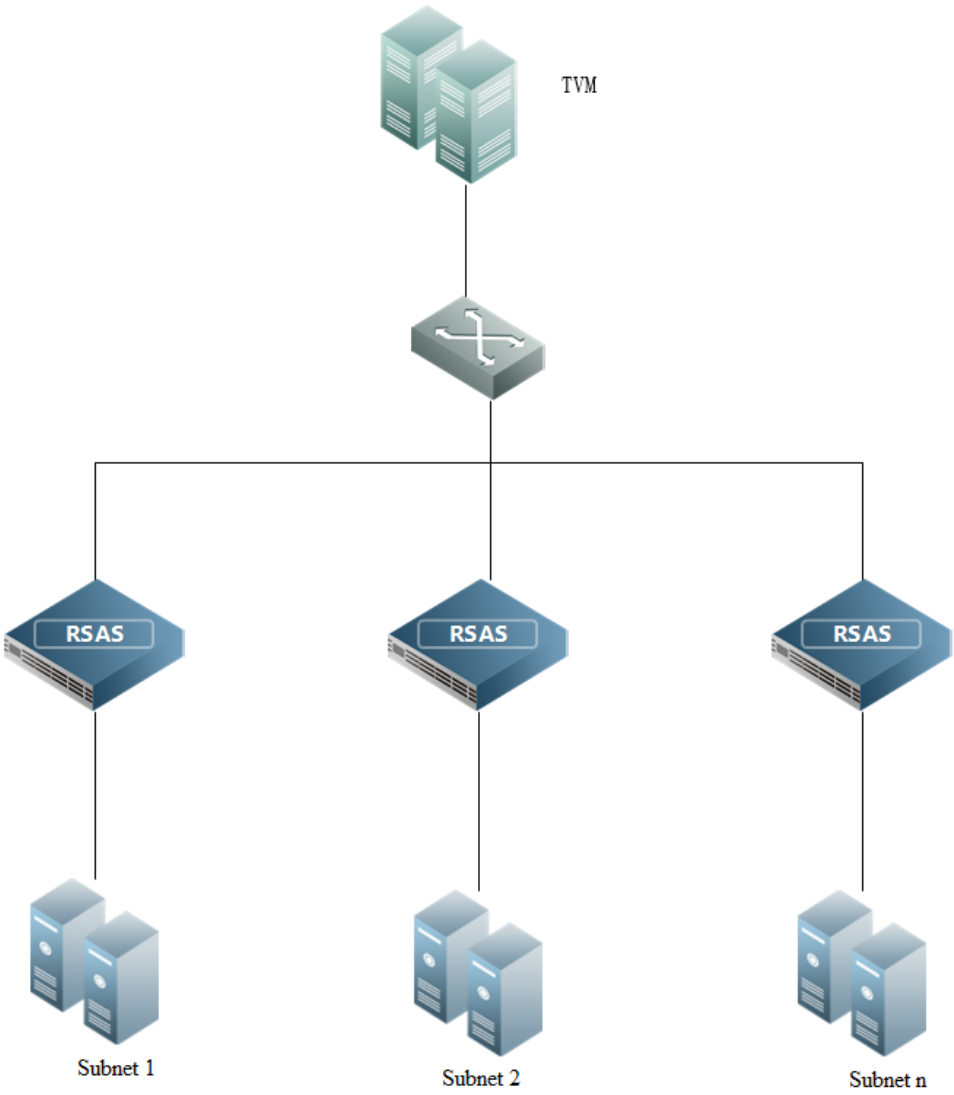
Figure 1-3 Deployment in a small and medium-scale network



1.3.3 Deployment in a Subnet with Limited Access

In certain circumstances, a business subnet may fail to RSAS, or RSAS cannot be directly deployed due to too many subnets. To cater to such situations, multiple RSAS devices can be deployed with TVM, under management of the latter. See Figure 1-4.

Figure 1-4 Deployment in a subnet with limited access



2 Installation Procedure

This chapter describes how to install the hardware edition and virtual edition of RSAS. It contains the following sections:

Section	Description
Installing RSAS	Describes how to install the hardware edition of RSAS.
Installing vRSAS	Describes how to install the virtual edition of RSAS (vRSAS).

2.1 Installing RSAS

This section describes how to install the hardware edition of RSAS.

2.1.1 Hardware Information

RSAS models include RSAS NX3-P (portal), RSAS NX3-A (portal), RSAS NX3-X (1U), RSAS NX3-S (1U), RSAS NX3-HHA (1U), and RSAS NX3-E (2U).

2.1.2 Hardware Appearance

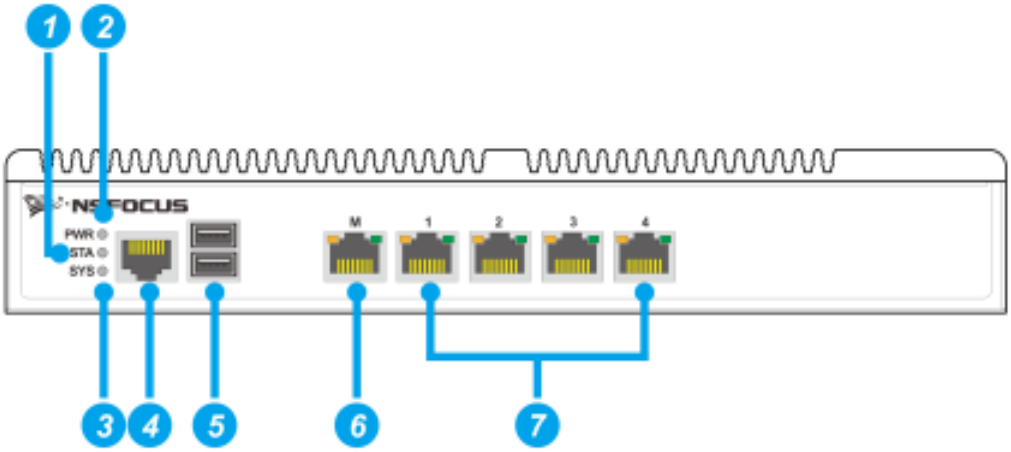
This section describes the front panels and rear panels of RSAS.

2.1.2.1 RSAS NX3-P (Portable)

Figure 2-1 and Figure 2-2 show the front panel and rear panel of RSAS NX3-P respectively.

Front Panel

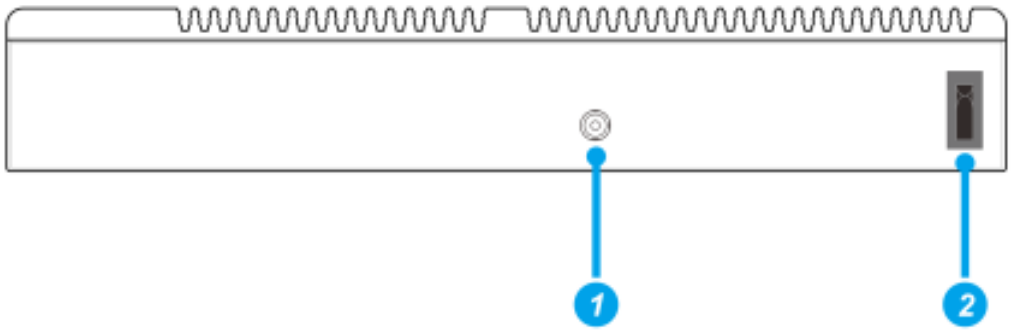
Figure 2-1 Front panel of RSAS NX3-P



①	STA: status LED	②	PWR: power LED
③	SYS: system LED	④	RJ45 console port
⑤	USB port	⑥	M: management port
⑦	Working ports		—

Rear Panel

Figure 2-2 Rear panel of RSAS NX3-P



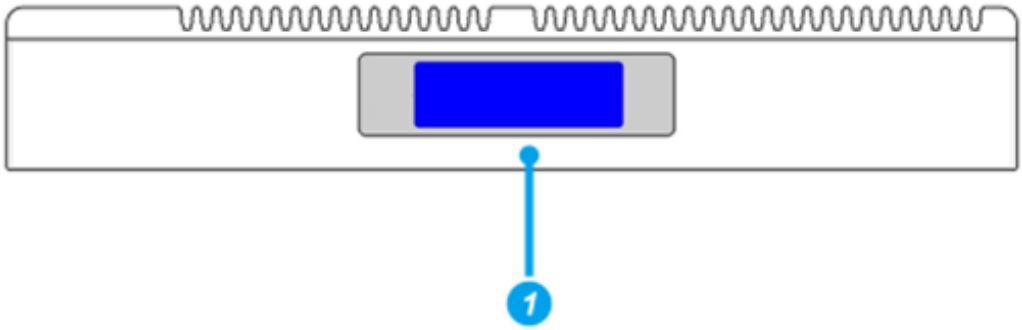
①	Power adapter port	②	Power switch

2.1.2.2 RSAS NX3-A (Portable)

Figure 2-3 and Figure 2-4 show the front panel and rear panel of RSAS NX3-A respectively.

Front Panel

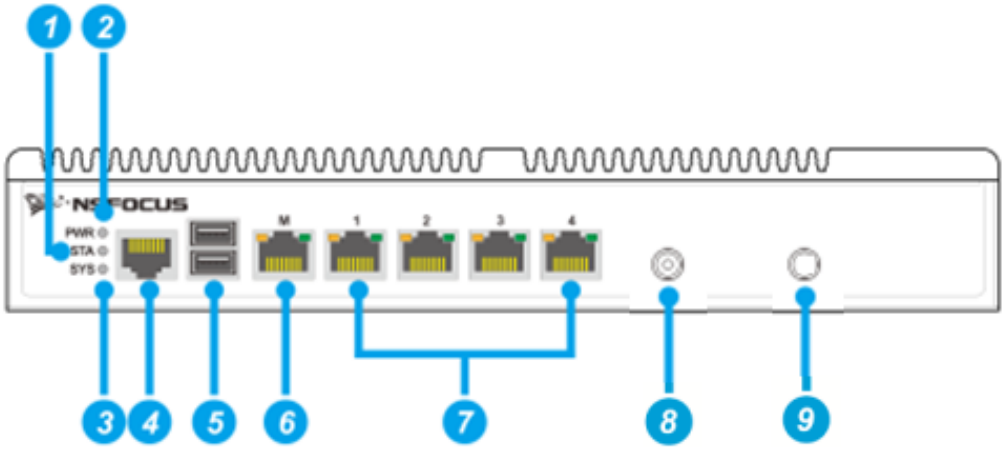
Figure 2-3 Front panel of RSAS NX3-A



① Monitor	—

Rear Panel

Figure 2-4 Rear panel of RSAS NX3-A



① STA: status LED	② PWR: power LED
③ SYS: system LED	④ RJ45 console port
⑤ USB port	⑥ M: management port
⑦ Working ports: electrical	⑧ Power adapter port

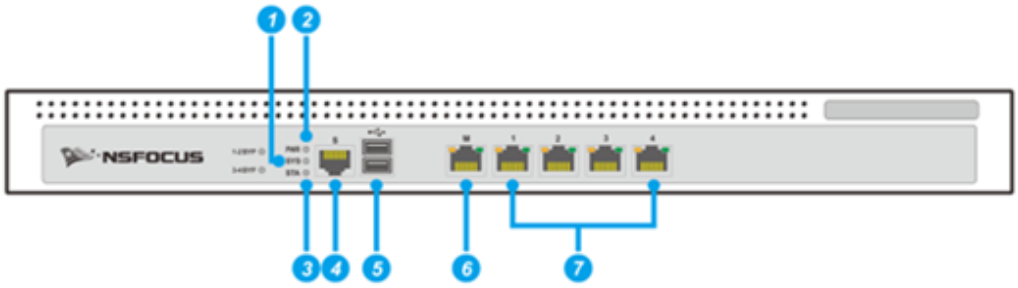
⑨ Power switch	—

2.1.2.3 RSAS NX3-X (1U)

Figure 2-5 and Figure 2-6 show the front panel and rear panel of RSAS NX3-X respectively.

Front Panel

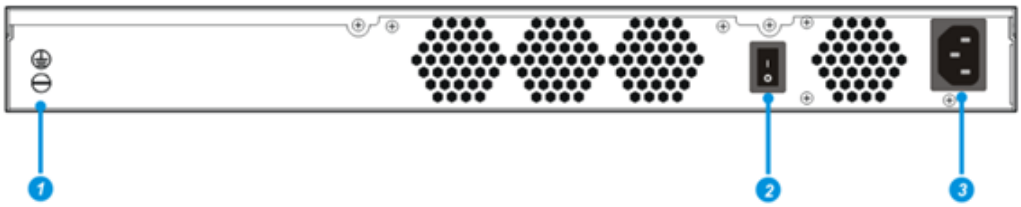
Figure 2-5 Front panel of RSAS NX3-X



① SYS: system LED	② PWR: power LED
③ STA: status LED	④ RJ45 console port
⑤ USB port	⑥ M: management port
⑦ Working ports: electrical	—

Rear Panel

Figure 2-6 Rear panel of RSAS NX3-X



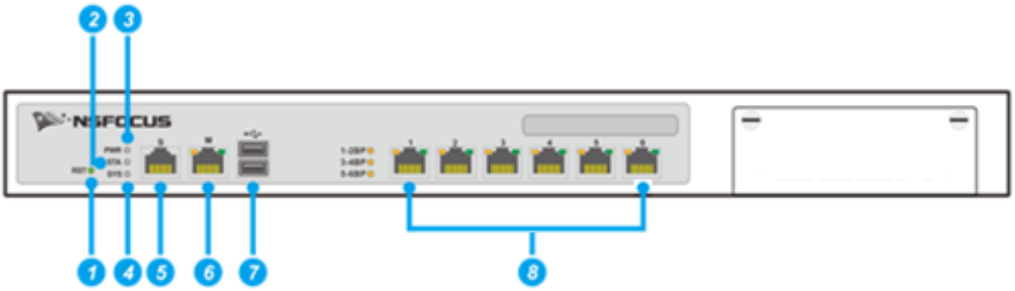
① Ground connector	② Power switch
③ Power connector	—

2.1.2.4 RSAS NX3-S (1U)

Figure 2-7 and Figure 2-8 show the front panel and rear panel of RSAS NX3-S respectively.

Front Panel

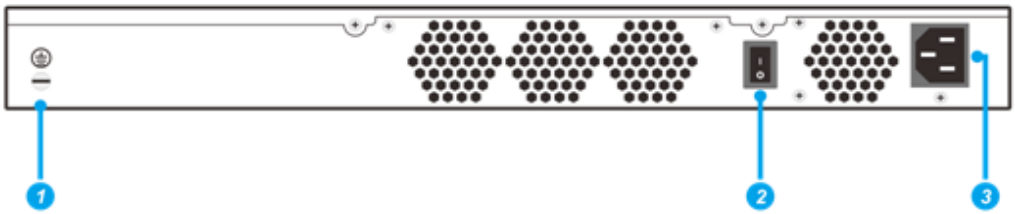
Figure 2-7 Front panel of RSAS NX3-S



①	RST: reset LED	②	STA: status LED
③	PWR: power LED	④	SYS: system LED
⑤	RJ45 console port	⑥	M: management port
⑦	USB port	⑧	Working ports: electrical

Rear Panel

Figure 2-8 Rear panel of RSAS NX3-S



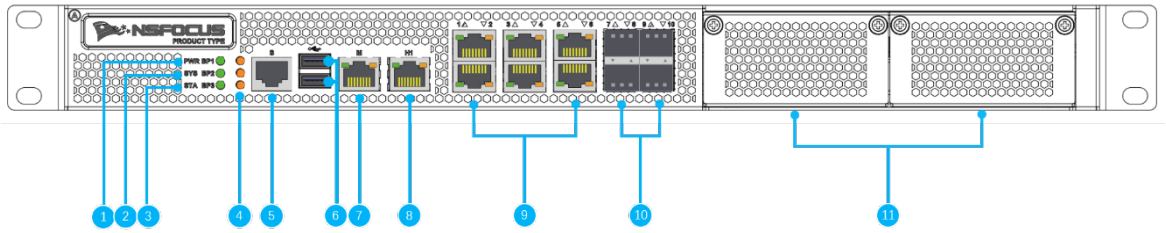
①	Ground connector	②	Power switch
③	Power connector		—

2.1.2.5 RSAS NX3-HHA (1U)

Figure 2-9 and Figure 2-10 show the front panel and rear panel of RSAS NX3-HHA respectively.

Front Panel

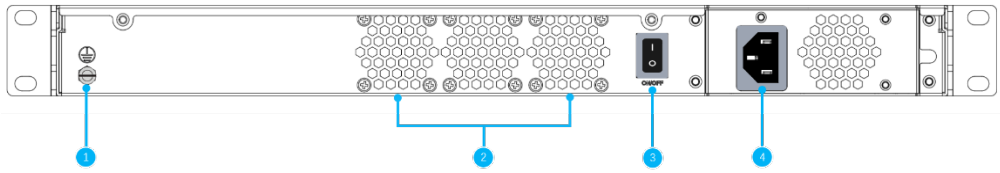
Figure 2-9 Front panel of RSAS NX3-HHA



①	PWR: power LED	②	SYS: system LED
③	STA: status LED	④	Bypass LED
⑤	RJ45 console port	⑥	USB port
⑦	M: management port	⑧	H1: management port
⑨	Working ports: electrical ports 1–6	⑩	Working ports: optical ports 7–10
⑪	Expansion module		—

Rear Panel

Figure 2-10 Rear panel of RSAS NX3-HHAFigure 2-9



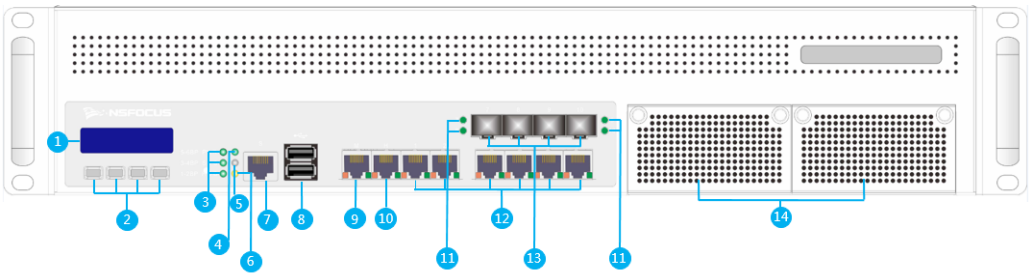
①	Ground connector	②	Fan
③	Power switch	④	Power connector

2.1.2.6 RSAS NX3-E (2U)

Figure 2-11 and Figure 2-12 show the front panel and rear panel of RSAS NX3-E respectively.

Front Panel

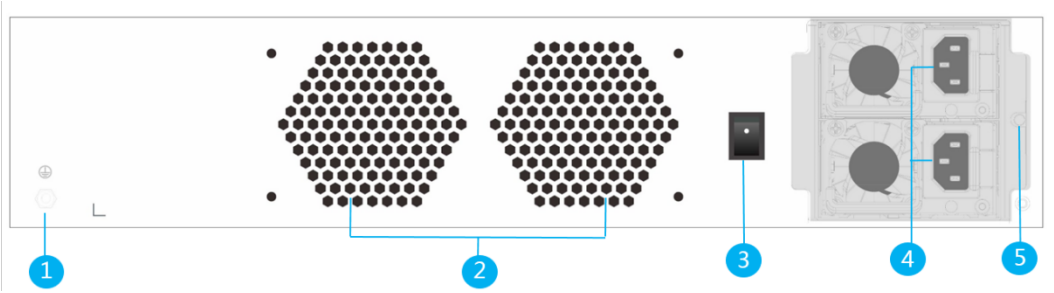
Figure 2-11 Front panel of RSAS NX3-E



①	Monitor	②	Monitor buttons
③	1–6 BP: status LED (top-down: 5–6, 3–4, 1–2)	④	PWR: power LED
⑤	SYS: system LED	⑥	HDD: hard disk LED
⑦	S: RJ45 console port	⑧	USB port
⑨	M: management port	⑩	H: management port
⑪	1000M optical port LEDs	⑫	1000M electrical port
⑬	1000M optical port	⑭	Expansion slots

Rear Panel

Figure 2-12 Rear panel of RSAS NX3-E



①	Ground connector	②	Fans
③	Power switch	④	Power connectors
⑤	Power reset button	—	

2.1.3 Hardware Parameters

Note	Hardware parameters may vary slightly with lots and models.

Table 2-1 shows hardware parameters of RSAS models

Table 2-1 Hardware parameters of RSAS

Model	Dimensions W*D*H (unit: mm)	Power Supply	Weight
RSAS NX3-P	271*175*44	Single AC power supply • Input voltage range: 100–240 V • Input current: 1.6 A • Maximum output power: 60 W	2.35 kg
RSAS NX3-A	324*220*62	Single AC power supply • Input voltage range: 100–240 V • Input current: 2 A • Maximum output power: 150 W	3.8 kg
RSAS NX3-X	430*390*44	Single AC power supply • Input voltage range: 100–240 V • Input current: 0–5 A • Maximum output power: 65 W	5 kg
RSAS NX3-S	430*390*44	Single AC power supply • Input voltage range: 110–240 V • Input current: 1.5–3 A • Maximum output power: 250 W	6.7 kg
RSAS NX3-HHA	450*435*44	Single/redundant AC power supply • Input voltage range: 100–240 V • Input current: 5A • Maximum output power: 250 W/300 W	8.5 kg
RSAS NX3-E	435*560*88	Redundant AC power supply • Input voltage range: 100–240 V • Input current: 5–2.5 A • Maximum output power: 300 W	11.59 kg

2.1.4 LEDs

Table 2-2 describes LEDs on the front panel.

Table 2-2 LED meanings

LED Type	LED Status	Description
Power LED (PWR)	On	The power supply is working.
	Off	The power supply is unavailable or not working.
Status LED (STA)	Blinking	The system is reading or writing data.
	Off	The system is idle.
System LED (SYS)	Off	The power supply is unavailable or not working.
	Green	The device is working under a proper load.
	Orange	The CPU usage of the device is on the high side.
	Red	The CPU usage of the device is too high.
Network LED (on either side of a network port)	Green (LINK/ACT)	• Off: indicates that no link is established. • On: indicates that a link is already established without data transmission. • Blinking: indicates that a link is already established and data transmission is ongoing.
	Yellow/Green (Speed)	• On (green): indicates the link works at 100 MB. • On (yellow): indicates that the link works at 1000 MB. • Off: indicates data transmission is lower than 10 MB.
Bypass LED (numbered)	On	The bypass function is enabled for the numbered ports.
	Off	The bypass function is disabled for the numbered ports.
HDD LED	Blinking	The hard disk is reading or writing data
	Off	The hard disk is not inserted.
	On	The hard disk is idle.
HDD LED	Blinking	The HDD is reading or writing data.
	Off	The HDD is not inserted.

2.1.5 Installation Preparations

Before installing RSAS, you need to check accessories and prepare the network environment, common tools, and equipment room environment.

2.1.5.1 Accessories

Before installation, check that all accessories are included in the accessory kit delivered with the device. If any accessories are missing or broken, please contact the local distributor.

Accessories vary with the device model. For the specific accessories, see the packing list.

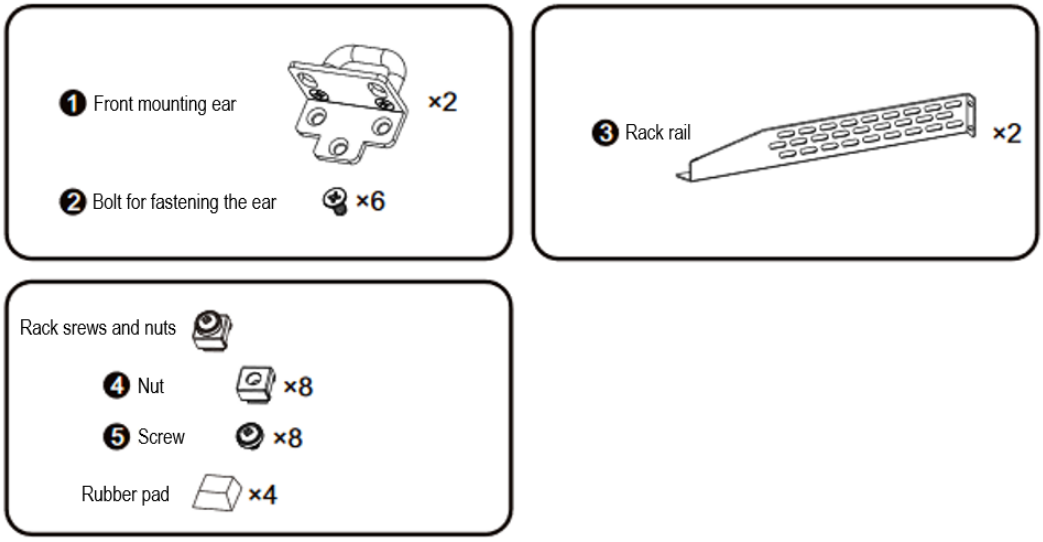
Accessories of 1U Devices

Table 2-3 lists accessories of 1U devices and Figure 2-13 illustrates the appearances of rackmount accessories.

Table 2-3 Accessories of 1U devices

Accessory	Description
Straight-through cable (green)	Used to connect a device to the network.
Crossover cable (yellow)	Used to connect a PC to the management interface of RSAS so that you can log in to the web-based manager of RSAS to perform configurations.
Power cable	One or two power cables are provided for each device.
Serial cable	A serial cable (one end is the DB9 female connector and the other end is the RJ45 plug) is required for device configuration via the console port.
Rackmount accessories	Rackmount accessories include the following: • Front mounting ear: fixes the front end of the chassis onto the rack. • Front mounting ear bolt: used with front mounting ears. • Rack rail: adjusts the distance between the device and the rack. • Rack rail bolt: used with rack rails. • Rubber pad: You can cut it into four smaller ones along the dotted line and attach them to the four corners of or marked places on the device to avoid abrasion. • Rear mounting ear: fixes rack rails onto the rack. • Rear mounting ear bolt: used with rear mounting ears. • Rack screws and nuts: fixes front and rear mounting ears onto rack rails.

Figure 2-13 Accessories for mounting a device onto a 1U rack



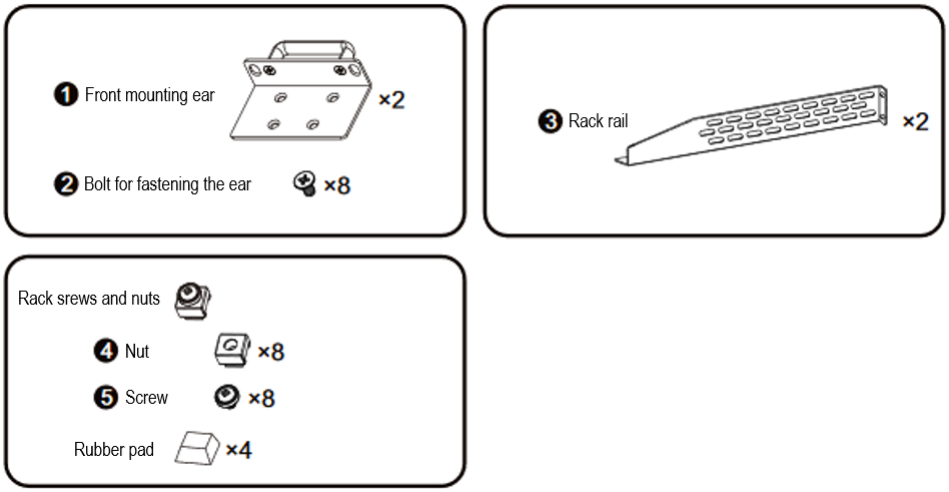
Accessories of 2U Devices

Table 2-4 lists accessories of 2U devices and Figure 2-14 illustrates the appearances of rackmount accessories.

Table 2-4 Accessories of 2U devices

Accessory	Description
Straight-through cable (green)	Used to connect a device to the network.
Crossover cable (yellow)	Used to connect a PC to the management interface of RSAS so that you can log in to the web-based manager of RSAS to perform configurations.
Power cable	One or two power cables are provided for each device.
Serial cable	A serial cable is required for device configuration via the console port.
Rackmount accessories	Rackmount accessories include the following: • Front mounting ear: fixes the front end of the chassis onto the rack. • Front mounting ear bolt: used with front mounting ears. • Rack rail: adjusts the distance between the device and the rack. • Rack rail bolt: used with rack rails. • Rubber pad: You can cut it into four smaller ones along the dotted line and attach them to the four corners of or marked places on the device to avoid abrasion. • Rear mounting ear: fixes the rail onto the rack. • Rear mounting ear bolt: used with rear mounting ears. • Rack screws and nuts: fixes front and rear mounting ears onto rack rails.

Figure 2-14 Accessories for mounting a device onto a 2U rack



2.1.5.2 Network Environment

Table 2-5 describes the network environment required for RSAS to go live.

Table 2-5 Items required for setting up a network environment

Item	Description
IP address	IP address reserved for RSAS.
Computer	Directly connected to the management port of RSAS so that you can log in to the web-based manager of RSAS in HTTPS mode for management.
Terminal software	Software used for connecting to the console port, for example, HyperTerminal that comes with the Windows operating system.
Browser	• The latest Firefox, Chrome, or Microsoft Edge browser are recommended. • The recommended screen resolution is 1280 x 1024 or greater. • You should clear the **Turn on Pop-up Blocker** check box on the browser.

2.1.5.3 User-provided Tools and Devices

- Screwdrivers and screws of various specifications
- Instruments and meters such as the terminal and multimeter
- ESD wrist strap
- Tape

2.1.5.4 Installation Environment

Table 2-6 lists specific requirements for the installation environment.

Table 2-6 Installation environment

Item	Requirements
Temperature and humidity	• Good ventilation and cooling system • Temperature: 0°C–45°C • Relative humidity: 10%–95% (non-condensing)
Electrostatic discharge (ESD)	• Make sure that the device and floor are well grounded. • Use a dust-proof room. • Wear ESD gloves or wrist straps when handling the circuit board.
Executive standards for radiation	Class A, EN55022, FCC Part 15
Rack	The rack must be secure enough and fit for the device.

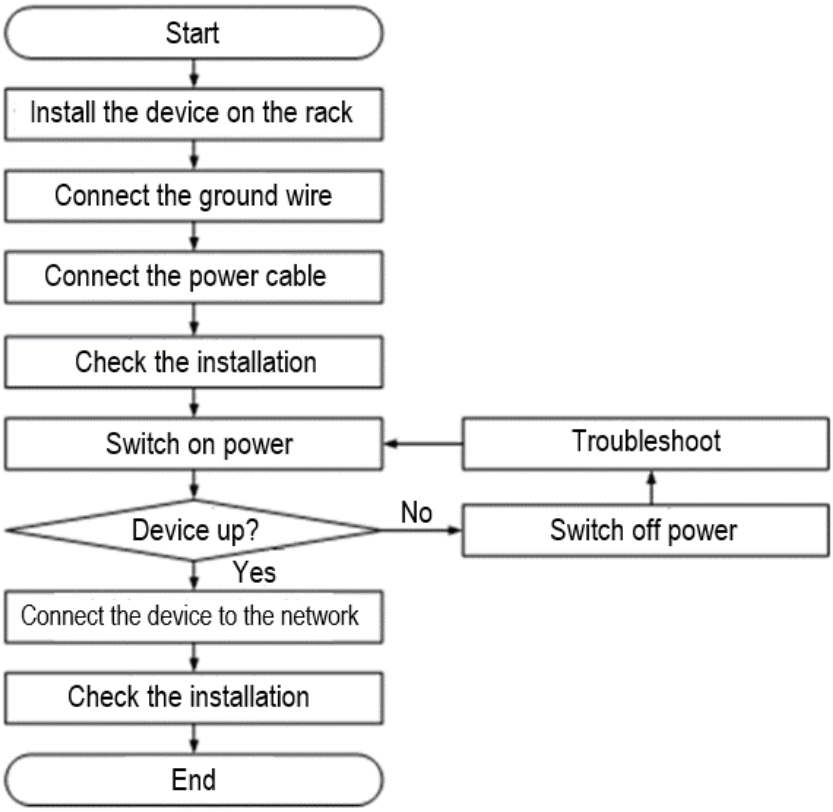
2.1.6 Installation Methods

This section describes how to install the device onto the rack.

2.1.6.1 Installation Procedure

Figure 2-15 shows the installation procedure.

Figure 2-15 Installation flow chart



2.1.6.2 Mounting a Device onto the Rack

The appearances and numbers of rackmount accessories for 1U and 2U devices are shown in Figure 2-13 and Figure 2-14 respectively.

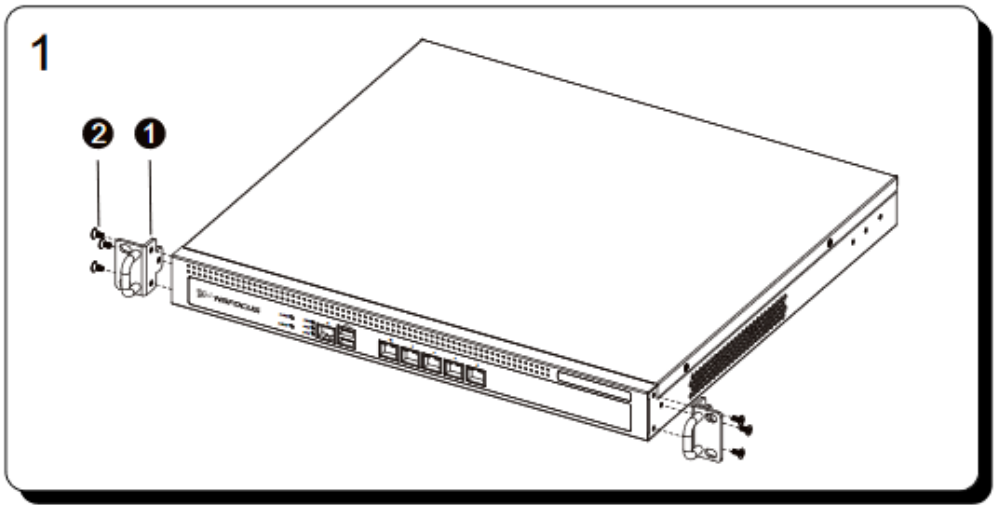
1U Device

To mount a 1U device onto the rack, follow these steps:

Step 1 Install front mounting ears.

Fix front mounting ears (①) with bolts (②) on the left and right sides of the device in the front end (three screws at each side, total six). See Figure 2-16.

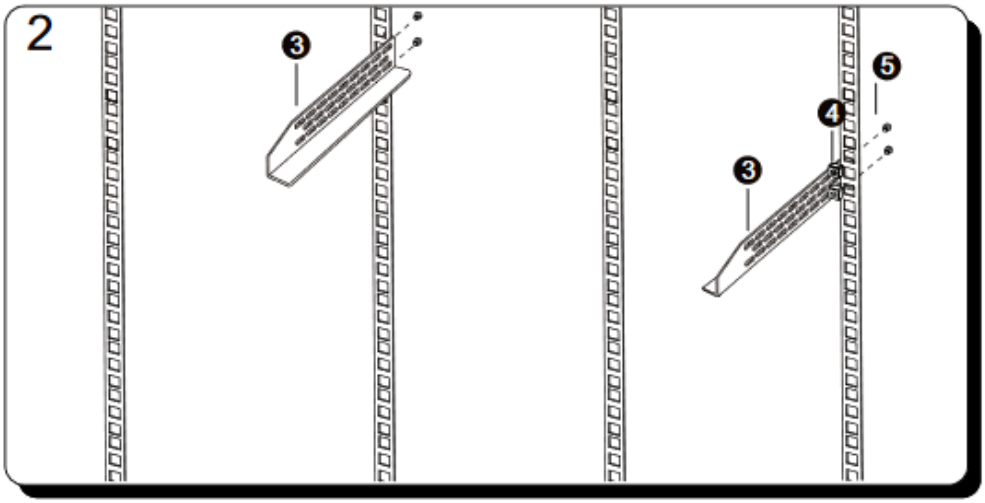
Figure 2-16 Installing front mounting ears



Step 2 Install rack rails.

Install four nuts (④) at the rear end of the chassis (two nuts on either side). Take rack rails (③) out of the accessory kit and fix them onto the chassis with four screws (⑤) (two on either side). See Figure 2-17.

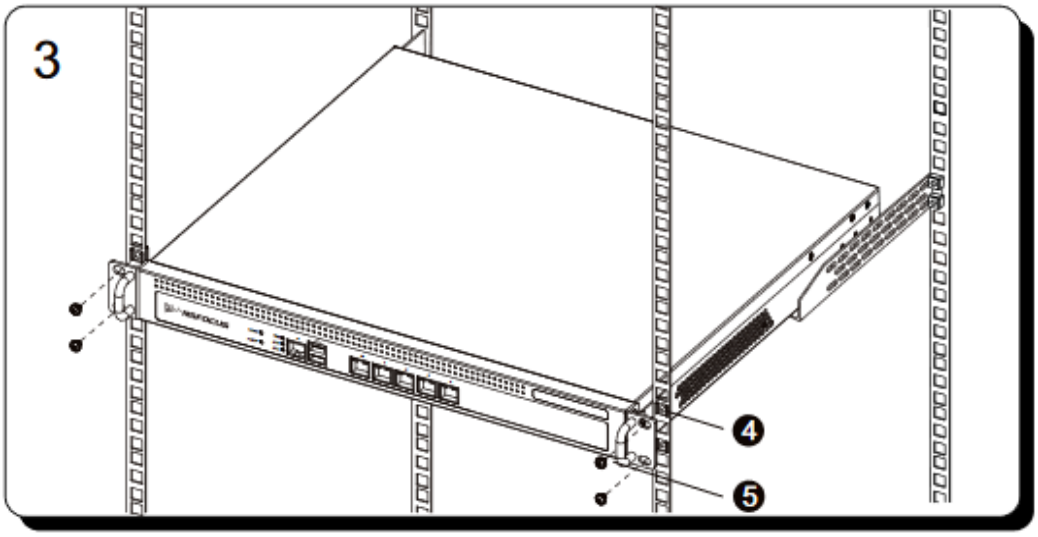
Figure 2-17 Installing rack rails



Step 3 Mount the device onto the rack.

Install four nuts (④) at the front end of the chassis (two nuts on either side). Place the device on the rails already installed on the chassis and fix it with four screws (⑤) (two on either side). See Figure 2-18.

Figure 2-18 Mounting the device onto the rack



----End

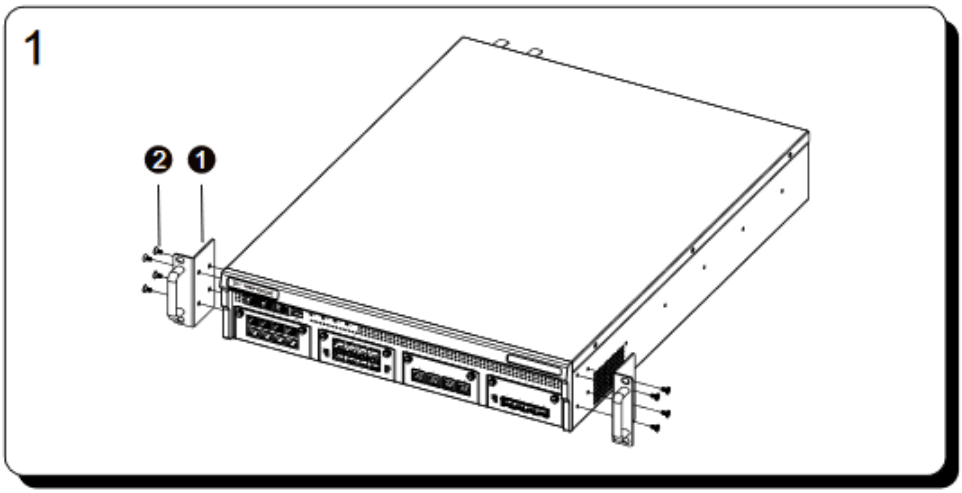
2U Device

To mount a 2U device onto the rack, follow these steps:

Step 1 Install front mounting ears.

Fix front mounting ears (①) with bolts (②) on the left and right sides of the device in the front end (four screws at each side, total eight). See Figure 2-19.

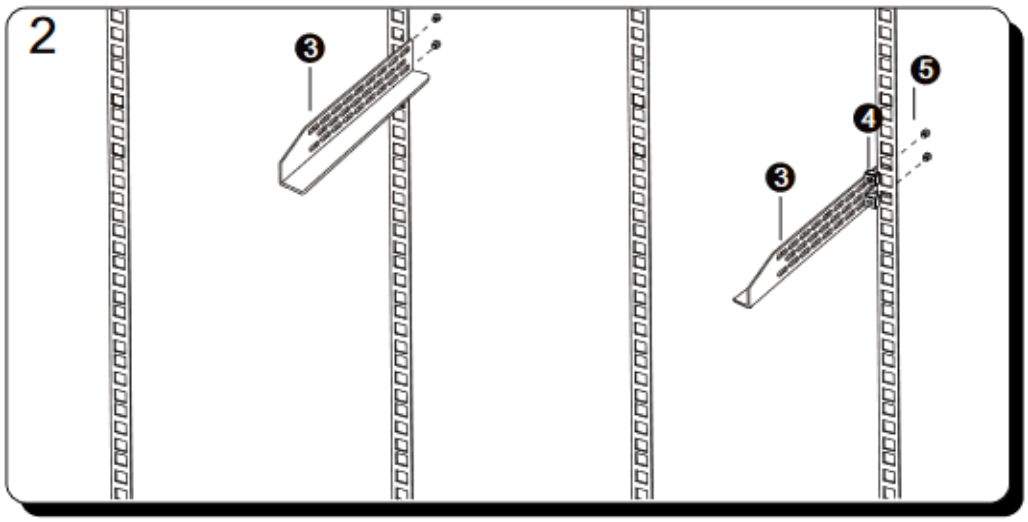
Figure 2-19 Installing front mounting ears



Step 2 Install rack rails.

Install four nuts (④) at the rear end of the chassis (two nuts on either side). Take rack rails (③) out of the accessory kit and fix them onto the chassis with four screws (⑤) (two on either side). See Figure 2-20.

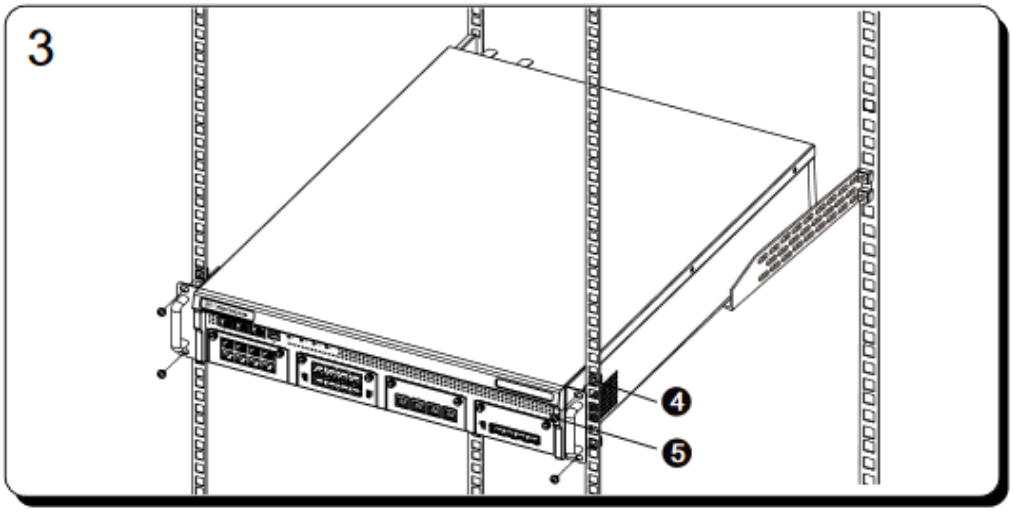
Figure 2-20 Installing rack rails



Step 3 Mount the device onto the rack.

Install four nuts (④) at the front end of the chassis (two nuts on either side). Place the device on the rails already installed on the chassis and fix it with four screws (⑤) (two on either side). See Figure 2-21.

Figure 2-21 Mounting the device onto the rack



----End

2.1.6.3 Connecting the Power Cable

RSAS supports both AC and DC power supplies.

Connecting the AC Power Cable

To connect the AC power cable, follow these steps:

Step 1 Make sure that the device is properly grounded.

Step 2 Turn the power switch of the AC power module to the OFF position.

Step 3 Connect one end of the power cable to the AC power socket on RSAS and the other end to the power socket of the equipment room.

Step 4 Turn the power switch of the AC power module to the ON position.

Step 5 Check the status of the power LED on the front panel.

For the status meanings of the power LED, see Table 2-2.

----End

Connecting the DC Power Cable

The input DC voltage of security devices is –48 V. Before installing an RSAS device, ensure that the power supply specifications of the equipment room meet the requirements of the product, avoiding product damage.

Different devices or models have different DC power sockets that may require a Positronic connector or a binding post.

Positronic Connector

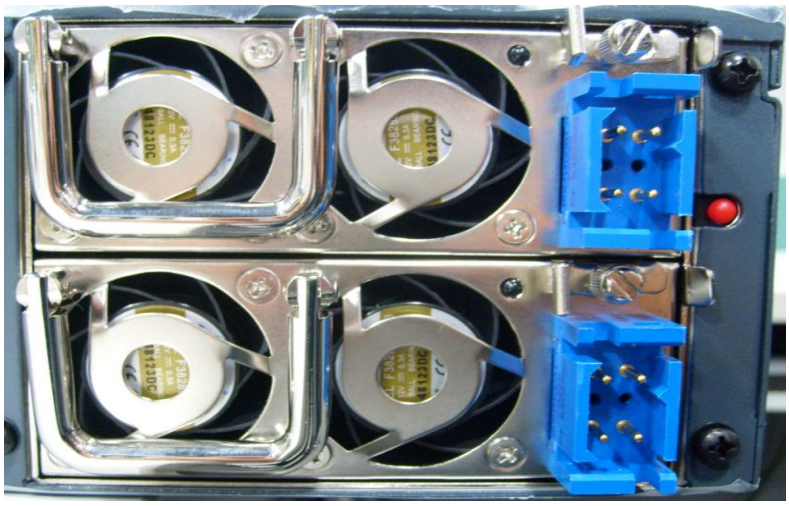
For a Positronic connector, the procedure is as follows:

Step 1 Make sure that the power switch of the device is in the OFF position.

Step 2 Take out the power plug from the packing case.

Figure 2-22 shows the power socket appearance. A DC power supply includes a power cable packed in the accessory kit and a socket integrated in the power supply module.

Figure 2-22 Sockets for Positronic connectors



Step 3 Insert the lead wires of the –48 V DC power supply of the equipment room into the jacks of a DC power supply socket on the device.

Step 4 In the case of dual power supplies, repeat Step 3 to connect the other power cable.

----End

Binding Post

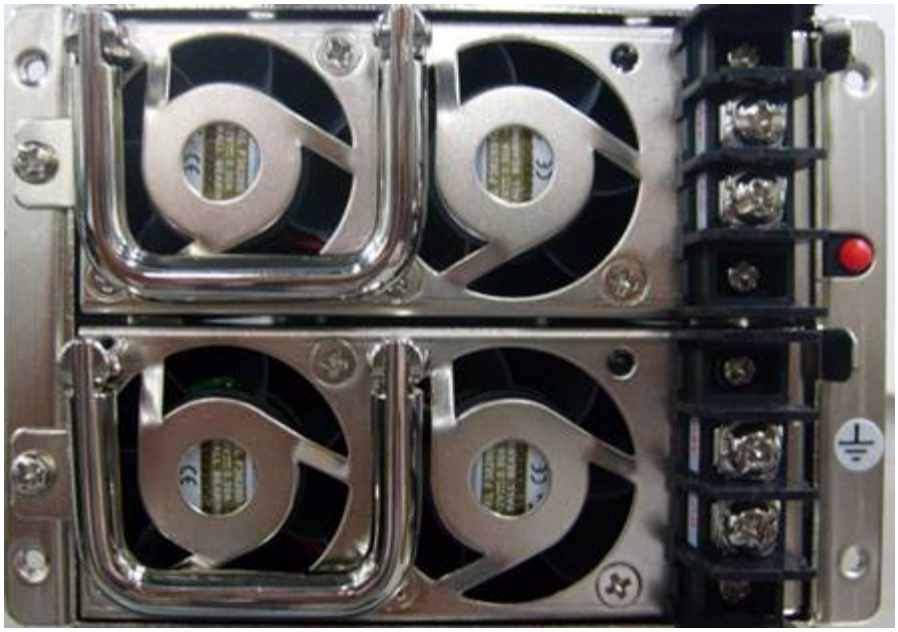
For a binding post, the procedure is as follows:

Step 1 Make sure that the power switch of the device is in the OFF position.

Step 2 Take out the power plug from the packing case.

Figure 2-23 shows the power socket appearance. A DC power supply includes a power cable packed in the accessory kit and a socket integrated in the power supply module.

Figure 2-23 Binding post terminals



Step 3 Insert lead wires of the –48 V DC power supply of the equipment room into two jacks of the DC power supply socket of the device.

Ensure that lead wires are inserted into proper jacks. The positive (+) is connected to the anode (0 V) with the black wire and the negative (–) to the cathode (–48 V) with the red wire.

Step 4 Insert the DC power plug into the DC power socket, and tighten the two screws at both ends of the plug with a screw driver.

Step 5 In the case of dual power supplies, repeat Step 3 and Step 4 to connect the power cable to the other DC power supply.

----End

2.1.6.4 Connecting the Network Cable

Connect one end of an Ethernet cable or optical fiber to the electrical or optical port (optical module is required) on RSAS and the other end to the network port on the peer device. After RSAS is powered up, check the status of network port LEDs on its front panel. For the meanings of status LEDs, see Table 2-2.

2.1.6.5 Shutting Down the Device

Turn the power switch to the OFF position to power off the device.

2.1.7 Notes Concerning Scrap Products

To protect the environment, you have the following responsibilities when disposing of products whose lifecycle has expired:

- Separate them from household waste and then deliver them to a qualified recycling station.

- The treatment method should conform to national laws and regulations concerning comprehensive utilization of the resources, environment protection, labor safety, and safeguarding human health.
- Do not use any technique or process that has been explicitly announced for elimination to dispose of waste electrical and electronic products.

2.2 Installing vRSAS

This section describes how to install the virtual edition of RSAS (vRSAS).

2.2.1 Configuration Requirements

vRSAS should run on a host with the virtual machine software installed. Make sure that the hardware meets all requirements listed in Table 2-1 and the virtual machine meets those listed in Table 2-2.

Table 2-1 Hardware configuration requirements

Hardware	CPU	Memory	HDD	NIC	USB Port
Recommended configuration	x86 series (3.2 GHz 8-core or faster)	16 GB or more	500 GB or more	10/100/1000 Mbps	USB 3.0 or earlier
Minimum configuration for common scanning tasks	x86 series (2.4 GHz dual-core)	4 GB	150 GB		
Minimum configuration for image scanning tasks	x86 series (2.4 GHz quad-core)	8 GB	150 GB		
Minimum configuration for code audit tasks	x86 series (2.4 GHz octa-core)	16 GB	500 GB		
Minimum configuration for agent-aided full scan	x86 series (2.4 GHz quad-core)	4 GB	500 GB		

Table 2-2 Software configuration requirements

Platform	Version
VMware Workstation	Version 9.0 or later
VMware vSphere ESXi	Version 6.0 or later
FusionCompute	V100R005C10SPC700
Standard KVM	2.11.1
Standard OpenStack	3.14.2
XenServer	7.3.0

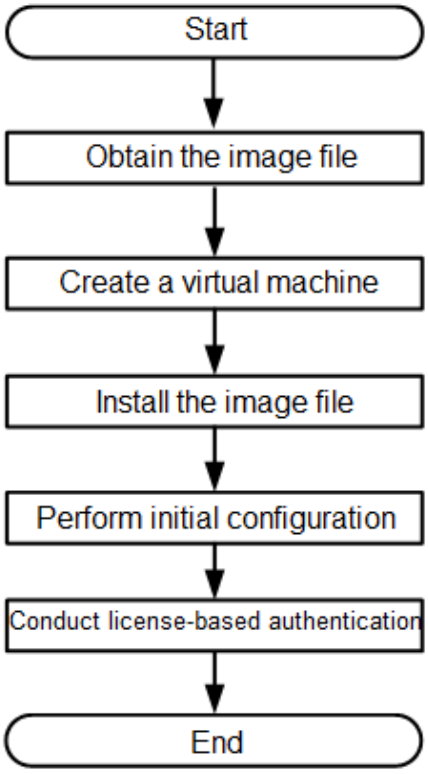
Caution	• Running multiple VMs on a host will degrade the performance of vRSAS. Therefore, you are advised to shut down unused ones. • If dual hard disks are installed, the first one must be larger than 4 GB. • The VM CPU with two cores slows down the scanning. To improve the scanning speed, you are advised to use a VM CPU with four or more cores, and the number of CPU cores must be the same as that authorized by the license.

2.2.2 Installation Procedure

Figure 2-24 shows the installation procedure.

Platforms such as OpenStack and Xen do not support dongle authentication. Therefore, you are advised to use a centralized authentication and authorization (CAA) management platform or NSFOCUS security cloud for the authentication.

Figure 2-24 Installation process



2.2.3 Installation on VMware Workstation

This section describes how to install vRSAS on VMware Workstation.

2.2.3.1 Preparations

Table 2-3 lists preparations to be made for installing vRSAS on VMware Workstation.

Table 2-3 Preparations to be made for installing vRSAS on VMware Workstation

Item		Description
VMware Workstation host	IP address	IP address of a computer that can properly connect to the network.
	Account	Account with privileges of a system administrator.
vRSAS	CD	Contains an image file (.iso) of vRSAS.
	IP address	IP address of the scan interface of vRSAS.
	Authentication license	• License that enables vRSAS to be launched properly. • Unique authorization hash value granted to vRSAS.
		• IP address of a CAA platform and license of vRSAS. • License of vRSAS for authentication by NSFOCUS security cloud. • Dongle and license: The dongle should be already installed on the VMware Workstation host. Note You can select any one of the three authentication modes.

2.2.3.2 Installation Procedure

Obtaining the Image File of vRSAS

Insert the CD into the CD-ROM drive. The CD runs automatically. Click **Remote Security Assessment System** under **Installation File**. The folder that contains the image file appears.

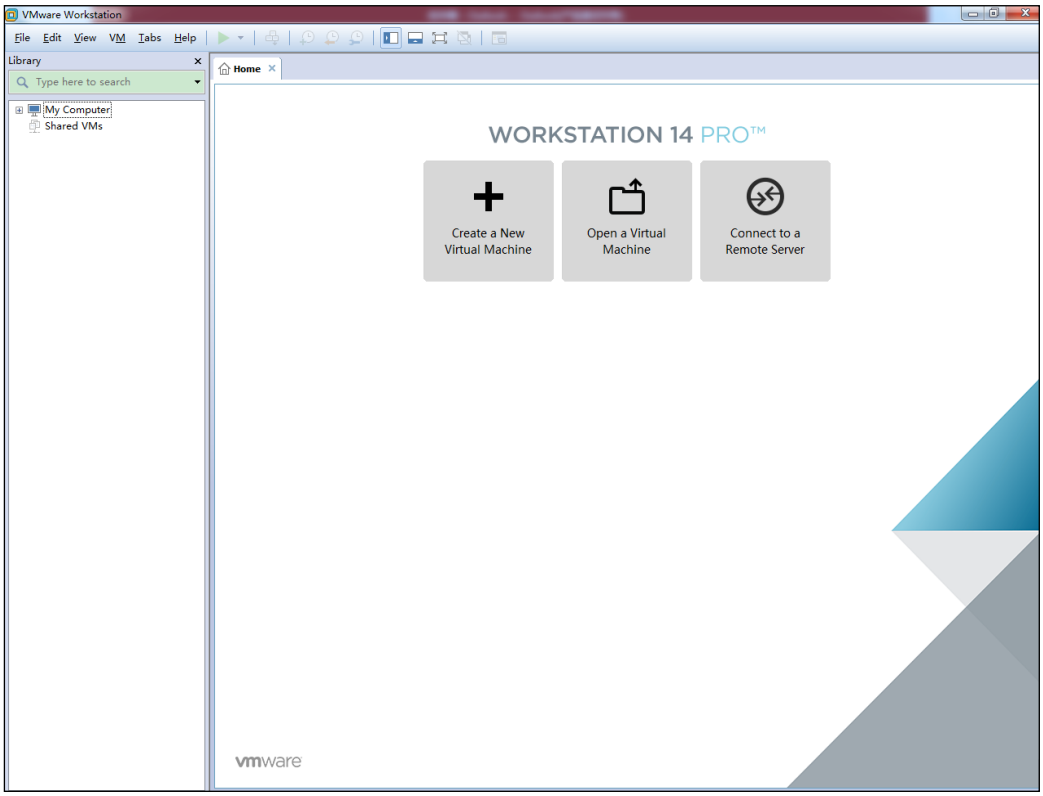
Creating a VM

To create a VM, follow these steps:

Step 1 Start VMware Workstation 14.

The home page of VMware Workstation 14 appears, as shown in Figure 2-25.

Figure 2-25 Home page of VMware Workstation 14



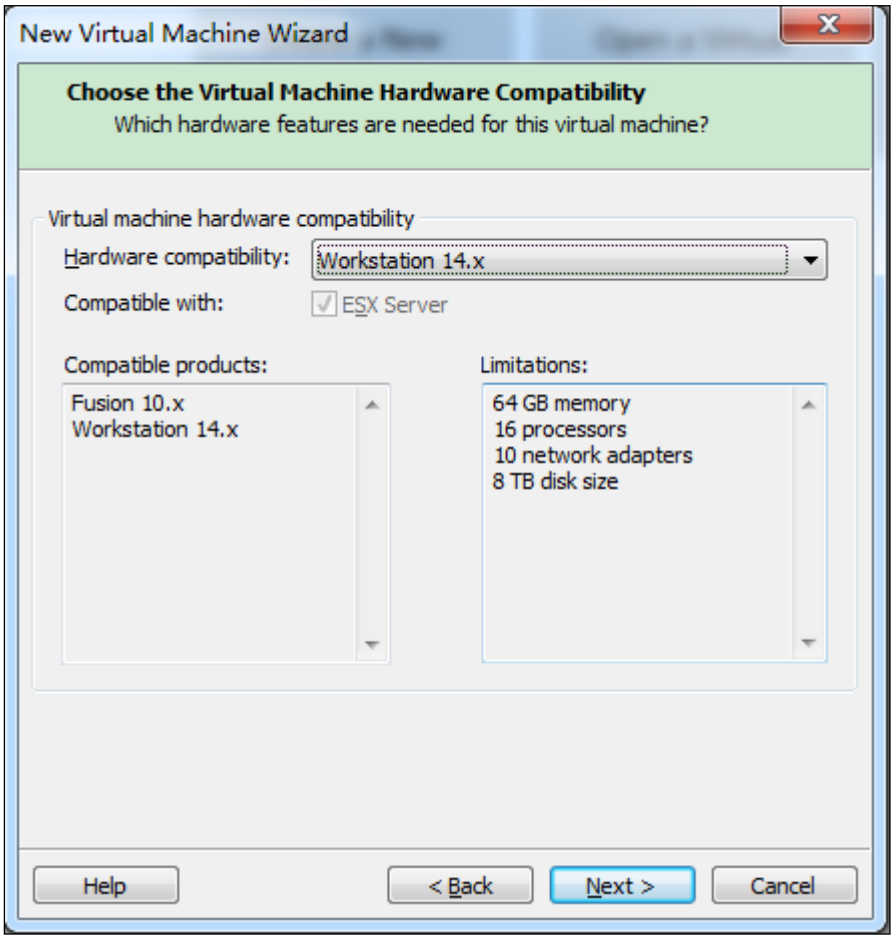
Step 2 Choose **File** and click **Create a New Virtual Machine**.

Step 3 In the **New Virtual Machine Wizard** dialog box, select **Custom (advanced)** and click **Next**.

Figure 2-26 Selecting a configuration type

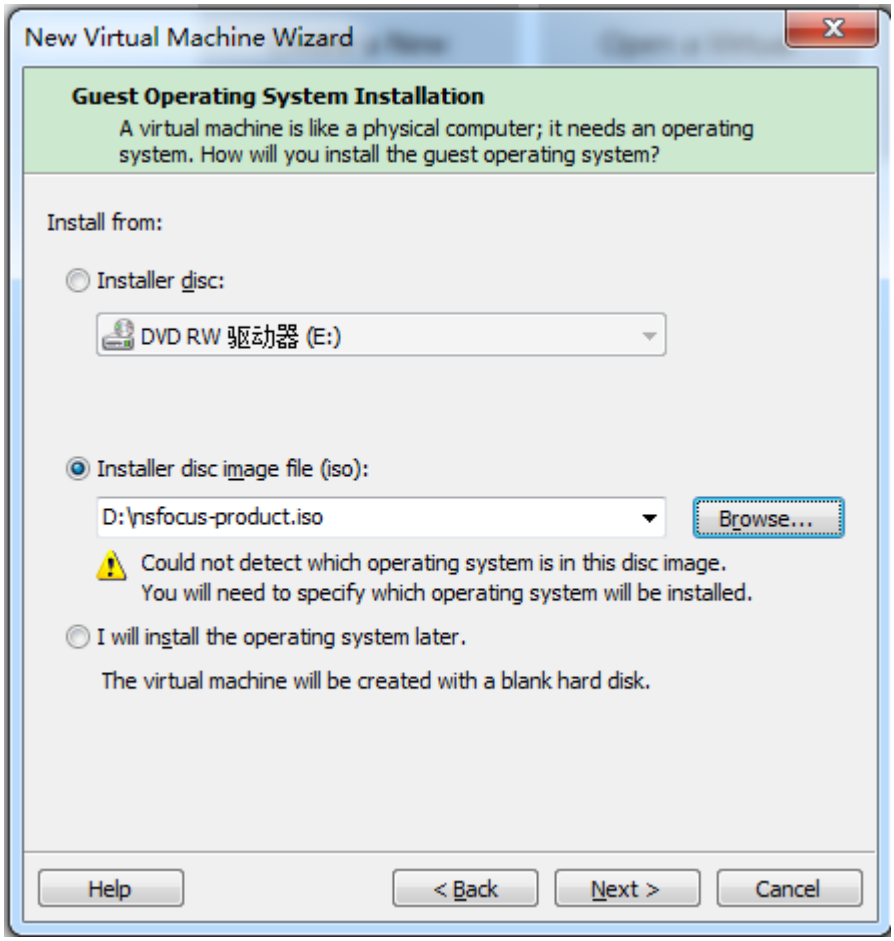
Step 4 In the **Choose the Virtual Machine Hardware Compatibility** dialog box, select **Workstation 14.x** for **Hardware compatibility**, and then click **Next**.

Figure 2-27 Selecting a compatible workstation version



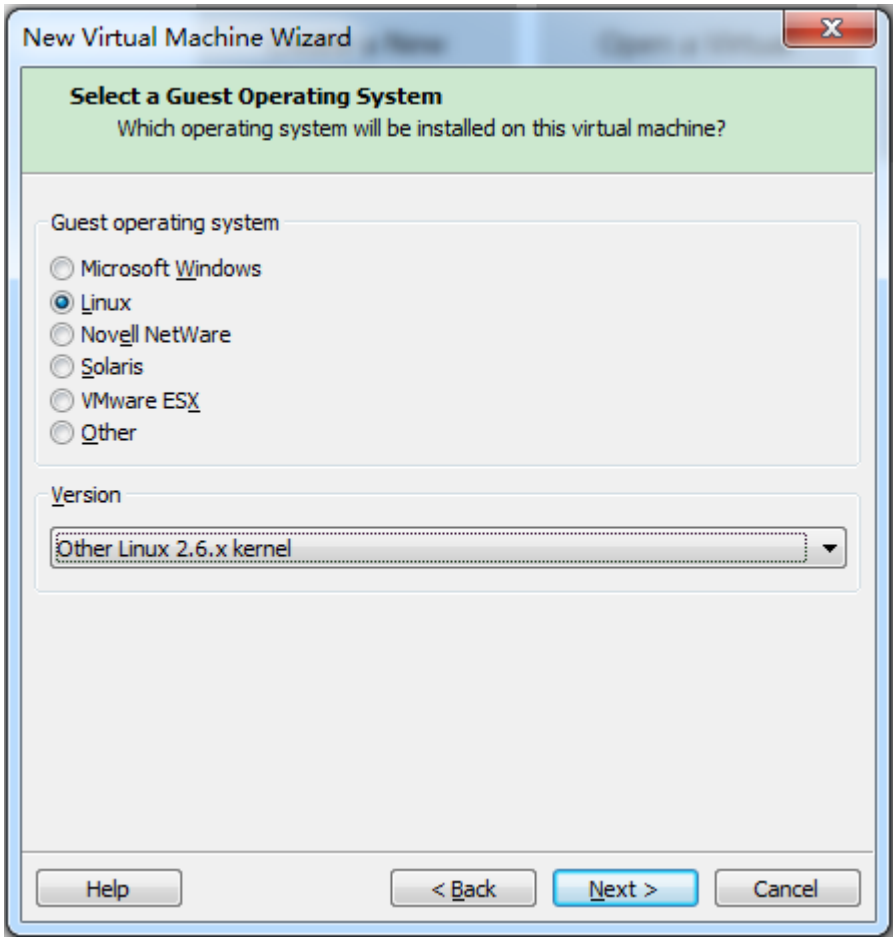
Step 5 In the **Guest Operating System Installation** dialog box, select **Installer disc image file (iso)**, browse to the vRSAS image file in the CD, and click **Next**.

Figure 2-28 Choosing to install from an image file



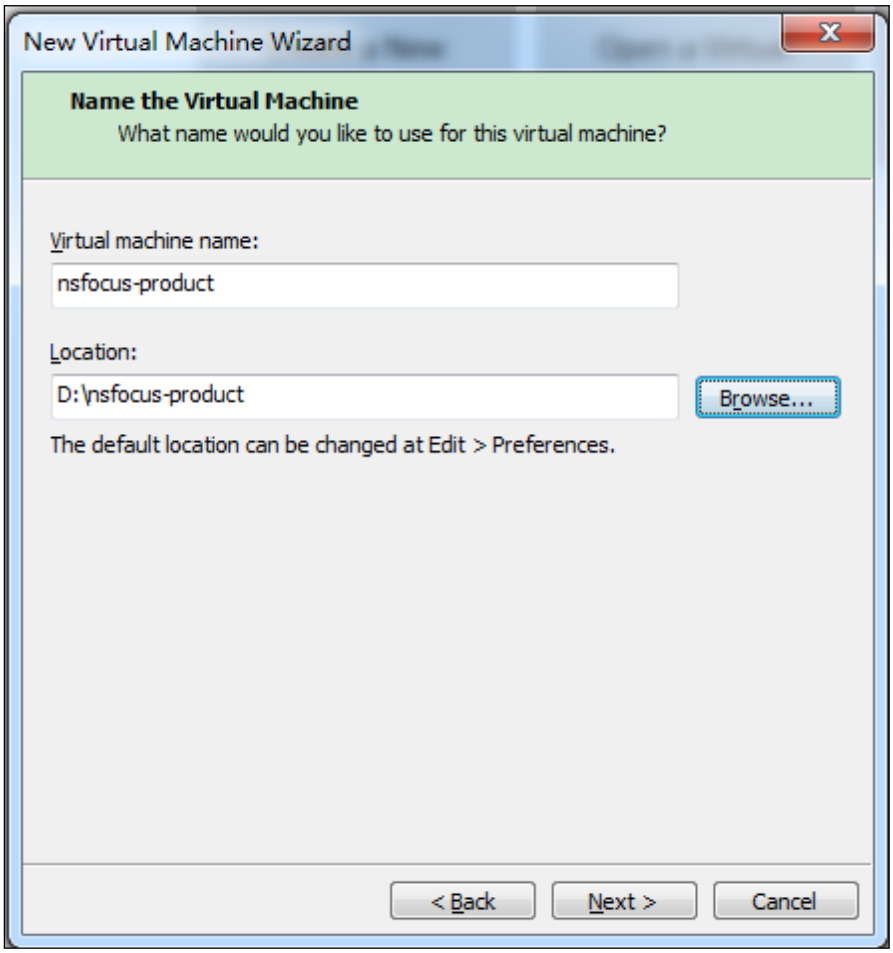
Step 6 In the **Select a Guest Operating System** dialog box, select **Linux** as the guest operating system (OS) and **Other Linux 2.6.x kernel** for **Version**, and then click **Next**.

Figure 2-29 Selecting a guest OS and version



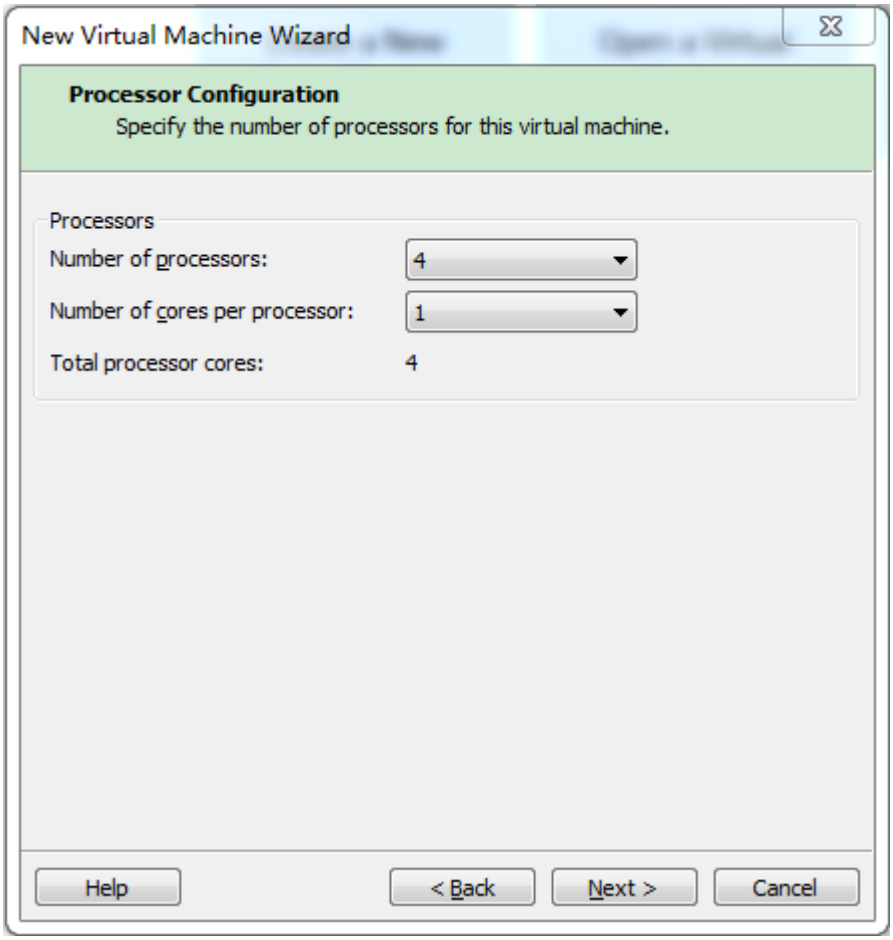
Step 7 In the **Name the Virtual Machine** dialog box, specify a name for the virtual machine and an installation location, and then click **Next**.

Figure 2-30 Naming the VM



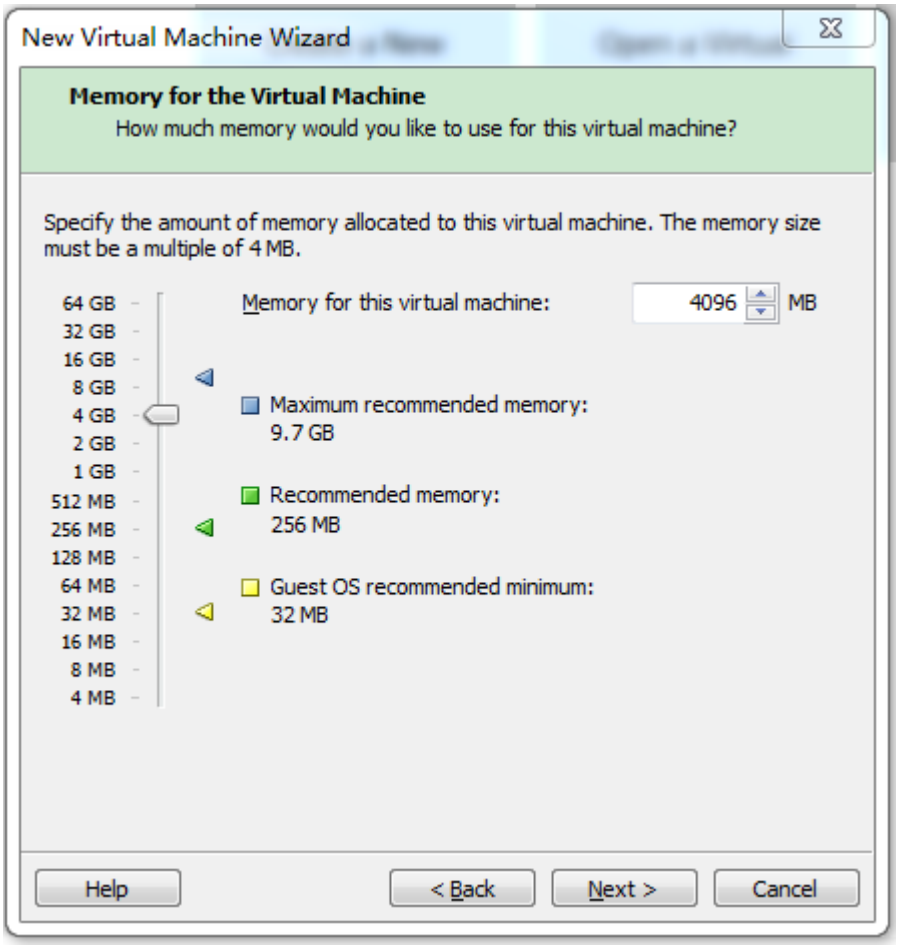
Step 8 In the **Processor Configuration** dialog box, configure processors according to the minimum requirements listed in Table 2-1, and click **Next**.

Figure 2-31 Configuring processors



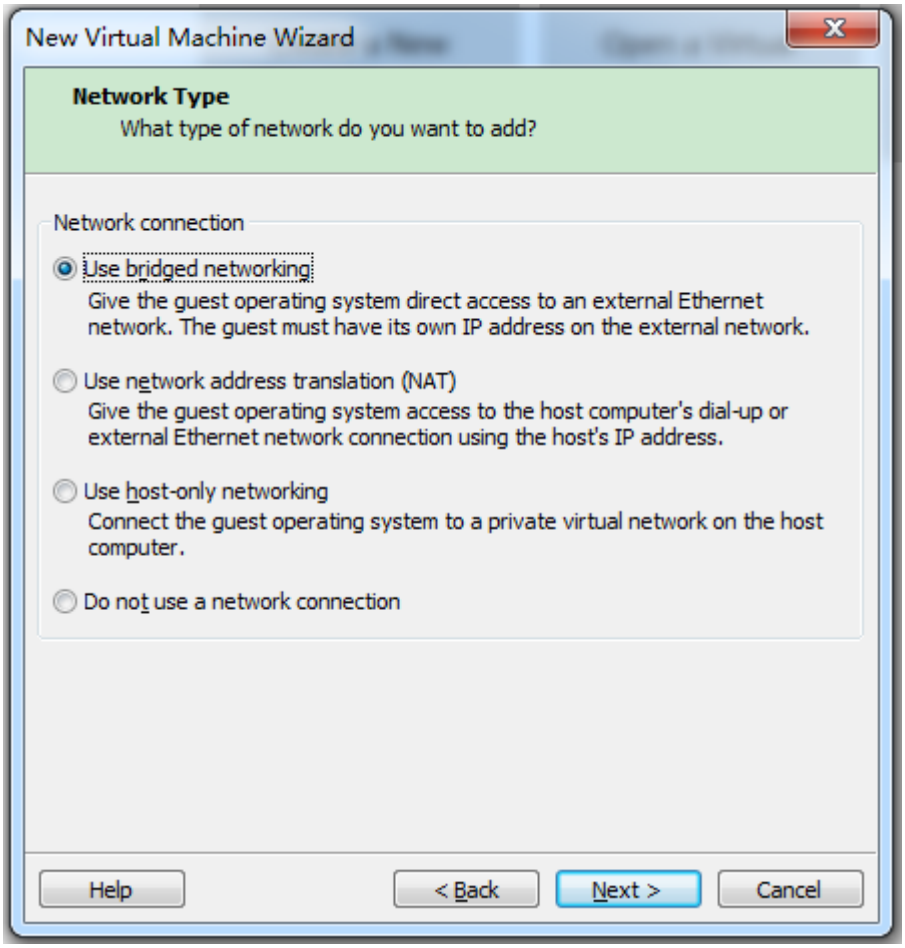
Step 9 In the **Memory for the Virtual Machine** dialog box, configure memory according to the minimum requirements listed in Table 2-1, and click **Next**.

Figure 2-32 Specifying the memory size



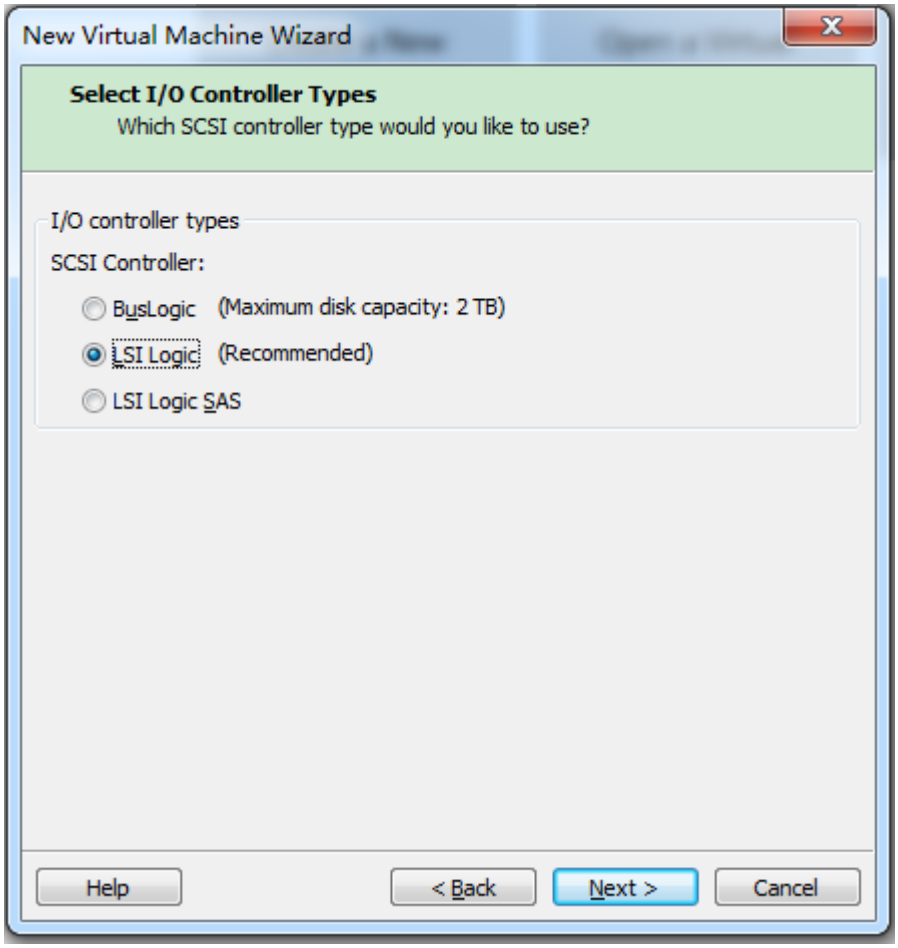
Step 10 In the **Network Type** dialog box, select **Use bridged networking** and click **Next**.

Figure 2-33 Selecting a network type



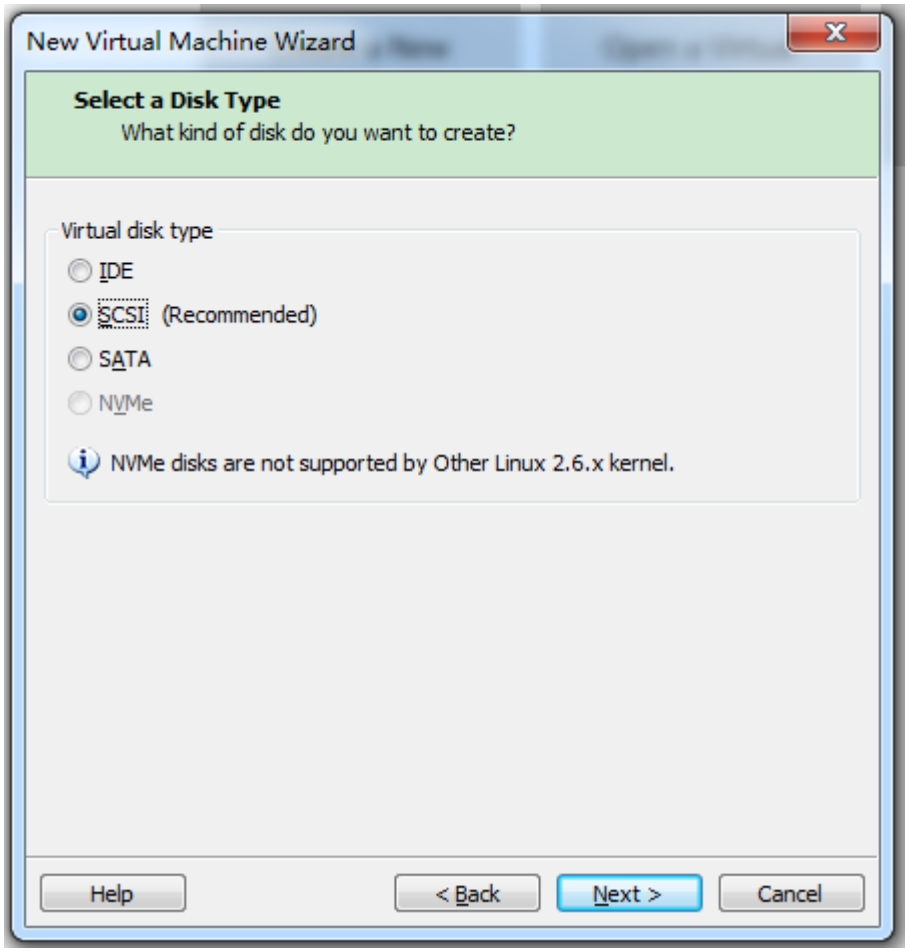
Step 11 In the **Select I/O Controller Types** dialog box, select **LSI Logic** and click **Next**.

Figure 2-34 Selecting I/O controller types



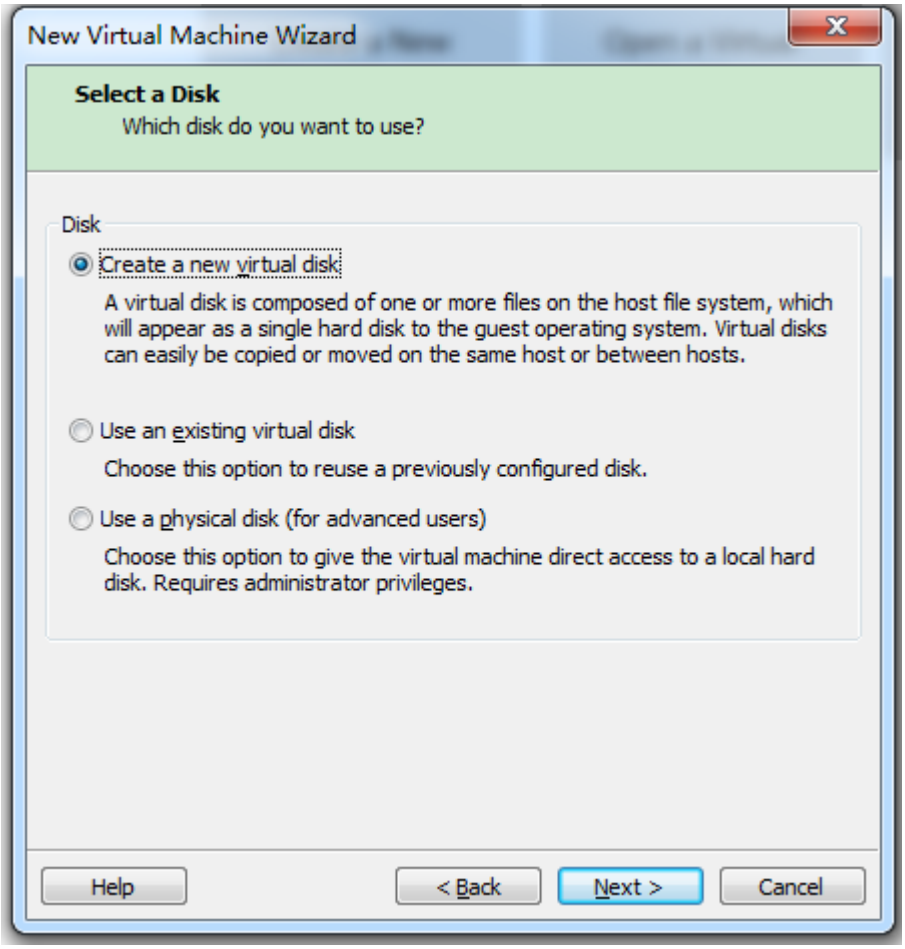
Step 12 In the **Select a Disk Type** dialog box, select **SCSI (Recommended)** and click **Next**.

Figure 2-35 Selecting a disk type



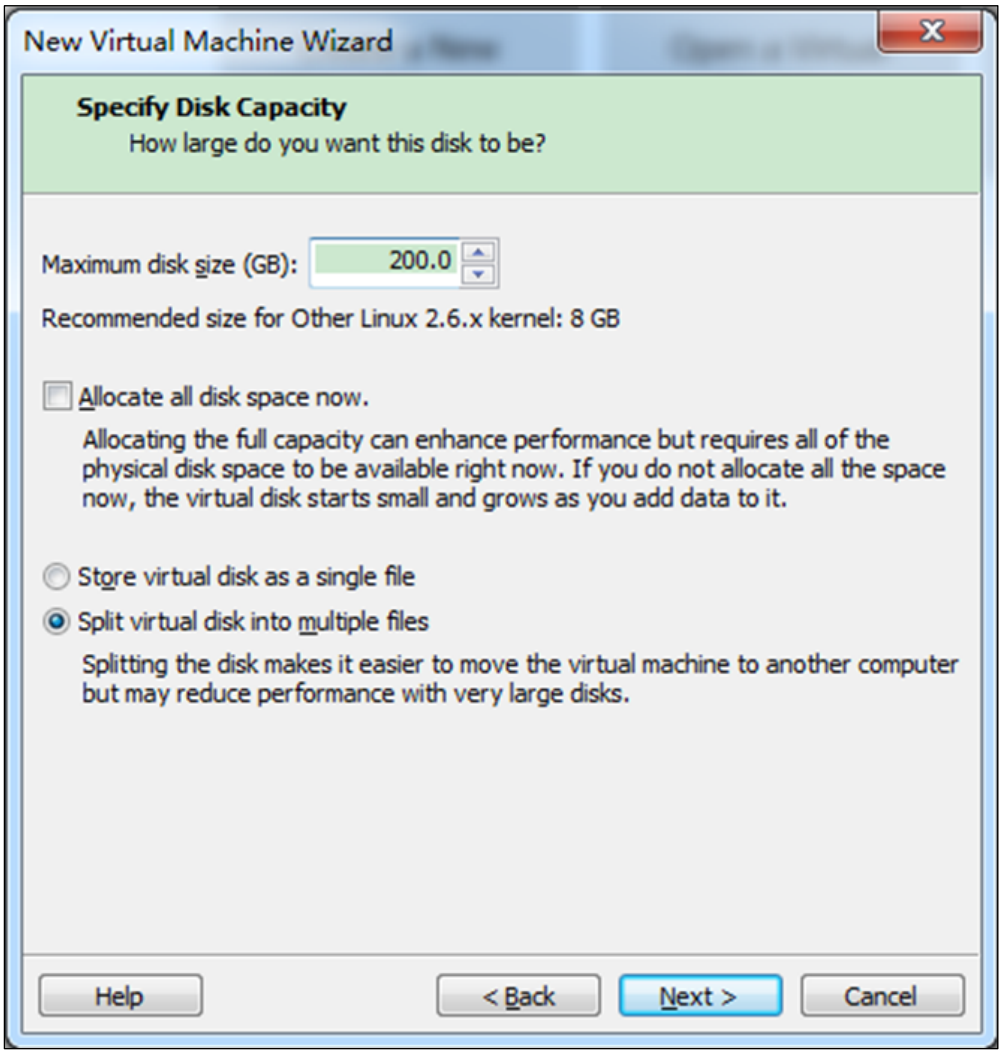
Step 13 In the **Select a Disk** dialog box, select **Create a new virtual disk** and click **Next**.

Figure 2-36 Selecting a disk



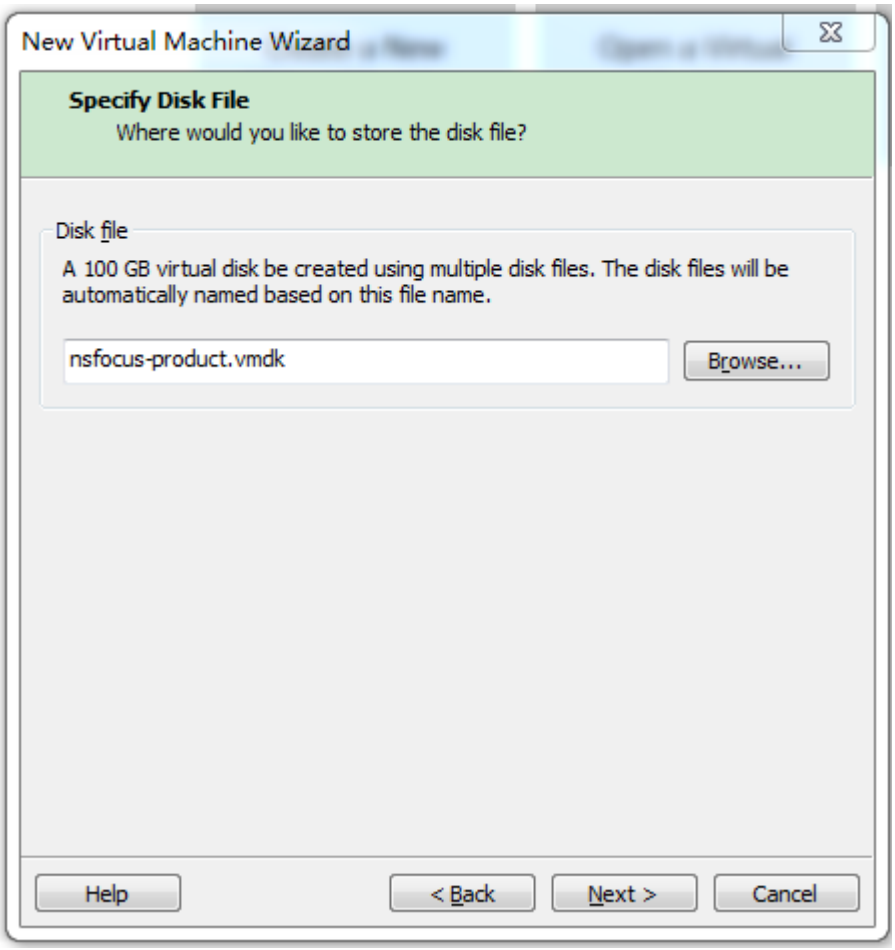
Step 14 In the **Specify Disk Capacity** dialog box, set the maximum disk size, select **Split virtual disk into multiple files**, and click **Next**.

Figure 2-37 Specifying the disk capacity



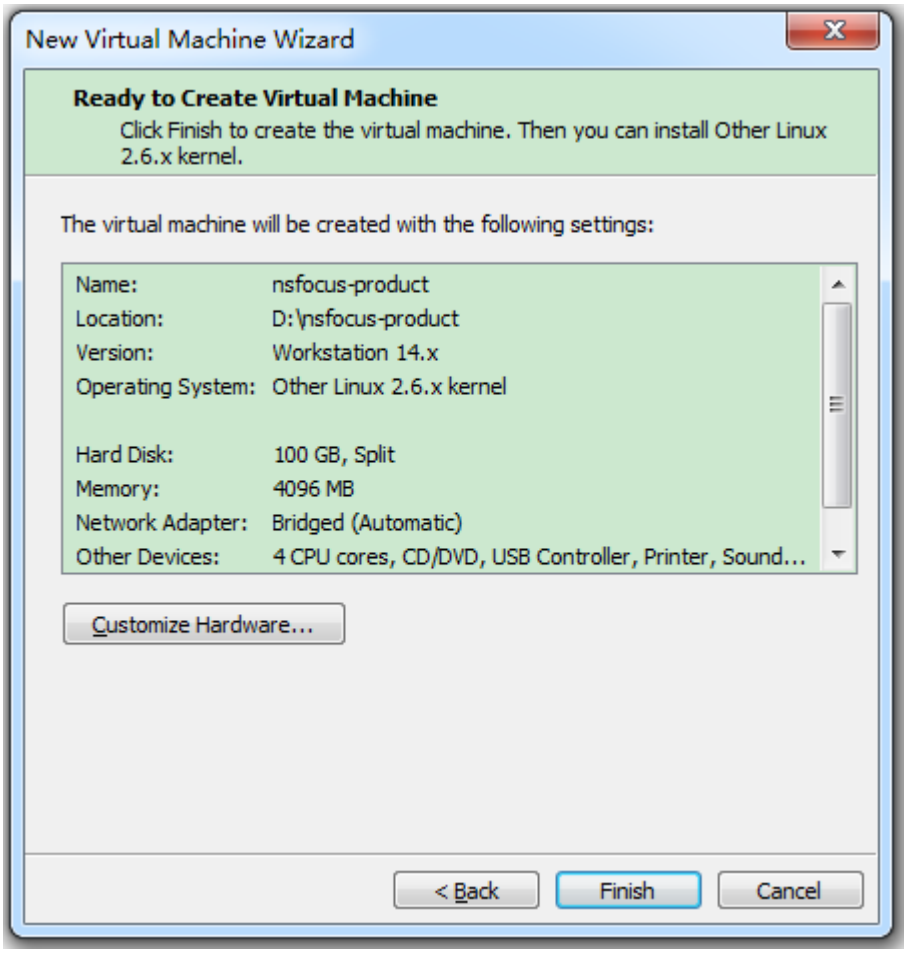
Step 15 In the **Specify Disk File** dialog box, specify a disk file and click **Next**.

Figure 2-38 Specifying a disk file



Step 16 In the **Ready to Create Virtual Machine** dialog box, click **Finish** to complete creation of the virtual machine.

Figure 2-39 Virtual machine created for vRSAS



----End

Installing the Image File of vRSAS

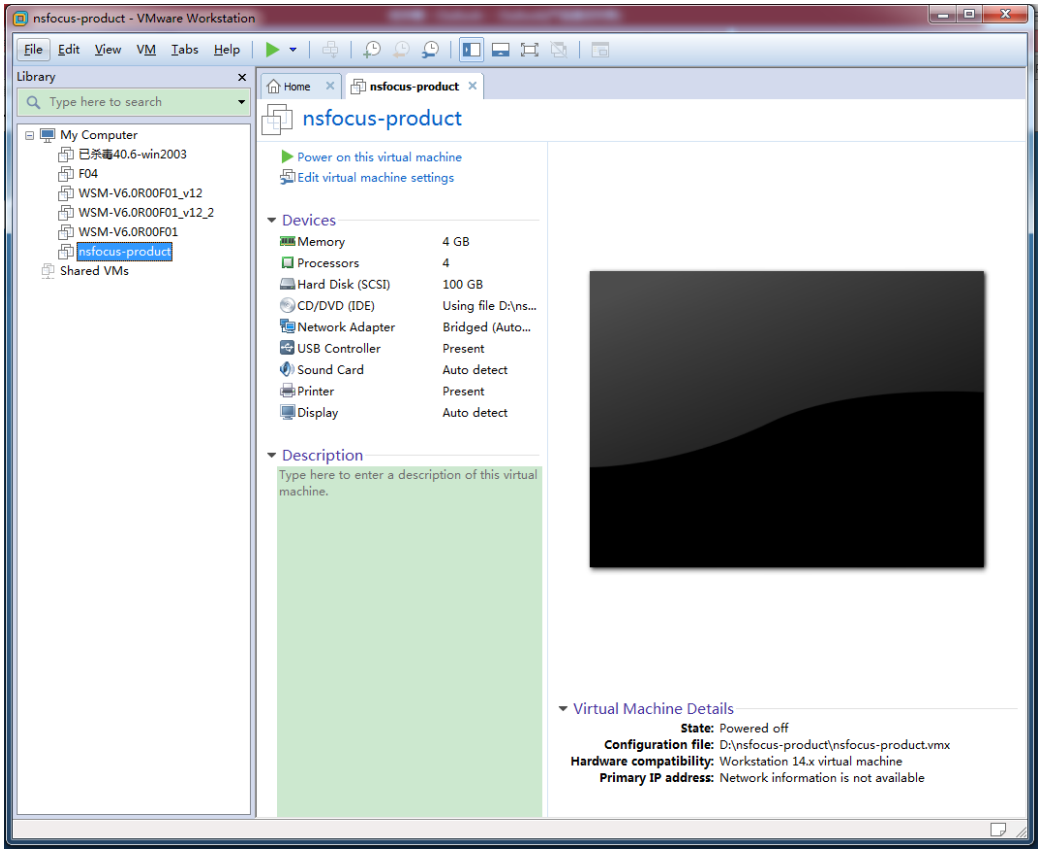
To install the image file of vRSAS, follow these steps:

Step 1 Start VMware Workstation 14.

The home page of VMware Workstation 14 appears, as shown in Figure 2-25.

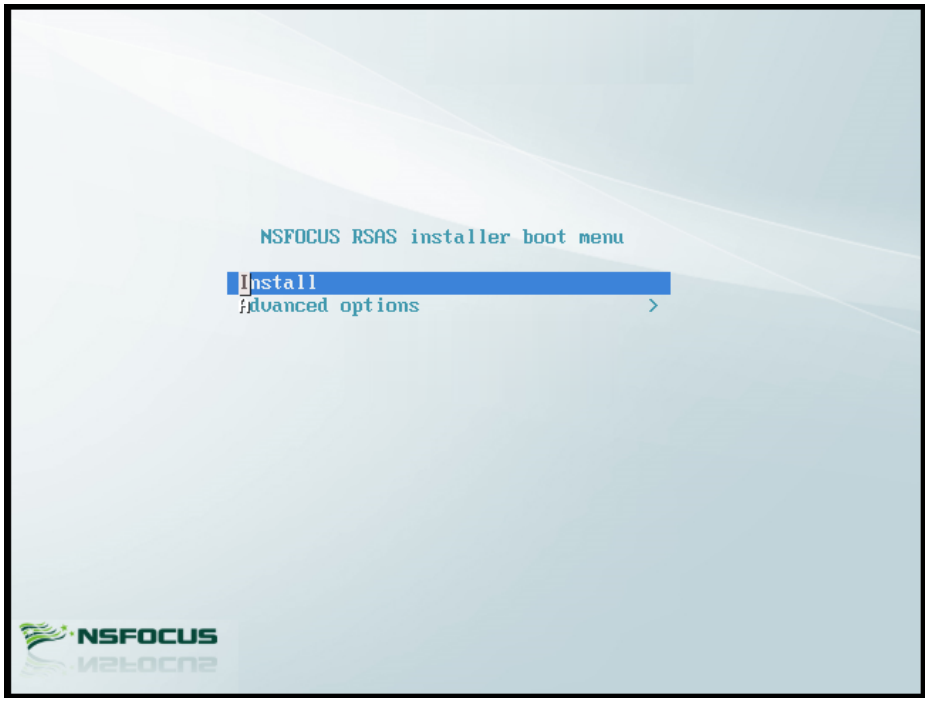
Step 2 Choose vRSAS (**nsfocus-product** in this document) from the left navigation tree and click **Power on this virtual machine**.

Figure 2-40 Selecting vRSAS to be installed



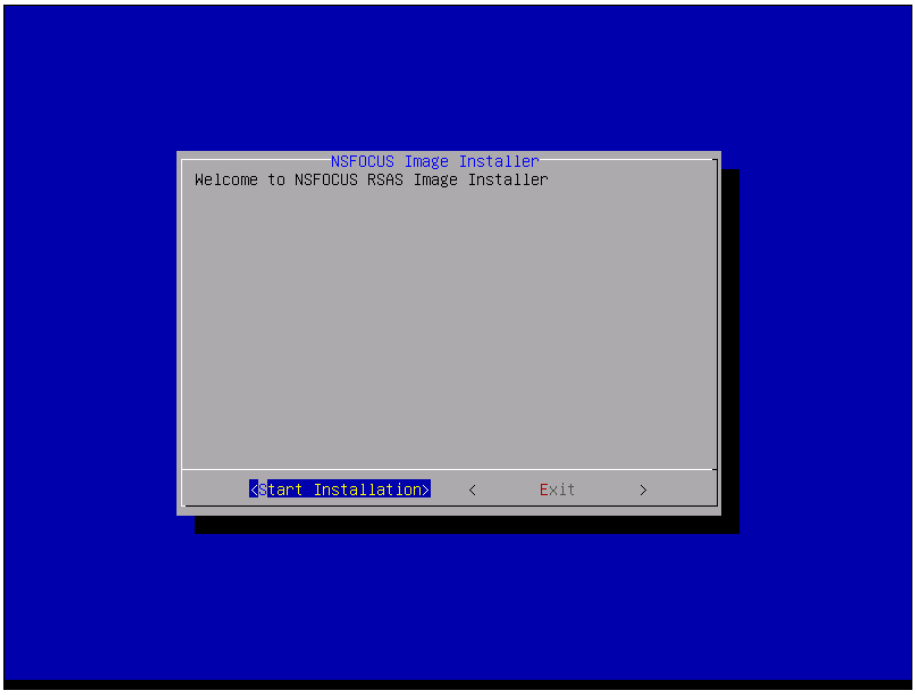
Step 3 On the installation page, select **Install**.

Figure 2-41 vRSAS installer boot menu



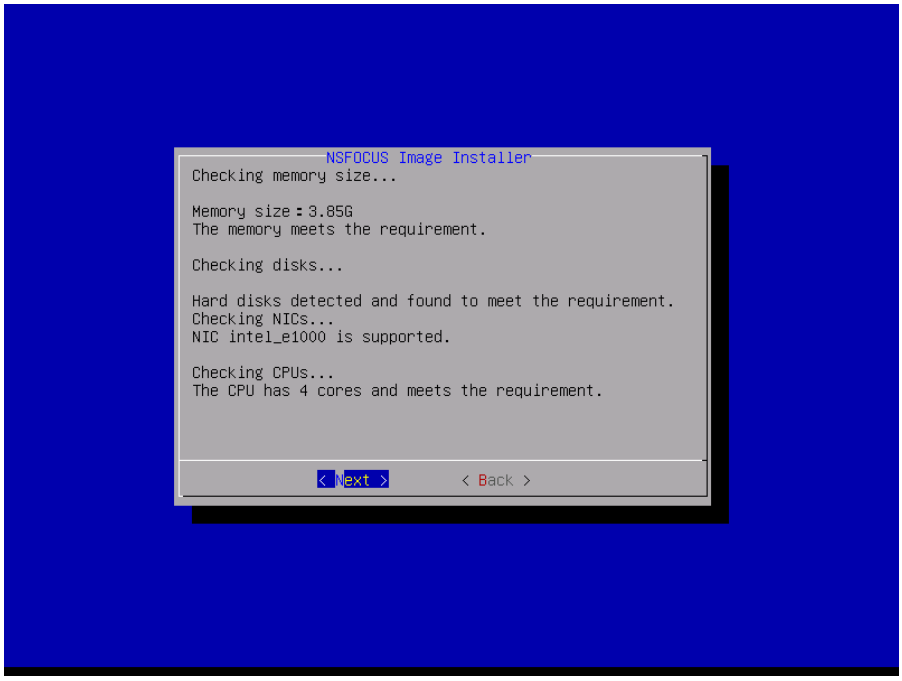
Step 4 On the welcome page, select **Start Installation**.

Figure 2-42 Starting to install vRSAS



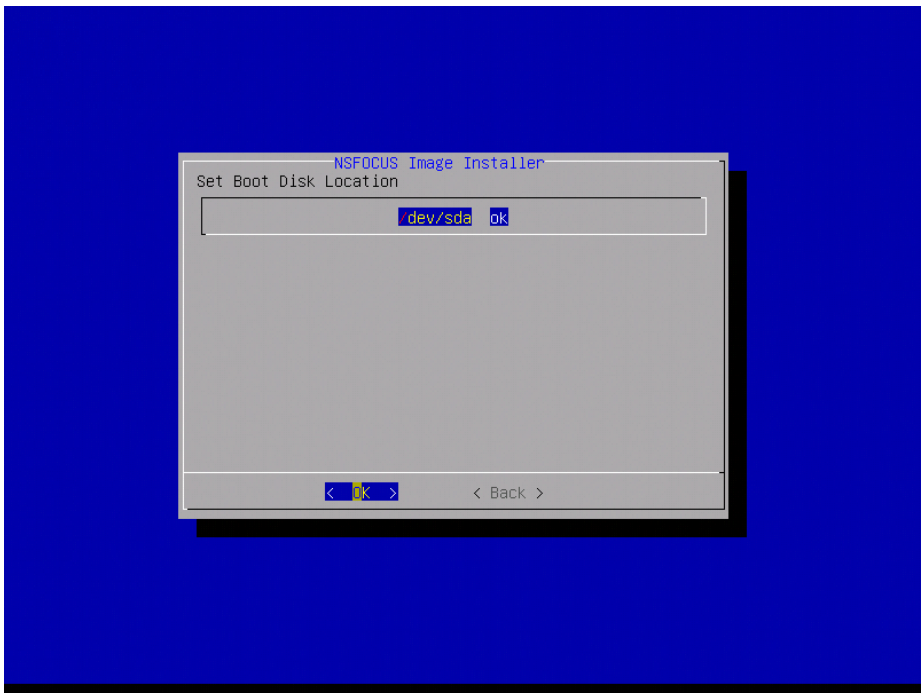
Step 5 After the system completes the check of VM configurations, select **Next**.

Figure 2-43 Checking configurations



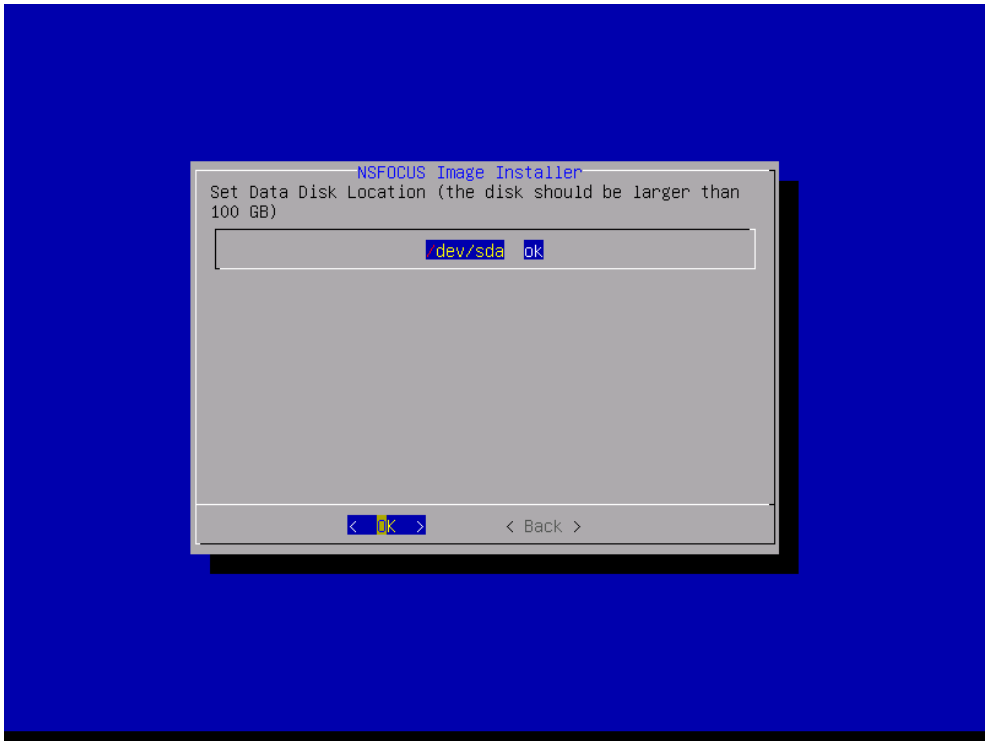
Step 6 Specify the boot drive location and select **OK**.

Figure 2-44 Specifying the boot drive location



Step 7 Specify the data disk location and select **OK**.

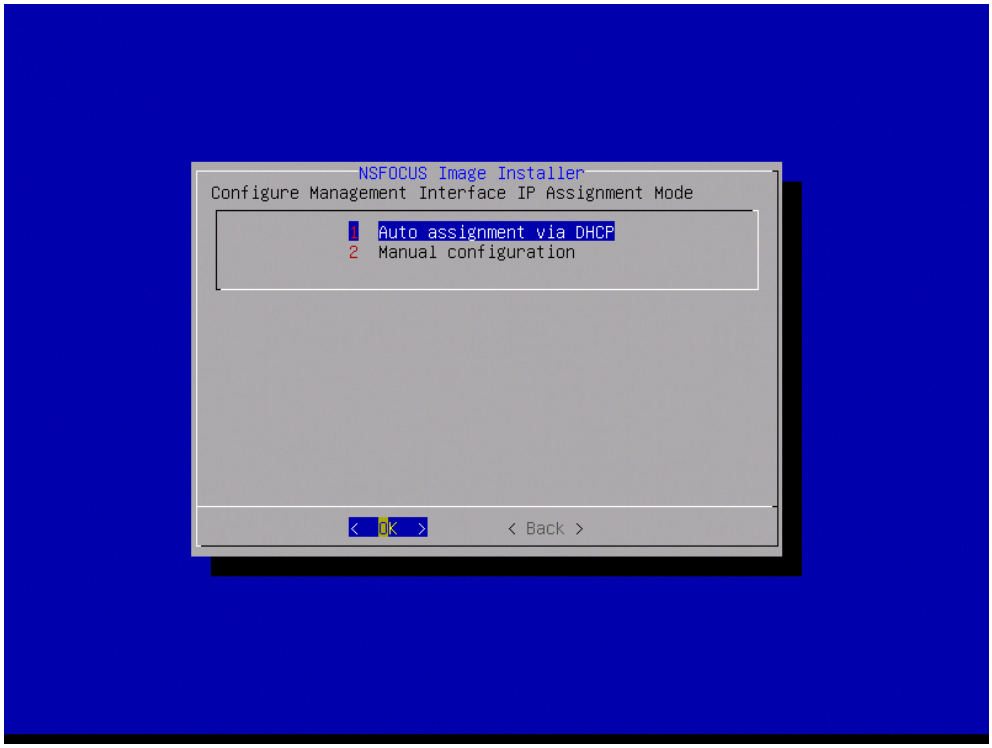
Figure 2-45 Specifying the data disk location



Note	The "later_install" prompt indicates that there is only one virtual disk, which is smaller than 150 GB, and the subsequent system startup verification fails. In this case, you need to manually add a disk larger than 150 GB after completing all installation procedures and turning off vRSAS.

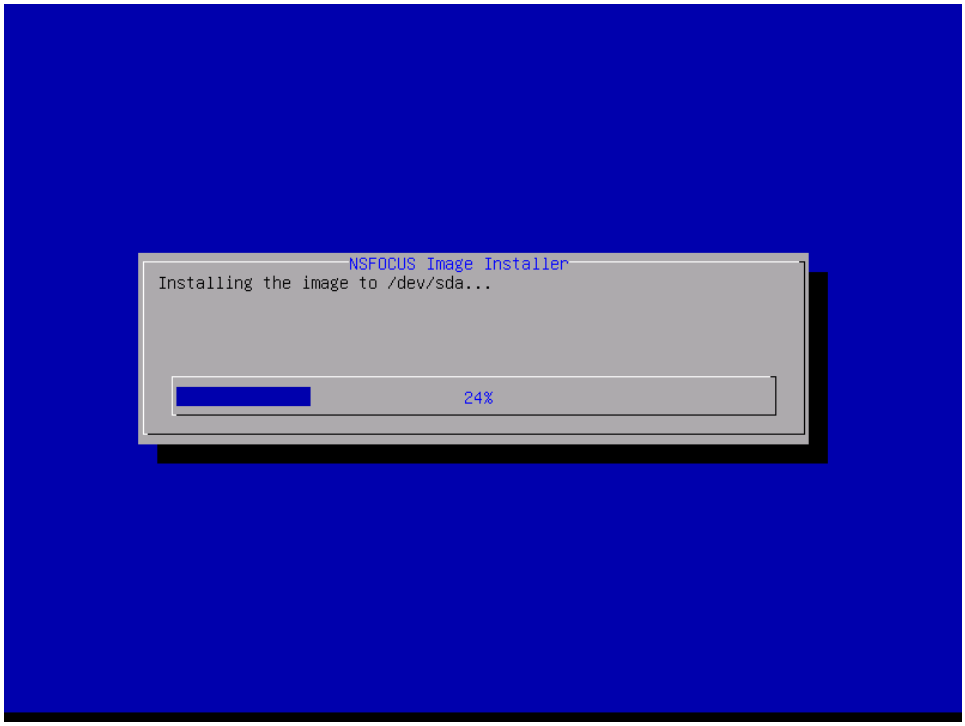
Step 8 Specify a method for obtaining the management interface IP address and select **OK**.

Figure 2-46 Configuring an IP address for the management interface



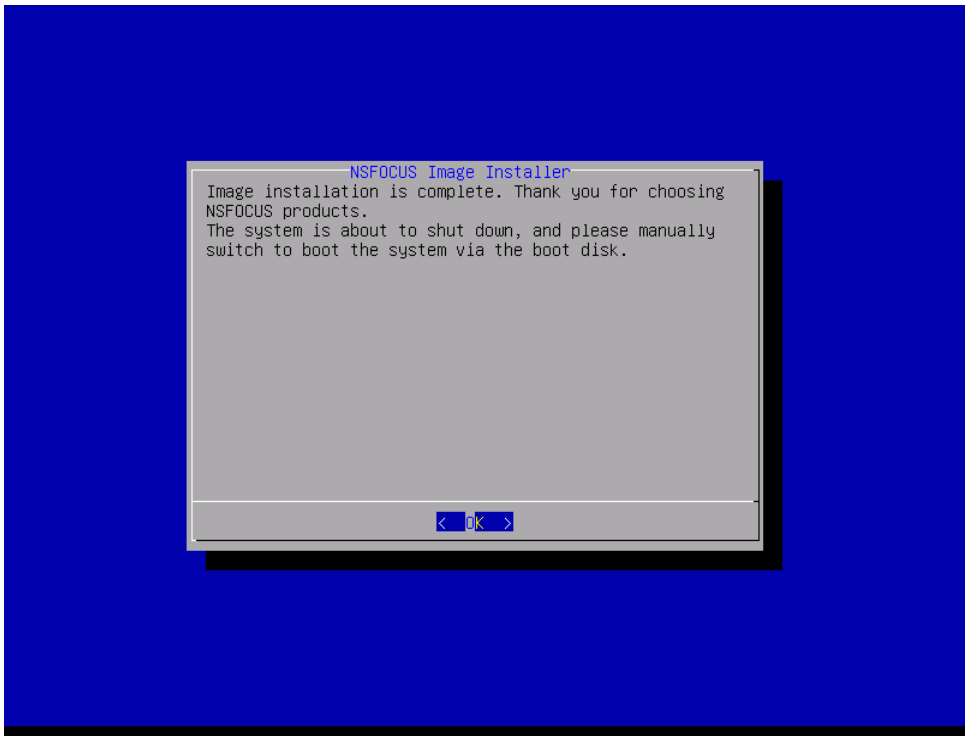
vRSAS starts to be installed, as shown in Figure 2-47.

Figure 2-47 Installing the image file of vRSAS



Step 9 After the installation is complete, select **OK**.

Figure 2-48 Installation completed



Step 10 Add a network adapter.

vRSAS only provides one network interface (that is, management interface) by default. You need to add a network adapter to enable the scan interface.

a. Choose the vRSAS image from the left navigation tree, as shown in Figure 2-40.

b. Choose **VM > Settings**.

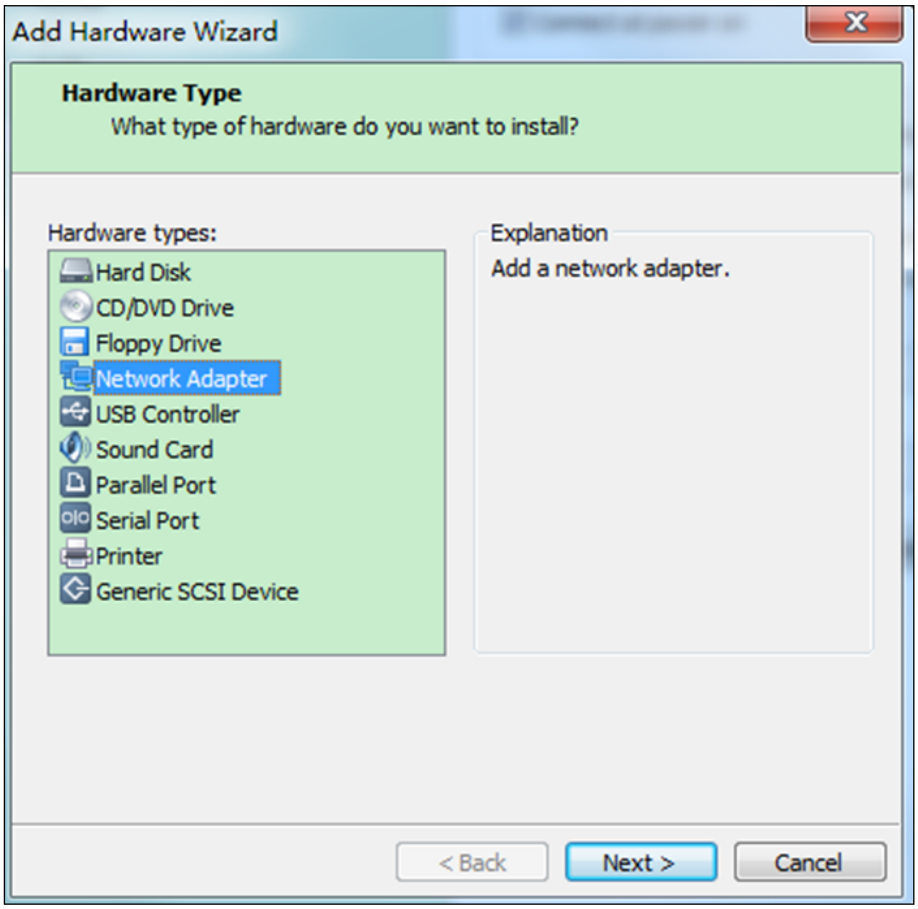
The **Virtual Machine Settings** dialog box appears.

Note	The network adapter matches the management interface of vRSAS. Network adapters 2–7 match scan interfaces eth1–6 of vRSAS.

c. Click **Add**.

The **Add Hardware Wizard** appears, as shown in Figure 2-49.

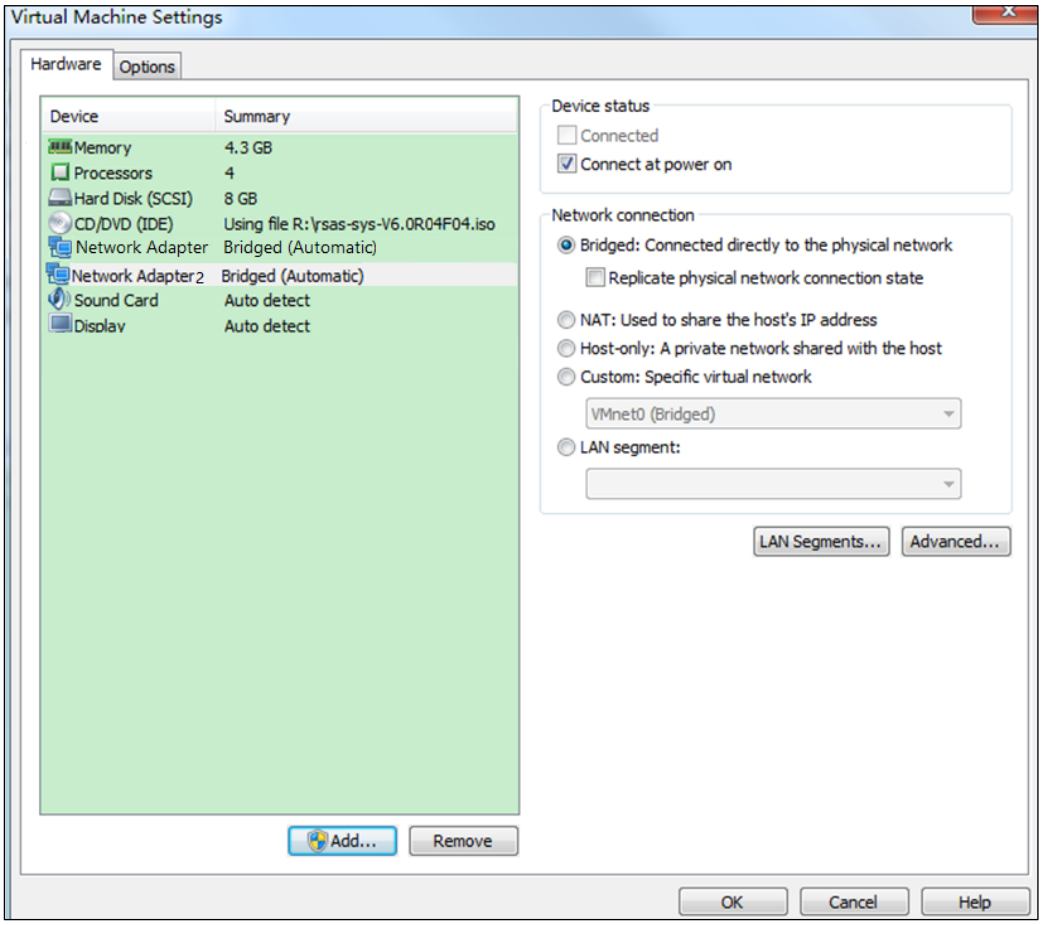
Figure 2-49 Adding hardware



d. In the **Add Hardware Wizard** dialog box, select **Network Adapter** and click **Finish** to return to the **Virtual Machine Settings** page.

e. On the page shown in Figure 2-50, select **Network Adapter 2**. In the **Device status** area, select the **Connect at power on** check box. Configure the network connection mode as required.

Figure 2-50 Configuring the network adapter 2



f. Click **OK** to finish the creation of the network adapter.

g. (Optional) Add other network adapters as required.

----End

Performing Initial Configuration

To perform the initial configuration of vRSAS, follow these steps:

Step 1 Start VMware Workstation 14.

The home page of VMware Workstation 14 appears, as shown in Figure 2-25.

Step 2 Log in to the console.

a. Choose vRSAS from the left navigation tree, as shown in Figure 2-40.

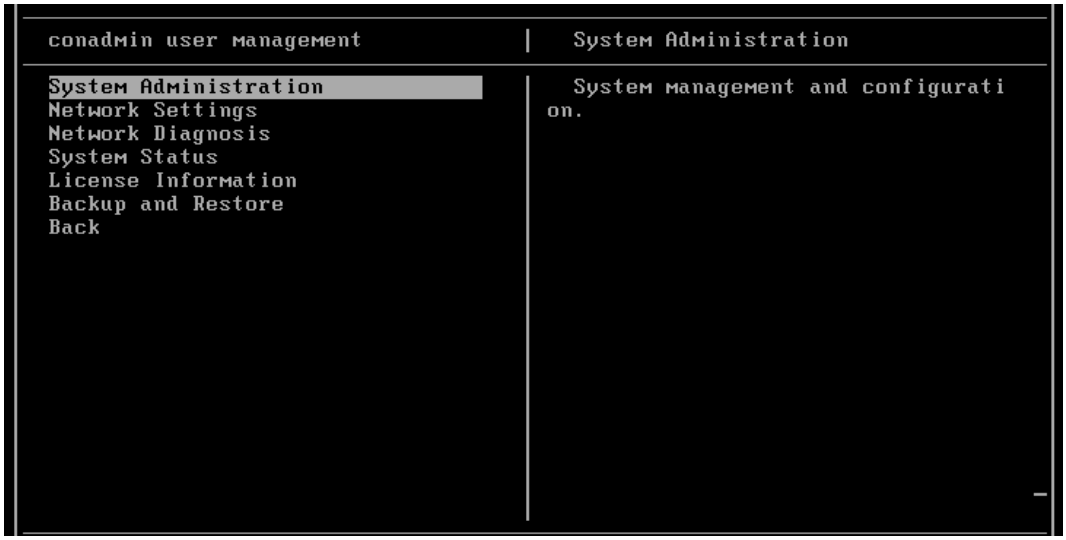
b. Choose **VM > Power > Start Up Guest** to start vRSAS.

Note	When started for the first time, vRSAS will be automatically installed. This will take several minutes. In other cases, the window shown in Figure 2-51 automatically opens.

Figure 2-51 Console

c. Type the console user name and password (initially **conadmin** for both) and press **Enter**. Then the configuration window appears, as shown in Figure 2-52.

Figure 2-52 Console configuration window



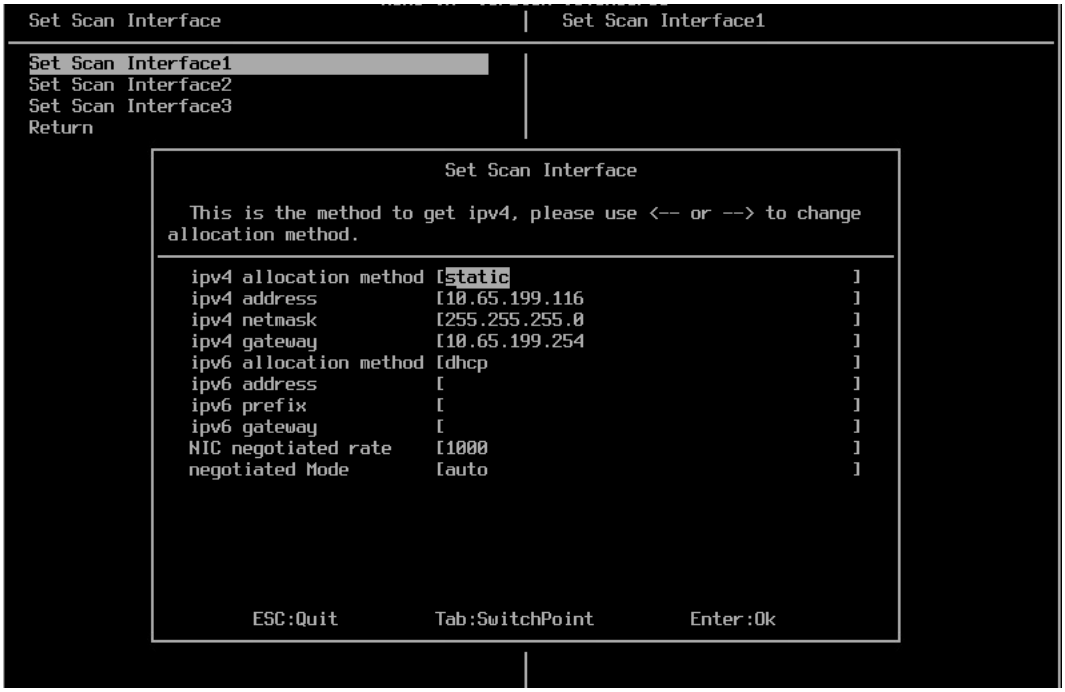
Step 3 Configure network settings.

a. Choose **Network Settings > Set Scan Interface > Set** *Scan Interface 1*.

b. In the window shown in Figure 2-53, use the left arrow (←) or right arrow (→) to select an IP address allocation method (**static** or **dhcp**). In the case of static configuration, further configure the IP address, netmask, and gateway of the scan interface *eth1*.

Note	• The network adapter matches the management interface of vRSAS. Network adapters 2–7 match scan interfaces eth1–6 of vRSAS. • For static IP address allocation, you need to manually configure an IP address. For DHCP, the DHCP server automatically allocates an IP address. In this case, vRSAS must properly connect to the DHCP server.

Figure 2-53 Configuring network settings



c. Press **Enter** to save the settings.

Step 4 (Optional) On the host, configure an IP address that is in the same network segment as the IP address of the eth1 interface. In addition, ensure the network connectivity of the host.

----End

Conducting License-based Authentication

Mounting the Dongle

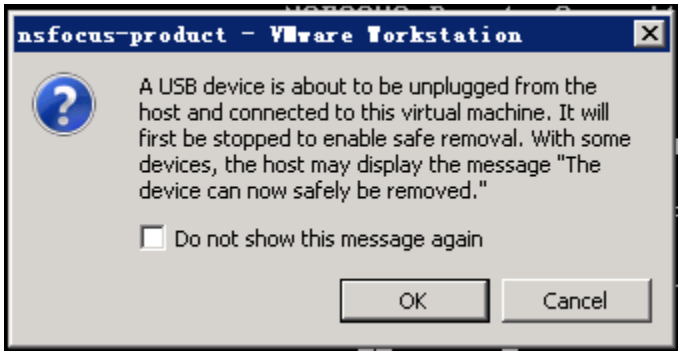
Caution	Do not remove the dongle when vRSAS is in use. Otherwise, vRSAS would automatically exit.

To mount the dongle, follow these steps:

Step 1 Insert the dongle in the VMware Workstation host.

Step 2 Choose **VM > Removable Devices >** *Philips USB device* > **Connect (Disconnect from host)** to connect the dongle to vRSAS.

Figure 2-54 Message prompting dongle connection

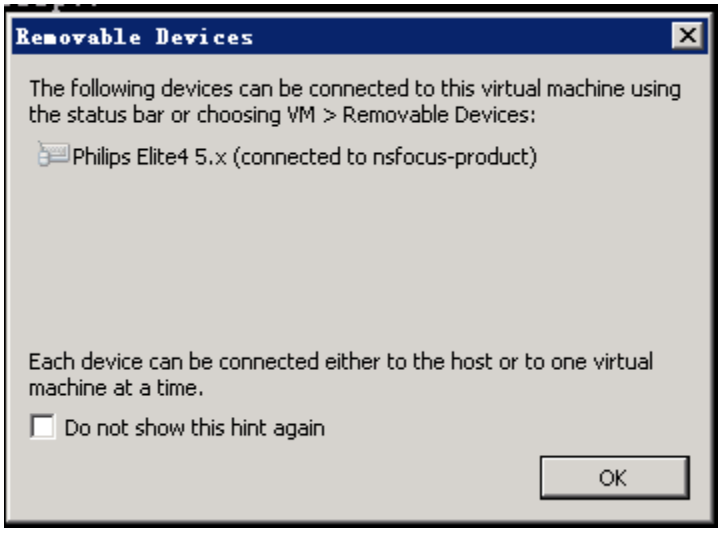


Step 3 Select the **Do not show this message again** check box and click **OK**.

Step 4 Choose **VM > Removable Devices >** *Philips USB device* > **Show in Status Bar**.

In the dialog box shown in Figure 2-55, select the **Do not show this hint again** check box and click **OK**.

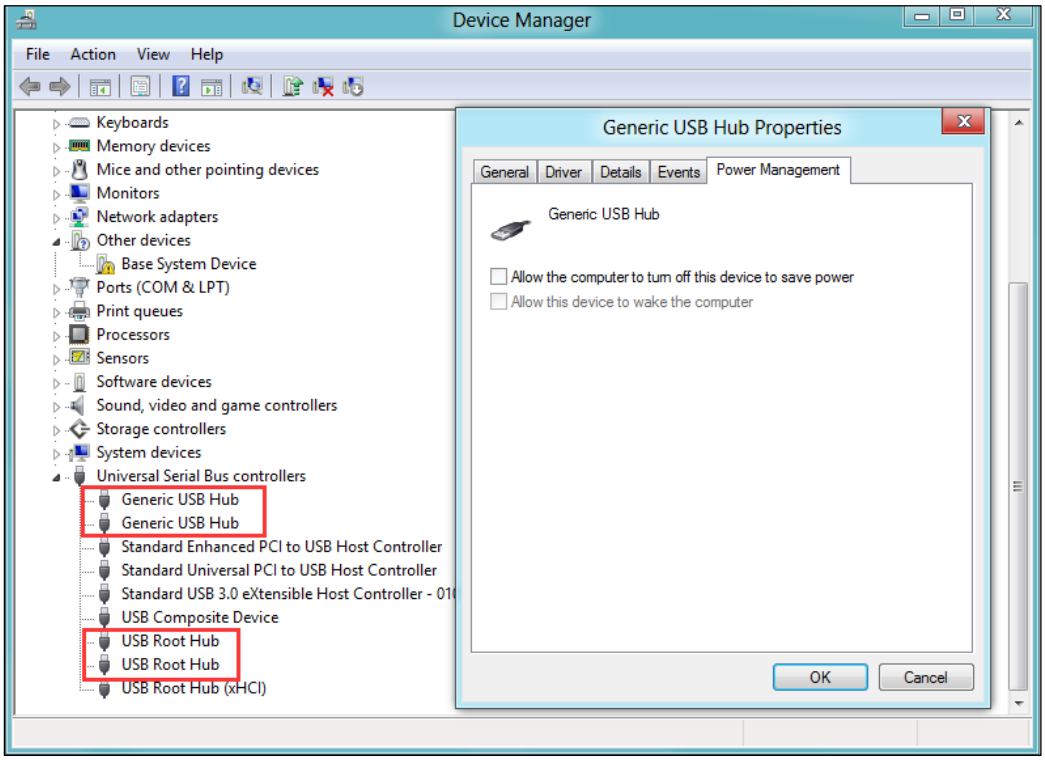
Figure 2-55 Removable Devices dialog box



Step 5 (Optional) Disable the power saving mode of the USB port.

Choose **Start > Control Panel > Device Manager**, expand **Universal Serial Bus controllers**, and double-click **Generic USB Hub** or **USB Root Hub**. In the **Generic USB Hub Properties** dialog box, click the **Power Management** tab and clear the **Allow the computer to turn off this device to save power** check box.

Figure 2-56 Power management



----End

Importing a License

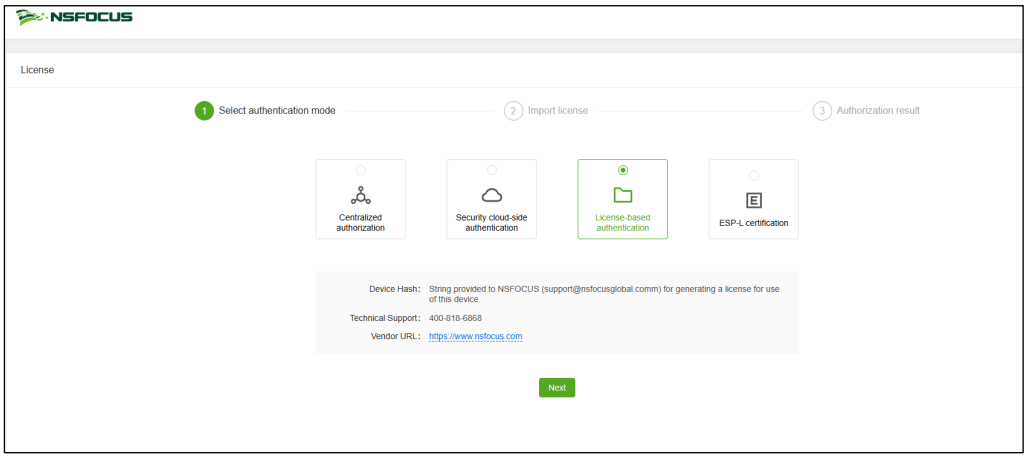
vRSAS can be activated only after a license is imported.

For details about authentication by a CAA platform and authentication by NSFOCUS security cloud, see Conducting License-based Authentication. To import a license, follow these steps:

Step 1 Access vRSAS by typing **https**://*IP address of scan interface eth1* in the address bar.

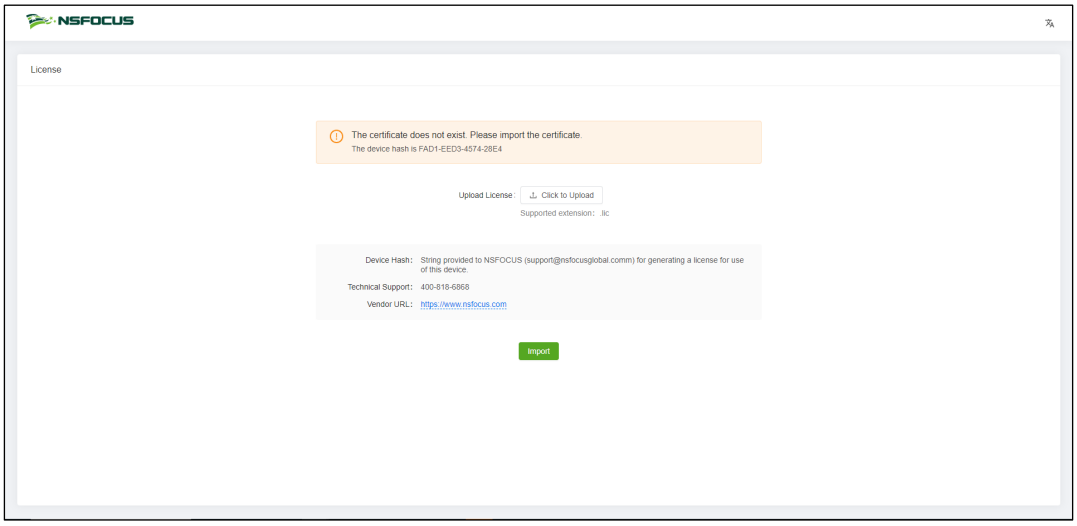
A page for authentication mode selection then appears, as shown in Figure 2-57.

Figure 2-57 Authentication mode selection page



Step 2 Select **License-based authentication** and click **Next**.

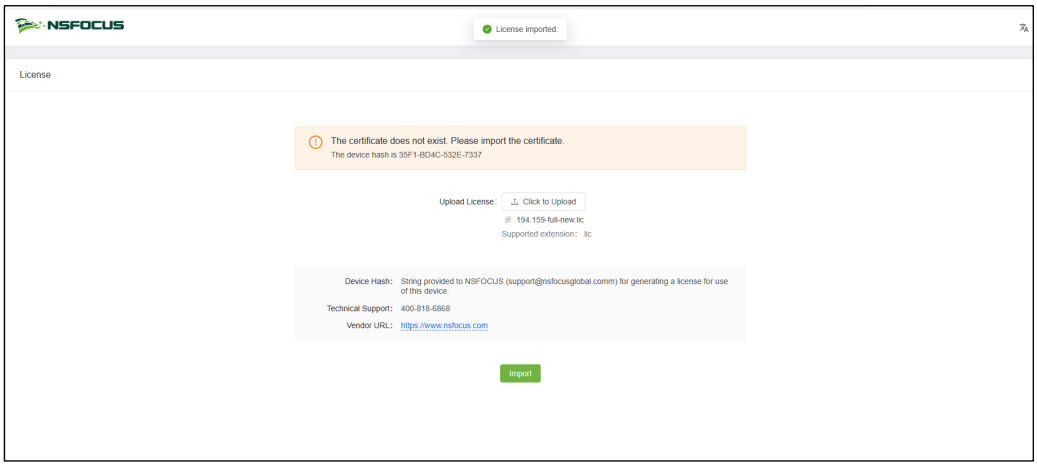
Figure 2-58 License import page



Step 3 Browse to a valid license and click **Import**.

Step 4 After the license is successfully imported, a dialog box prompting the import success appears. In this dialog box, click **OK**.

Figure 2-59 License imported



Step 5 On the RSAS login page that appears, type the user name and password.

----End

2.2.3.3 Uninstallation Procedure

To delete vRSAS from VMware Workstation 14, follow these steps:

Step 1 Start VMware Workstation 14.

The home page of VMware Workstation 14 appears, as shown in Figure 2-25.

Step 2 Choose vRSAS from the left navigation tree.

Step 3 Choose **VM > Power > Shut Down Guest** to shut down vRSAS.

Step 4 Choose **VM > Manage > Delete from Disk** to delete vRSAS from the hard drive.

vRSAS is then completely removed from the datastore.

----End

2.2.4 Installation on VMware vSphere ESXi

This section describes how to install vRSAS on VMware vSphere ESXi.

2.2.4.1 Preparations

Table 2-4 lists preparations to be made for installing vRSAS on VMware vSphere ESX.

Table 2-4 Preparations to be made for installing vRSAS on the ESXi platform

Item		Description
VMware vSphere ESXi server	IP address	IP address of a computer that can properly connect to the network.
	Account	Account with privileges of a system administrator.
vRSAS	CD	Contains an image file (.iso) of vRSAS.
	IP address	IP address of the scan interface of vRSAS.

Item		Description
	Authentication license	• License that enables vRSAS to be launched properly. • Unique authorization hash value granted to vRSAS.
		• IP address of a CAA platform and license of vRSAS. • License of vRSAS for authentication by NSFOCUS security cloud. • Dongle and license: The dongle should be already installed on the VMware vSphere ESXi server. Note You can select any one of the three authentication modes.

2.2.4.2 Installation Procedure

Obtaining the Image File of vRSAS

For how to obtain the image file of vRSAS, see Obtaining the Image File of vRSAS.

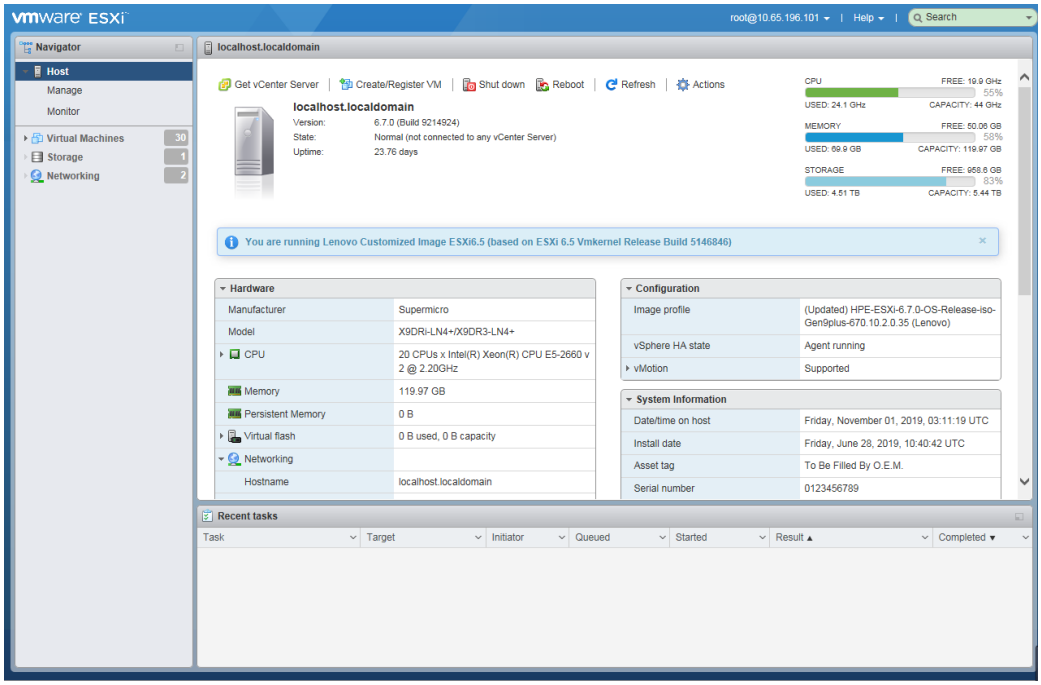
Creating a VM

To create a VM, follow these steps:

Step 1 Log in to the ESXi platform.

The ESXi home page appears, as shown in Figure 2-60.

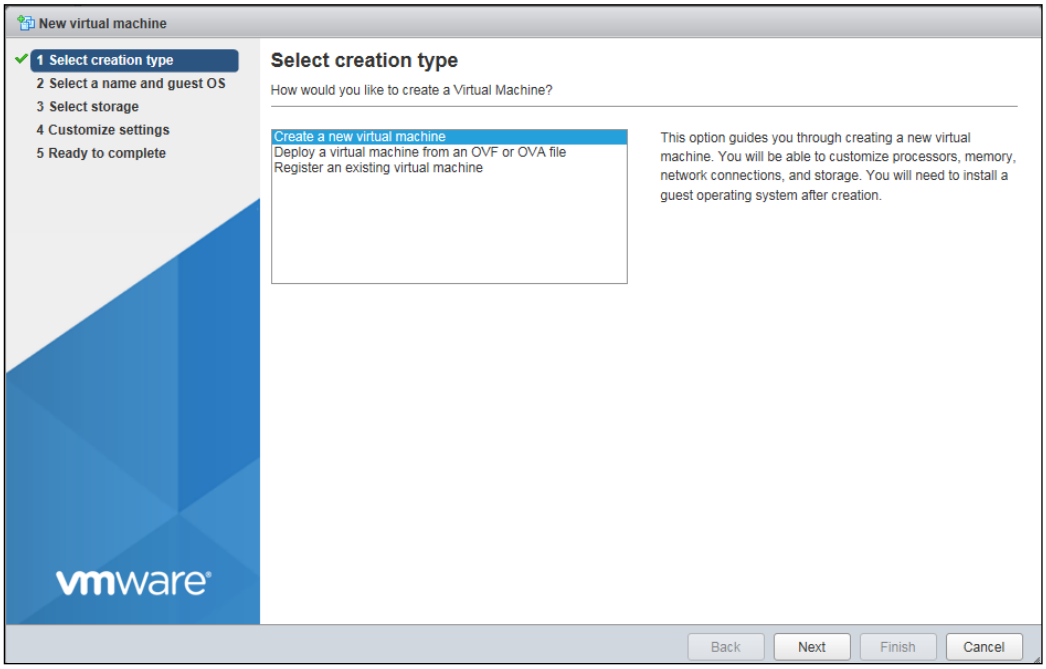
Figure 2-60 ESXi home page



Step 2 On the home page, click **Create/Register VM**.

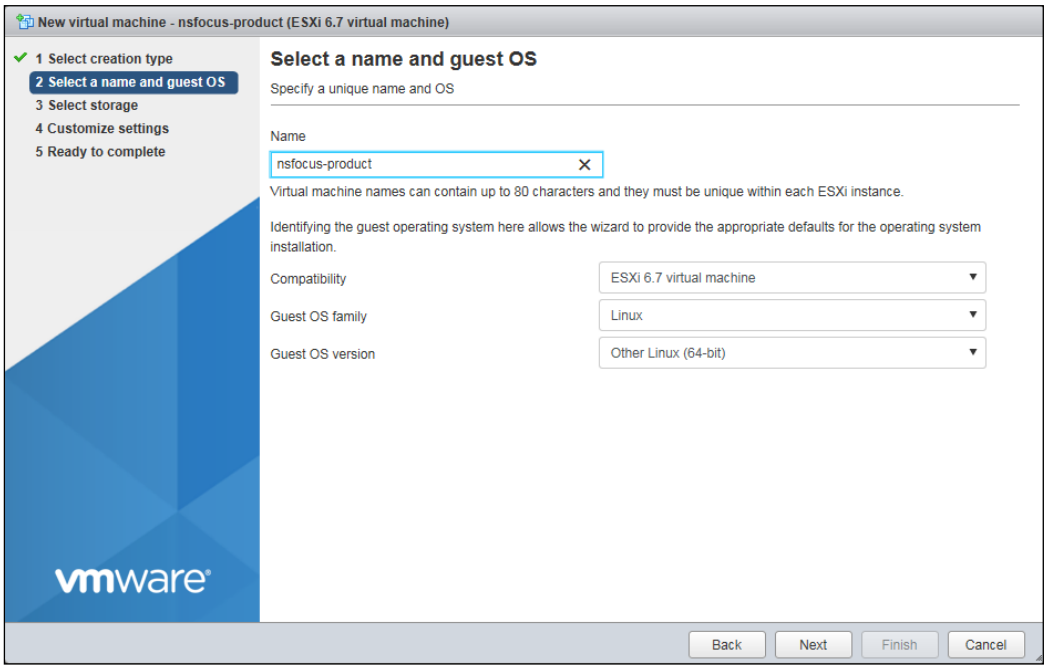
Step 3 On the **Select creation type** page, select **Create a new virtual machine** and click **Next**.

Figure 2-61 Selecting a creation type



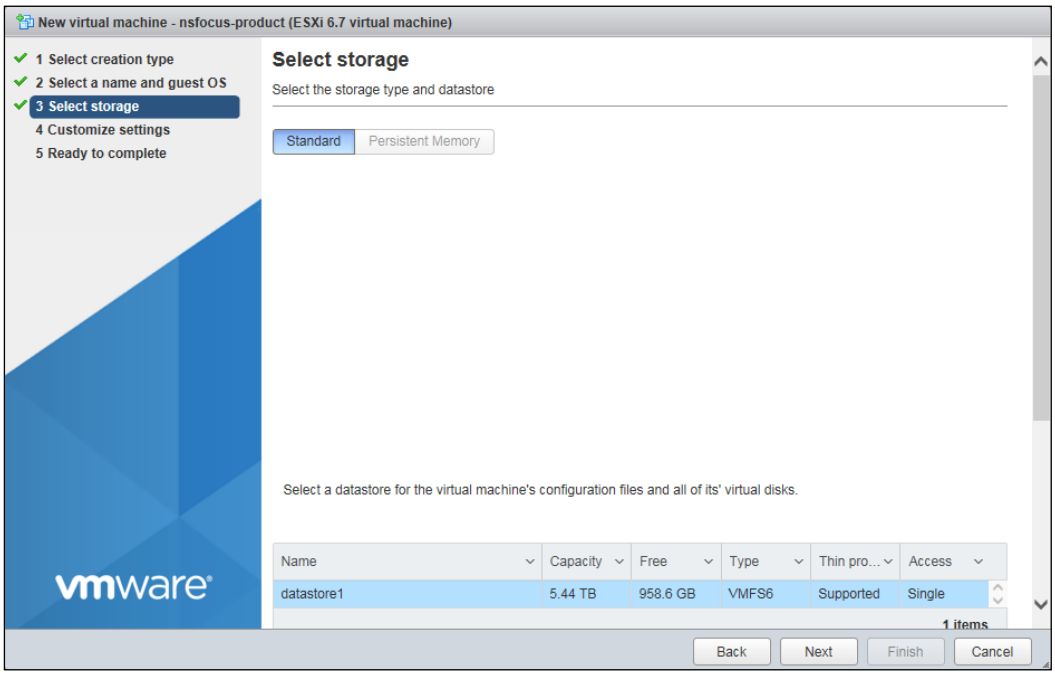
Step 4 On the **Select a name and guest OS** page, specify the name, compatible VM, guest OS family, and guest OS version, and then click **Next**.

Figure 2-62 Specifying a name and guest OS



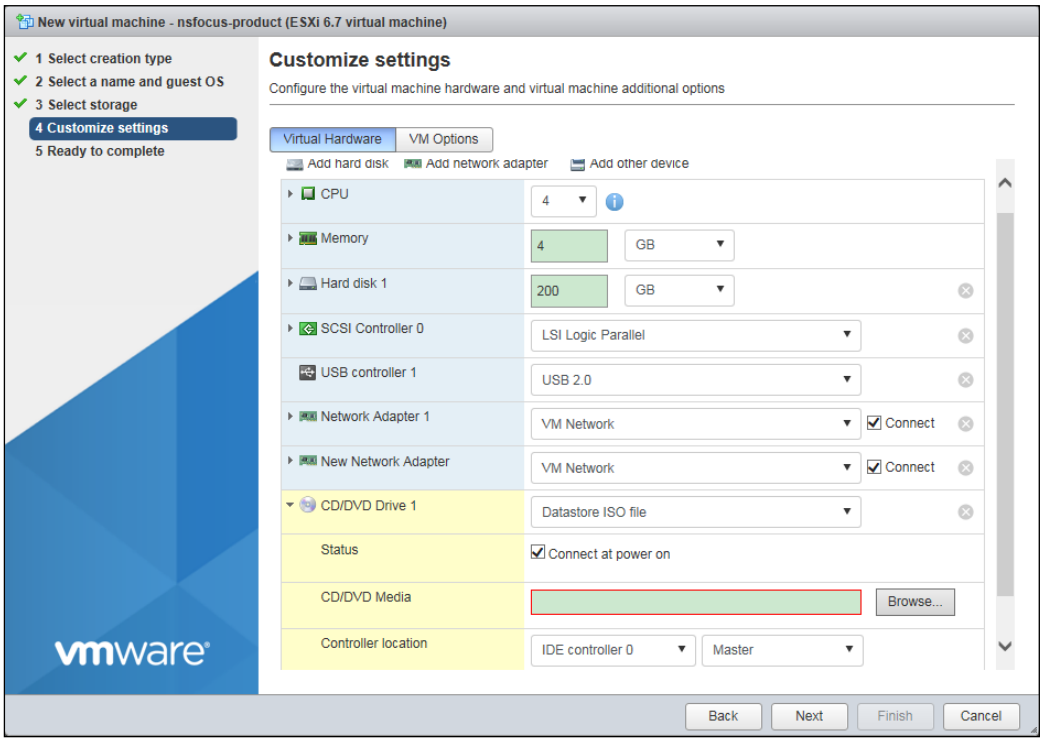
Step 5 On the **Select storage** page, click **Standard**, select **datastore1**, and click **Next**.

Figure 2-63 Selecting a storage



Step 6 On the **Customize settings** page, configure virtual hardware parameters according to the minimum configuration requirements listed in Table 2-1.

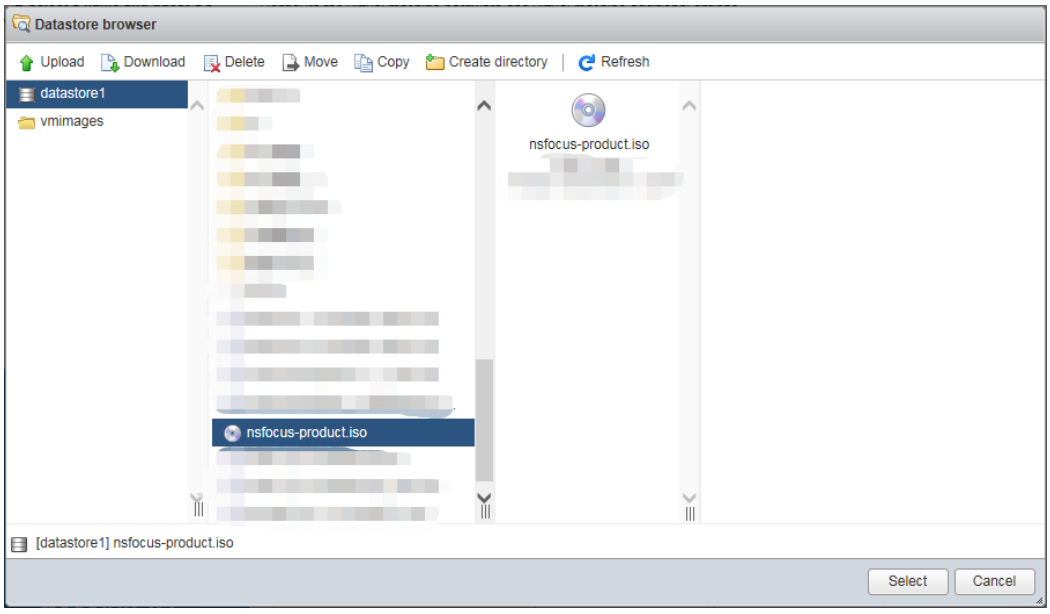
Figure 2-64 Customizing settings



Step 7 Mount the vRSAS image file.

a. In the **Customize settings** pane, select **Datastore ISO file** for **CD/DVD Drive 1**. The **Datastore browser** page appears, as shown in Figure 2-65.

Figure 2-65 Datastore browser page



b. Click **Upload** and, in the dialog box that appears, select the local vRSAS image file.

The upload progress is displayed in the upper-right corner of the page, as shown in Figure 2-66.

After the upload is complete, the icon of the image file is displayed, as shown in Figure 2-67.

Figure 2-66 Upload progress displayed

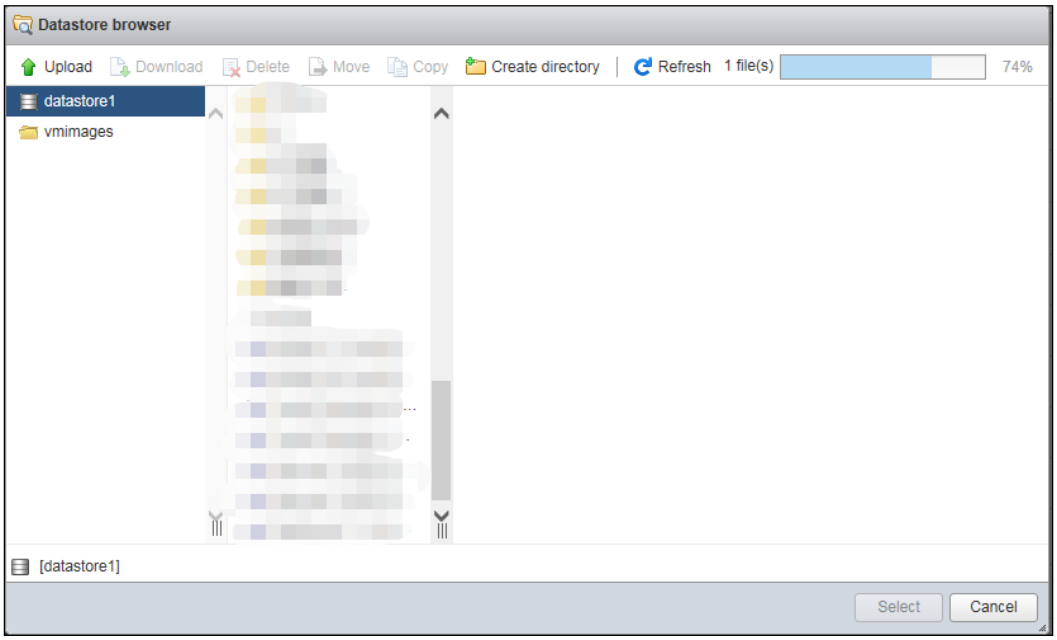
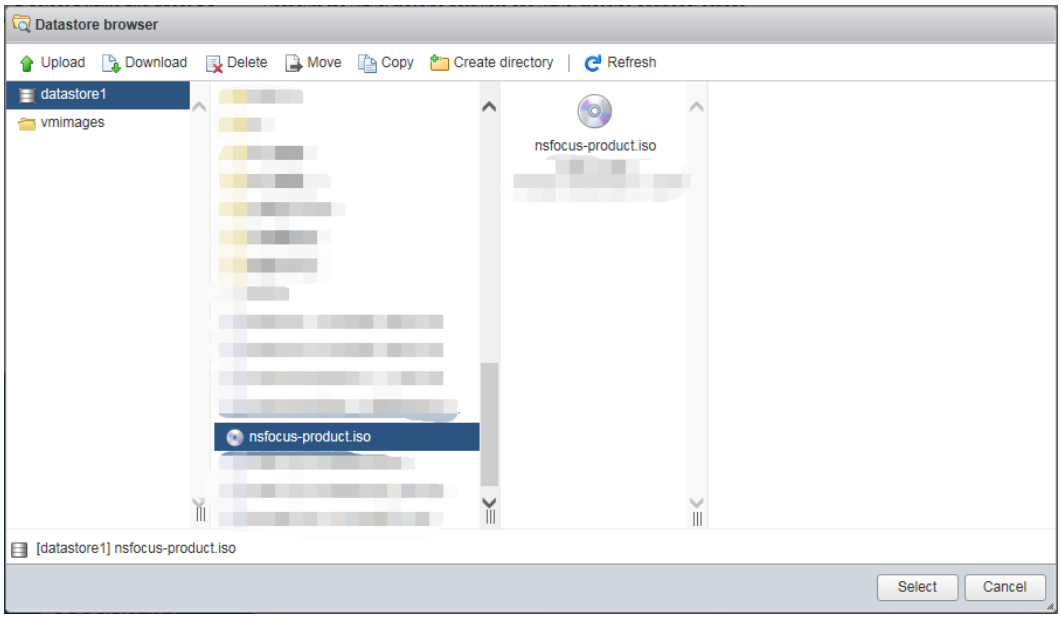


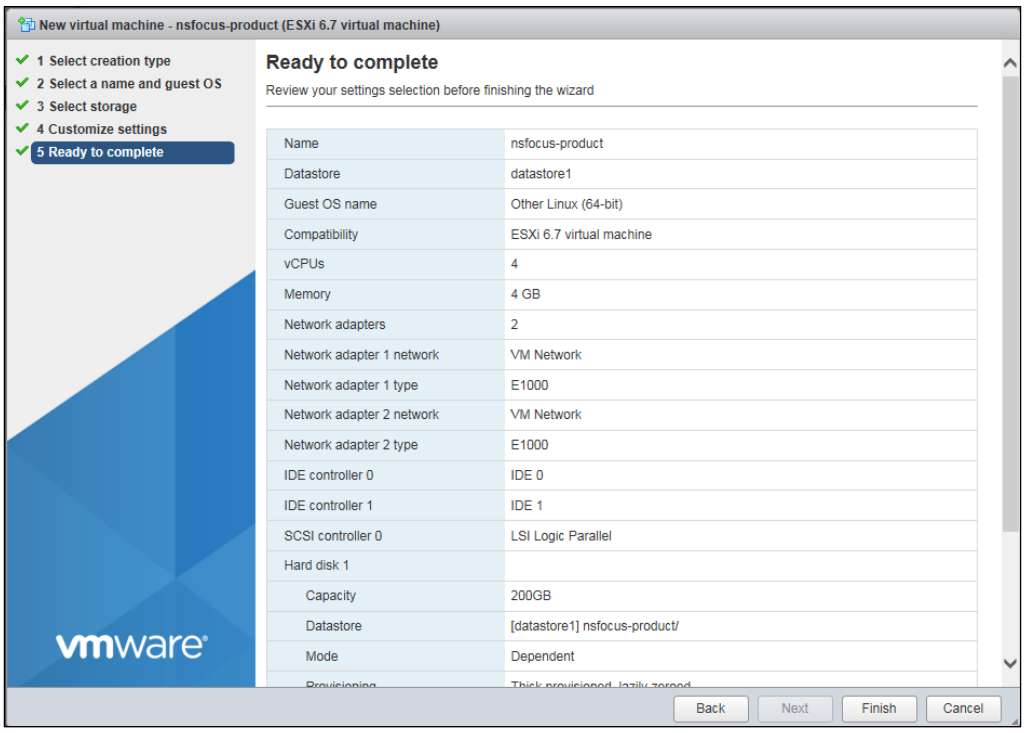
Figure 2-67 Upload completed



Step 8 Select the image file, click **Select** to return to the **Customize settings** page, and click **Next**.

Step 9 On the **Ready to complete** page, click **Finish**.

Figure 2-68 VM created for vRSAS



----End

Installing the Image File of vRSAS

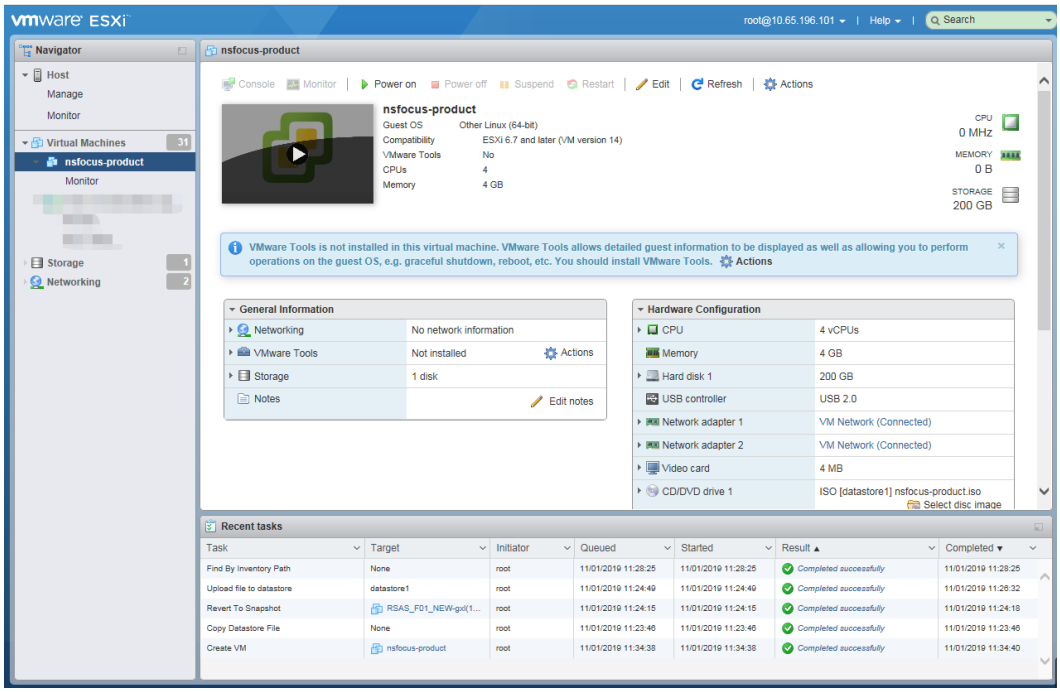
To install the image file of vRSAS, follow these steps:

Step 1 Log in to the ESXi platform.

The ESXi home page appears, as shown in Figure 2-60.

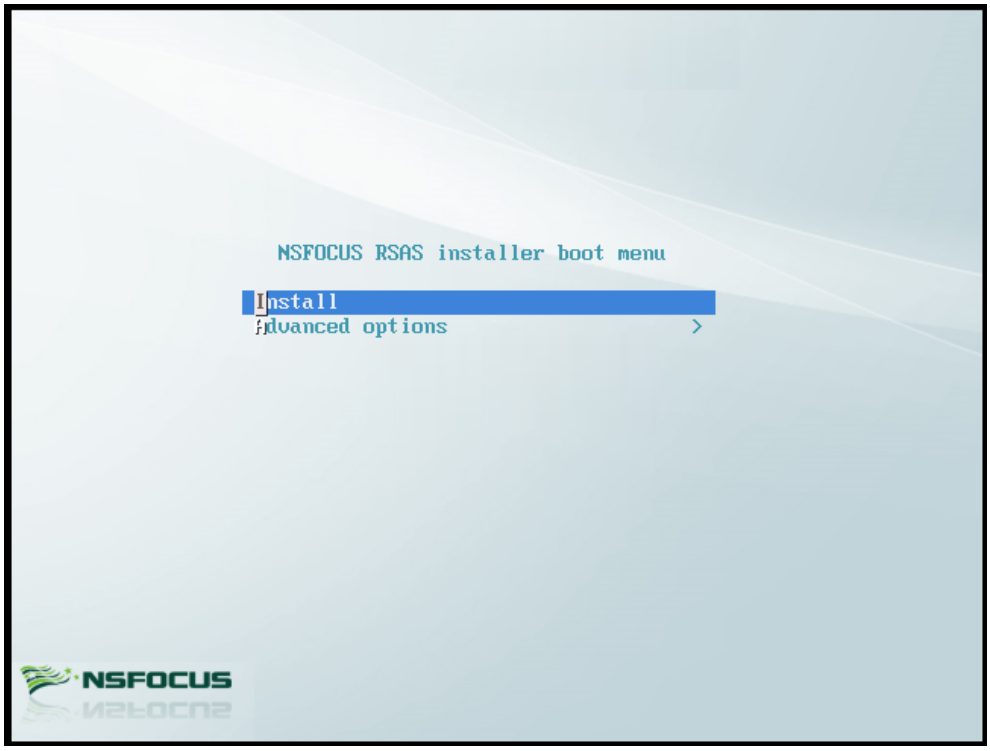
Step 2 Choose vRSAS (**nsfocus-product** in this document) from the left navigation tree, as shown in Figure 2-69.

Figure 2-69 Selecting vRSAS to be installed



Step 3 In the right pane, click **Power on**.

Figure 2-70 Console



Step 4 Install vRSAS.

The procedure of installing vRSAS on the ESXi platform is the same as that for the VMware Workstation platform described in Installing the Image File of vRSAS.

Step 5 Add a network adapter.

vRSAS only provides one network interface (that is, management interface) by default. Perform the following steps to add a network adapter to enable the scan interface.

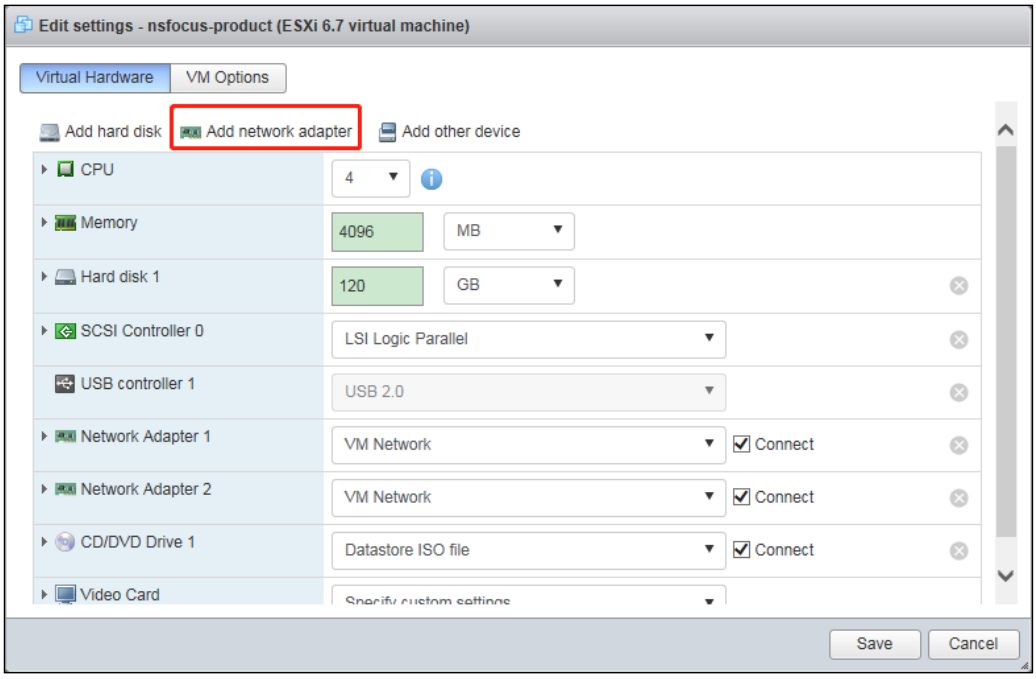
a. Choose vRSAS from the left navigation tree, as shown in Figure 2-69.

b. Click **Edit**.

The **Edit settings** dialog box appears.

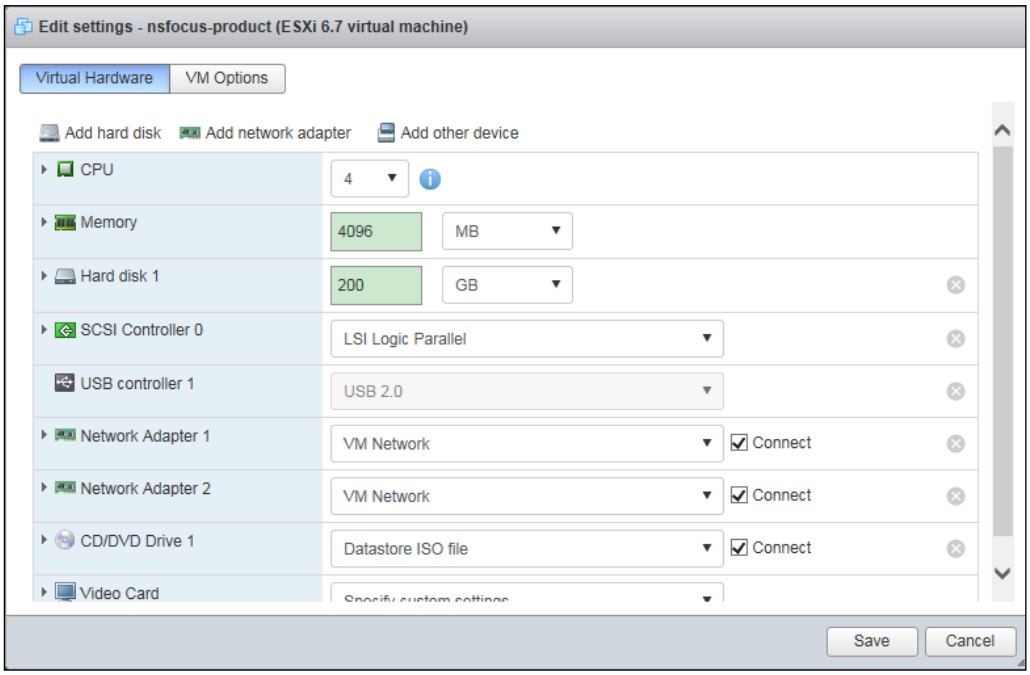
c. Click **Add network adapter** to add Network Adapter 2.

Figure 2-71 Adding a network adapter



d. On the page shown in Figure 2-72, configure the mode of Network Adapter 2 as required, and select the **Connect** check box in the right pane.

Figure 2-72 Configuring the network adapter 2



e. Click **Save**.

f. (Optional) Add other network adapters as required.

----End

Performing Initial Configuration

For how to perform initial configuration, see Performing Initial Configuration.

Conducting License-based Authentication

Mounting the Dongle

Caution	Do not remove the dongle when vRSAS is in use. Otherwise, vRSAS would automatically exit.

To mount the dongle, follow these steps:

Step 1 Insert the dongle in the VMware vSphere ESXi server.

Step 2 Log in to the ESXi platform.

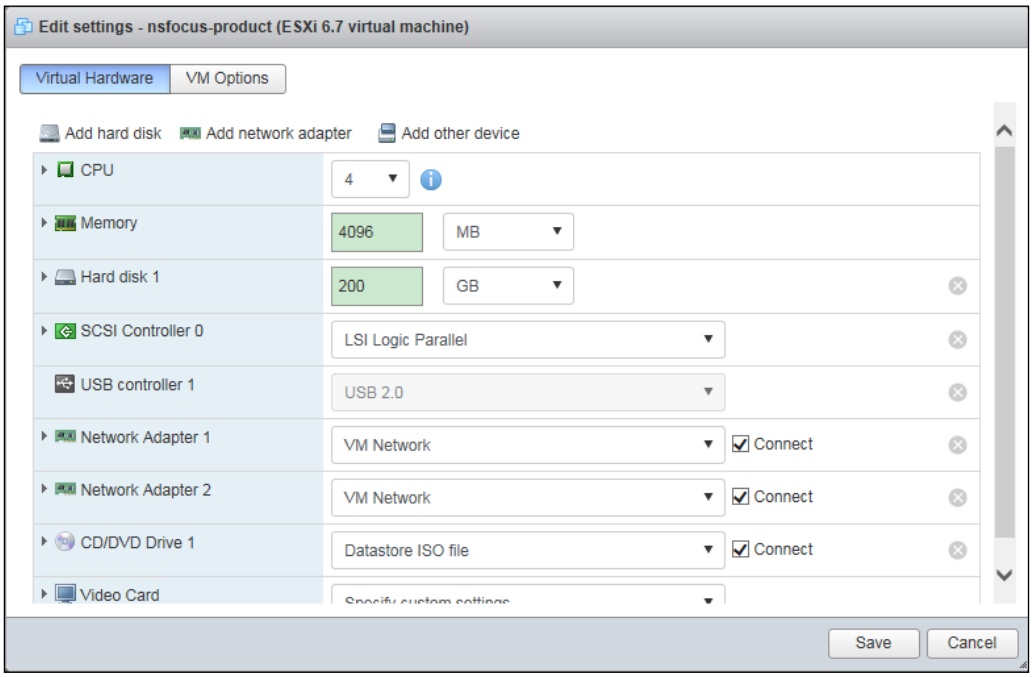
The ESXi home page appears, as shown in Figure 2-60.

Step 3 Choose vRSAS from the left navigation tree, as shown in Figure 2-69.

Step 4 Click **Edit**.

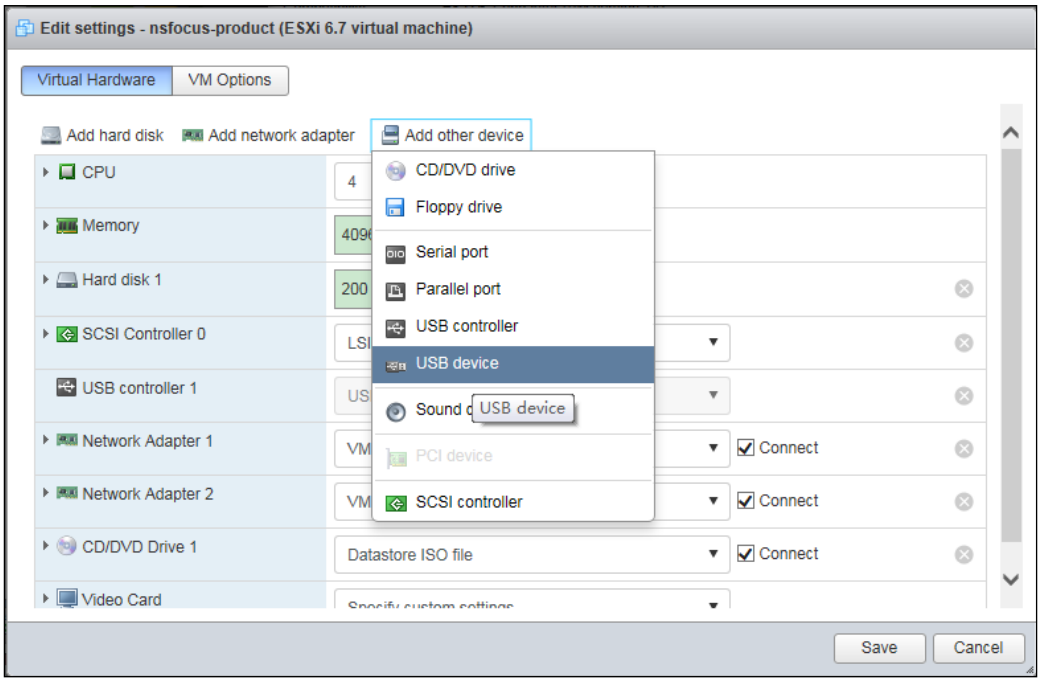
The **Edit settings** page appears, as shown in Figure 2-73.

Figure 2-73 Editing settings



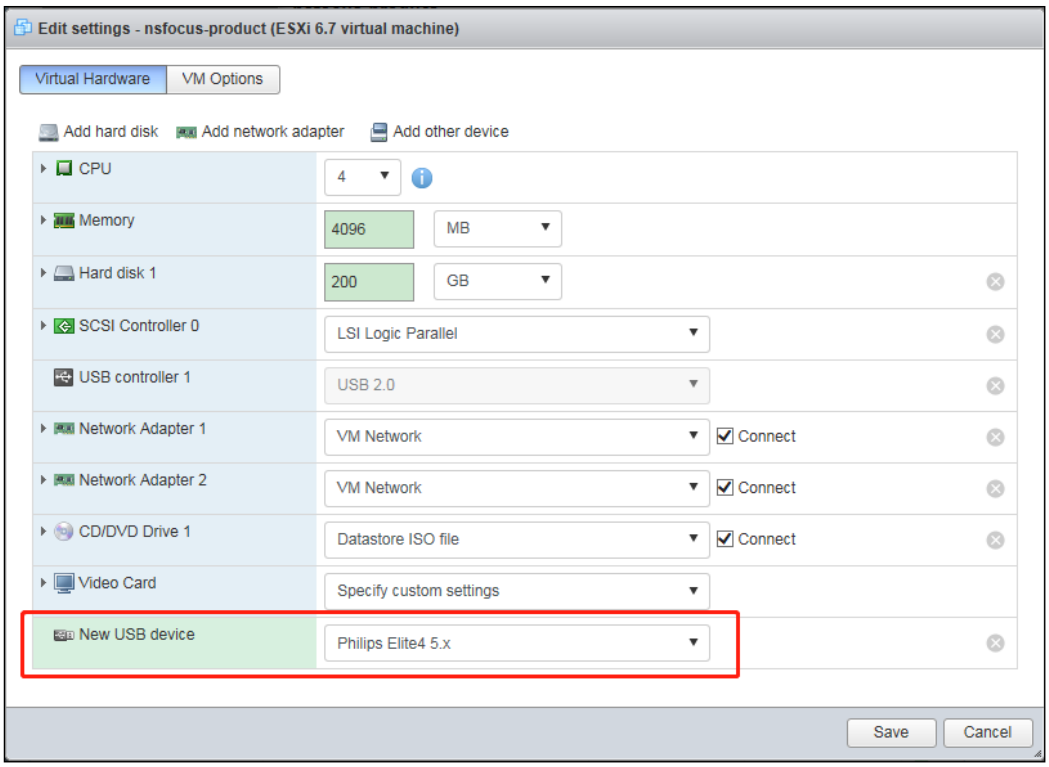
Step 5 On the **Edit settings** page, click **Add other device** and choose **USB device**.

Figure 2-74 Adding a USB device



Step 6 On the **Edit settings** page, select **Philips Elite4 5.x** as the new USB device and click **Save**.

Figure 2-75 Saving the dongle configuration



----End

Importing a License

For how to import a license, see Importing a License.

2.2.4.3 Uninstallation Procedure

To delete vRSAS from the ESXi platform, follow these steps:

Step 1 Log in to the ESXi platform.

The ESXi home page appears, as shown in Figure 2-60.

Step 2 Choose vRSAS from the left navigation tree, as shown in Figure 2-69.

Step 3 Click **Power off** to shut down RSAS.

Step 4 Choose **Actions > Delete**.

vRSAS is then completely removed from the datastore.

----End

2.2.5 Installation on FusionCompute

This section describes how to install vRSAS on FusionCompute.

2.2.5.1 Preparations

Table 2-5 lists preparations to be made for installing vRSAS on FusionCompute.

Table 2-5 Preparations to be made for installing vRSAS on the FusionCompute platform

Item		Description
FusionCompute server	IP address	IP address of a computer that can properly connect to the network.
	Account	Account with privileges of a system administrator.
vRSAS	CD	Contains an image file (.iso) of vRSAS.
	IP address	IP address of the scan interface of vRSAS.
	Authentication license	• License that enables vRSAS to be launched properly. • Unique authorization hash value granted to vRSAS.
		• IP address of a CAA platform and license of vRSAS. • License of vRSAS for authentication by NSFOCUS security cloud. • Dongle and license: The dongle should be already installed on the FusionCompute server. Note You can select any one of the three authentication modes.

2.2.5.2 Installation Procedure

Obtaining the Image File of vRSAS

For how to obtain the image file of vRSAS, see Obtaining the Image File of vRSAS.

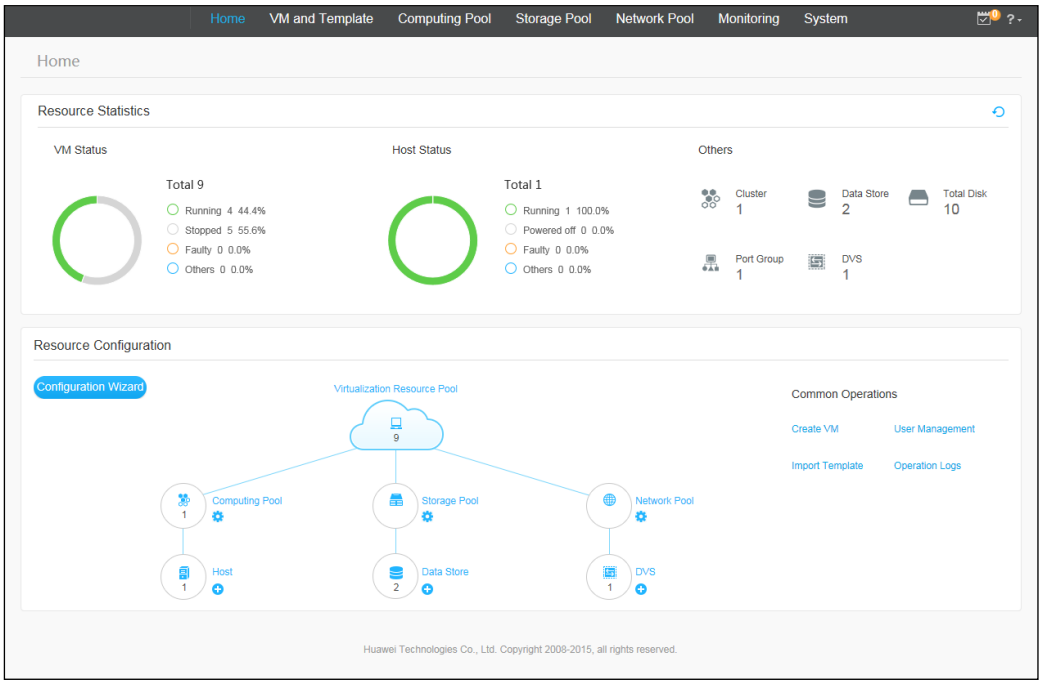
Creating a VM

To create a VM, follow these steps:

Step 1 Log in to the FusionCompute platform.

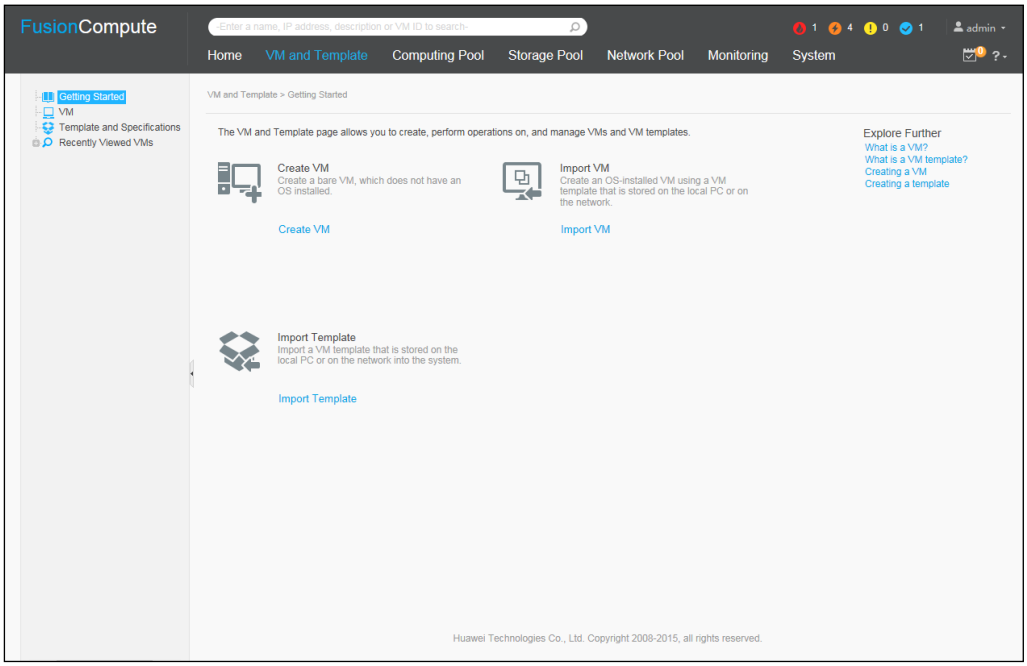
The FusionCompute home page appears, as shown in Figure 2-76.

Figure 2-76 Home page of FusionCompute



Step 2 Choose **VM and Template**.

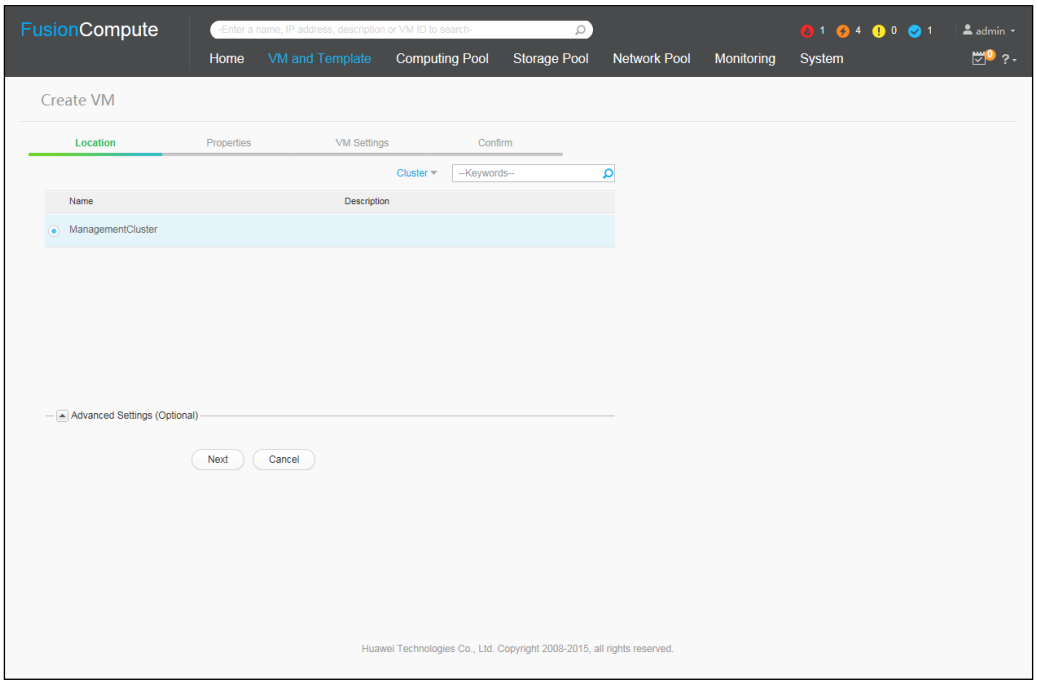
Figure 2-77 VM and Template page



Step 3 Click **Create VM**.

The **Create VM** page appears, as shown in Figure 2-78.

Figure 2-78 Create VM page

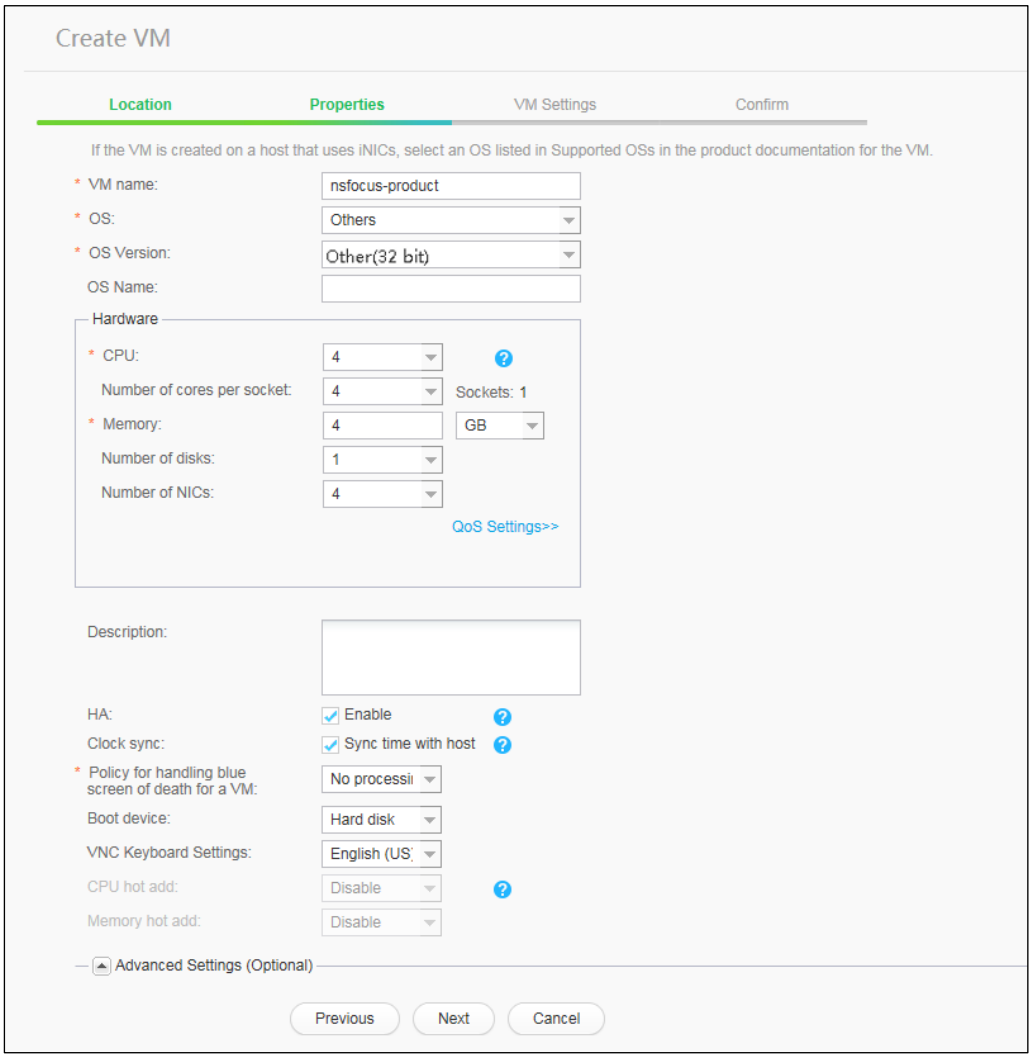


Step 4 Specify a location for the VM and click **Next**.

Step 5 On the **Properties** page, configure parameters and click **Next**.

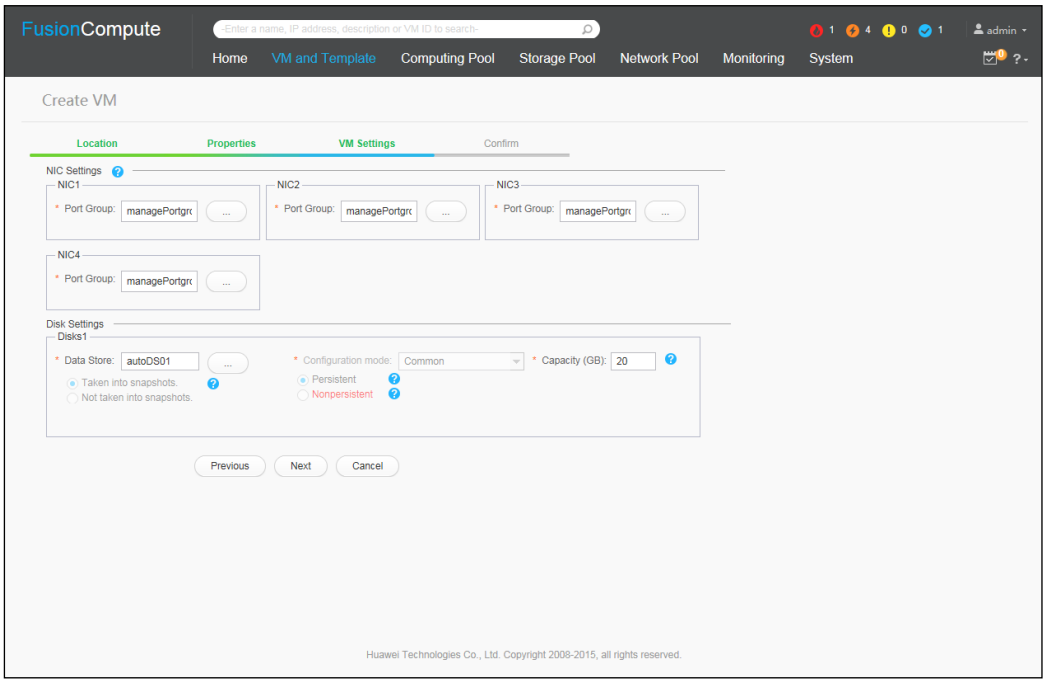
- Select **Others for OS** and **Other(32 bit)** for **OS Version**.
- Specify the size of memory and the number of CPUs according to the minimum configuration requirements listed in Table 2-1. Select **1** for **Number of disks**.

Figure 2-79 Properties page



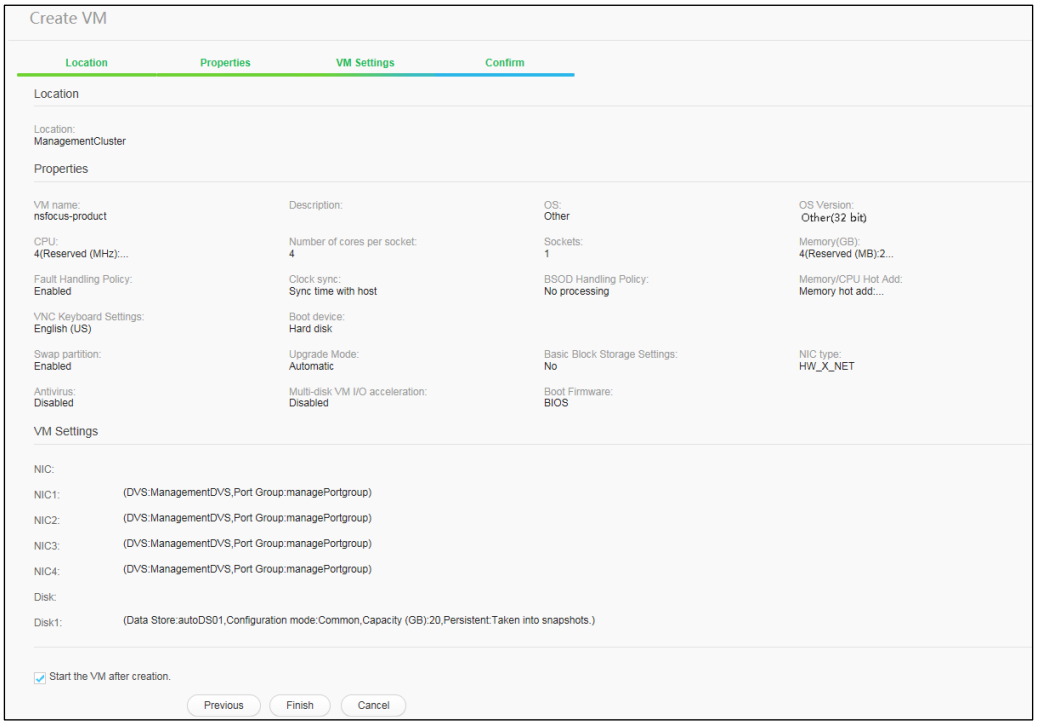
Step 6 On the **VM Settings** page, configure network interface cards (NICs) and disk parameters, and then click **Next**.

Figure 2-80 VM Settings page



Step 7 On the **Confirm** page, confirm that all information is correct and click **Finish**.

Figure 2-81 Confirm page



----End

Installing the Image File of vRSAS

To install the image file of vRSAS, follow these steps:

Step 1 Log in to the FusionCompute platform.

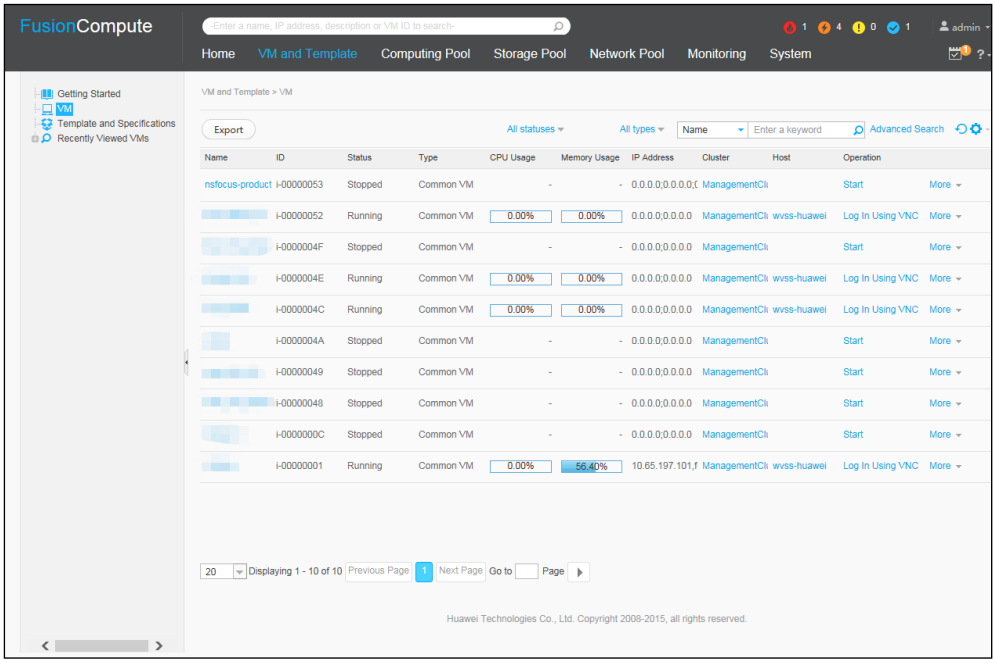
The FusionCompute home page appears, as shown in Figure 2-76.

Step 2 Choose **VM and Template**.

Step 3 On the page shown in Figure 2-77, choose **VM** from the left navigation tree.

The VM list appears, as shown in Figure 2-82.

Figure 2-82 VM list



Step 4 On the line of vRSAS, click **Start** in the **Operation** column. In the dialog box that appears, click **OK**.

Step 5 Log in to the console.

a. On the line of vRSAS, click **Log in Using VNC** in the **Operation** column.

b. In the dialog box that appears, click **noVNC**.

Figure 2-83 Selecting a VNC-based login method

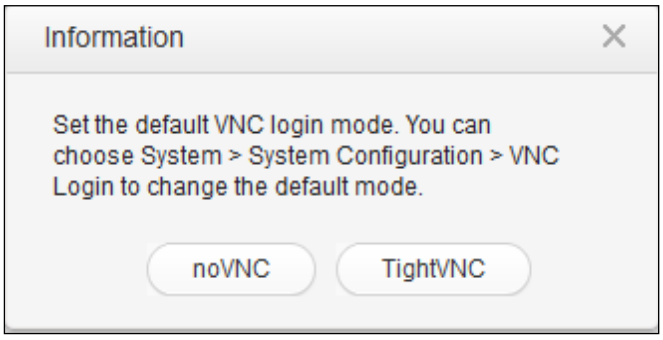
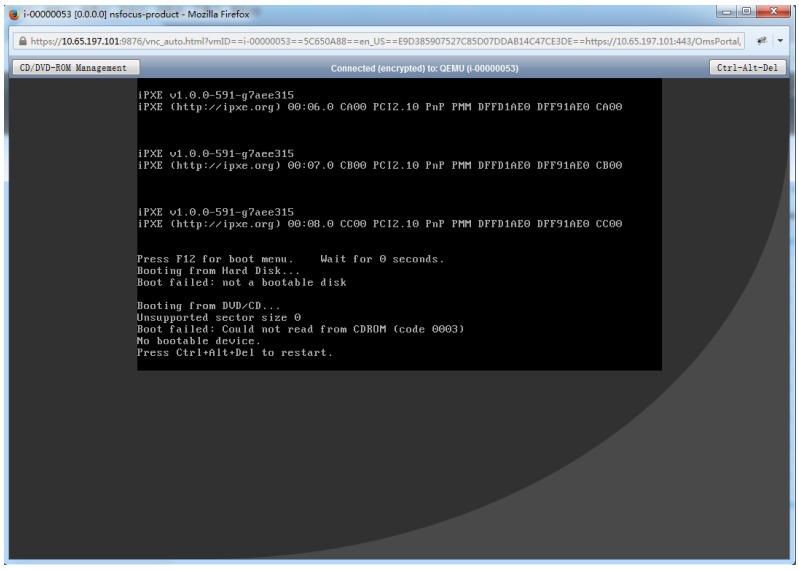


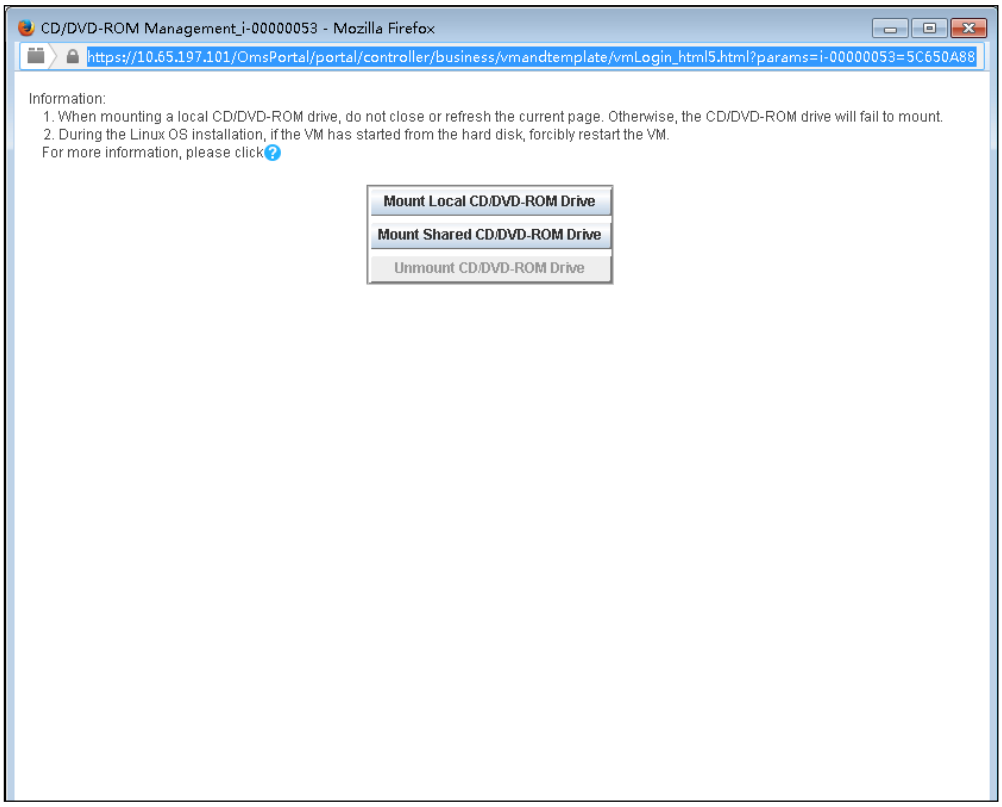
Figure 2-84 Page appearing after successful login



Step 6 Mount a CD/DVD-ROM drive.

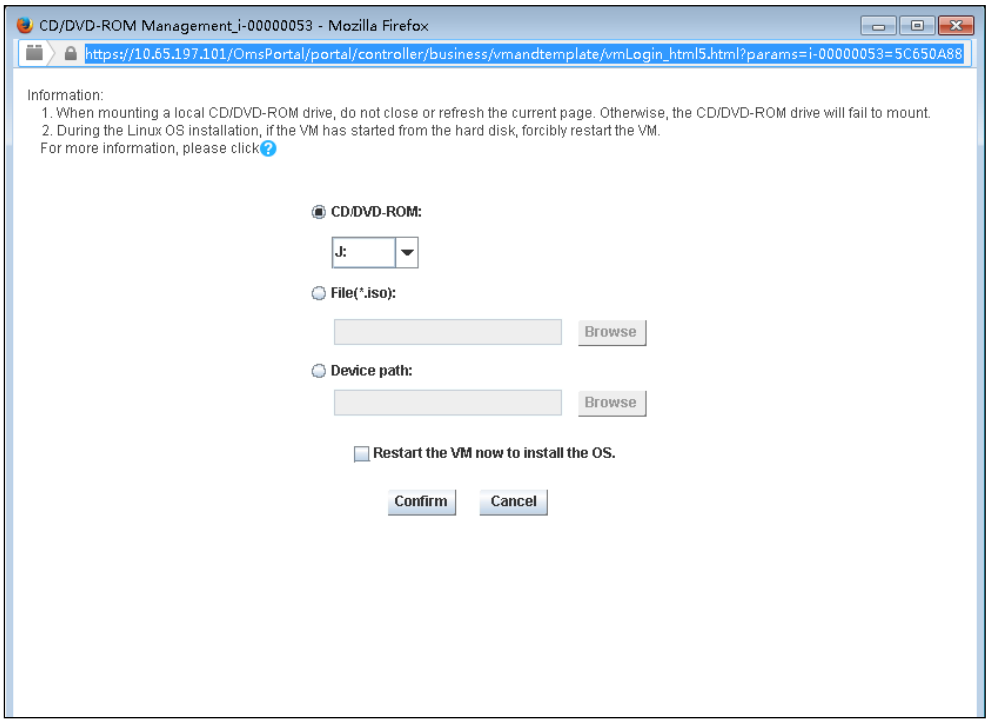
a. In the window shown in Figure 2-77, click **CD/DVD-ROM Management**. A page appears, as shown in Figure 2-85.

Figure 2-85 Mounting a CD/DVD-ROM drive



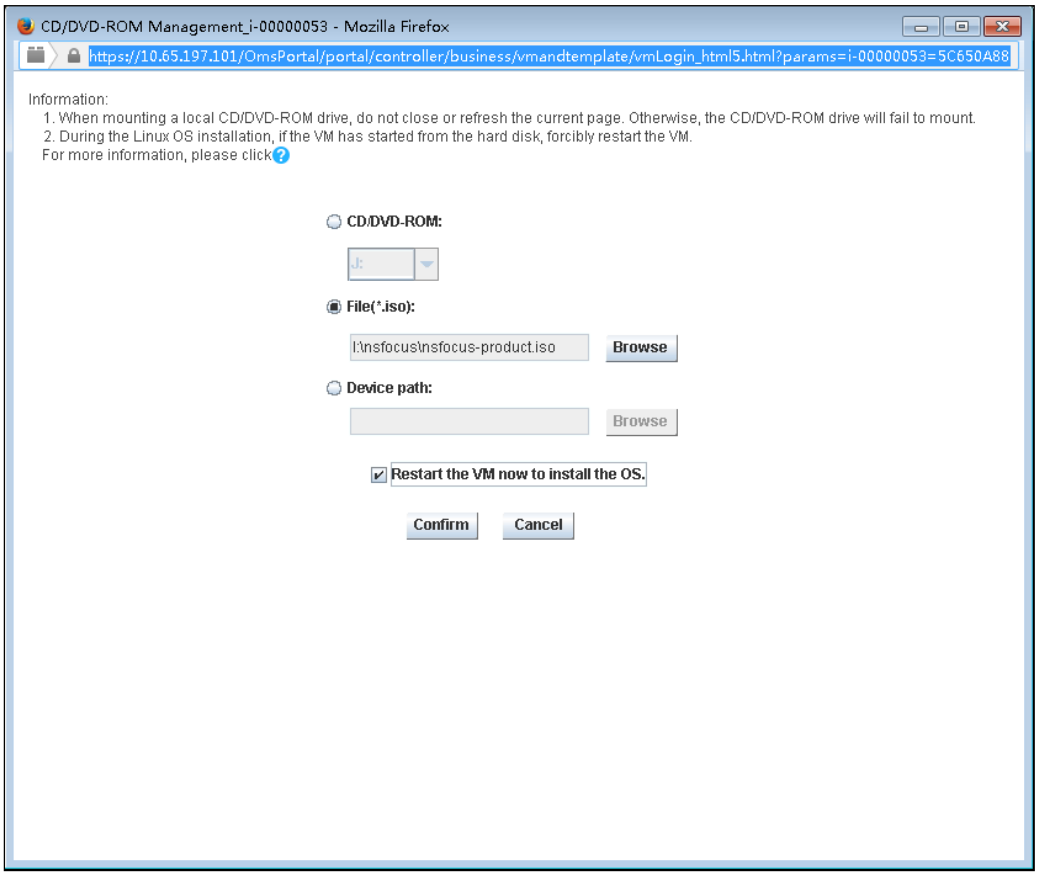
b. Click **Mount Local CD/DVD-ROM Drive**.

Figure 2-86 Selecting the vRSAS image file to be mounted



c. Click **File** and browse to the local vRSAS image file. Select **Restart the VM now to install the OS** and click **Confirm**.

Figure 2-87 Starting vRSAS



Step 7 Install vRSAS.

The procedure of installing vRSAS on the FusionCompute platform is the same as that for the VMware Workstation platform described in Installing the Image File of vRSAS.

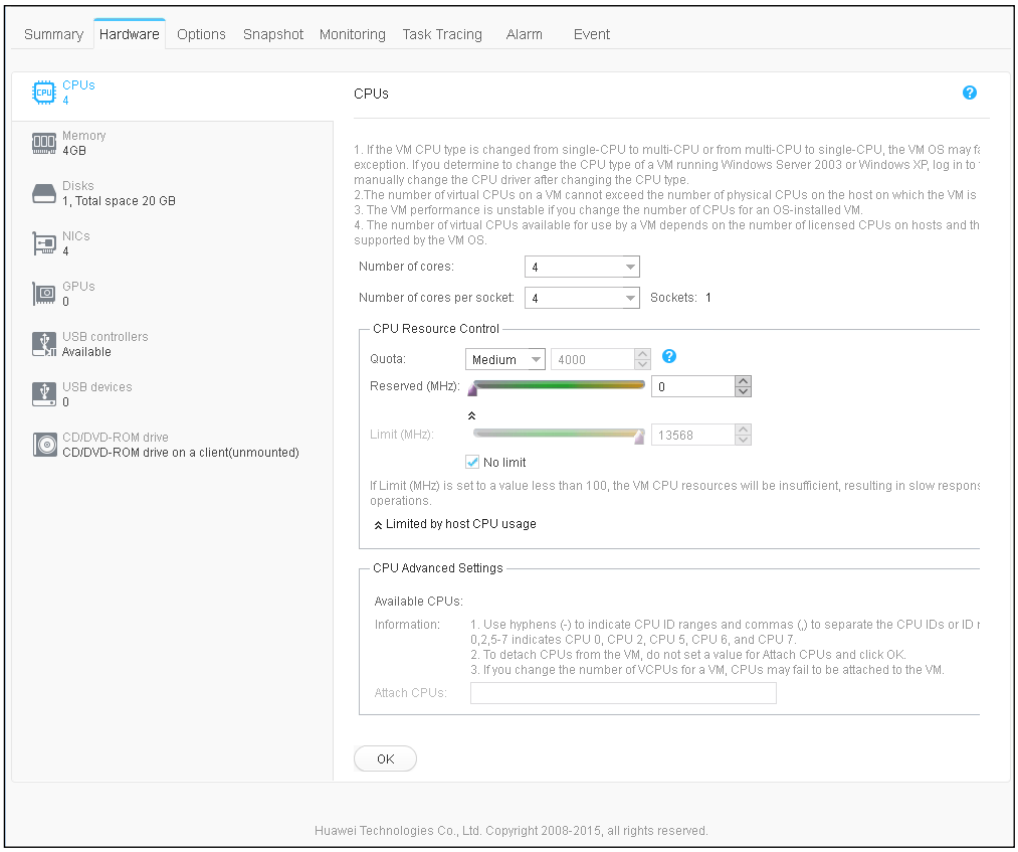
Step 8 Add a network adapter.

vRSAS only provides one network interface (that is, management interface) by default. Perform the following steps to add a network adapter to enable the scan interface.

a. Choose **VM and Template**.

b. Choose **Recently Viewed VMs >** *RSAS* > **Hardware**.

Figure 2-88 Hardware page



c. On the **Hardware** page, choose **NICs** from the left pane.

d. Click **Add**.

e. Configure the NIC parameters and click **OK**.

f. (Optional) Add other network adapters as required.

----End

Performing Initial Configuration

For how to perform initial configuration after login to vRSAS (as detailed in Installing the Image File of vRSAS), see Performing Initial Configuration.

Conducting License-based Authentication

Mounting the Dongle

Caution	Do not remove the dongle when vRSAS is in use. Otherwise, vRSAS would automatically exit.

To mount the dongle, follow these steps:

Step 1 Insert the dongle in the FusionCompute server.

Step 2 Log in to the FusionCompute platform.

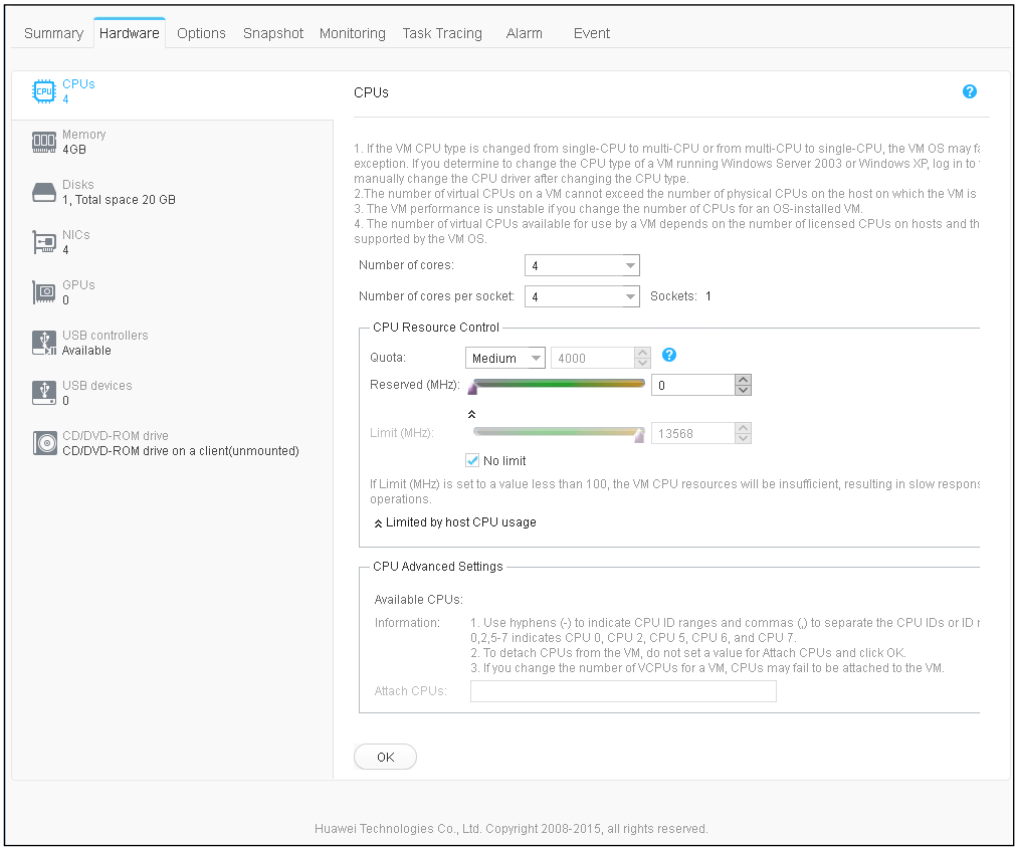
The FusionCompute home page appears, as shown in Figure 2-76.

Step 3 Choose **VM and Template**.

Step 4 On the page shown in Figure 2-77, choose **Recently Viewed VMs** > *RSAS* > **Hardware**.

Step 5 On the **Hardware** page, choose USB devices from the left pane.

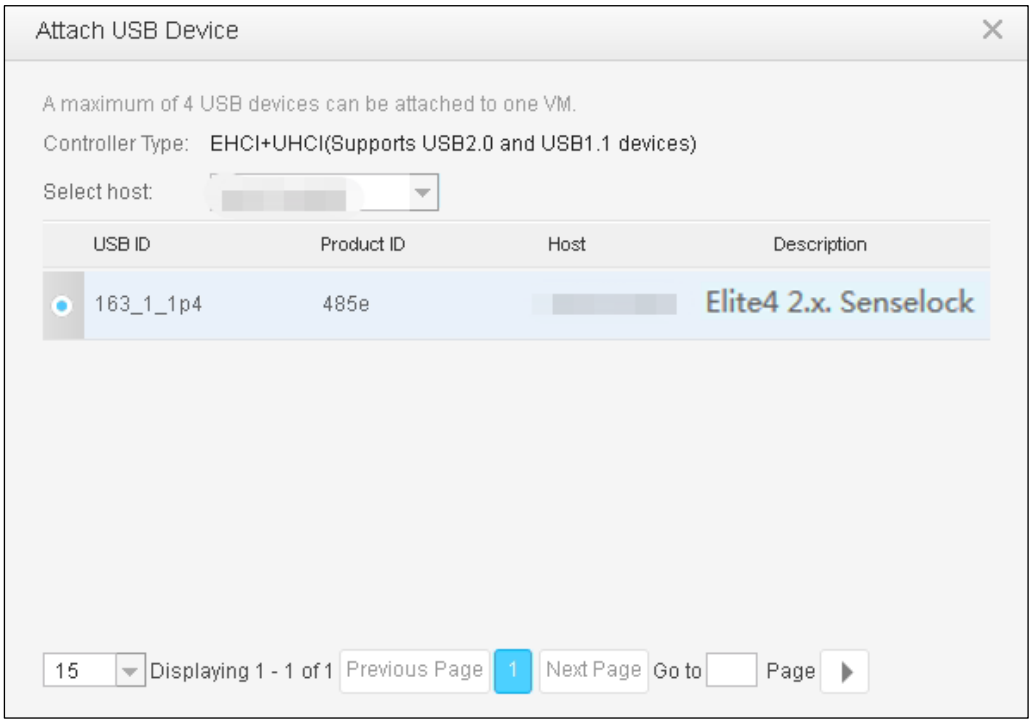
Figure 2-89 USB device page



Step 6 Click **Attach USB device**.

Step 7 In the **Attach USB Device** dialog box, select **Philips Elite4 2.x** and click **OK**.

Figure 2-90 Attaching a USB device



----End

Importing a License

For how to import a license, see Importing a License.

2.2.5.3 Uninstallation Procedure

To delete vRSAS from the FusionCompute platform, follow these steps:

Step 1 Log in to the FusionCompute platform.

Step 2 Choose **VM and Template**.

Step 3 On the page shown in Figure 2-77, choose **VM** from the left navigation tree.

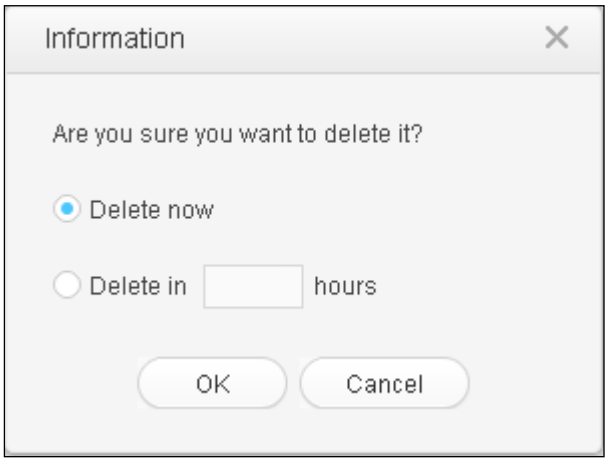
The VM list appears, as shown in Figure 2-82.

Step 4 On the line of vRSAS, click **More > Safely delete** in the **Operation** column.

Step 5 In the dialog box that appears, select a time to delete vRSAS and then click **OK**.

vRSAS is then completely removed from the datastore.

Figure 2-91 Confirming the deletion



----End

2.2.6 Installation on KVM

This section describes how to install vRSAS on a standard KVM platform.

2.2.6.1 Preparations

Table 2-6 lists preparations to be made for installing vRSAS on KVM.

Table 2-6 Preparations to be made for installing vRSAS on the KVM platform

Item		Description
KVM server (standard platform)	IP address	IP address of a computer that can properly connect to the network.
	Account	Account with privileges of a system administrator.

	Bridge NIC	Run the following sample command to create a bridge NIC. The created bridge NIC is as shown in Figure 2-92.
		`virsh iface-bridge --interface ens192 --bridge br0`
		`#ens192 indicates the name of a physical NIC for bridging; br0 indicates the name of a bridge NIC`

vRSAS	CD	Contains an image file (.iso or .qcow2) of vRSAS.
	IP address	IP address of the scan interface of vRSAS.
	Authentication license	• License that enables vRSAS to be launched properly. • Unique authorization hash value granted to vRSAS.
		• IP address of a CAA platform and license of vRSAS. • License of vRSAS for authentication by NSFOCUS security cloud. • Dongle and license: The dongle should be already installed on the KVM server.

Item		Description
		Note You can select any one of the three authentication modes.

Figure 2-92 Creating the bridge NIC successfully

```
[root@localhost ~]# brctl show
bridge name     bridge id               STP enabled     interfaces
br0             8000.000c29488e4c       yes             ens192
virbr0          8000.5254000ab3d5       yes             virbr0-nic
[root@localhost ~]#
```

2.2.6.2 Installation Procedure

This document takes **rsas** as an example to describe how to install vRSAS by using command lines.

Installing an ISO Image File

If the disk space is greater than 150 GB, use the single-disk installation. Otherwise, mount a second disk with more than150 GB space and use the dual-disk installation

Single-Disk Installation

If the disk space is greater than 150 GB, install vRASA in one disk.

Step 1 Create a disk file that is greater than 150 GB, for example, 160 GB.

```
qemu-img create -f qcow2 /kvm/images/rsas.qcow2 160G
```

Step 2 Create a VM, as shown in Figure 2-93.

```
virt-install --name rsas --ram 8192 --vcpus 4 --cdrom=/iso_store/RSAS-VM-
V6.0R04F00-37872.iso --disk /kvm/images/rsas.qcow2,format=qcow2,size=160 --vnc --
vncport=5910 --vnclisten=0.0.0.0 --network bridge=br0 --os-type=linux

###
--name: indicates the VM name.
--ram: indicates the memory.
--vcpus: indicates the number of CPU core.
--cdrom: indicates the absolute path of the vRSAS image file.
--vnc: indicates the listening port and listening address for Virtual Network
Console (VNC).
```

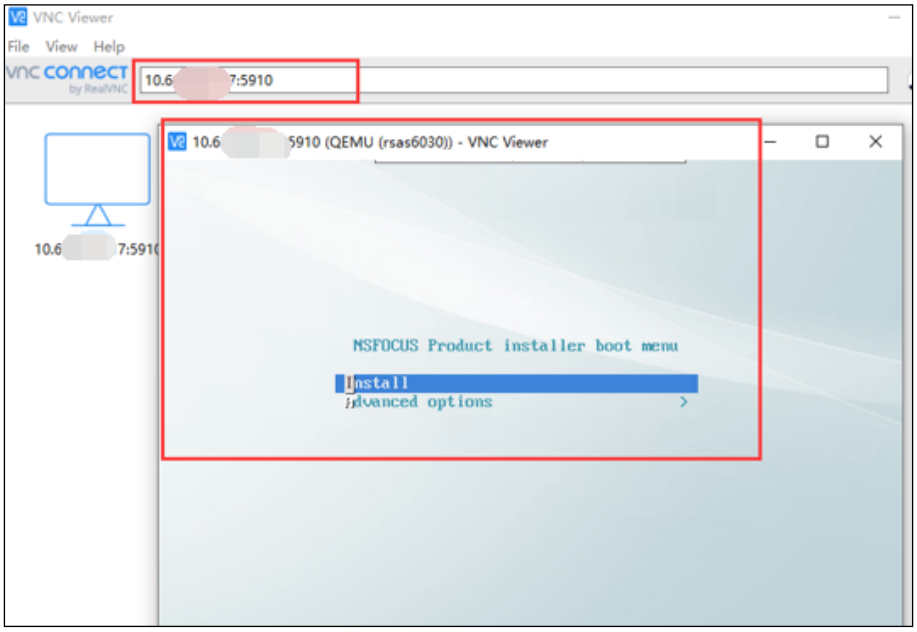
Figure 2-93 Creating a VM

```
root@kvm-debian:~# virt-install  --name rsas --ram 8192 --vcpus 4 --cdrom=/iso_store/RSAS-VM-V6.0R04F00-
37872.iso --disk /kvm/images/rsas.qcow2,format=qcow2,size=160 --vnc --vncport=5910 --vnclisten=0.0.0.0 --
network bridge=br0 --os-type=linux

Starting install...
Creating domain...                                                                          |    0 B
00:00:00

(virt-viewer:24096): Gtk-WARNING **: cannot open display: localhost:11.0
Domain installation still in progress. You can reconnect to
the console to complete the installation process.
root@kvm-debian:~#
```

Step 3 Install vRSAS by using VNC, as shown in Figure 2-94.

Type *IP:PORT* in the address bar to connect VNC Viewer, where IP is the IP address of the Linux host of vRSAS, and PORT is **5910** specified during the creation of VM.

Figure 2-94 Connecting to VNC



Step 4 Install the vRSAS image file.

The procedure of installing vRSAS on VNC is the same as that for the VMware Workstation platform described in Installing the Image File of vRSAS.

----End

Two-Disk Installation

If the disk space is less than 150 GB, mount a second disk with a capacity of greater than 150 GB, and install vRSAS with dual disks.

Step 1 Create a code disk that is greater than 4 GB, for example, 8 GB, as shown in Figure 2-95.

```
qemu-img create -f qcow2 /kvm/images/rsas-code.qcow2 8G
```

Figure 2-95 Creating a code disk

```
[root@localhost rsas]# qemu-img create -f qcow2 /kvm/images/rsas-code.qcow2 8G
Formatting '/kvm/images/rsas-code.qcow2', fmt=qcow2 size=8589934592 encryption=off cluster_size=65536 lazy_refcounts=o
ff
[root@localhost rsas]#
```

Step 2 Create a VM, as shown in Figure 2-96.

```
virt-install --name rsas --ram 8192 --vcpus 4 --cdrom=/iso_store/RSAS-VM-
V6.0R04F00-37872.iso --disk /kvm/images/rsas-code.qcow2,format=qcow2,size=8 --vnc -
-vncport=5910 --vnclisten=0.0.0.0 --network bridge=br0 --os-type=linux

###
--name: indicates the VM name
--ram: indicates the memory
--vcpus: indicates the number of CPU cores
--cdrom: indicates the absolute path of the vRSAS image file
--vnc: indicates the listening port and listening address for VNC
```

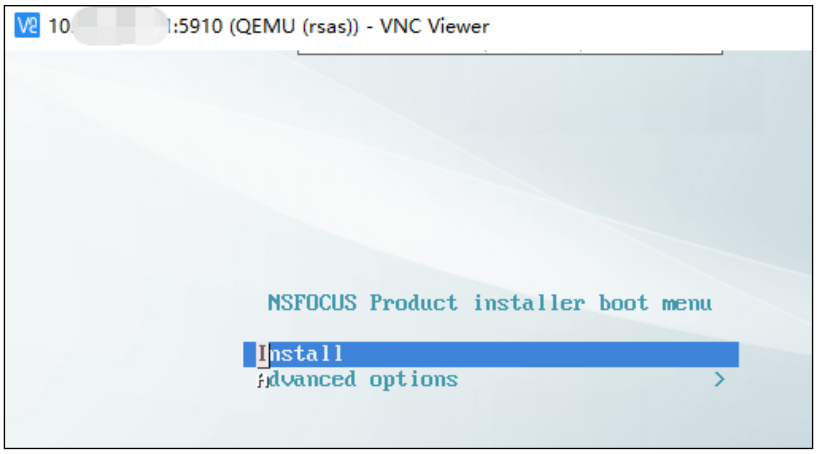
Figure 2-96 Creating a VM

```
root@kvm-debian:~# virt-install  --name rsas --ram 8192 --vcpus 4 --cdrom=/iso_store/RSAS-VM-V6.0R04F00-37872.iso --disk
/kvm/images/rsas-code.qcow2,format=qcow2,size=8 --vnc --vncport=5910 --vnclisten=0.0.0.0 --network bridge=br0 --os-type=linux

Starting install...
Creating domain...                                          |    0 B  00:00:00

(virt-viewer:9098): Gtk-WARNING **: cannot open display: localhost:11.0
Domain installation still in progress. You can reconnect to
the console to complete the installation process.
root@kvm-debian:~#
```

Step 3 Install vRSAS by using VNC, as shown in Figure 2-97.

Type *IP:PORT* in the address bar to connect VNC Viewer, where IP is the IP address of the Linux host of vRSAS, and PORT is **5910** specified during the creation of VM.

Figure 2-97 Installing vRSAS using VNC



Step 4 Install the vRSAS image file.

The procedure of installing vRSAS on VNC is the same as that for the VMware Workstation platform described in Installing the Image File of vRSAS.

Step 5 Create a data disk in a custom path, as shown in Figure 2-98.

```
qemu-img create -f qcow2 /kvm/images/rsas-data.qcow2 160G
```

Figure 2-98 Creating a data disk

```
[root@localhost ~]# qemu-img create -f qcow2 /kvm/images/rsas-data.qcow2 160G
Formatting '/kvm/images/rsas-data.qcow2', fmt=qcow2 size=171798691840 encryption=off cluster_size=65536 lazy_refcounts
=off
[root@localhost ~]#
```

Step 6 Mount the data disk to vRSAS.

a. After vRSAS is installed, it is shut down. In this status, run the following command to confirm that the code disk ID is **hda**, as shown in Figure 2-99.

```
virsh dumpxml rsas
```

Figure 2-99 Querying the ID of the code disk

```
[root@localhost ~]# virsh dumpxml rsas
<domain type='kvm' id='9'>
  <name>rsas</name>
  <uuid>f79ff54a-4ccb-47a5-c71f-bf938812995f</uuid>
  <memory unit='KiB'>8388608</memory>
  <currentMemory unit='KiB'>8388608</currentMemory>
  <vcpu placement='static'>4</vcpu>
  <resource>
    <partition>/machine</partition>
  </resource>
  <os>
    <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
    <boot dev='cdrom'/>
    <boot dev='hd'/>
  </os>
  <features>
    <acpi/>
    <apic/>
    <pae/>
  </features>
  <clock offset='utc'/>
  <on_poweroff>destroy</on_poweroff>
  <on_reboot>destroy</on_reboot>
  <on_crash>destroy</on_crash>
  <devices>
    <emulator>/usr/libexec/qemu-kvm</emulator>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2'/>
      <source file='/kvm/images/rsas-code.qcow2'/>
      <backingStore/>
      <target dev='hda' bus='ide'/>
      <alias name='ide0-0-0'/>
      <address type='drive' controller='0' bus='0' target='0' unit='0'/>
    </disk>
```

b. Mount the data disk, with an ID numbered sequentially based on the ID of the code disk obtained in the previous step. For example, if the code disk is hda, the data disk must be set to **hdb**, as shown in Figure 2-100.

```
virsh attach-disk --domain rsas --subdriver qcow2 --source /kvm/images/rsas-
data.qcow2 --target hdb --persistent

###
--domain: indicates the name of vRSAS.
--source: indicates the source path of the disk to be installed.
--target: indicates the target disk added to the VM.
```

Figure 2-100 Adding a data disk

```
[root@localhost ~]# virsh attach-disk --domain rsas  --subdriver qcow2 --source /kvm/images/rsas-data.qcow2 --target h
db --persistent
```

c. After the configuration is complete, check the configuration files of vRSAS, which already contains the data disk, as shown in Figure 2-101.

```
virsh dumpxml rsas
```

Figure 2-101 Checking the data disk configuration

```
[root@localhost ~]# virsh dumpxml rsas
<domain type='kvm'>
  <name>rsas</name>
  <uuid>f79ff54a-4ccb-47a5-c71f-bf938812995f</uuid>
  <memory unit='KiB'>8388608</memory>
  <currentMemory unit='KiB'>8388608</currentMemory>
  <vcpu placement='static'>4</vcpu>
  <os>
    <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
    <boot dev='hd'/>
  </os>
  <features>
    <acpi/>
    <apic/>
    <pae/>
  </features>
  <clock offset='utc'/>
  <on_poweroff>destroy</on_poweroff>
  <on_reboot>restart</on_reboot>
  <on_crash>restart</on_crash>
  <devices>
    <emulator>/usr/libexec/qemu-kvm</emulator>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2'/>
      <source file='/kvm/images/rsas-code.qcow2'/>
      <target dev='hda' bus='ide'/>
      <address type='drive' controller='0' bus='0' target='0' unit='0'/>
    </disk>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2'/>
      <source file='/kvm/images/rsas-data.qcow2'/>
      <target dev='hdb' bus='ide'/>
      <address type='drive' controller='0' bus='0' target='0' unit='1'/>
    </disk>
```

Step 7 Start the vRSAS and wait until the installation is complete.

```
virsh start rsas
```

----End

Installing a QCOW2 Image File

Single-Disk Installation

1. Create a single-disk image

You can perform the following steps to create a qcow2 image file or obtain it from NSFOCUS's after-sales personnel.

Step 1 Create a disk file that is greater than 150 GB, for example, 160 GB.

```
qemu-img create -f qcow2 /kvm/images/rsas.qcow2 160G
```

Step 2 Create a VM, as shown in Figure 2-102.

```
virt-install --name rsas --ram 8192 --vcpus 4 --cdrom=/iso_store/RSAS-VM-
V6.0R04F00-37872.iso --disk /kvm/images/rsas.qcow2,format=qcow2,size=160 --vnc --
vncport=5910 --vnclisten=0.0.0.0 --network bridge=br0 --os-type=linux
###
--name: indicates the VM name.
--ram: indicates the memory.
--vcpus: indicates the number of CPU cores.
--cdrom: indicates the absolute path of the vRSAS image file.
--vnc: indicates the listening port and listening address for VNC.
```

Figure 2-102 Creating a VM

```
root@kvm-debian:~# virt-install  --name rsas --ram 8192 --vcpus 4 --cdrom=/iso_store/RSAS-VM-V6.0R04F00-37872.iso --disk
/kvm/images/rsas.qcow2,format=qcow2,size=160 --vnc --vncport=5910 --vnclisten=0.0.0.0 --network bridge=br0 --os-type=linux

Starting install...
Creating domain...                                          |  0 B  00:00:00

(virt-viewer:31080): Gtk-WARNING **: cannot open display: localhost:11.0
Domain installation still in progress. You can reconnect to
the console to complete the installation process.
root@kvm-debian:~#
```

Caution	After the ISO installation is complete, the window shown in Figure 2-103 appears. Do not run the **virsh start** command to start the new VM. Otherwise, the image is automatically installed, and the qcow2 image cannot be created.

Figure 2-103 VM created

Step 3 Check the path of the .qcow2 image file, as shown in Figure 2-104 or Figure 2-105.

Figure 2-104 Viewing the path of the disk image file visually

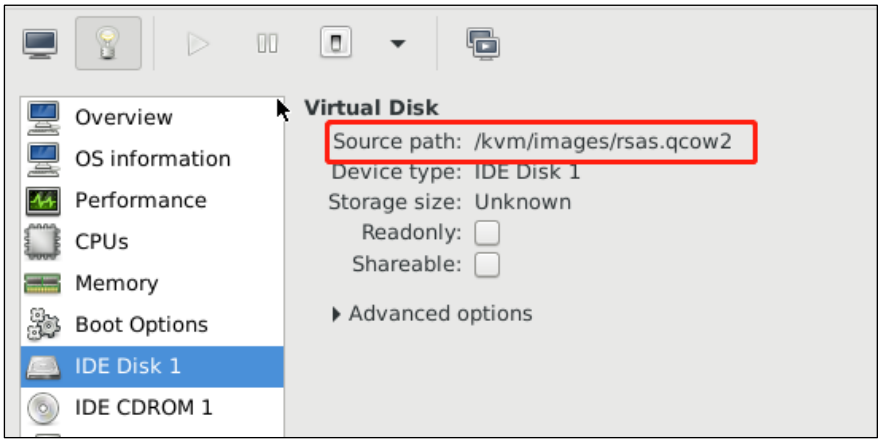


Figure 2-105 Viewing the path of the disk image file by using commands

```
[root@localhost images]# virsh dumpxml rsas
<domain type='kvm' id='15'>
  <name>RSAS</name>
  <uuid>d988c2d6-0f15-5032-116c-74807f6f906e</uuid>
  <memory unit='KiB'>8388608</memory>
  <currentMemory unit='KiB'>8388608</currentMemory>
  <vcpu placement='static'>4</vcpu>
  <resource>
    <partition>/machine</partition>
  </resource>
  <os>
    <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
    <boot dev='cdrom'/>
    <boot dev='hd'/>
  </os>
  <features>
    <acpi/>
    <apic/>
    <pae/>
  </features>
  <clock offset='utc'/>
  <on_poweroff>destroy</on_poweroff>
  <on_reboot>destroy</on_reboot>
  <on_crash>destroy</on_crash>
  <devices>
    <emulator>/usr/libexec/qemu-kvm</emulator>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2'/>
      <source file='/kvm/images/rsas.qcow2'/>
      <backingStore/>
      <target dev='hda' bus='ide'/>
      <alias name='ide0-0-0'/>
      <address type='drive' controller='0' bus='0' target='0' unit='0'/>
    </disk>
```

Step 4 Compress the image file.

```
qemu-img convert -c -O qcow2 /kvm/images/rsas.qcow2 /kvm/images/rsas-danpan.qcow2
#rsas-danpan.qcow2: indicates a compressed .qcow2 image that is close to the size
of the ISO image.
```

----End

2. Install vRSAS in one disk

Step 1 Install vRSAS by using the single-disk qcow2 image, as shown in Figure 2-106.

```
virt-install --name rsas --ram 8192 --vcpus 4 --import --disk
path=/kvm/images/rsas-danpan.qcow2 --network bridge=br0 --vnc --vncport=5910 --
vnclisten=0.0.0.0 --os-type=linux

###
--name: indicates the VM name.
--ram: indicates the memory.
--vcpus: indicates the number of CPU cores.
--disk: indicates the absolute path of the single-disk qcow2 image file.
--vnc: indicates the listening port and listening address for VNC.
```

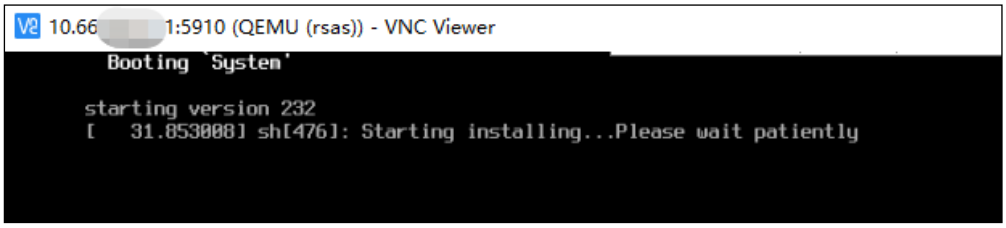
Figure 2-106 Using the single-disk qcow2 image

```
root@kvm-debian:~# virt-install --name rsas --ram 8192 --vcpus 4 --import --disk path=/kvm/images/rsas-danpan.qcow2 --network
bridge=br0 --vnc --vncport=5910 --vnclisten=0.0.0.0 --os-type=linux

Starting install...
Creating domain...                                          |  0 B  00:00:00

(virt-viewer:7550): Gtk-WARNING **: cannot open display: localhost:11.0
Domain creation completed. You can restart your domain by running:
  virsh --connect qemu:///system start rsas
root@kvm-debian:~#
```

Step 2 Connect to vRSAS by using VNC.

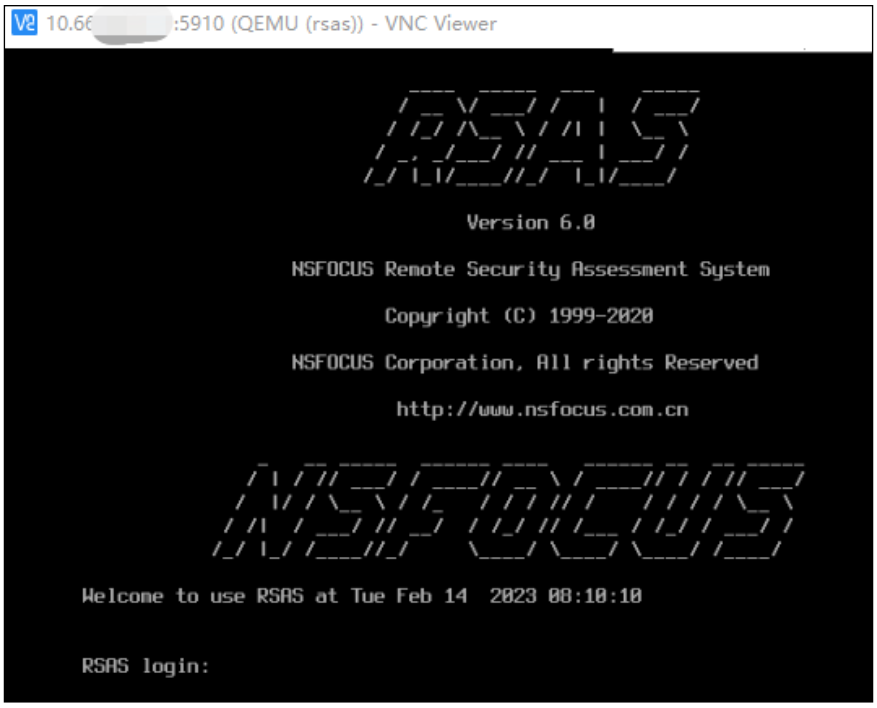
Type *IP:PORT* in the address bar to connect VNC Viewer, where IP is the IP address of the Linux host of vRSAS, and PORT is **5910** specified during the creation of VM, as shown in Figure 2-107.

Figure 2-107 Connecting to vRSAS via VNC



Step 3 Wait until the installation is complete.
The console-based login page appears, as shown in Figure 2-108.

Figure 2-108 Installation completed



----End

Dual-Disk Installation

1. Create a dual-disk image

   You can perform the following steps to create a qcow2 image file or obtain it from NSFOCUS's after-sales personnel.

   If the disk space is less than 150 GB, mount a second disk with a capacity of more than 150 GB, and install vRSAS with dual disks.

Step 1 Create a code disk that is greater than 4 GB, for example, 8 GB, as shown in Figure 2-109.

```
qemu-img create -f qcow2 /kvm/images/rsas-code.qcow2 8G
```

Figure 2-109 Creating a code disk

```
[root@localhost rsas]# qemu-img create -f qcow2 /kvm/images/rsas-code.qcow2 8G
Formatting '/kvm/images/rsas-code.qcow2', fmt=qcow2 size=8589934592 encryption=off cluster_size=65536 lazy_refcounts=o
ff
[root@localhost rsas]#
```

Step 2 Create a VM, as shown in Figure 2-110.

```
virt-install --name rsas --ram 8192 --vcpus 4 --cdrom=/iso_store/RSAS-VM-
V6.0R04F00-37872.iso --disk /kvm/images/rsas-code.qcow2,format=qcow2,size=8 --vnc -
-vncport=5910 --vnclisten=0.0.0.0 --network bridge=br0 --os-type=linux

###
--name: indicates the VM name.
--ram: indicates the memory.
--vcpus: indicates the number of CPU cores.
--cdrom: indicates the absolute path of the vRSAS image file.
--vnc: indicates the listening port and listening address for VNC.
```

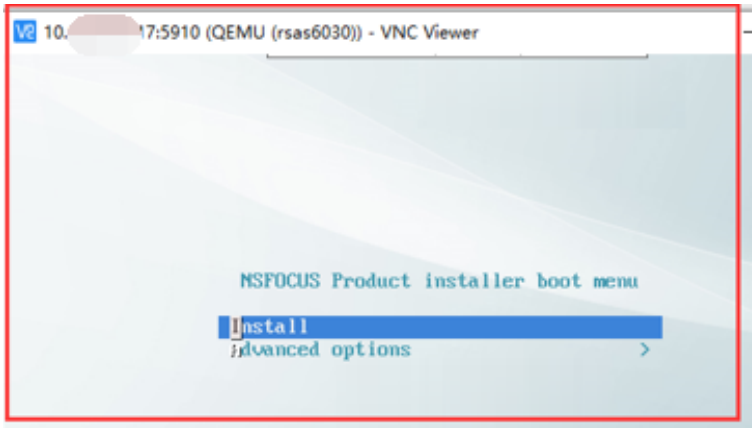
Figure 2-110 Creating a VM

```
root@kvm-debian:~# virt-install --name rsas --ram 8192 --vcpus 4 --cdrom=/iso_store/RSAS-VM-V6.0R04F00-37872.iso --disk
/kvm/images/rsas-code.qcow2,format=qcow2,size=8 --vnc --vncport=5910 --vnclisten=0.0.0.0 --network bridge=br0 --os-type=linux

Starting install...
Creating domain...                                          |  0 B  00:00:00

(virt-viewer:9098): Gtk-WARNING **: cannot open display: localhost:11.0
Domain installation still in progress. You can reconnect to
the console to complete the installation process.
root@kvm-debian:~#
```

Step 3 Install vRSAS by using VNC, as shown in Figure 2-111.

Type *IP:PORT* in the address bar to connect VNC Viewer, where IP is the IP address of the Linux host of vRSAS, and PORT is **5910** specified during the creation of VM.

Figure 2-111 Installing vRSAS using VNC



Step 4 Install the vRSAS image file.

The procedure of installing vRSAS on VNC is the same as that for the VMware Workstation platform described in Installing the Image File of vRSAS.

a. During the installation, click **OK** when you are prompted to mount the data disk, as shown in Figure 2-112.

Figure 2-112 Only one hard disk detected

b. Click **later_install** when specifying the data disk location, as shown in Figure 2-113.

Figure 2-113 later_install

Caution	After the ISO installation is complete, the window shown in Figure 2-114 appears. Do not run the **virsh start** command to start the new VM. Otherwise, the image is automatically installed, and the qcow2 image cannot be created.

Figure 2-114 VM created

Step 5 Check the path of the .qcow2 image file, as shown in Figure 2-115 or Figure 2-116.

Figure 2-115 Viewing the path of the disk image file visually

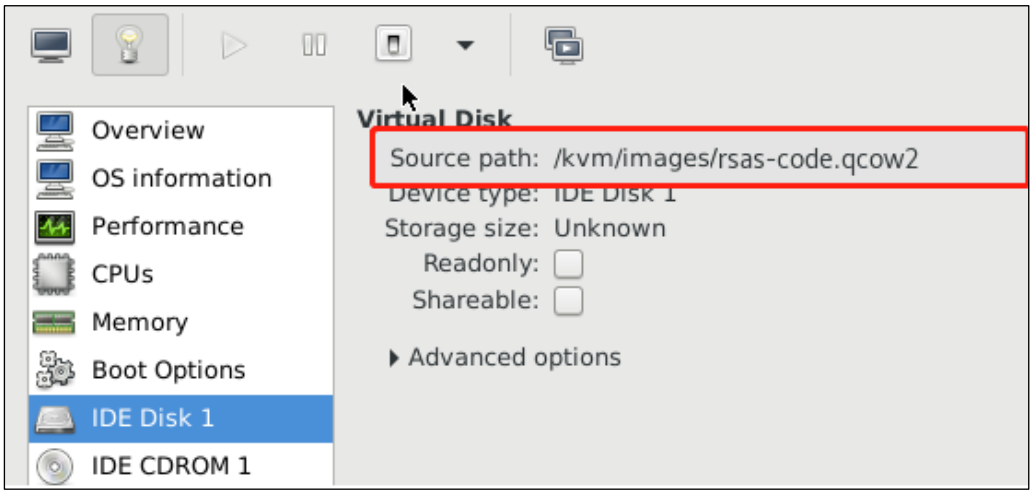


Figure 2-116 Viewing the path of the disk image file by using commands

```
[root@localhost ~]# virsh dumpxml rsas
<domain type='kvm' id='9'>
  <name>rsas</name>
  <uuid>f79ff54a-4ccb-47a5-c71f-bf938812995f</uuid>
  <memory unit='KiB'>8388608</memory>
  <currentMemory unit='KiB'>8388608</currentMemory>
  <vcpu placement='static'>4</vcpu>
  <resource>
    <partition>/machine</partition>
  </resource>
  <os>
    <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
    <boot dev='cdrom'/>
    <boot dev='hd'/>
  </os>
  <features>
    <acpi/>
    <apic/>
    <pae/>
  </features>
  <clock offset='utc'/>
  <on_poweroff>destroy</on_poweroff>
  <on_reboot>destroy</on_reboot>
  <on_crash>destroy</on_crash>
  <devices>
    <emulator>/usr/libexec/qemu-kvm</emulator>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2'/>
      <source file='/kvm/images/rsas-code.qcow2'/>
      <backingStore/>
      <target dev='hda' bus='ide'/>
      <alias name='ide0-0-0'/>
      <address type='drive' controller='0' bus='0' target='0' unit='0'/>
    </disk>
```

Save the code disk as a dual-disk image for use.

```
cp /kvm/images/rsas-code.qcow2 /kvm/images/shuangpan.qcow2
```

----End

2. Install vRSAS with two disks

Step 1 Install vRSAS by using the dual-disk qcow2 image, as shown in Figure 2-117.

```
virt-install --name rsas --ram 8192 --vcpus 4 --import --disk
path=/kvm/images/rsas-shuangpan.qcow2 --network bridge=br0 --vnc --vncport=5911 --
vnclisten=0.0.0.0 --os-type=linux

###
--name: indicates the VM name.
--ram: indicates the memory.
--vcpus: indicates the number of CPU cores.
--disk: indicates the absolute path of the dual-disk qcow2 image file.
--vnc: indicates the listening port and listening address for VNC.
```

Figure 2-117 Using the dual-disk qcow2 image

```
root@kvm-debian:~# virt-install --name rsas --ram 8192 --vcpus 4 --import --disk path=/kvm/images/rsas-shuangpan.qcow2 --network
bridge=br0 --vnc --vncport=5911 --vnclisten=0.0.0.0 --os-type=linux

Starting install...
Creating domain...                                          |   0 B  00:00:00

(virt-viewer:6616): Gtk-WARNING **: cannot open display: localhost:11.0
Domain creation completed. You can restart your domain by running:
  virsh --connect qemu:///system start RSAS
root@kvm-debian:~#
```

Step 2 Type *IP:PORT* in the address bar to connect vRSAS via VNC, where IP is the IP address of the Linux host of vRSAS, and PORT is **5911** specified during the creation of VM. After the booting process ends, vRSAS will be automatically shut down, as shown in Figure 2-118 and Figure 2-119.

Figure 2-118 Dual-disk image loading

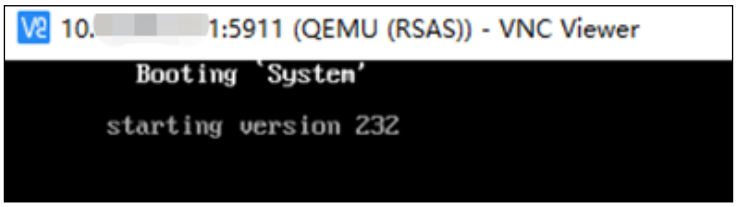
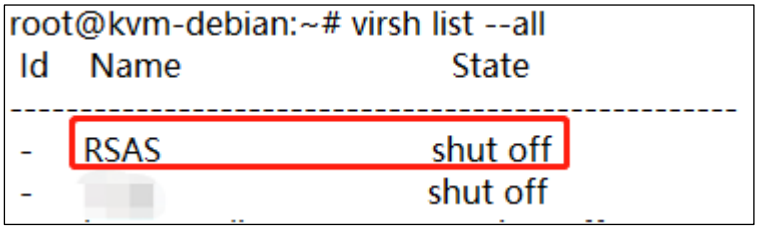


Figure 2-119 vRSAS shutdown



Step 3 Create a data disk.

```
qemu-img create -f qcow2 /kvm/images/rsas-data.qcow2 160G
```

Step 4 Mount the disk data to vRSAS.

a. After vRSAS is installed, it is shutdown. In this status, run the following command to confirm that the code disk ID is **hda**, as shown in Figure 2-120.

```
virsh dumpxml RSAS
```

Figure 2-120 Querying the device ID of the code disk

```
[root@localhost images]# virsh dumpxml RSAS
<domain type='kvm'>
  <name>RSAS</name>
  <uuid>dddc0a0c-8675-ee98-8e21-4ef9bef35e37</uuid>
  <memory unit='KiB'>8388608</memory>
  <currentMemory unit='KiB'>8388608</currentMemory>
  <vcpu placement='static'>4</vcpu>
  <os>
    <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
    <boot dev='hd'/>
  </os>
  <features>
    <acpi/>
    <apic/>
    <pae/>
  </features>
  <clock offset='utc'/>
  <on_poweroff>destroy</on_poweroff>
  <on_reboot>restart</on_reboot>
  <on_crash>restart</on_crash>
  <devices>
    <emulator>/usr/libexec/qemu-kvm</emulator>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2'/>
      <source file='/kvm/images/rsas-shuangpan.qcow2'/>
      <target dev='hda' bus='ide'/>
      <address type='drive' controller='0' bus='0' target='0' unit='0'/>
    </disk>
```

b. Mount the data disk, with an ID numbered sequentially based on the ID of the code disk obtained in the previous step. For example, if the code disk is hda, the data disk must be set to **hdb**, as shown in Figure 2-121.

```
virsh attach-disk --domain RSAS --subdriver qcow2 --source /kvm/images/rsas-
data.qcow2 --target hdb --persistent

###
--domain: indicates the name of vRSAS.
--source: indicates the source path of the disk to be installed.
--target: indicates the target disk added to the virtual machine.
```

Figure 2-121 Adding a data disk

```
[root@localhost images]# virsh attach-disk --domain RSAS --subdriver qcow2 --source /kvm/images/rsas-data.qcow2 --targ
et hdb --persistent
成功附加磁盘
```

c. After the configuration is complete, check the configuration files of vRSAS, which already contains the data disk, as shown in Figure 2-101.

```
virsh dumpxml RSAS
```

Figure 2-122 Checking the data disk in the configuration file

```
[root@localhost images]# virsh dumpxml RSAS
<domain type='kvm'>
  <name>RSAS</name>
  <uuid>dddc0a0c-8675-ee98-8e21-4ef9bef35e37</uuid>
  <memory unit='KiB'>8388608</memory>
  <currentMemory unit='KiB'>8388608</currentMemory>
  <vcpu placement='static'>4</vcpu>
  <os>
    <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
    <boot dev='hd'/>
  </os>
  <features>
    <acpi/>
    <apic/>
    <pae/>
  </features>
  <clock offset='utc'/>
  <on_poweroff>destroy</on_poweroff>
  <on_reboot>restart</on_reboot>
  <on_crash>restart</on_crash>
  <devices>
    <emulator>/usr/libexec/qemu-kvm</emulator>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2'/>
      <source file='/kvm/images/rsas-shuangpan.qcow2'/>
      <target dev='hda' bus='ide'/>
      <address type='drive' controller='0' bus='0' target='0' unit='0'/>
    </disk>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2'/>
      <source file='/kvm/images/rsas-data.qcow2'/>
      <target dev='hdb' bus='ide'/>
      <address type='drive' controller='0' bus='0' target='0' unit='1'/>
    </disk>
```

Step 5 Start the vRSAS and wait until the installation is complete.

```
virsh start rsas
```

----End

Adding a NIC

Initially, vRSAS only has a NIC enabled for its management interface. To use the scan interface, follow these steps to add a NIC:

Step 1 Keep vRSAS in the shutdown state and add a NIC.

```
virsh attach-interface rsas --type bridge --source br0 --persistent

#bridge indicates the bridge mode, and br0 indicates the name of a bridge NIC on
the host. Select a NIC as required. Multiple network interfaces cannot be bridged
to the same bridge NIC.
```

Figure 2-123 Adding a NIC

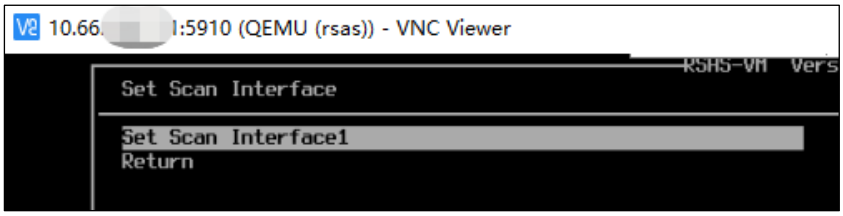
```
root@kvm-debian:~# virsh attach-interface rsas --type bridge --source br0 --persistent
Interface attached successfully

root@kvm-debian:~# virsh domiflist rsas          Query NIC information of vRSAS
Interface  Type       Source     Model      MAC
-------------------------------------------------------
-          bridge     br0        rtl8139    52:54:00:b4:23:b6
-          bridge     br0        rtl8139    52:54:00:20:df:5e

root@kvm-debian:~#
```

Step 2 Start vRSAS.

```
virsh start rsas
```

Step 3 Log in to the console user interface and check that the network configuration already contains the scan interface.

Figure 2-124 Scan interface added



----End

Mounting the Dongle

Caution	Do not remove the dongle when vRSAS is in use. Otherwise, vRSAS would automatically exit.

Step 1 Create an XML file, for example, **usb.xml**.

The product ID in the XML should be the same as that in the result of the **lsusb** command.

- Method 1: In the example file as follows, the **product id** parameter is set to be the same as the execution result of the **lsusb** command, as shown in Figure 2-125.

```
<hostdev mode='subsystem' type='usb'>
        <source>
            <vendor id='0x0471'/>
            <product id='0x485e'/>
        </source>
```

```
</hostdev>
```

Figure 2-125 Result of the lsusb command in method 1

```
[root@localhost images]# lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 004: ID 0471:485e Philips (or NXP)
Bus 002 Device 003: ID 0e0f:0002 VMware, Inc. Virtual USB Hub
Bus 002 Device 002: ID 0e0f:0003 VMware, Inc. Virtual Mouse
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
[root@localhost images]#
```

- Method 2: In the example file as follows, both the **bus** and **device** parameters are set to be the same as the execution result of the **lsusb** command, as shown in Figure 2-126.

```
<hostdev mode='subsystem' type='usb'>
        <source>
            <address bus= '002' device='004' />
        </source>
</hostdev>
```

Figure 2-126 Result of the lsusb command in method 2

```
[root@localhost images]# lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 004: ID 0471:485e Philips (or NXP)
Bus 002 Device 003: ID 0e0f:0002 VMware, Inc. Virtual USB Hub
Bus 002 Device 002: ID 0e0f:0003 VMware, Inc. Virtual Mouse
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
[root@localhost images]#
```

Step 2 Check the VM's instance name and mount the dongle to the corresponding device, as shown in Figure 2-127.

```
virsh attach-device rsas usb.xml --persistent
```

Figure 2-127 Mounting the dongle

```
root@kvm-debian:~# virsh attach-device rsas usb.xml --persistent
Device attached successfully
```

Step 3 Run the following command to verify that the mount is successful, as shown in Figure 2-128.

```
virsh dumpxml rsas
```

Figure 2-128 Dongle mounted permanently

```
<hostdev mode='subsystem' type='usb' managed='no'>
  <source>
    <address bus='2' device='4'/>
  </source>
  <address type='usb' bus='0' port='1'/>
</hostdev>
```

----End

Performing Initial Configuration

After logging in to the console of vRSAS, you should continue to perform initial configuration. For details, see Performing Initial Configuration.

Importing a License

For how to import a license, see Importing a License.

2.2.6.3 Uninstallation Procedure

To delete vRSAS from the KVM platform, run the following commands

```
virsh destroy rsas                                    #Shuts down vRSAS.
virsh undefine rsas                                   #Undefines vRSAS.
locate rsas                                          #Finds vRSAS-related files.
Run the rm command to delete the files found in the previous command line.
updatedb                                              #Updates the locate data file.
```

2.2.7 Installation on OpenStack

This section describes how to install vRSAS on a standard OpenStack platform.

2.2.7.1 Preparations

Table 2-7 lists preparations to be made for installing vRSAS on OpenStack.

Table 2-7 Preparations to be made for installing vRSAS on the OpenStack platform

Item		Description
OpenStack server (standard platform)	IP address	IP address of a computer that can properly connect to the network.
	Account	Account with privileges of a system administrator.
vRSAS	CD	Contains an image file (.iso) of vRSAS.
	IP address	IP address of the scan interface of vRSAS.
	Authentication license	• License that enables vRSAS to be launched properly. • Unique authorization hash value granted to vRSAS.
		• IP address of a CAA platform and license of vRSAS. • License of vRSAS for authentication by NSFOCUS security cloud. Note You can select either of the authentication modes.

2.2.7.2 Installation Procedure

Obtaining the Image File of vRSAS

For how to obtain the image file of vRSAS, see Obtaining the Image File of vRSAS.

Creating a VM

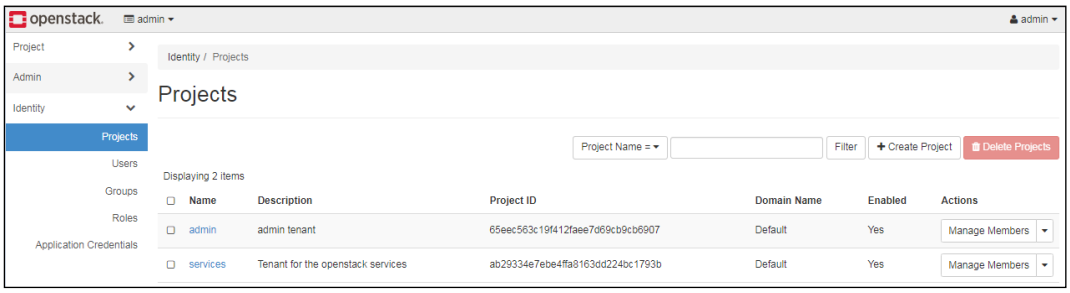
To create a VM, follow these steps:

Step 1 Create and obtain the .qcow2 image file.

For how to create the image file, see Installing a QCOW2 Image File.

Step 2 Log in to the OpenStack platform.

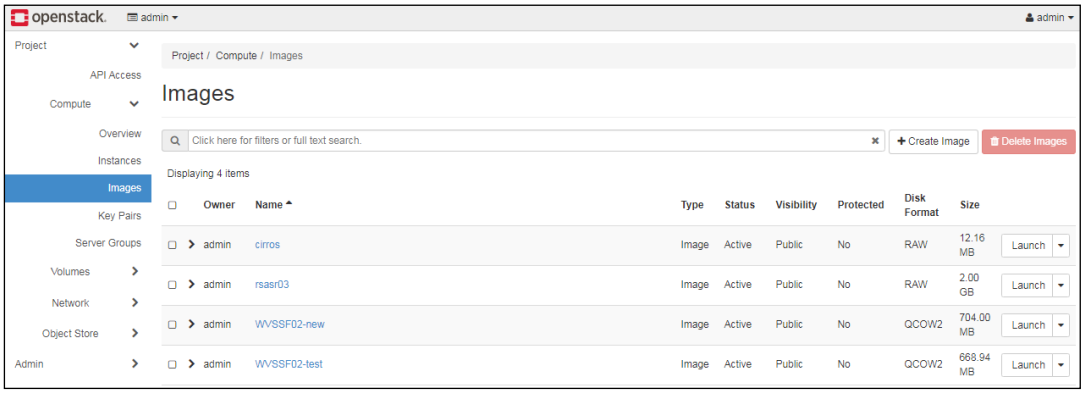
Figure 2-129 OpenStack platform



Step 3 Upload the vRSAS image file to OpenStack.

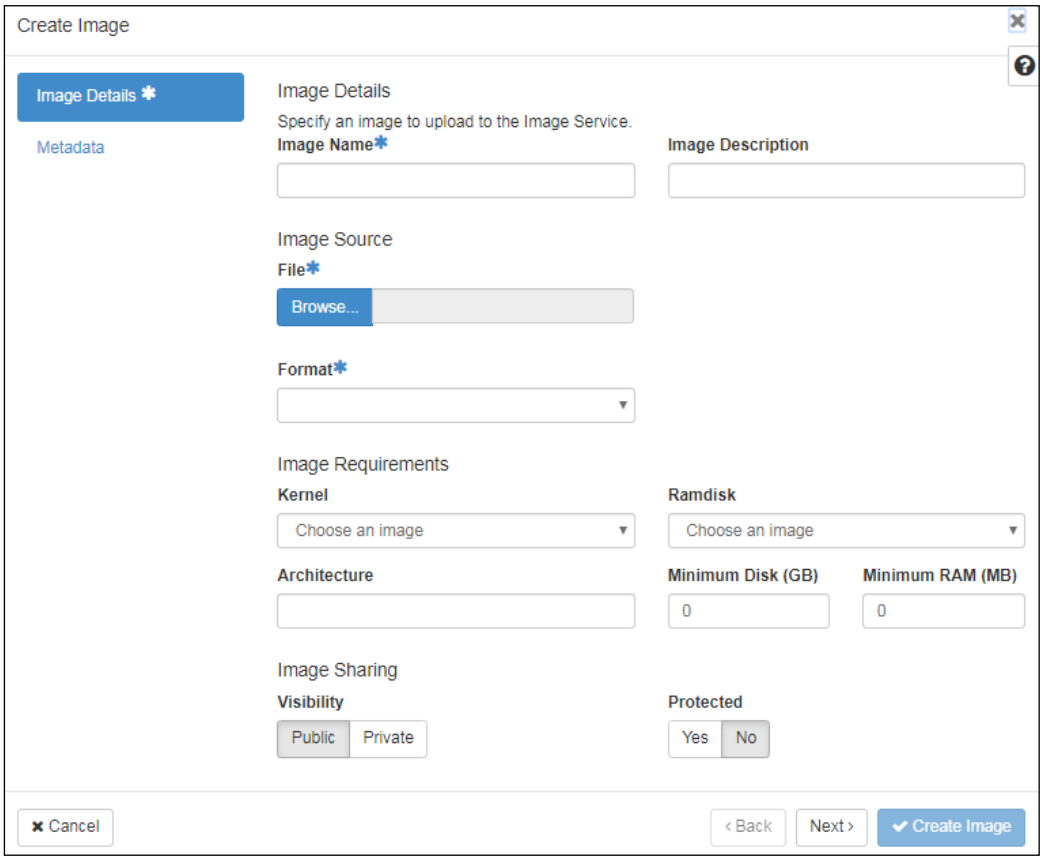
a. Choose **Project > Compute > Images**.

Figure 2-130 Images page



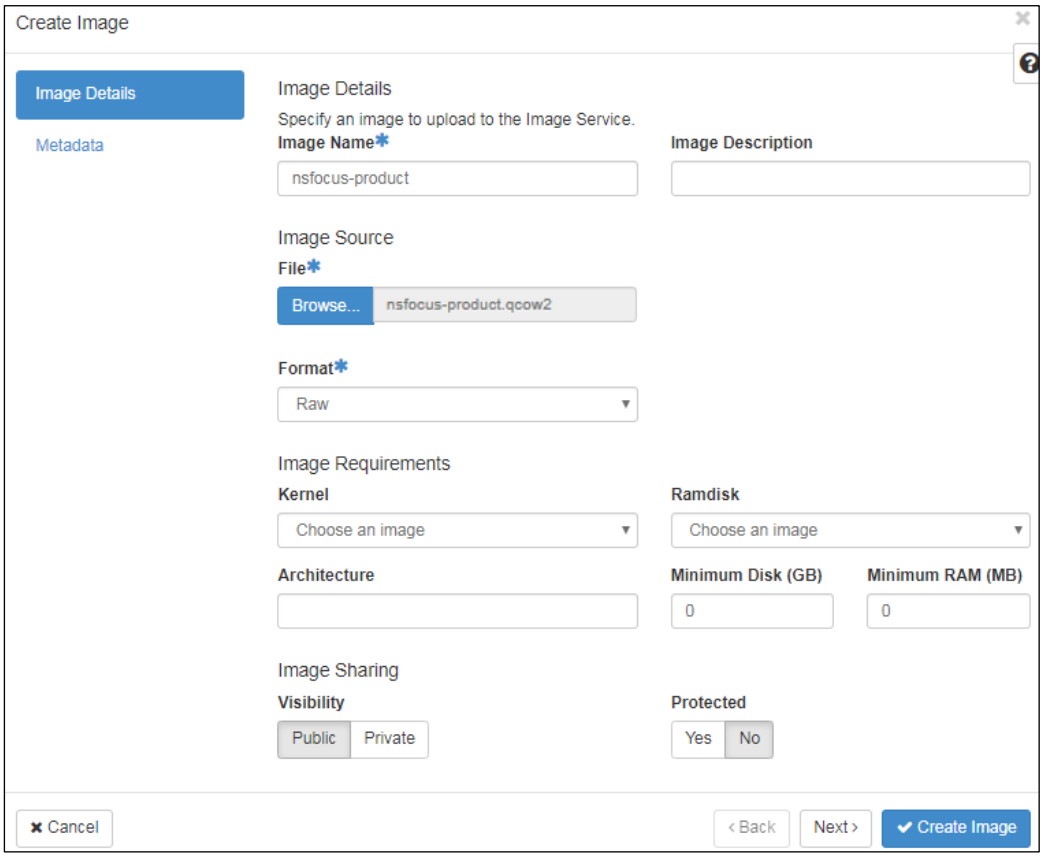
b. Click **Create Image**.

Figure 2-131 Creating an image



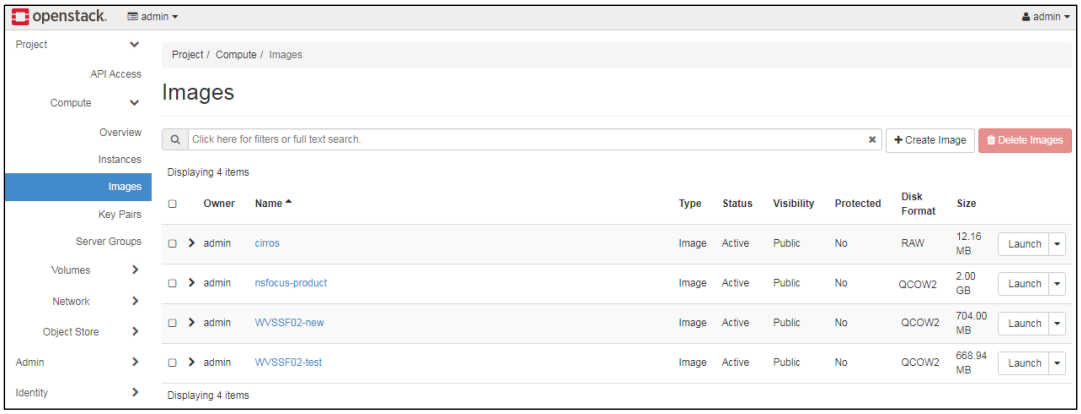
c. Specify a name for the image file, browse to the .qcow2 vRSAS image file, select **Raw** as the image format, and click **Create Image**.

Figure 2-132 Uploading the .qcow2 vRSAS image file



d. On the **Images** page, the uploaded image file is listed, as shown in Figure 2-133.

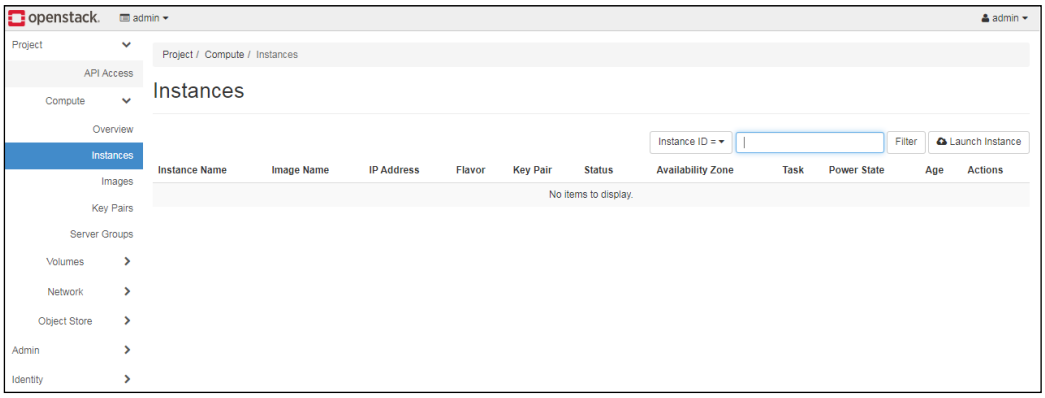
Figure 2-133 Images page



Step 4 Create an instance.

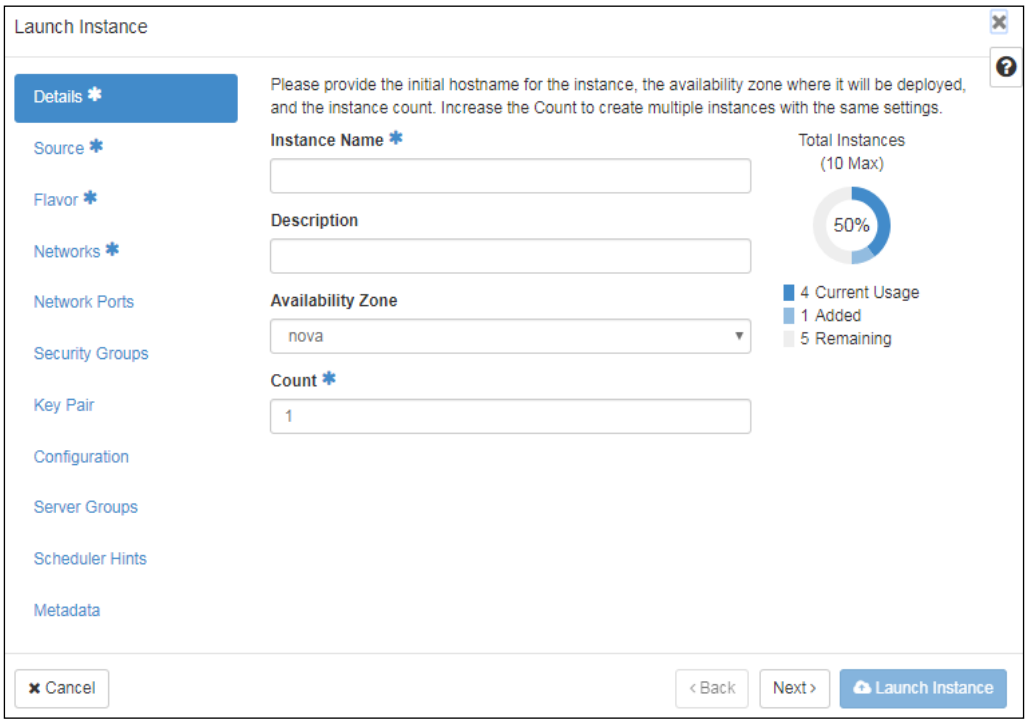
a. Choose **Project > Compute > Instances**.

Figure 2-134 Instances page



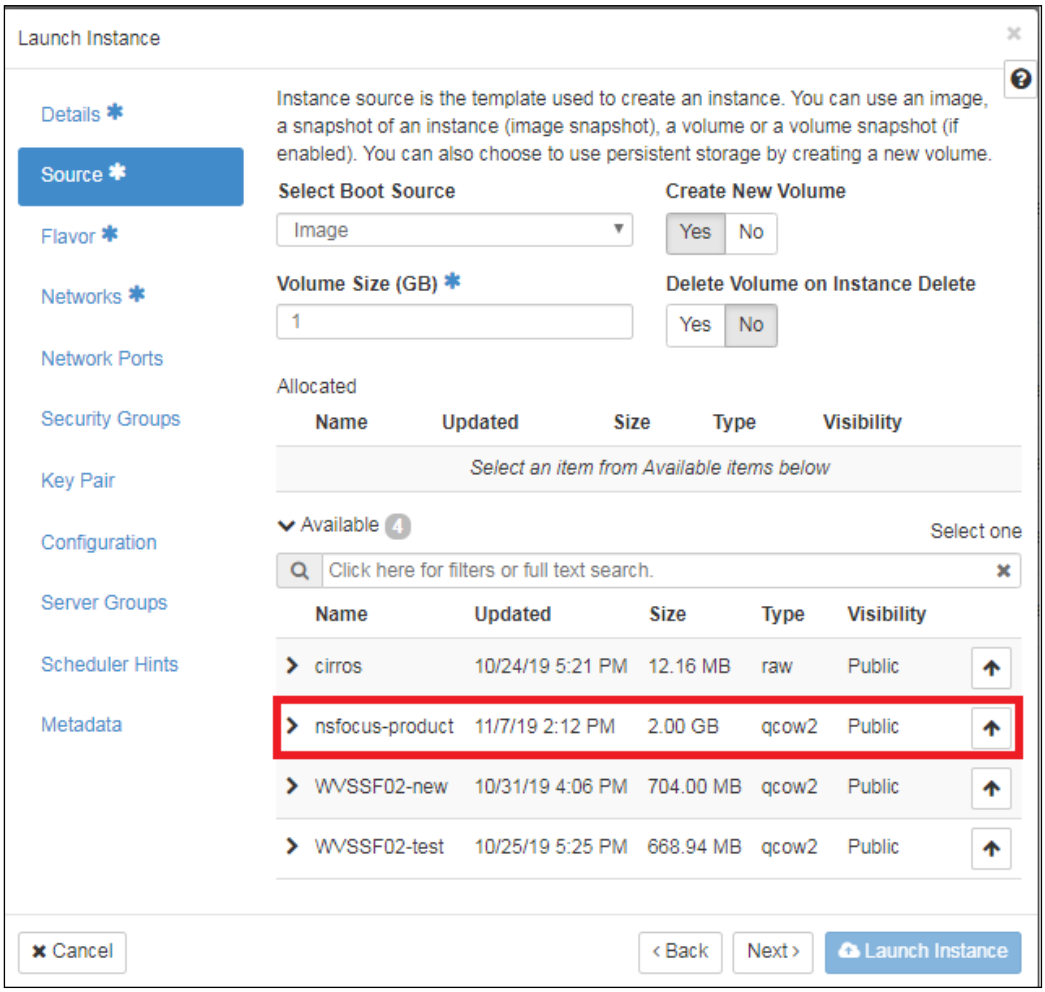
b. Click **Launch Instance**.

Figure 2-135 Creating an instance



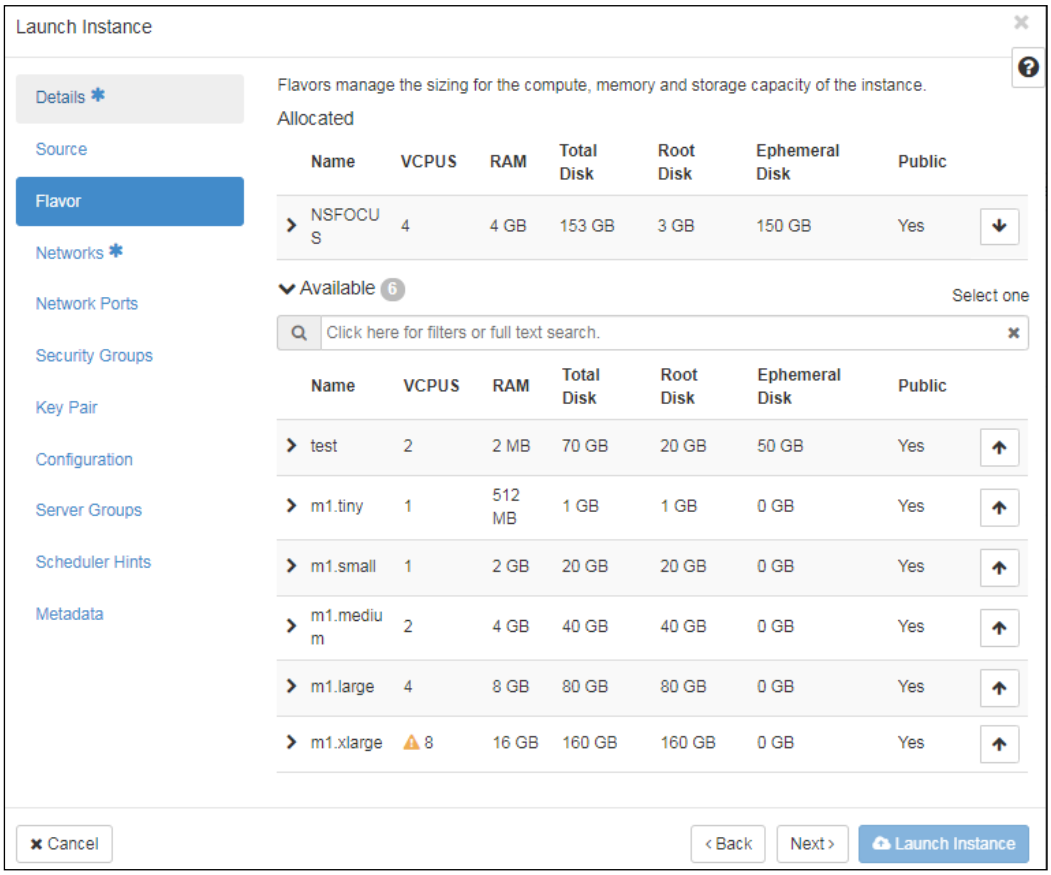
c. Configure the instance name and count and click **Next** to open the **Source** page.

Figure 2-136 Source page



d. Configure the volume size. In the **Available** area, click  in the line of the vRSAS image file to upload the file, which is then displayed in the **Allocated** area. Click **Next** to open the **Flavor** page.

Figure 2-137 Flavor page

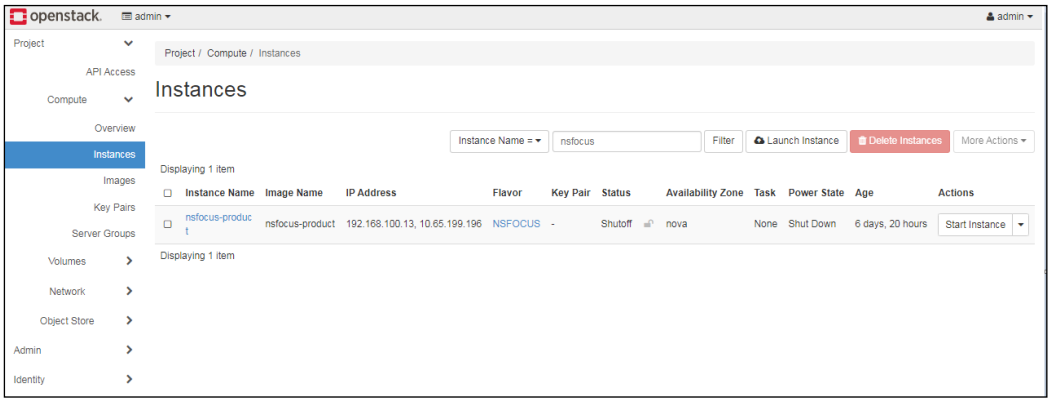


e. Click  to allocate the storage disk space, which should be up to the minimum configuration requirements listed in Table 2-1. Click **Next** to open the **Networks** page.

f. Configure network settings and click **Next**. Continue to configure other settings until metadata configuration is complete.

g. Click **Launch Instance** to return to the **Instances** page. The created instance is displayed on this page, as shown in Figure 2-138.

Figure 2-138 New instance created



----End

Installing the Image File of vRSAS

The procedure of installing vRSAS on the OpenStack platform after it is started is the same as that for the VMware Workstation platform described in Installing the Image File of vRSAS.

To start vRSAS, follow these steps:

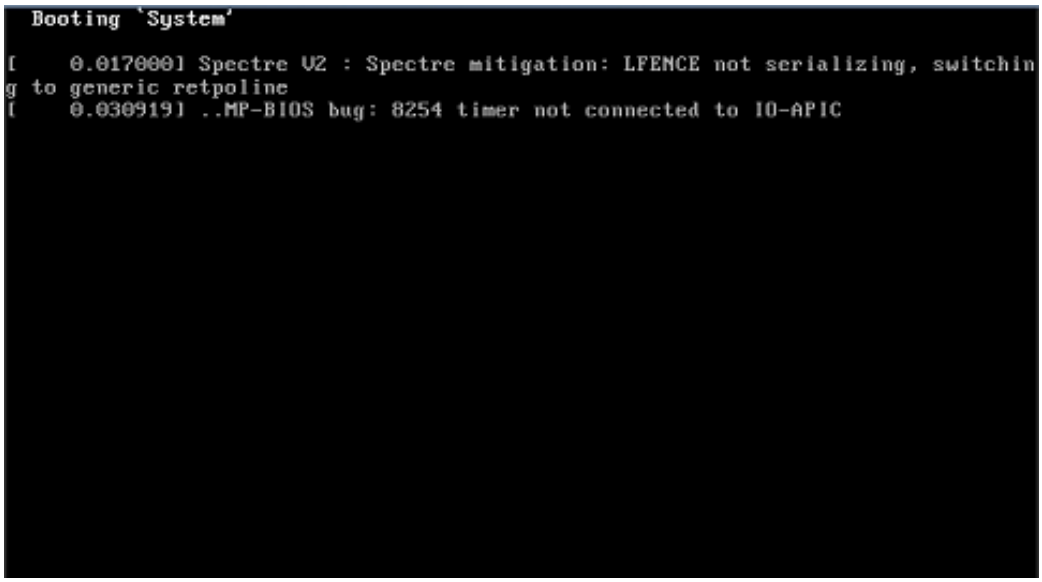
Step 1 Log in to the OpenStack platform.

Step 2 Choose **Project > Compute > Instances**.

Step 3 On the Instances page, in the line of vRSAS (**nsfocus-product** in this document), click **Start Instance** in the **Actions** column.

If a window shown in Figure 2-139 appears, wait patiently until the installation page appears.

Figure 2-139 Instance being started



----End

Performing Initial Configuration

After logging in to the console of vRSAS, you should continue to perform initial configuration. For details, see Performing Initial Configuration. To log in to the console of vRSAS, follow these steps:

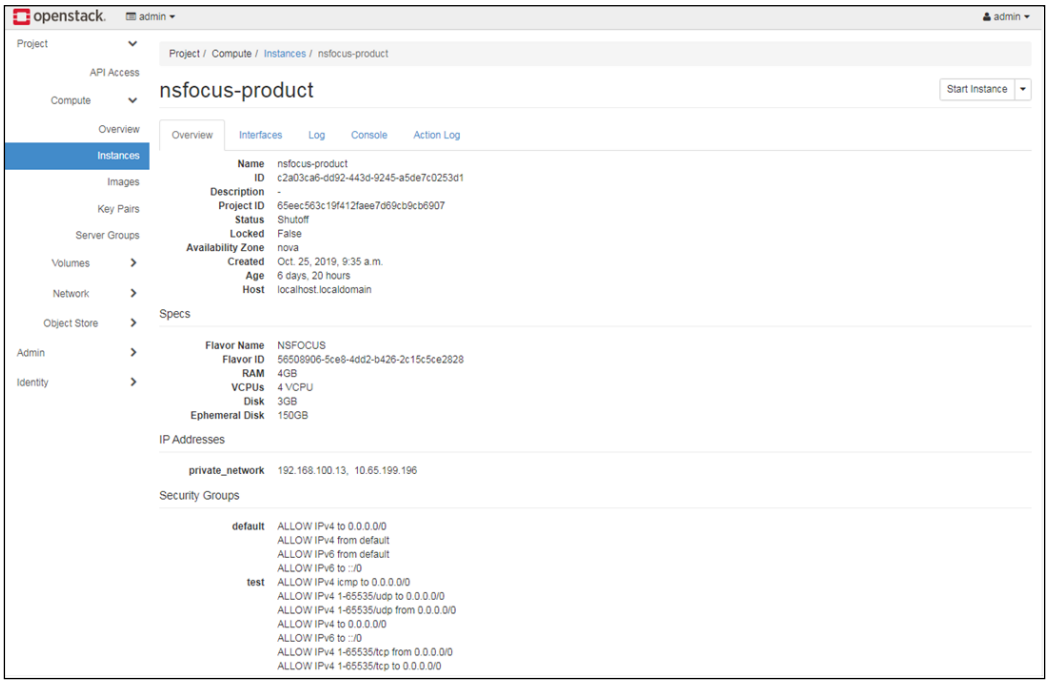
Step 1 Log in to the OpenStack platform.

Step 2 Choose **Project > Compute > Instances**.

Step 3 On the Instances page, in the line of vRSAS (**nsfocus-product** in this document), click **Start Instance** in the **Actions** column.

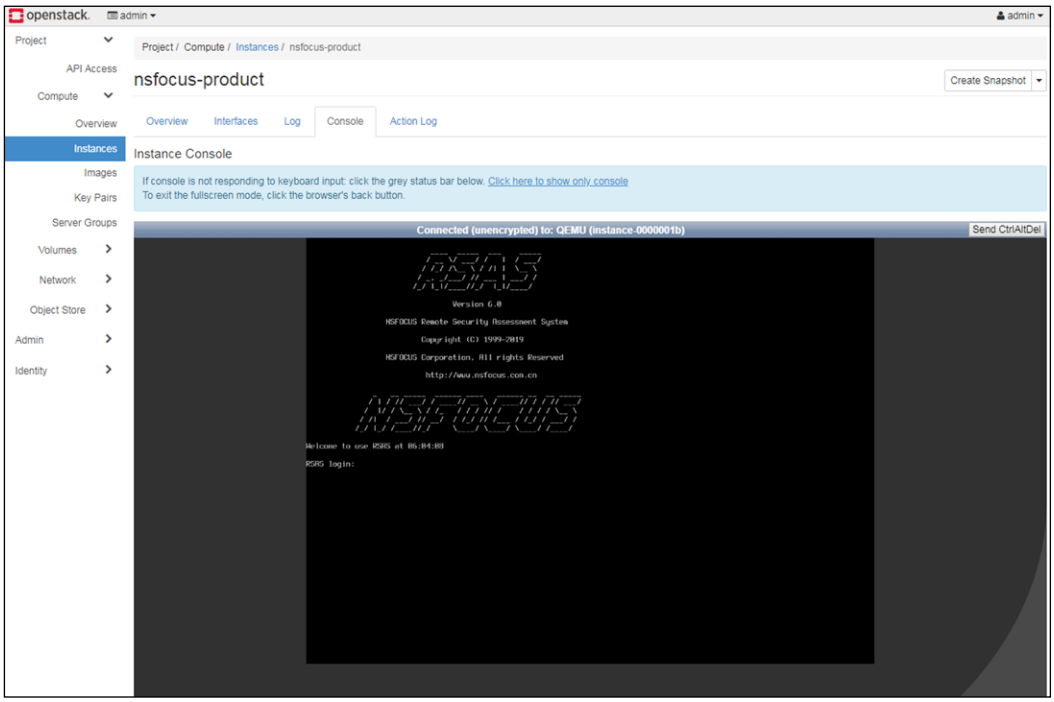
Step 4 Click the instance name of vRSAS to display an overview of the instance.

Figure 2-140 Instance overview



Step 5 Click the **Console** tab.

Figure 2-141 Console



----End

Conducting License-based Authentication

Authentication by the Centralized Authorization Platform

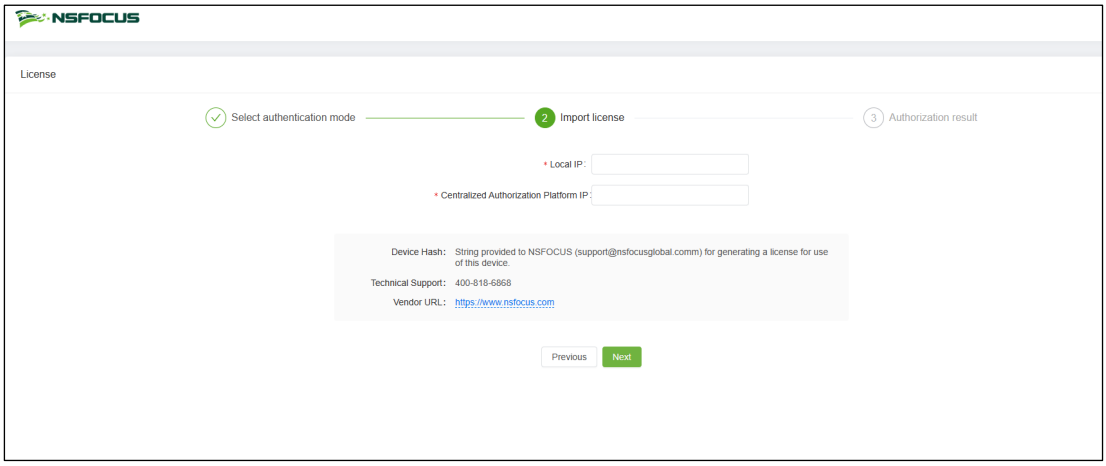
To authenticate vRSAS by using a centralized authorization platform, follow these steps:

Step 1 Access vRSAS by typing **https**://*IP address of scan interface eth1* in the address bar.

A page for authentication mode selection then appears, as shown in Figure 2-57.

Step 2 Select **Centralized authorization** and click **Next**.

Figure 2-142 Configuring authentication by a centralized authorization platform



Step 3 Type **Local IP** and **Centralized Authorization Platform IP** and click **Next**.

Step 4 Authorize the device on the specified centralized authorization platform.

----End

Authentication by NSFOCUS Security Cloud

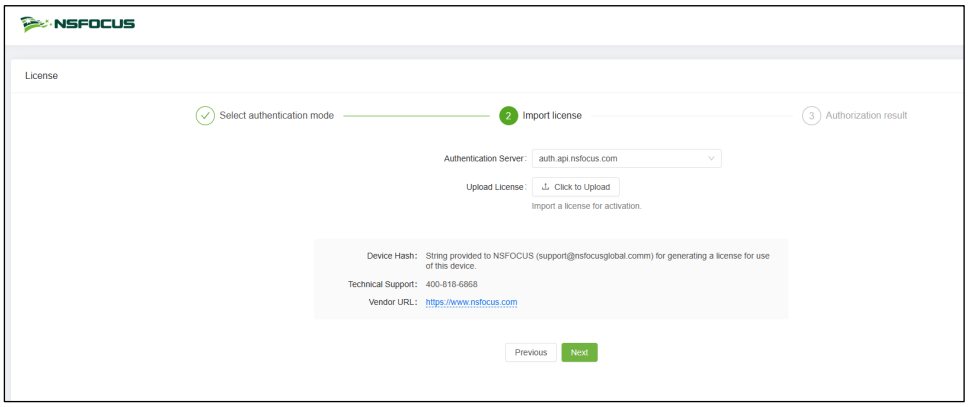
To authenticate vRSAS by using NSFOCUS security cloud, follow these steps:

Step 1 Access vRSAS by typing **https**://*IP address of scan interface eth1* in the address bar.

A page for authentication mode selection then appears, as shown in Figure 2-57.

Step 2 Select **Security cloud-side authentication** and click **Next** to upload a license.

Figure 2-143 Uploading a license



Step 3 Select the authorization server, import a valid license, and click **Next**.

----End

Authentication by the ESP-L Platform

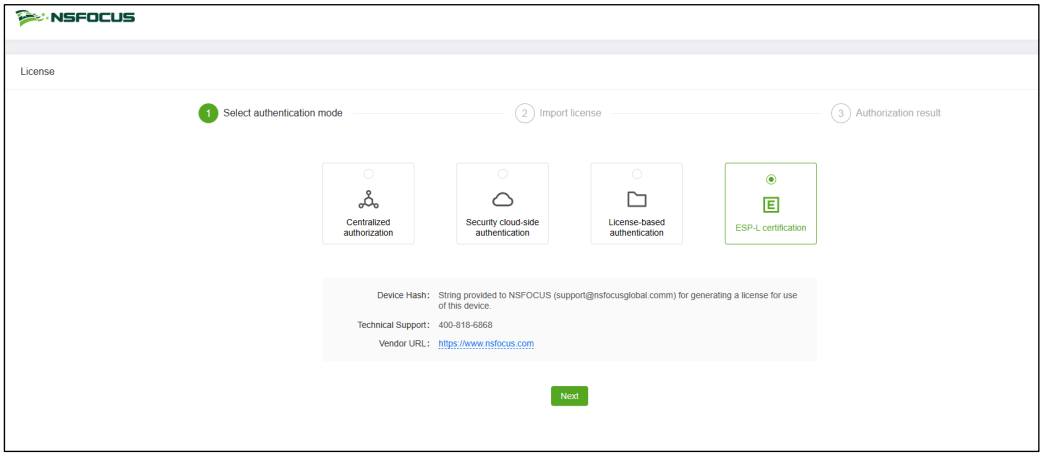
To authenticate vRSAS by using the ESP-L platform, follow these steps:

Step 1 Access vRSAS by typing **https**://*IP address of scan interface eth1* in the address bar.

A page for authentication mode selection then appears, as shown in Figure 2-57.

Step 2 Select **ESP-L certification** and click **Next**. Wait until ESP-L issues a license.

Figure 2-144 Selecting the ESP-L authentication



----End

2.2.7.3 Uninstallation Procedure

To delete vRSAS from the OpenStack platform, follow these steps:

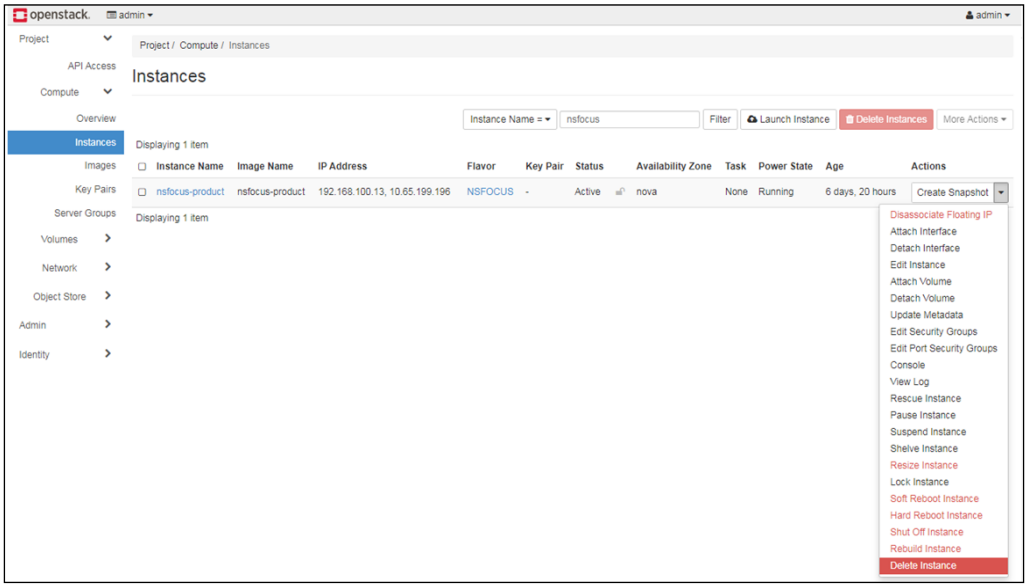
Step 1 Log in to the OpenStack platform.

Step 2 Choose **Project > Compute > Instances**.

Step 3 On the **Instances** page, in the line of vRSAS, select **Delete Instance** from the **Actions** drop-down list.

vRSAS is then completely removed from the datastore.

Figure 2-145 Deleting the vRSAS instance



----End

2.2.8 Installation on Xen

This section describes how to install vRSAS on XenServer.

2.2.8.1 Preparations

Table 2-8 lists preparations to be made for installing vRSAS on XenServer.

Table 2-8 Preparations to be made for installing vRSAS on the Xen platform

Item		Description
XenServer (server)	Host	Computer with XenServer installed.
	IP address	IP address of the host that can properly connect to the network.
	Account	Account with privileges of a system administrator.
XenCenter (client)	Host	Computer with XenCenter installed.
vRSAS	CD	Contains an image file (.iso) of vRSAS.
	IP address	IP address of the scan interface of vRSAS.
	Authentication license	• License that enables vRSAS to be launched properly. • Unique authorization hash value granted to vRSAS.

Item		Description
		• IP address of a CAA platform and license of vRSAS. • License of vRSAS for authentication by NSFOCUS security cloud. Note You can select either of the authentication modes.

2.2.8.2 Installation Procedure

Obtaining the Image File of vRSAS

For how to obtain the image file of vRSAS, see Obtaining the Image File of vRSAS.

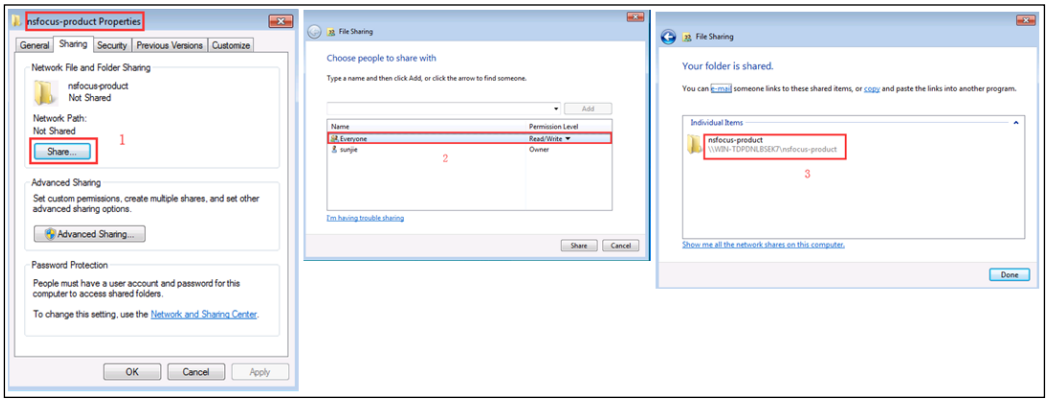
Creating a VM

To create a VM, follow these steps:

Step 1 Share the local folder that contains the vRSAS image file.

The following uses Windows 7 as an example to show how to share a folder.

Figure 2-146 Sharing a folder



Step 2 Log in to XenCenter.

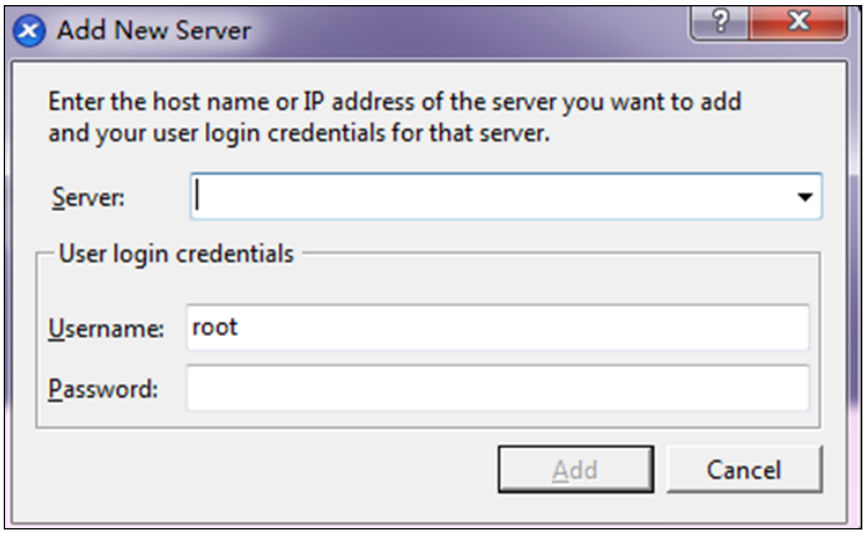
Step 3 Connect XenCenter to XenServer.

a. Click  Add a Server.

b. In the **Add New Server** dialog box, type the IP address, user name, and password of XenServer, and click **Add**.

XenCenter now connects to XenServer.

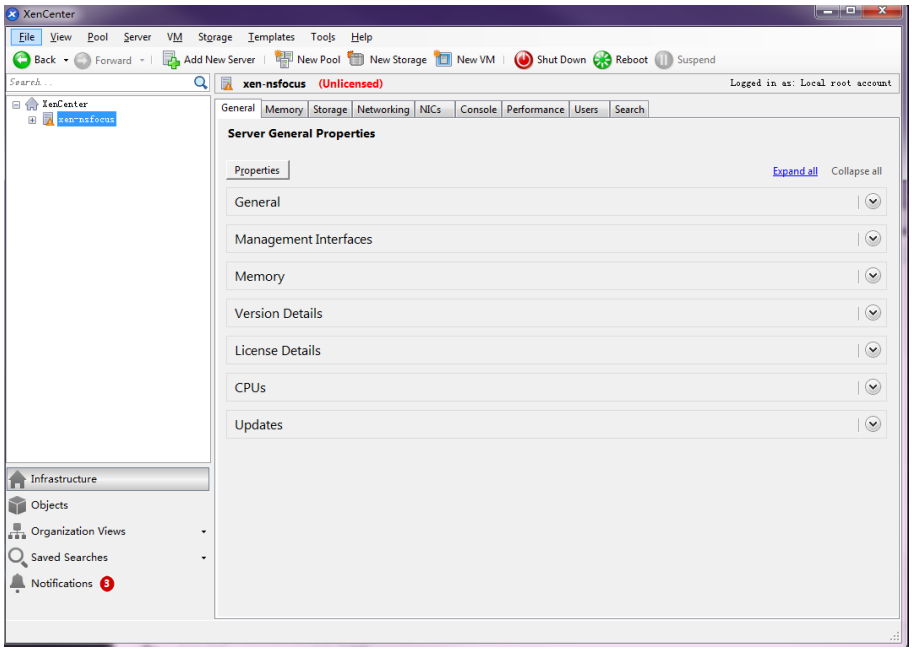
Figure 2-147 Adding a new server



Step 4 Upload the vRSAS image file to XenServer.

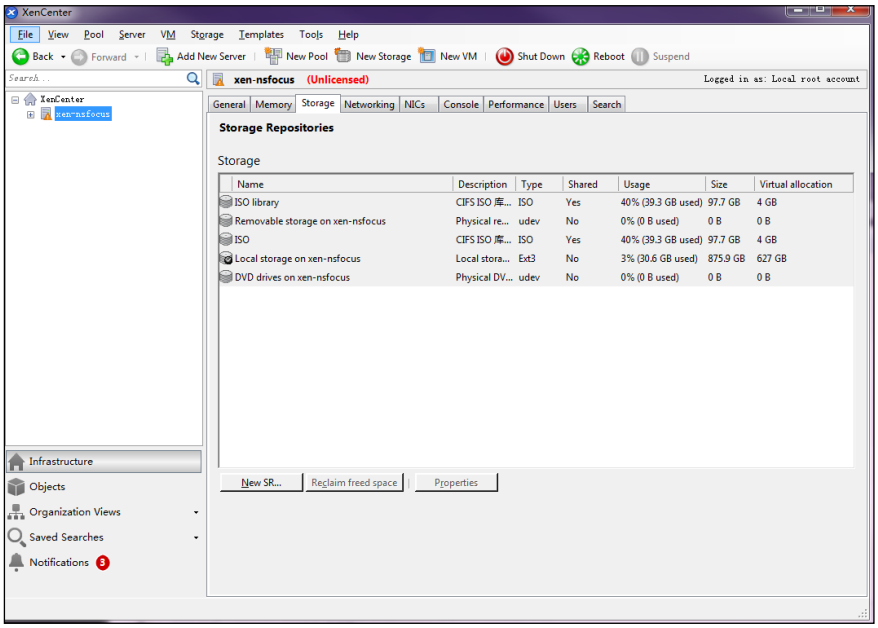
a. On the page shown in Figure 2-148, click the **Storage** tab in the right pane.

Figure 2-148 General properties of XenServer



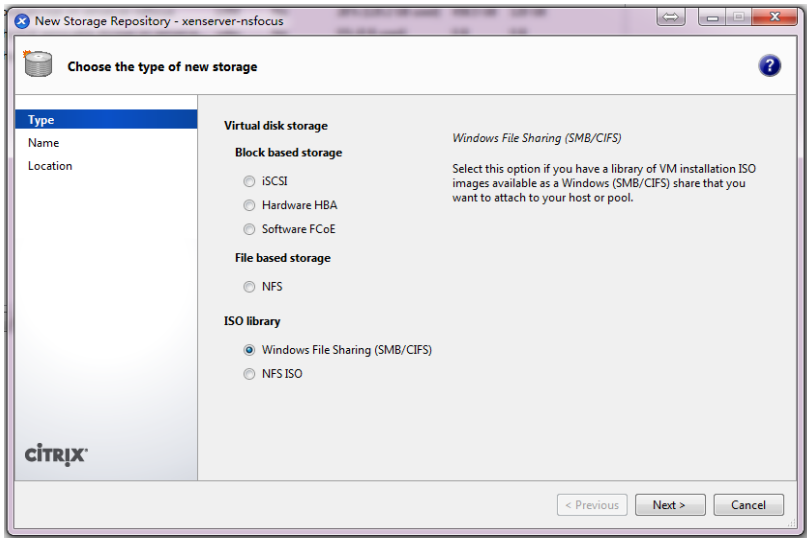
b. On the **Storage** tab page, click **New SR…**, which refers to New Storage Repository.

Figure 2-149 Storage repositories



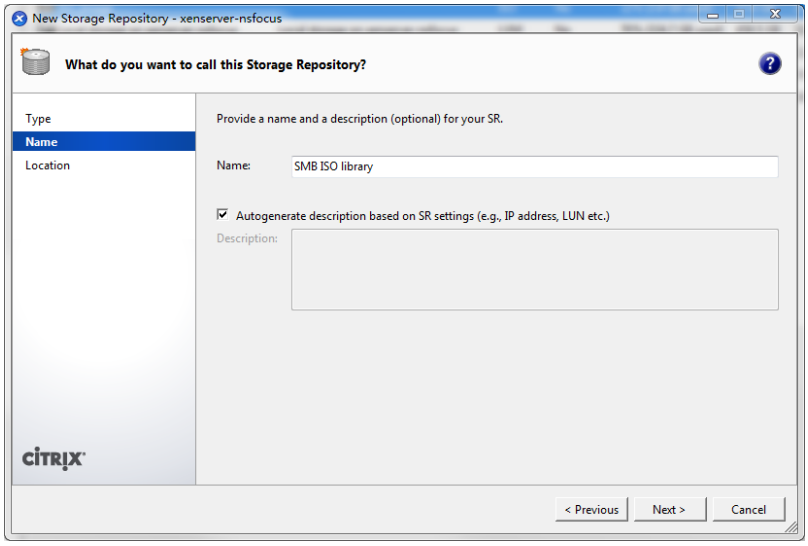
c. In the **New Storage Repository** dialog box, select **Windows File Sharing (SMB/CIFS)** and click **Next**.

Figure 2-150 Specifying the type of the new storage repository



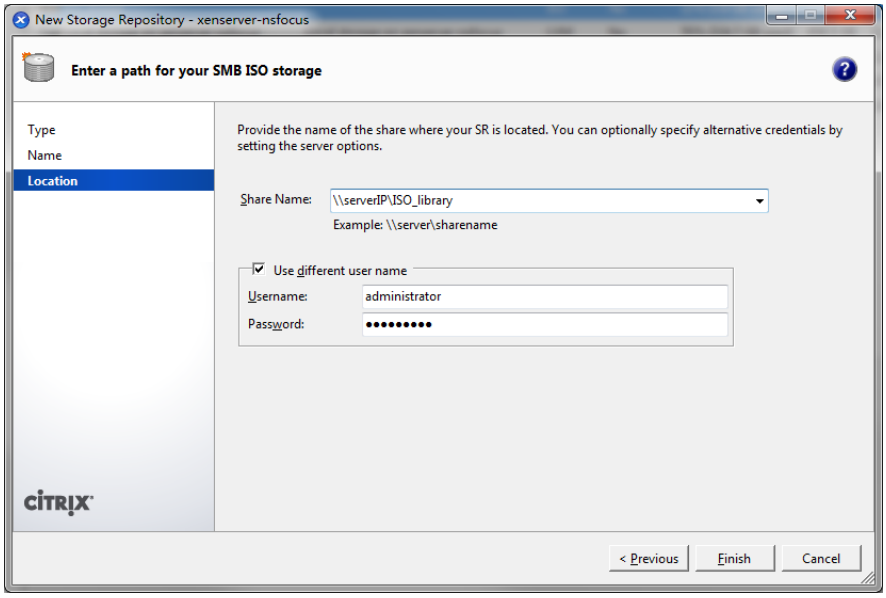
d. On the **Name** page, specify a name for the new storage repository and click **Next**.

Figure 2-151 Naming the new storage repository



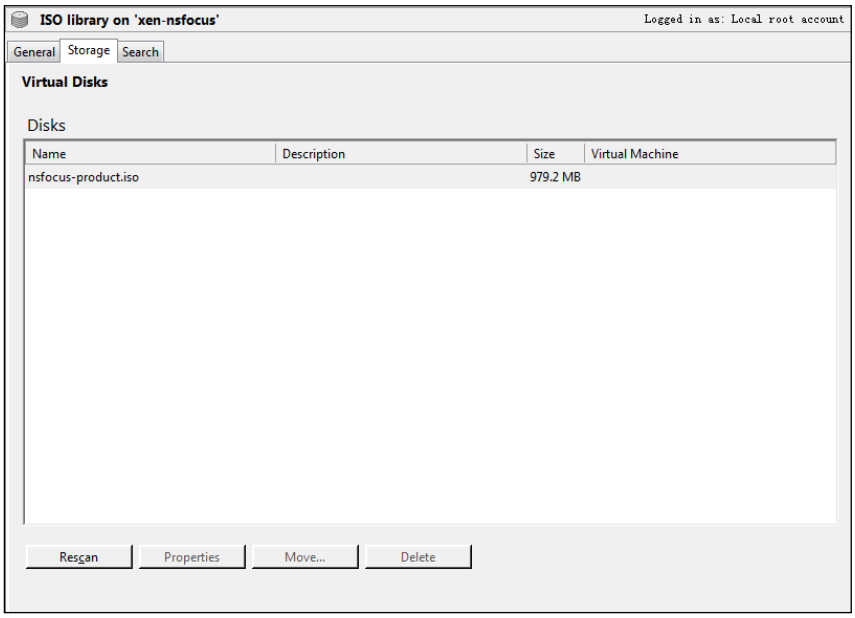
e. On the **Location** page, type the path of the shared folder configured in Step 1 and click **Finish**.

Figure 2-152 Typing the path of the ISO storage



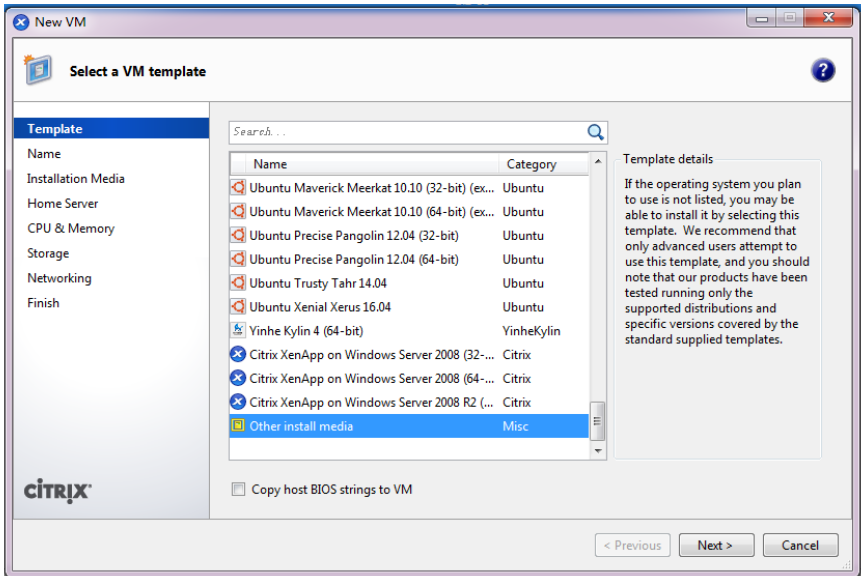
Step 5 Choose **ISO library** from the left pane, click the **Storage** tab, and then click **New VM**.

Figure 2-153 Storage page



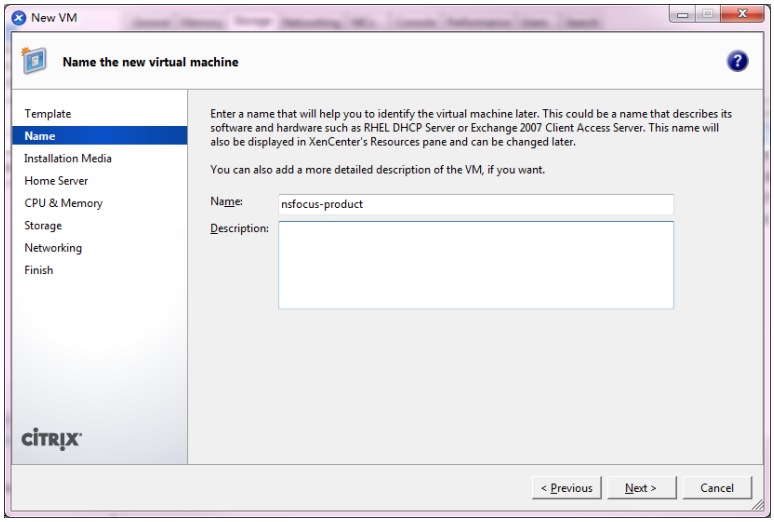
Step 6 In the **New VM** dialog box, choose **Template > Other install media** and click **Next**.

Figure 2-154 Selecting a VM template



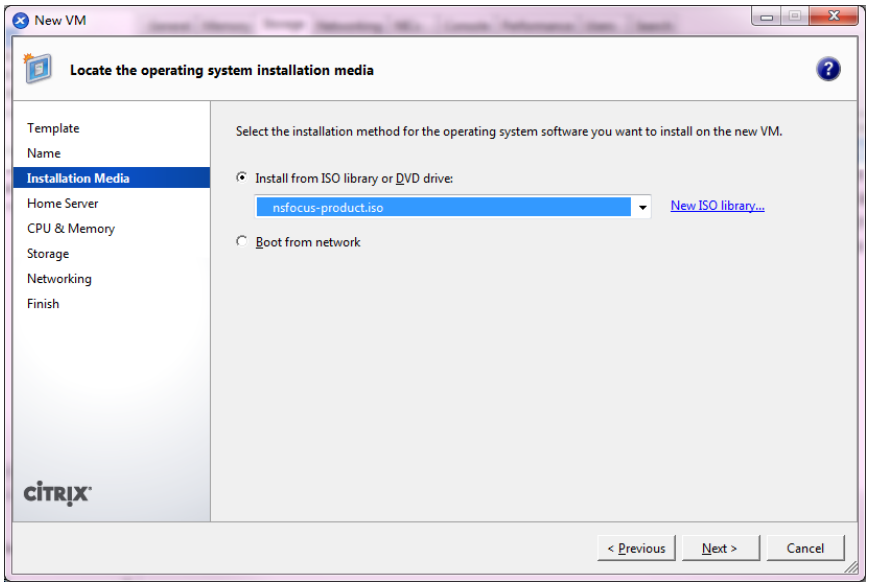
Step 7 On the **Name** page, type the name of the new VM and click **Next**.

Figure 2-155 Naming the new VM



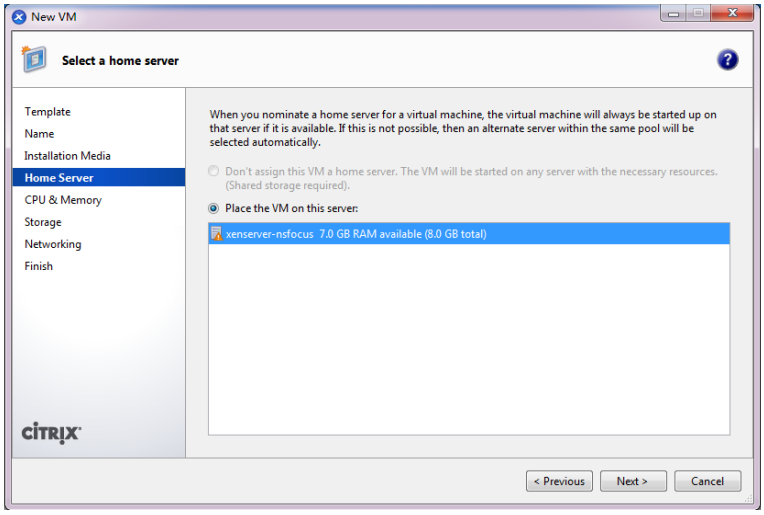
Step 8 On the **Installation Media** page, click **Install from ISO library or DVD drive**, select the vRSAS image file, and click **Next**.

Figure 2-156 Locating the operating system installation media



Step 9 On the **Home Server** page, click **Place the VM on this server** and click **Next**.

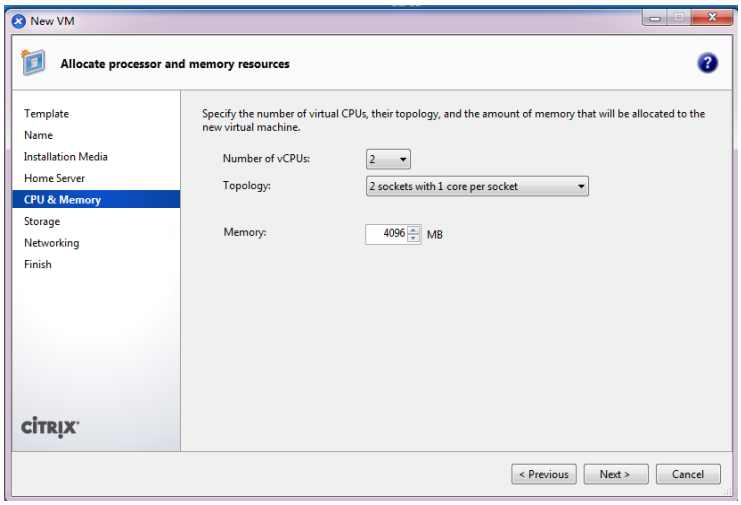
Figure 2-157 Specifying a home server



Step 10 On the **CPU & Memory** page, configure memory and CPU parameters and click **Next**.

The size of memory and the number of CPUs should meet the minimum configuration requirements listed in Table 2-1.

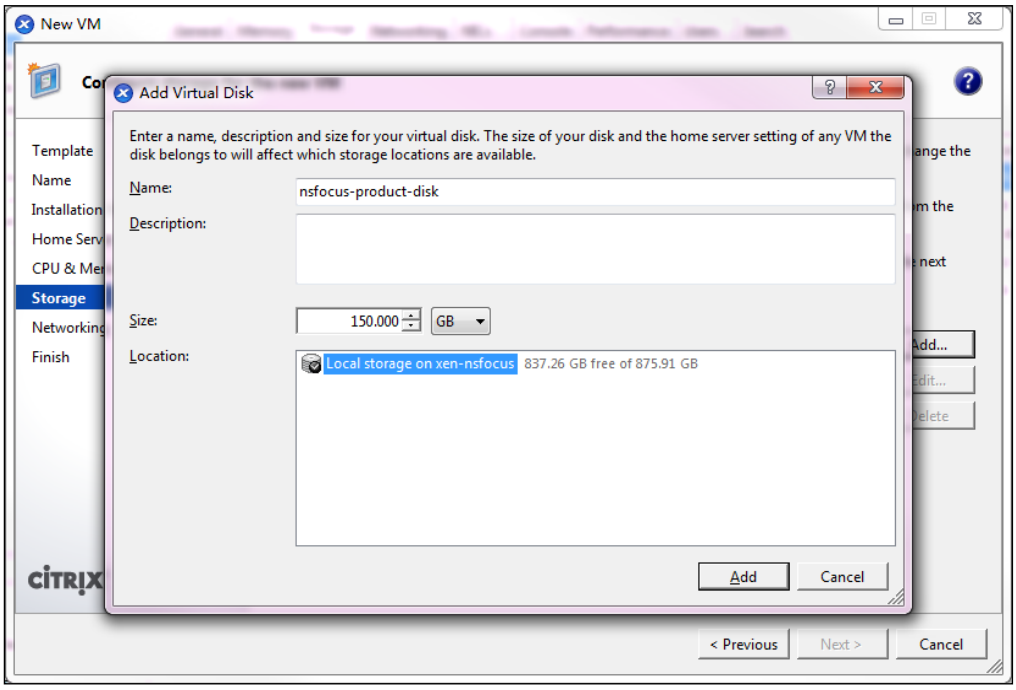
Figure 2-158 Configuring CPUs and memory



Step 11 On the **Storage** page, select **Use these virtual disks** and click **Add**.

In the **Add Virtual Disk** dialog box, configure the virtual disk name, specify the disk size, and click **Add**.

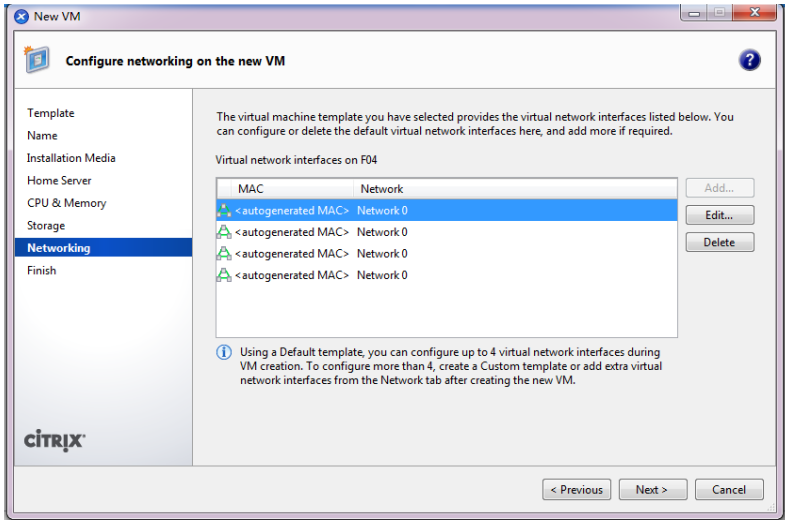
Figure 2-159 Adding a virtual disk



Step 12 On the **Storage** page, select a desired virtual disk and click **Next**.

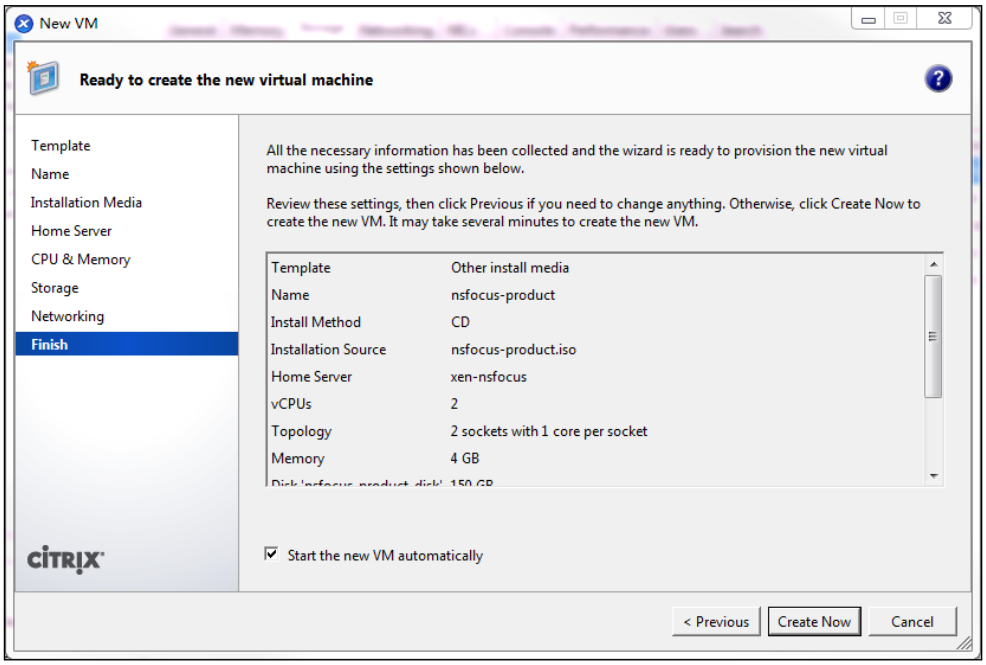
Step 13 On the **Networking** page, add network interfaces as required and click **Next**.

Figure 2-160 Adding network interfaces



Step 14 On the **Finish** page, confirm that all information is correct and click **Create Now**.

Figure 2-161 Finishing the creation process



----End

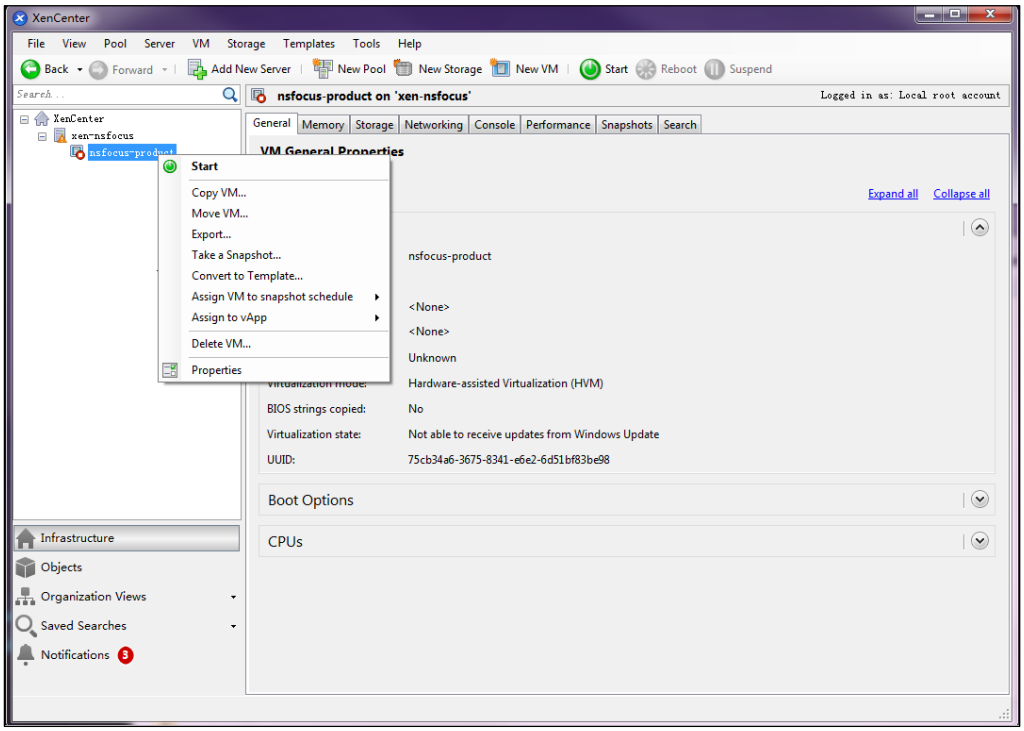
Installing the Image File of vRSAS

To install the image file of vRSAS, follow these steps:

Step 1 Log in to XenCenter.

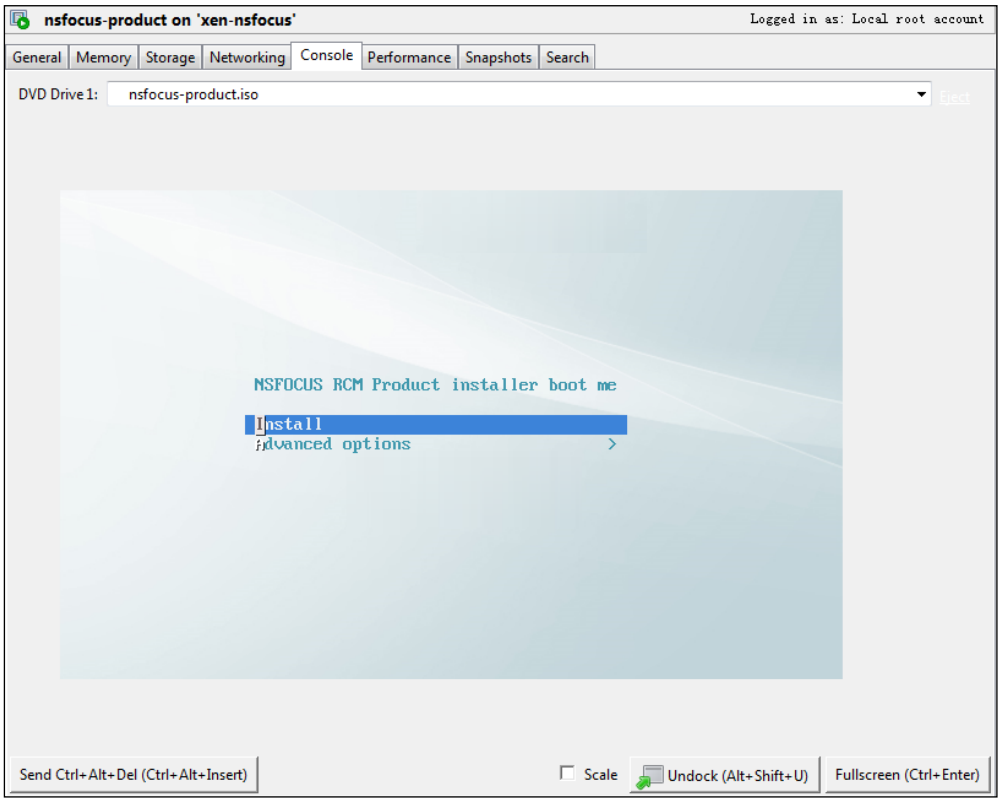
Step 2 Choose vRSAS (**nsfocus-product** in this document) from the left navigation tree and click **Start**.

Figure 2-162 Launching vRSAS



Step 3 Click the **Console** tab to open the console window of vRSAS.

Figure 2-163 Console of vRSAS



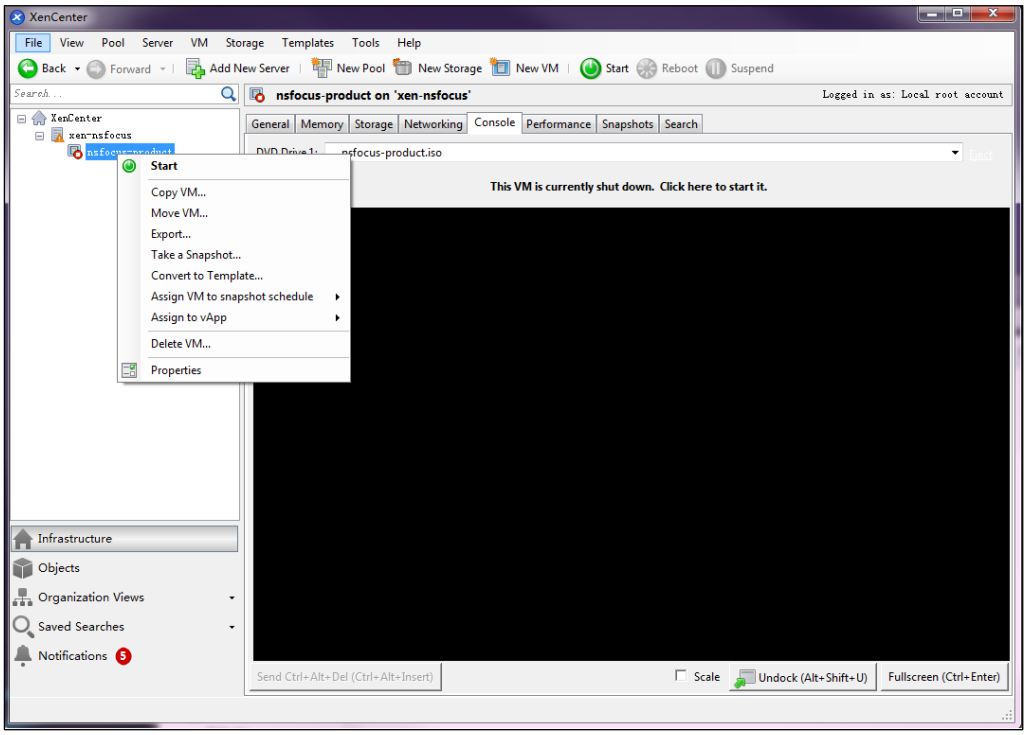
Step 4 Install vRSAS.

For details, see Installing the Image File of vRSAS.

Step 5 Change the boot mode to boot from hard disk as prompted.

a. Right-click vRSAS.

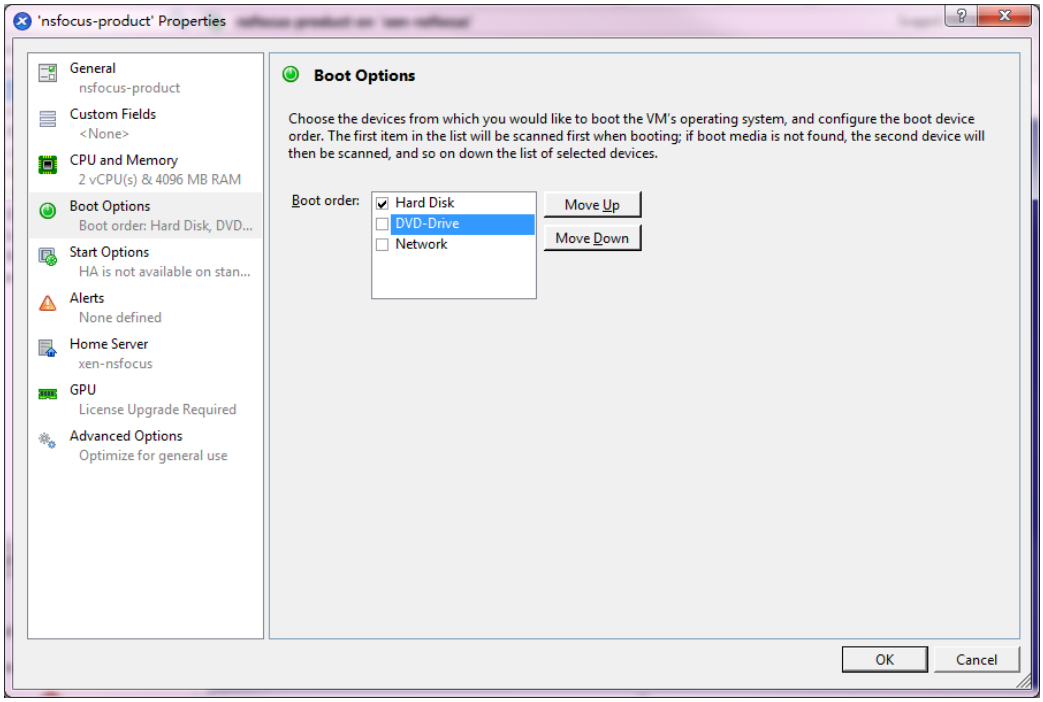
Figure 2-164 Shortcut menu of vRSAS



b. Choose **Properties** from the shortcut menu.

c. On the **Properties** page, choose **Boot Options** from the left pane, select **Hard Disk**, and click **OK**.

Figure 2-165 Boot options

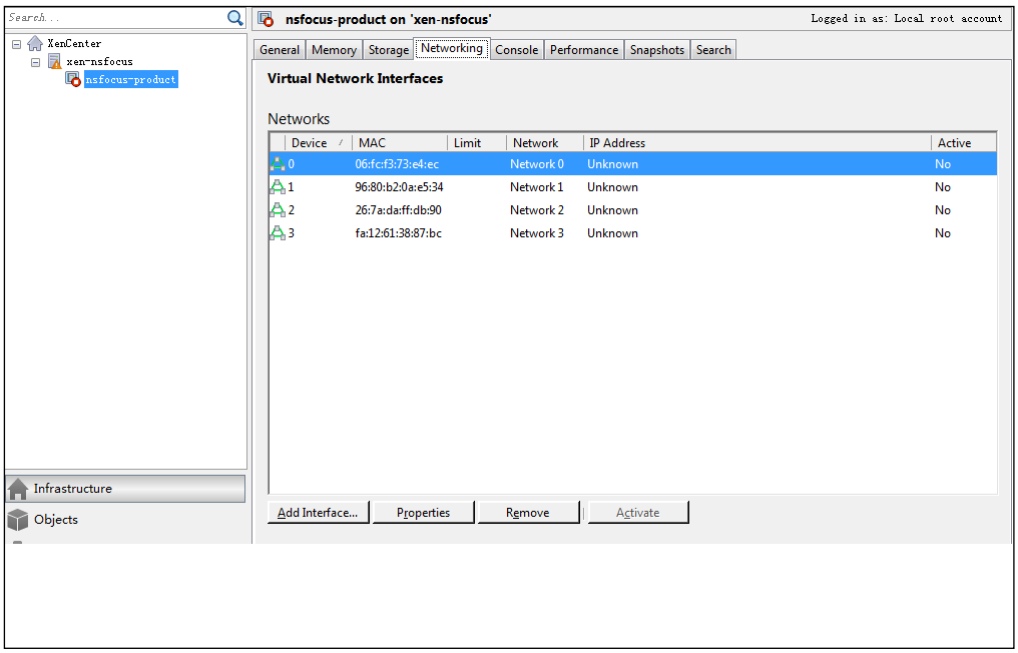


Step 6 Add a network adapter.

vRSAS only provides one network interface (that is, management interface) by default. You need to add a network adapter to enable the scan interface.

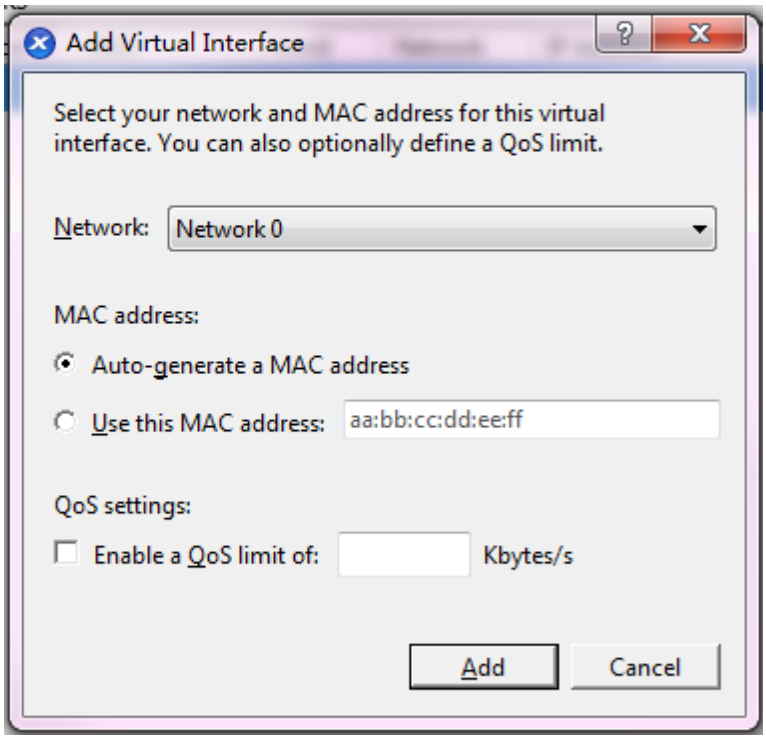
a. Click the **Networking** tab

Figure 2-166 Networking page



b. Click **Add Interface**.

Figure 2-167 Adding a virtual interface



c. In the **Add Virtual Interface** dialog box, configure parameters for the network adapter, and then click **Add**.

d. (Optional) Add other network adapters as required.

----End

Performing Initial Configuration

After logging in to the console of vRSAS (as detailed in Installing the Image File of vRSAS), you should continue to perform initial configuration. For details, see Performing Initial Configuration.

Conducting License-based Authentication

For how to import a license, see Conducting License-based Authentication.

2.2.8.3 Uninstallation Procedure

To delete vRSAS from XenServer, follow these steps:

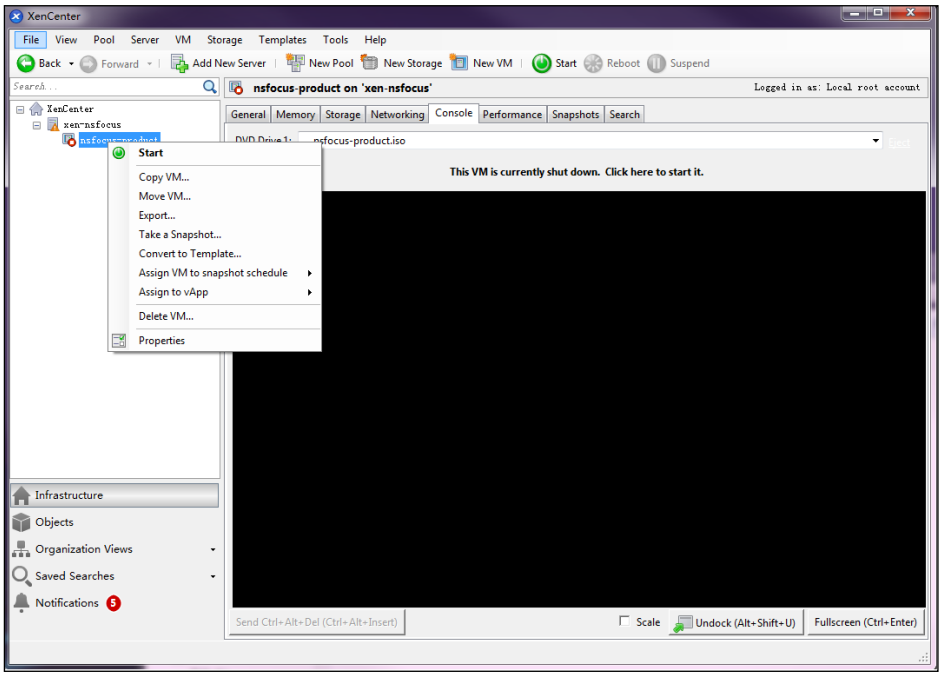
Step 1 Log in to XenCenter.

Step 2 Choose vRSAS from the left navigation tree.

Step 3 Right-click vRSAS and choose **Delete VM** from the shortcut menu.

vRSAS is then completely removed from the datastore.

Figure 2-168 Deleting vRSAS



----End

3 Initial Login

This chapter contains the following sections:

Section	Description
Console-based Management	Describes how to log in to the console.
Initial Configuration	Provides instructions for initial configuration of RSAS.
Web-based Management	Describes the login method and page layout of the web-based manager.
Importing a License for the Initial Use	Describes how to import a license.

3.1 Console-based Management

With serial connections, you can access the RSAS console to perform functions such as the initial configuration, status detection, and initialization restoration, which are unavailable on the web-based manager.

3.1.1 Login

This section describes how to log in to the console.

3.1.1.1 Preparations

Before logging in to the console, prepare the following:

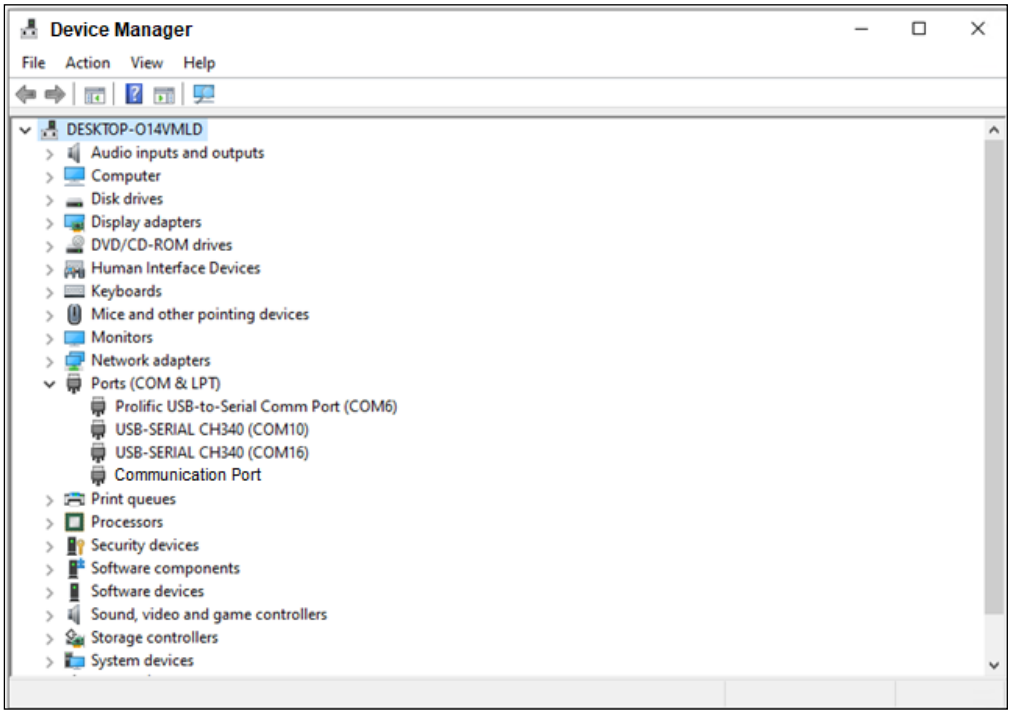
- One PC, on which terminal software, such as PuTTY, has been installed and can connect to the console.
- One serial cable (included in the accessory kit), with one end connecting to the device and the other to the serial port of the PC.
- Communication parameters, user name, and password (see Default Parameters).

3.1.1.2 Procedure

The following uses PuTTY as an example to describe how to log in to the console user interface.

Step 1 On the desktop of the PC, right-click **Computer/This Computer** and select **Properties** from the shortcut menu to open the device manager and view the serial port of the current machine.

Figure 3-1 Device manager



Step 2 Open PuTTY, configure connection properties of the serial port, and click **Open**.

Figure 3-2 Selecting a port for connection

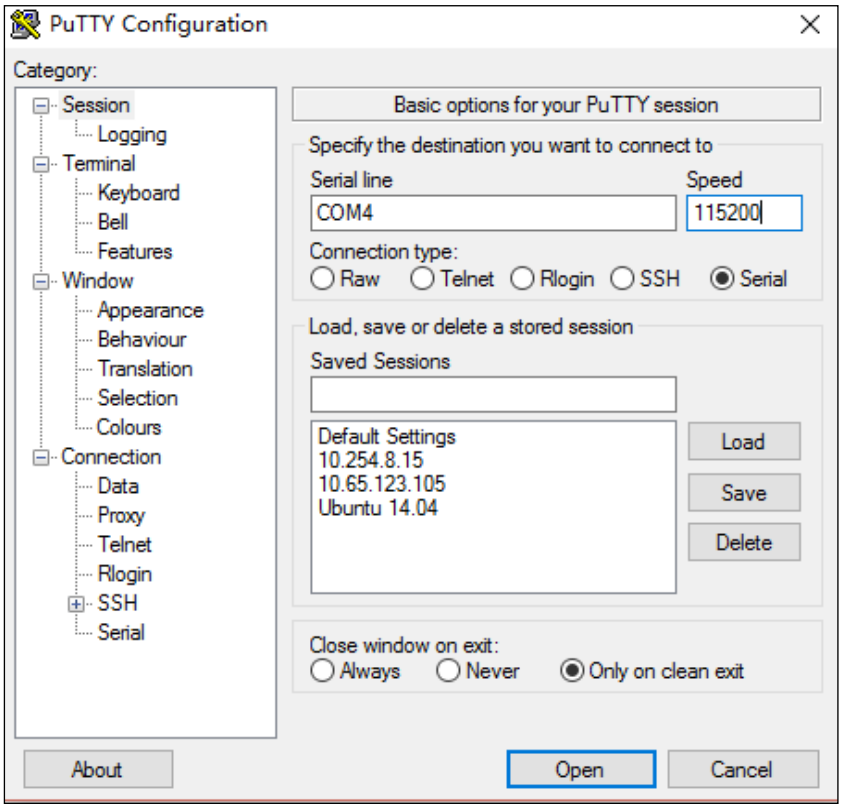
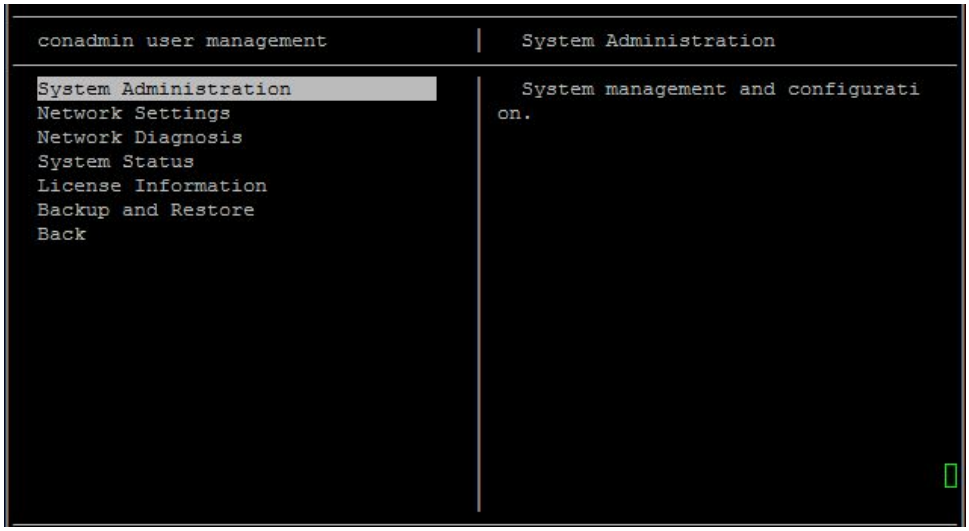


Table 3-1 Connection parameters of the serial port

Parameter	Value
Serial line	Specifies a COM port according to your computer system. For how to find out the serial port of the current computer, see Step 1.
Speed	Specifies the connection rate, which should be **115200** (bits per second).
Connection type	Specifies a connection type, which should be **Serial** here.

Step 3 Type the initial user name and password (both are **conadmin**) of the console administrator to log in to the console user interface.

Figure 3-3 Console user interface



----End

3.1.2 Meanings of Frequently Used Keys

On the console user interface, you can only perform operations with the keyboard. Table 3-2 describes meanings of the frequently used keys.

Table 3-2 Meanings of frequently used keys

Keyboard	Description
↑	Moves up.
↓	Moves down.
←	Moves left.
→	Moves right.
ESC	Cancels an operation.
Enter	Confirms an operation.
Tab	Switches between the input box, OK, and Cancel.
Backspace	Deletes the character to the left of the cursor.

3.1.3 Functions

This section describes main functions available on the console.

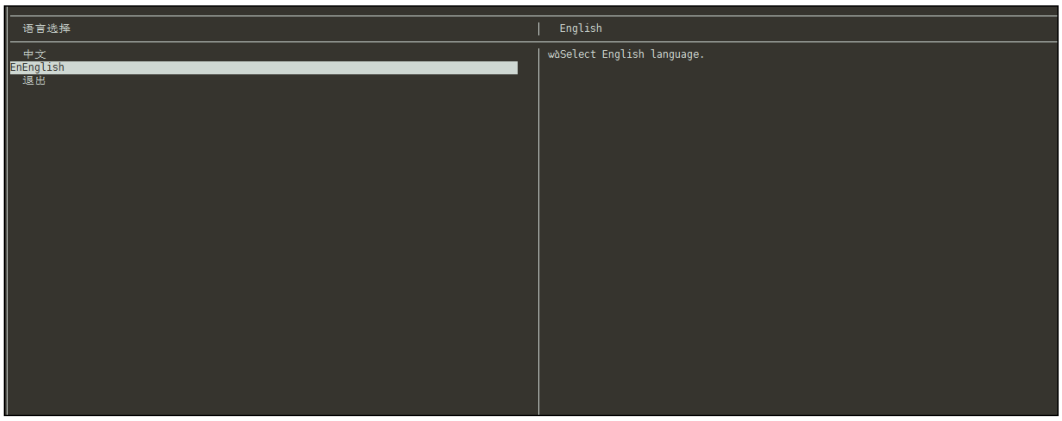
On your first login as **conadmin**, change the initial login password. Otherwise, the system reminds you every time you log in.

Figure 3-4 Password change reminder

In either of the following cases, a window shown in Figure 3-5 appears, prompting you to select a language:

- You do not change the initial password of the login account **conadmin** and click **RETURN**.
- You have changed the initial password of the login account **conadmin**.

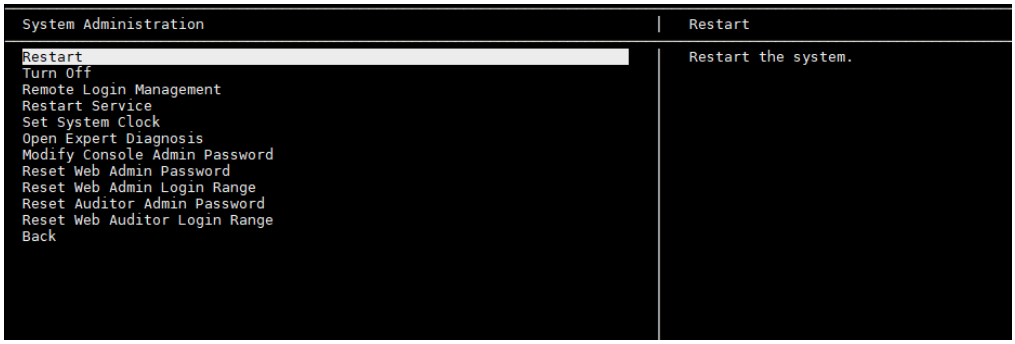
Figure 3-5 Selecting a language



3.1.3.1 System Management

Select **System Administration** on the main menu. The **System Administration** menu expands, as shown in Figure 3-6.

Figure 3-6 Console-based management — system administration



On this menu, you can perform the operations listed in Table 3-3.

Table 3-3 System administration operations on the console

Operation	Description
Restart	Restarts the RSAS system.
Turn Off	Shuts down the RSAS system.
Remote Login Management	After the SSH service is enabled, the technical support personnel of NSFOCUS can remotely log in to RSAS to diagnose faults. After it is enabled, type an IPv4 address and port number (in the range of 60000–65535) of the host that is accessible to RSAS. Then the login key and its QR code used for remote access to RSAS are displayed below.
Restart Service	Restarts RSAS services. When a system exception occurs, you can restart system services.
Set System Clock	Sets the date and time of the RSAS system.
Open Expert Diagnosis	When RSAS is faulty and requires remote assistance, technical support personnel of NSFOCUS can remotely log in to the faulty device via SSH and perform troubleshooting in the background.
Modify Console Admin Password	Changes the password of the console administrator. The password must contain 9 to 20 characters of at least two types of the following: letters, digits, and special characters (@ # $ ^ _).
Reset Web Admin Password	Restores the password for web login to the initial one when the administrator **admin** forgets it.
Reset Web Admin Login Range	Restores the default IP addresses through which the **admin** user can log in to RSAS.
Reset Auditor Admin Password	Restores the password for web login to the initial one when **auditor** forgets it.
Reset Web Auditor Login Range	Restores the default IP addresses through which **auditor** can log in to RSAS.

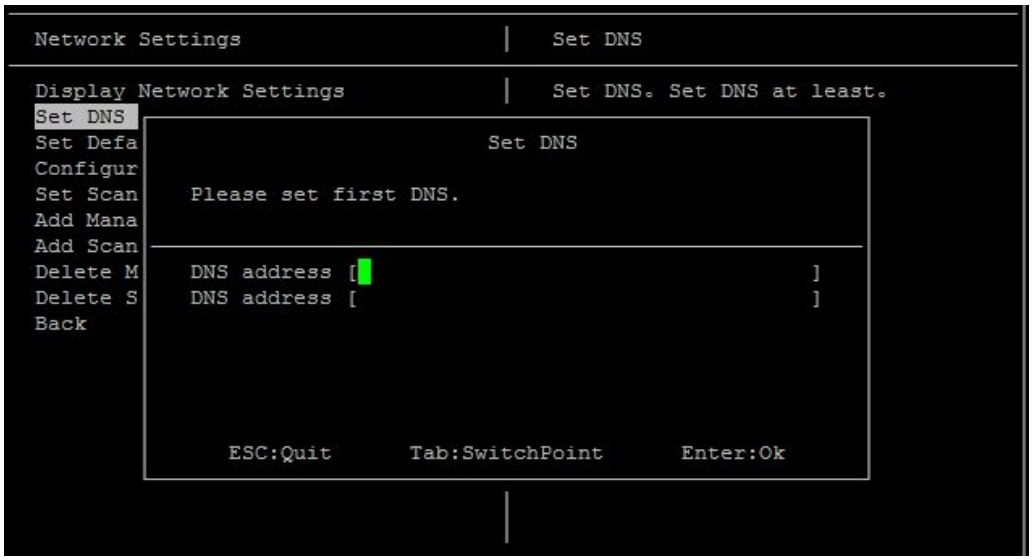
3.1.3.2 Network Configuration

RSAS provides a scan interface and a management interface. The scan interface is used for network scanning and the management interface is used for RSAS management. Also, the administrator can manage RSAS and perform task assessment only via the scan interface.

Configuring the DNS Server

Select **Network Settings** from the main menu and then select **Set DNS**, as shown in Figure 3-7.

Figure 3-7 Console-based management — setting a DNS server



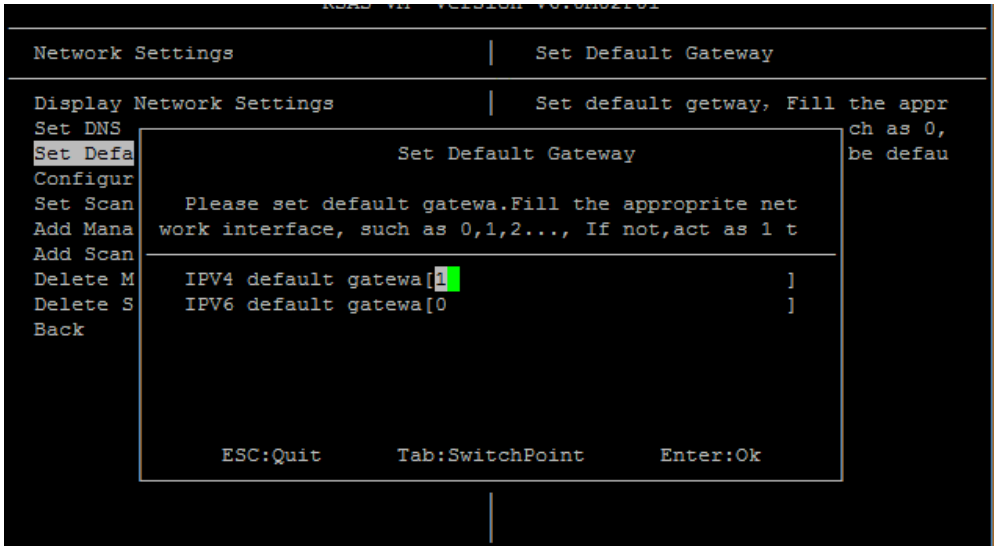
Pay attention to the following when configuring a DNS server:

- At least one DNS server should be configured.
- The first DNS address must be typed.
- Make sure that the DNS server are properly configured if the online upgrade is necessary for RSAS.

Setting the Default Gateway

Select **Network Settings** from the main menu and then select **Set Default Gateway**, as shown in Figure 3-8.

Figure 3-8 Console-based management — setting the default gateway



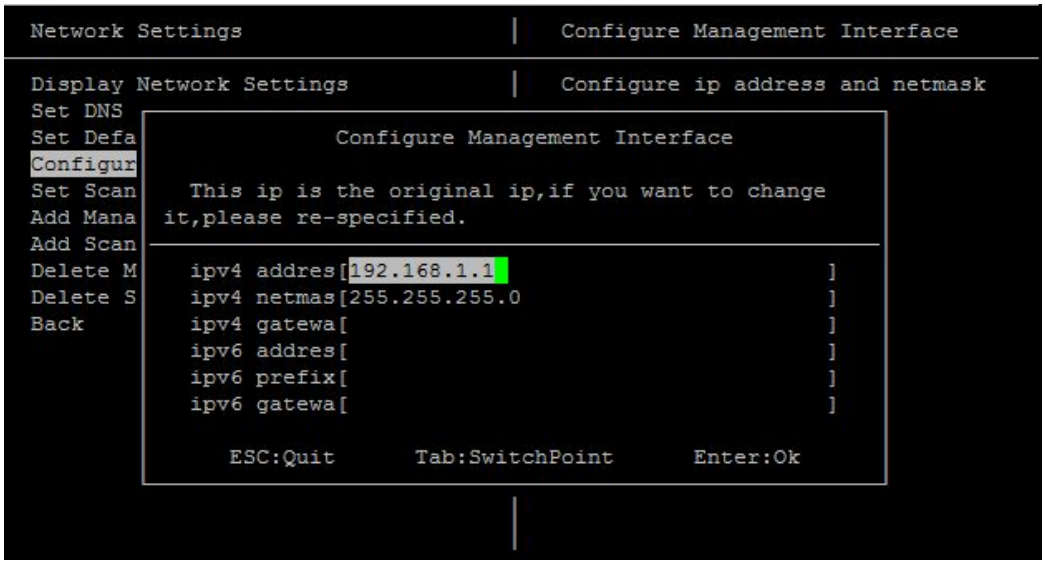
Fill in the interface number on which a default route will be generated, such as **0** for the management interface, **1** for the scan interface 1, and **2** for the scan interface 2. For example, if you fill in **1**, the default route **0.0.0.0 0.0.0.0 eth1** will be generated on the scan interface 1. If the default gateway is not specified here, the system uses the gateway of scan interface 1 as the default gateway.

Note	To generate a default route by setting the default gateway, the network interface must be correctly configured with the gateway address. For details, see Configuring the Management Interface.

Configuring the Management Interface

Select **Network Settings** from the main menu and then select **Configure Management Interface**, as shown in Figure 3-9.

Figure 3-9 Console management — configuring the management interface



Pay attention to the following when configuring the management interface:

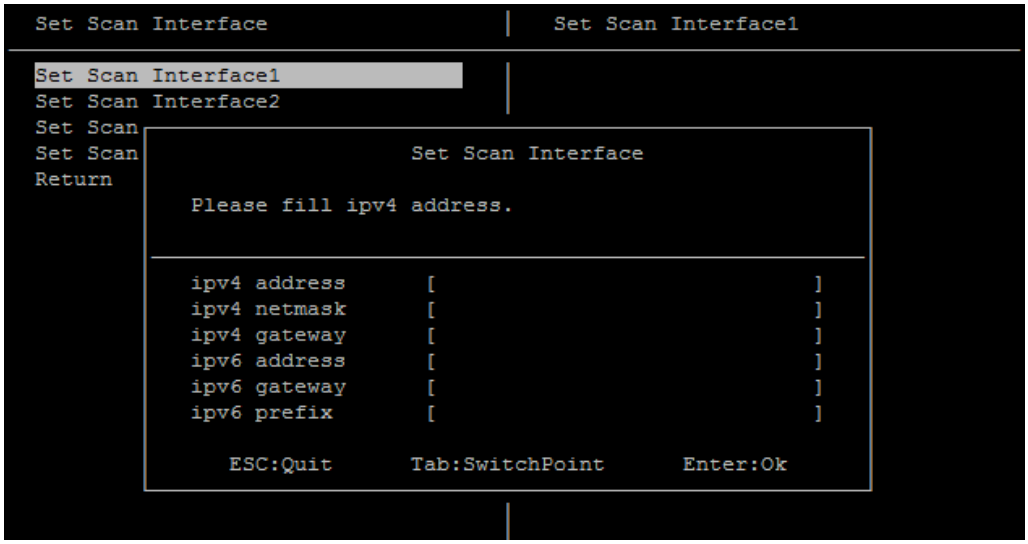
- IPv4 or IPv6 addresses are assigned via DHCP. After you press **Enter**, RSAS will automatically obtain the IP address of the scan interface.
- Either an IPv4 or IPv6 address can be configured for the management interface. The default IPv4 address is **192.168.1.1/24**.
- If the IP address of the RSAS host is on a different network segment from the IP address of the management interface, you need to add a route for the management interface.
- The negotiation mode must be set for the management interface.

  After the configuration, press Enter to make the settings take effect immediately.
- The management interface and scan interface cannot be configured in the same network segment.

Configuring the Scan Interface

Select **Network Settings** from the main menu and then choose **Set Scan Interface > Set Scan Interface 1**, as shown in Figure 3-10.

Figure 3-10 Console management — configuring the scan interface



Pay attention to the following when configuring a scan interface:

- IPv4 or IPv6 addresses are assigned via DHCP. After you press **Enter**, RSAS will automatically obtain the IP address of the scan interface.
- Either an IPv4 or IPv6 address is allowed for a scan interface. The setting takes effect immediately.

  After the configuration, click **OK** to make the settings take effect immediately.
- Make sure that the gateway and DNS server are properly configured if the online upgrade is necessary for RSAS.

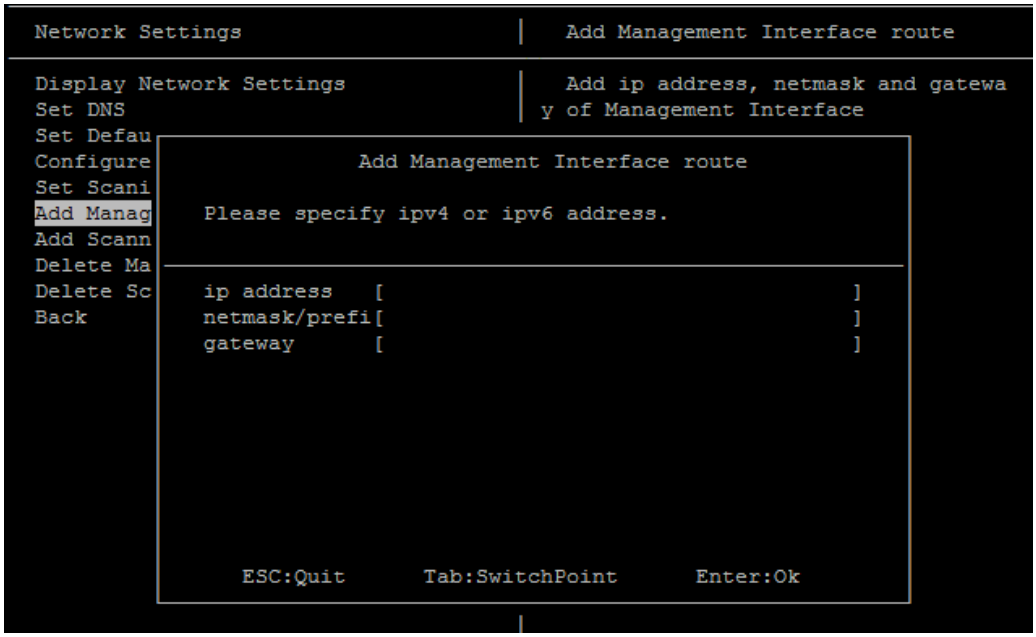
  Parameters must be set in the correct format, for example, 255.255.255.0 as the IPv4 netmask.
- The management interface and scan interface, and any two scan interfaces must be configured in different network segments.

Creating a Route for the Management Interface

You can specify an access path to the network by creating or deleting a static route.

Select **Network Settings** from the main menu and then select **Add Management Interface Route**, as shown in Figure 3-11.

Figure 3-11 Console management — creating a route for the management interface



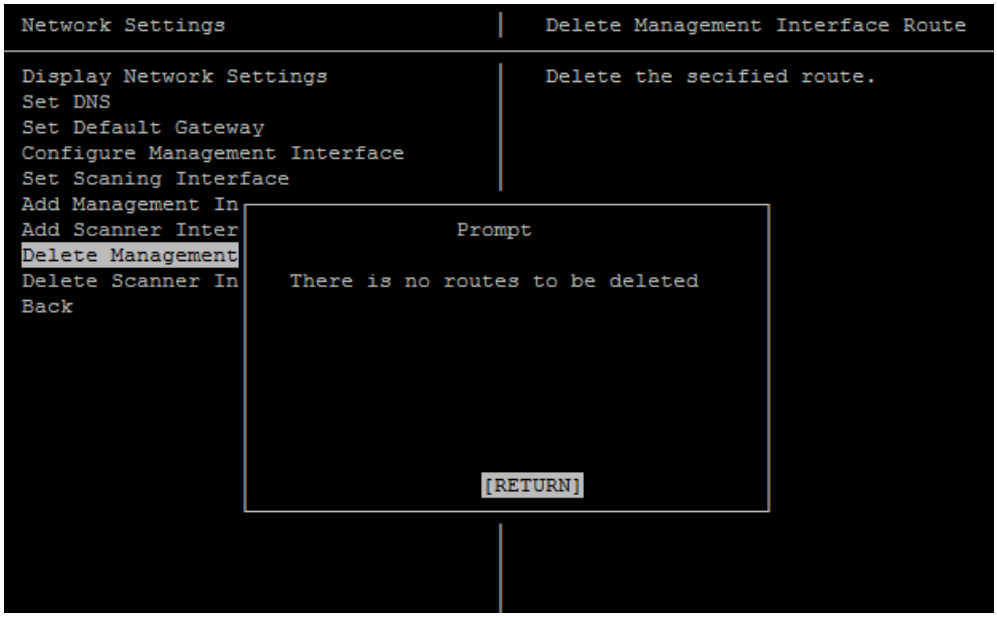
Pay attention to the following when creating a route:

- The default management interface is the M interface. Here, route parameters are set for this interface.
- After you set the IP address, subnet mask, and gateway address and click **OK**, the settings take effect immediately.
- If an error occurs after you click **OK**, check whether the IP address and gateway address are correct.

Deleting a Route of the Management Interface

Select **Network Settings** from the main menu and then select **Delete Management Interface Route**, as shown in Figure 3-12.

Figure 3-12 Console management — deleting a route of the management interface



Pay attention to the following when deleting a route:

- After you select **Delete Management Interface Route**, the routing table of the management interface appears. Select the route that you want to delete.
- After you select the route and click **OK**, the deleted route immediately loses effect and disappears from the routing table.

Creating a Route for a Scan Interface

Select **Network Settings** from the main menu and then select **Add Scan Interface Route**. A route for a scan interface is added in the same way as that for the management interface. For details, see Creating a Route for the Management Interface.

Deleting a Route of a Scan Interface

Select **Network Settings** from the main menu and then select **Delete Scan Interface Route**. A route of a scan interface is deleted in the same way as a route of the management interface. For details, see Deleting a Route of the Management Interface.

3.1.3.3 Network Diagnosis

Select **Network Diagnosis** from the main menu, as shown in Figure 3-13.

Figure 3-13 Console management — network diagnosis

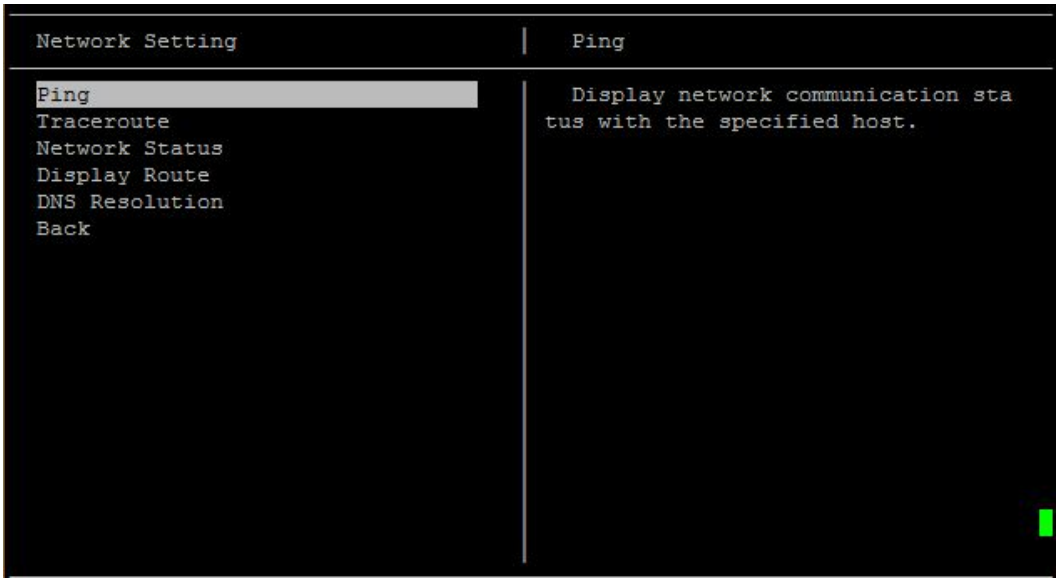


Table 3-4 lists network diagnosis tools available on RSAS.

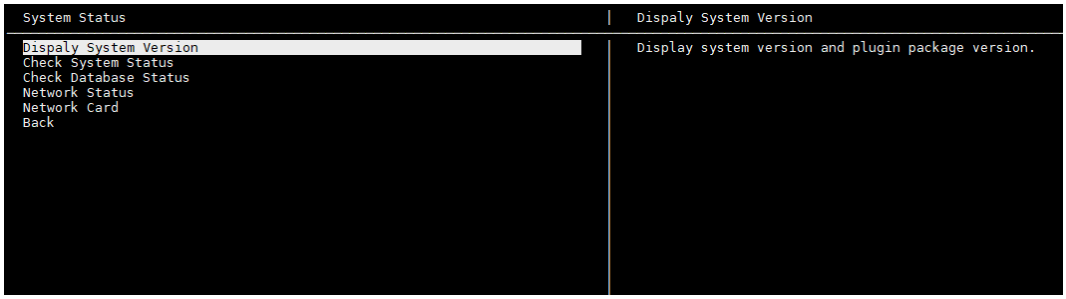
Table 3-4 Network diagnosis tools on the console

Tool	Function
Ping	Checks the connection between RSAS and the target host. IPv4 and IPv6 addresses are acceptable.
Traceroute	Traces the hops between RSAS and the target host.
Network Status	Displays the network connection status of RSAS.
Display Route	Displays parameters of the interface used by the routing device to connect to RSAS.
DNS Resolution	Displays the domain name resolution information.

3.1.3.4 System Status

Select **System Status** from the main menu. The **System Status** menu expands, as shown in Figure 3-14.

Figure 3-14 Console-based management — system status



On the **System Status** menu, you can view status information listed in Table 3-5.

Table 3-5 System status checking on the console

Operation	Description
Display System Version	Displays the system and plugin versions of RSAS.
Check System Status	Displays the system status of RSAS.
Check Database Status	Displays the background database status of RSAS.
Network Status	Displays the NIC configuration and routing table of RSAS. Usually, it is used to check the network configuration.
Network Card	Displays the IP address, MAC address, the number of bytes of data transmitted and received by the NIC. The information is usually used to check whether the NIC works properly.

Note	Ongoing assessment tasks will be stopped during the checking of the system status or database status. To avoid data loss, conduct status checks after all tasks are completed.

3.1.3.5 License Information

Select **License Information** from the main menu, as shown in Figure 3-15.

You can check the information about the authorized license file of the current system, including the product type, the start date, end date, and expiry date of the license, as well as your purchased modules.

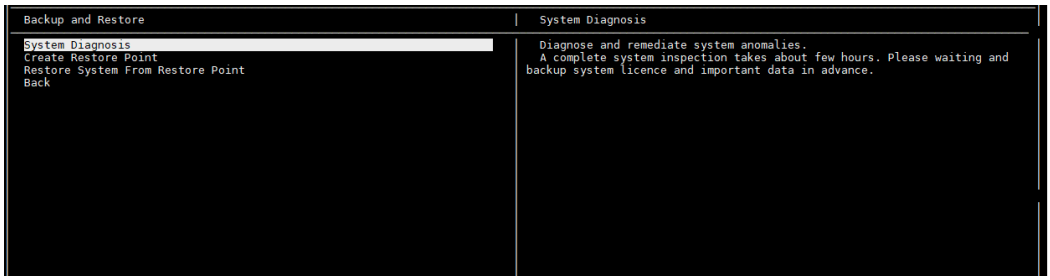
Figure 3-15 License Information

3.1.3.6 Backup and Restoration

Backup and restoration are very important functions of RSAS as the two functions can restore data in time once the device breaks down.

Select **Backup and Restore** from the main menu, as shown in Figure 3-16.

Figure 3-16 Backup and restoration

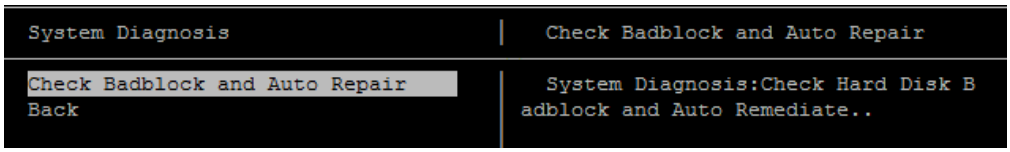


Performing System Diagnosis for Automatic Remediation

System diagnosis is to diagnose and fix system faults. The entire diagnosis process takes a long time. You must back up the system license and important scanning data in advance and patiently wait until the process is complete.

Select **Backup and Restore** from the main menu and then select **System Diagnosis**, as shown in Figure 3-17.

Figure 3-17 Console-based management — system diagnosis and automatic remediation



This function checks and fixes the hard disk for bad blocks.

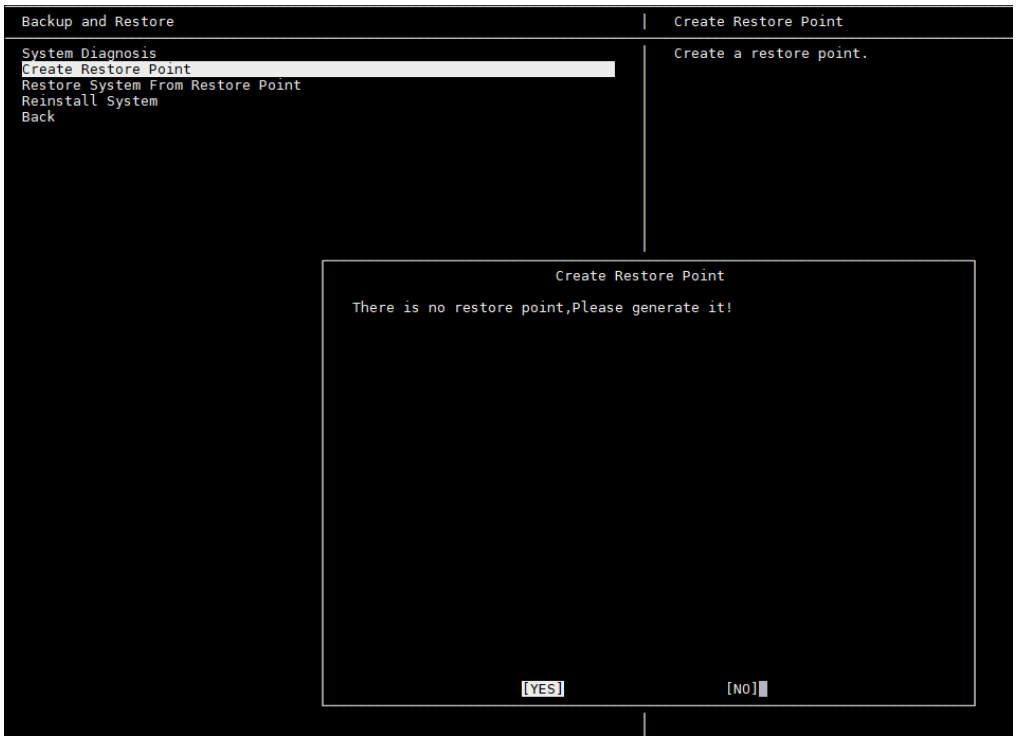
This process takes a long time, during which all services are stopped. After the process is complete, the system restarts automatically.

Creating a Restore Point

A restore point is created for system restoration. A restore point involves the following information: system configuration, asset information, scanning templates, scanning tasks, and user information.

Select **Backup and Restoration** from the main menu and then select **Create a Restore Point** to create a restore point. The administrator can manually create a user restore file.

Figure 3-18 Console-based management — creating a restore point



Note	You can create only one restore point each time.

Restoring the System by Using a Restore Point

From the **Backup and Restoration** menu, you can choose to restore the system using a restore point file. This method only applies to the system of the same version.

Select **Backup and Restore** from the main menu and then select **Restore System From Restore Point**, as shown in Figure 3-19.

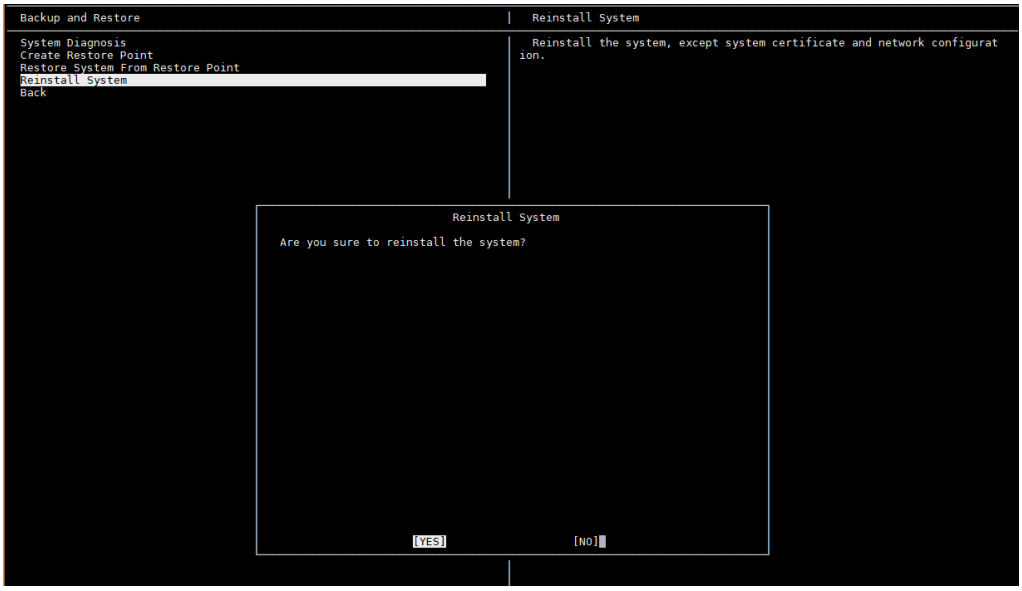
Figure 3-19 Console-based management — restoring the system using a restore point

Reinstalling the System

This function is available only to the RSAS hardware. System reinstallation means restoring the system to the default configuration. Except the network settings, license file, and the number of current scanned IP addresses, all data is restored to factory defaults during the process. This function can be used when RSAS is faulty.

Select **Backup and Restore** from the main menu and then select **Reinstall System**, as shown in Figure 3-20.

Figure 3-20 Console-based management — reinstalling the system



3.1.3.7 System Exiting

After configuring parameters for console-based management, return to the main menu, select **Back**, and then press **Enter**. For further configuration, log in to the system again.

3.2 Initial Configuration

This section describes how to configure RSAS for the first use. Initial configuration steps are different for the hardware edition and virtual edition of RSAS and are described in two separate sections.

3.2.1 Hardware Edition

The management interface can be configured only via console, while scanning interfaces can be configured via console or web-based manager (after a license is imported). Here, the management interface is used as an example to show to configure interfaces.

Prepare a computer, a serial cable, and terminal software for connecting to the console port and set default parameters listed in Default Parameters.

Step 1 Connect the RSAS device to the computer with the serial cable.

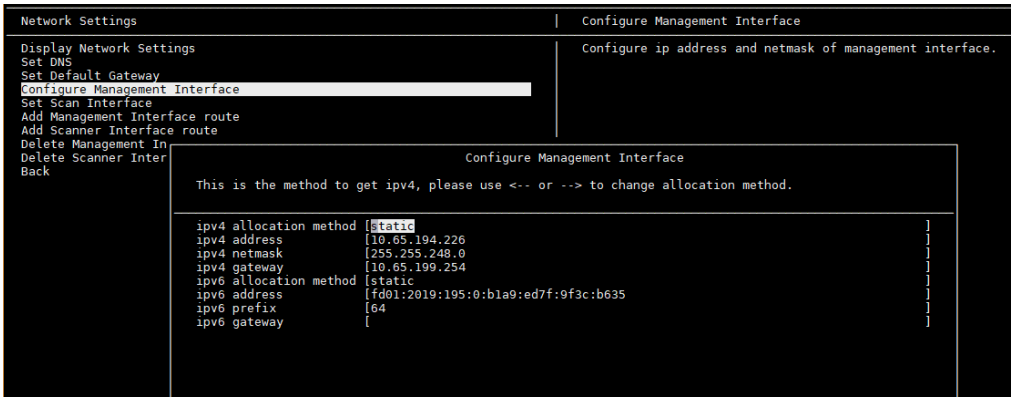
Step 2 Log in to the console.

a. Use terminal software to connect to the RSAS console via a serial port.

b. Type the initial user name and password (see Default Parameters) of the console administrator to open the main menu of the console.

Step 3 Configure the management interface. Choose **Network Settings > Network Settings**, set the IP address and subnet mask of the management interface, and then press **Enter** to commit the settings.

Figure 3-21 Configuring management interface parameters



----End

3.2.2 Virtual Edition

vRSAS can be installed on different virtualization platforms. The method for logging in to the console of vRSAS varies with the virtualization platform. For details, see Installing vRSAS.

Note	For how to import a license, see Importing a License for the Initial Use. You can log in to RSAS after importing a valid license. You must change the initial password after the first login.

3.3 Web-based Management

The web-based manager provides an intuitive human-machine interaction interface for users to manage and configure RSAS.

3.3.1 Supported Browsers

Browser	Version	Remarks
Firefox	Latest	Check whether the option of blocking pop-ups or disabling JavaScript is selected in the browser. If yes, clear the check box. Disable the enhanced protection mode.
Chrome	Latest	
Microsoft Edge	Latest	

3.3.2 Recommended Screen Resolution

The recommended screen resolution is 1280 x 1024 pixels or higher.

3.3.3 Web Login

Before login to the web-based manager, you must have completed Initial Configuration and ensure that RSAS is properly connected to the network.

Open a browser and access the IP address of the management interface via HTTPS by typing, for example, **https://192.168.1.1** in the address bar. After accepting prompted risks, you can view the web login page. Type a correct user name, password, and verification code. Click **Log In**.

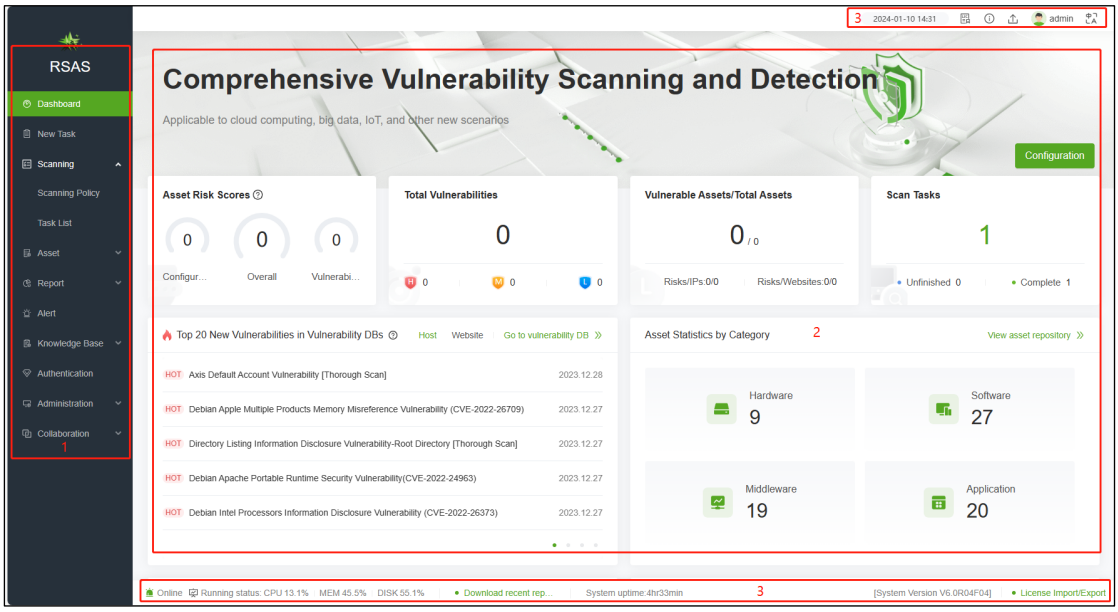
- For the default user name and password, see Default Parameters.
- When logging in for the first time, you need to change the initial password and log in again with the new password.

3.3.4 Page Layout

The page layout for all modules of RSAS is the same, as shown in Figure 3-22.

Note	The menus and work area vary with user roles and data permissions.

Figure 3-22 Page layout



No.	Area	Description
1	Menu bar	Area of function menus from which you can perform further operations.
2	Work area	Area where you can perform configurations and operations and view data.

No.	Area	Description
3	Quick access bar	Area providing the following quick access buttons of the system: • 2024-03-27 13:58 : allows you to view the system time. • / License Import/Export : allows you to import and export a license. • : allows you to query system information or online help. • : allows you to upgrade the system. • admin : allows you to manage the current login account and log out of the system. • : allows you to change the system language. • **Running status**: allows you to view the system running status. • **Download recent reports**: allows you to download reports on the **Report Management** page. • **System uptime**: allows you to view the system uptime. • **Update available**: allows you to immediately upgrade RSAS to the available version on the **System Upgrade** page when there is an upgrade prompt.

3.4 Importing a License for the Initial Use

You must import a correct license before using RSAS. To import a license, follow these steps:

Step 1 Open a browser and access the IP address of the management interface via HTTPS by typing, for example, **https://192.168.1.1**, in the address bar.

Step 2 After accepting prompted risks, you can view the license import page.

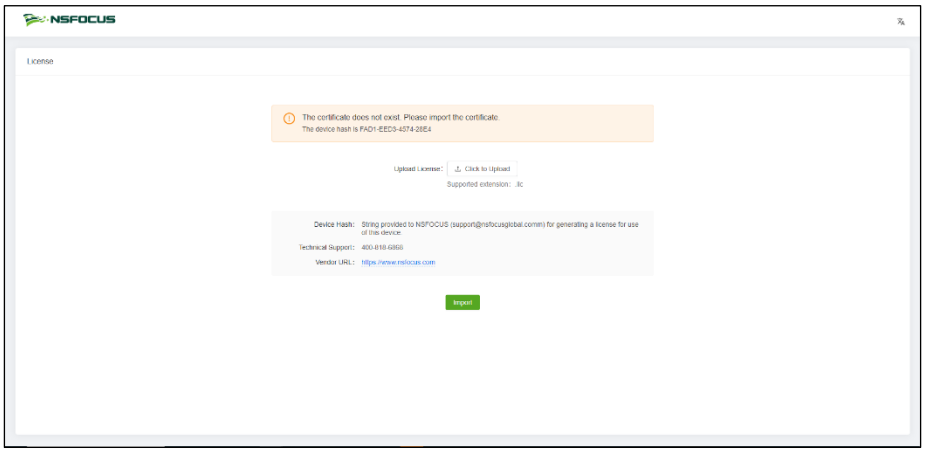
Step 3 Import a license file (.lic) that matches the hash value of RSAS.

----End

3.4.1 Authentication Methods for the Hardware Edition

A hardware RSAS can only be authenticated by importing a local license file that matches the hash value of RSAS shown on the home page of the web-based manager.

Figure 3-23 Importing a license



3.4.2 Authentication Methods for the VM Edition

You can select any of the authentication modes to import a license to a vRSAS device.

3.4.2.1 Dongle Authentication

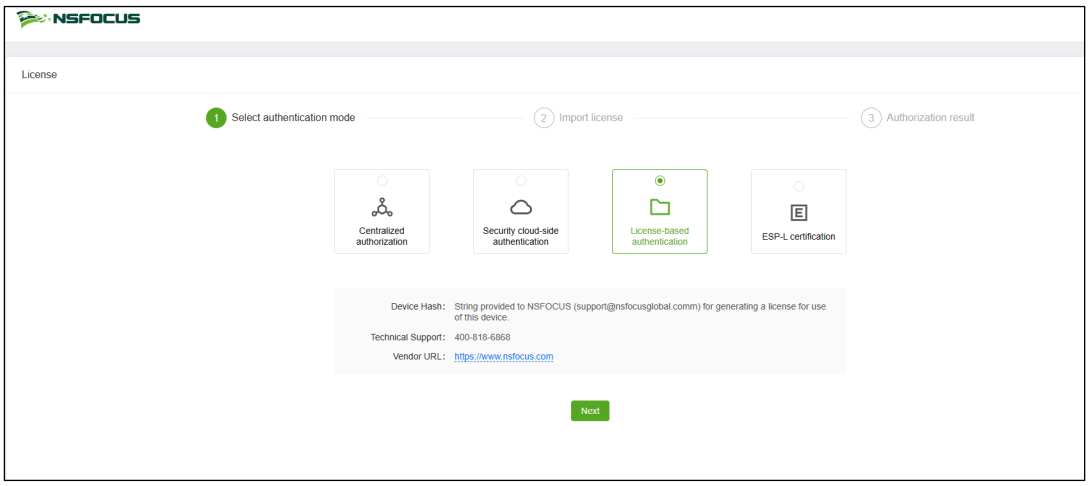
To authenticate vRSAS based on a dongle, follow these steps:

Step 1 Attach the dongle USB device to vRSAS.

Step 2 Open a browser and access the IP address of the management interface via HTTPS by typing, for example, **https://192.168.1.1**, in the address bar. Then accept prompted risks.

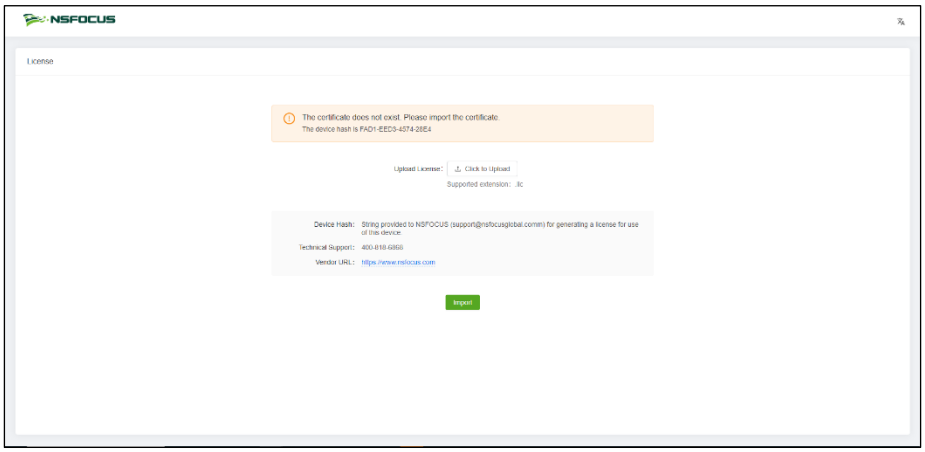
Step 3 Select **License-based authorization** on the page that appears.

Figure 3-24 Authentication method — license



Step 4 Click **Next** and import a license file (.lic) that matches the hash value granted to vRSAS.

Figure 3-25 Importing a local license



----End

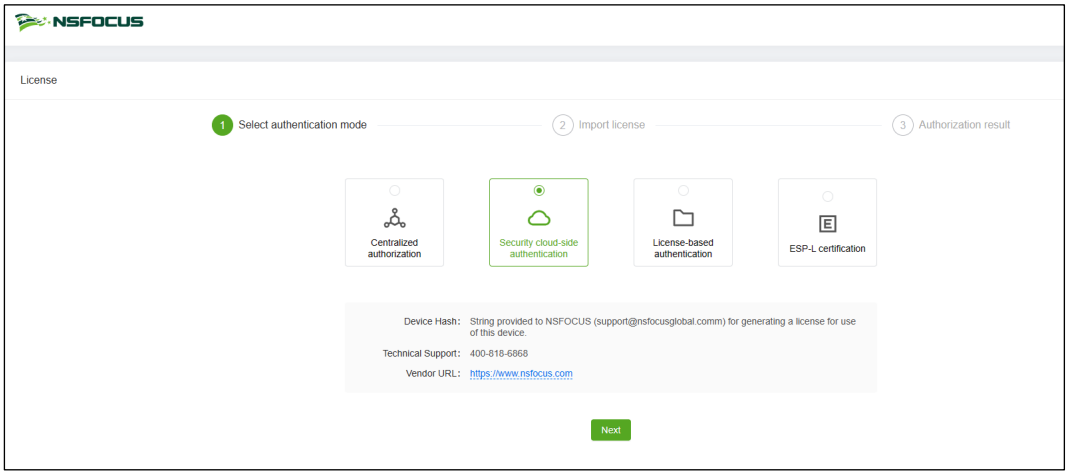
3.4.2.2 Cloud-based Authorization

To authenticate vRSAS by using NSFOCUS security cloud, follow these steps:

Step 1 Open a browser and access the IP address of the management interface via HTTPS by typing, for example, **https://192.168.1.1**, in the address bar. Then accept prompted risks.

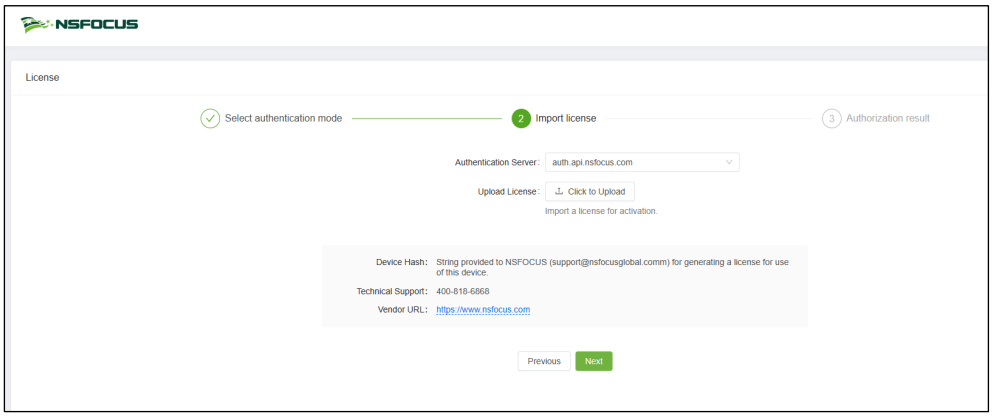
Step 2 Select **Security cloud-side authentication** on the page that appears.

Figure 3-26 Authentication method — NSFOCUS security cloud



Step 3 Click **Next** to select an authentication server and import the prepared license file (.lic).

Figure 3-27 Importing a license for cloud-based authorization



----End

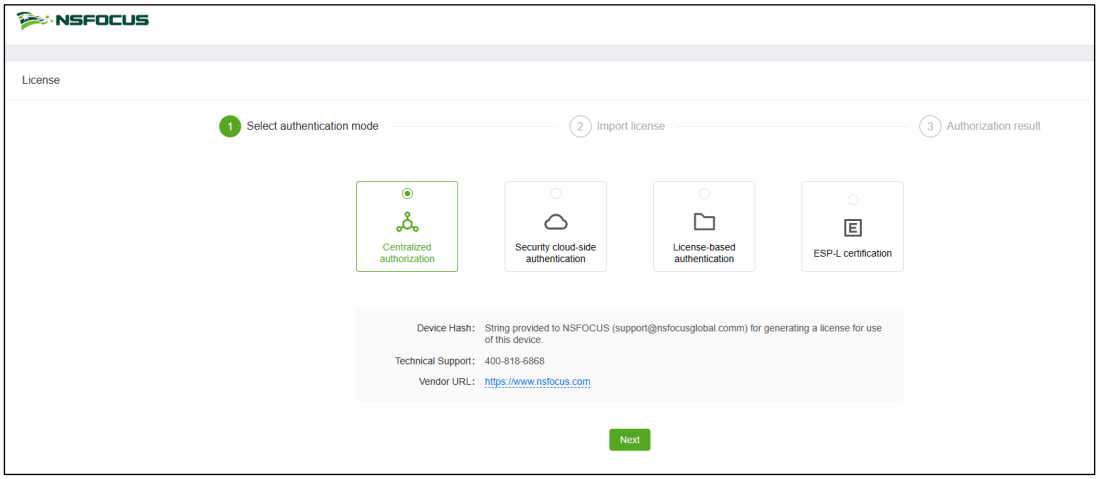
3.4.2.3 Centralized Authorization

To authenticate vRSAS by using a CAA platform, follow these steps:

Step 1 Open a browser and access the IP address of the management interface via HTTPS by typing, for example, https://192.168.1.1, in the address bar. Then, accept prompted risks.

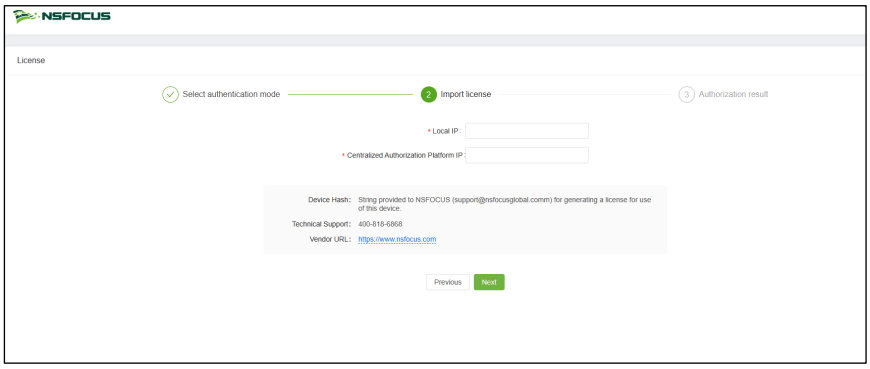
Step 2 Select **Centralized authorization** on the page that appears.

Figure 3-28 Authentication method — CAA platform



Step 3 Click **Next**. Set the IP address respectively for vRSAS and the CAA platform.

Figure 3-29 Configuring an authoritative server for centralized authorization



Step 4 Perform authorization on the CAA management platform.

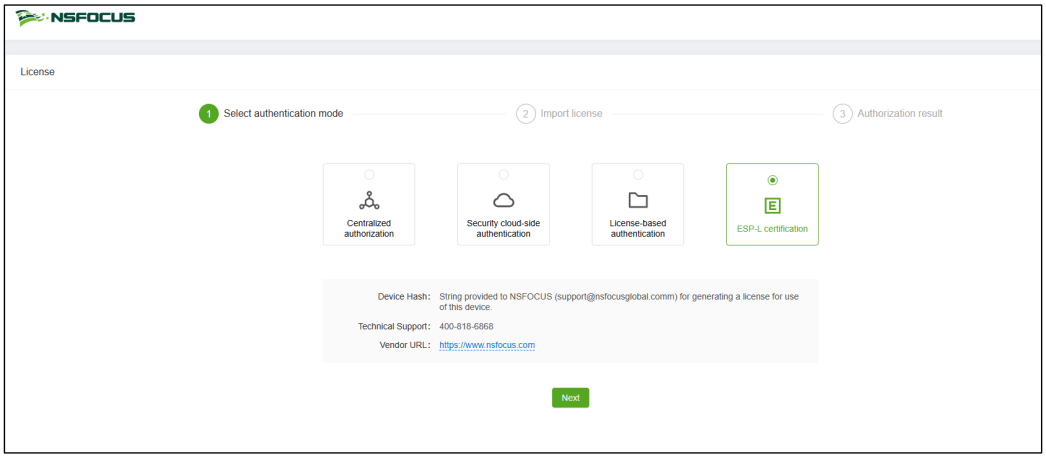
For details, see the respective user guide of the CAA management platform.

----End

3.4.2.4 ESP-L Authorization

Open a browser and access the IP address of the management interface via HTTPS by typing, for example, **https://192.168.1.1**, in the address bar. Then accept prompted risks. Select **ESP-L certification** and click **Next**. Wait until ESP-L issues a license.

Figure 3-30 Authentication method — ESP-L



A Default Parameters

Choose **Administration > Status** > **System Status** to check the factory version and view its factory defaults.

V6.0R02F00 and Later

Default Network Settings

Interface	IP Address	Subnet Mask
Management interface	192.168.1.1	255.255.255.0
Scan interface 1	192.168.2.1	255.255.255.0

Communication Parameters of the Console Port

User Name	Password	Baud Rate	Data Bits
conadmin	conadmin	115200	8

Default User Accounts

Role	User Name	Password
System administrator	admin	admin
Auditor	auditor	auditor

Versions Earlier Than V6.0R02F00

Default Network Settings

Interface	IP Address	Subnet Mask	Gateway IP Address	Negotiation Mode
Scan interface 1	192.168.1.1	255.255.255.0	192.168.1.254	auto
Management interface	1.1.1.1	255.255.255.0	N/A	N/A

Communication Parameters of the Console Port

User Name	Password	Baud Rate	Data Bits
conadmin	nsfocus	115200	8

Default User Accounts

Role	User Name	Password
System administrator	admin	nsfocus
Auditor	auditor	