Sangfor Cyber Command Deployment Guide

Version: **Cyber Command 3.0.50C**

Released On: **2021-4-29**

Sangfor Technologies Inc.

Disclaimer

The products, services or features you purchase shall be subject to the commercial contract and terms of Sangfor. Products, services or features described in this document, whether wholly or in part, may not be purchased or used by you. Unless otherwise provided in the contract, Sangfor disclaims warranties of any kind, either express or implied, for the content of this document.

Due to product deployment or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is only used as a guide, and all statements, information, and suggestions in this document do not constitute any express or implied warranties.

Preface

About This Document

This document introduces how to deploy Cyber Command 3.0.50C.

Product Version

Product	Version
Cyber Command	3.0.50C

This document will be updated when configuration is changed in new versions.

Intended Readers

- Network design engineer
- O&M personnel

Revision History

The revision history includes each document update. The latest document version contains updates from all previous document versions.

Version	Released On	Description
01	2021-4-29	This is the first release of this document.

Technical Support

Email: support@sangfor.com

Official Community: community.sangfor.com

International Service Centre: +60 127-117-129(7511)

Official Website: www.sangfor.com

Feedback

If you have any suggestions or comments for this document, you are welcomed to contact us in the following ways:

- Sangfor Community: https://community.sangfor.com

- Contact local Sangfor office
- After-Sales Support: +60 127-117-129(7511)

Content

1. Overview

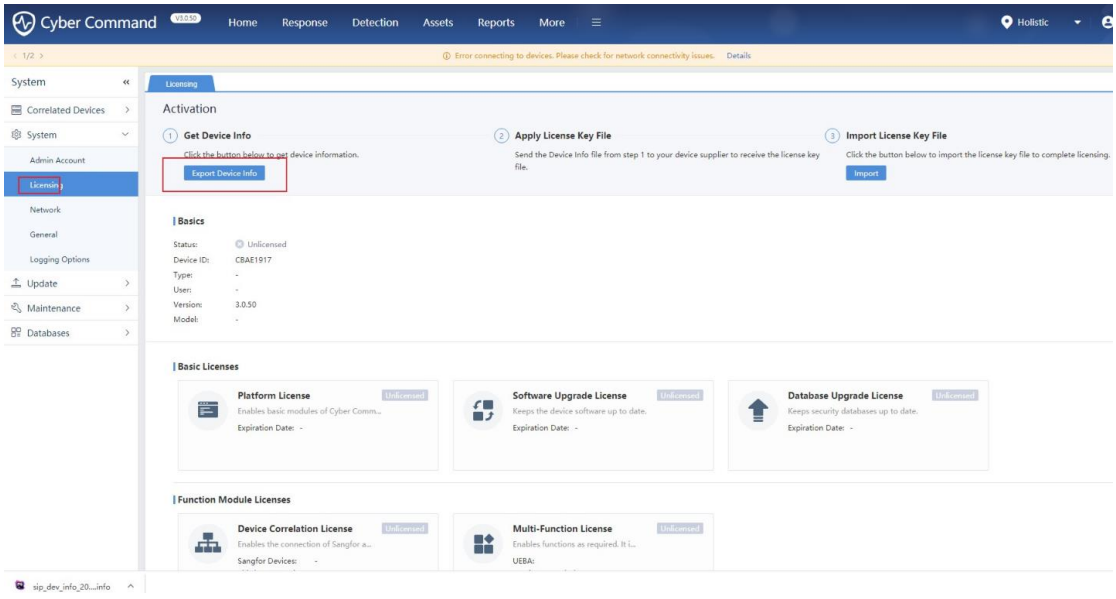
1.1. About This Version

1.1.1. What Is New

●New: The Licensing module is reconstructed.

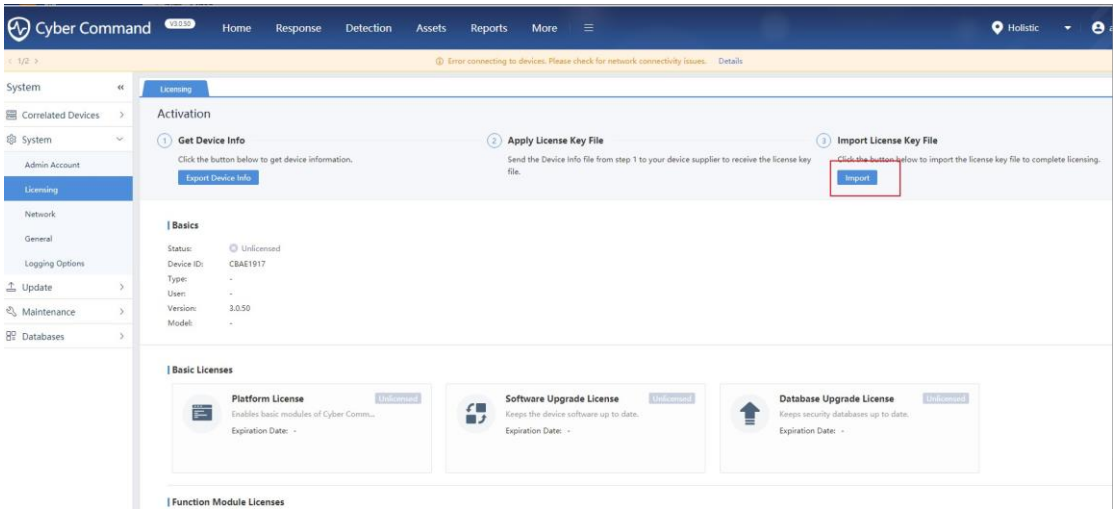
The administrator can export the device inofo and send it to the device supplier to obtain the offline license key file

1. Go to the Licensing module, export and save the device information.



2. Send the device information file to device supplier and you can receive the license file.

3.Go to Licensing module on Cyber Command, and import the obtained license file to get licensed.



●New: This version can be deployed on VMware ESXi.

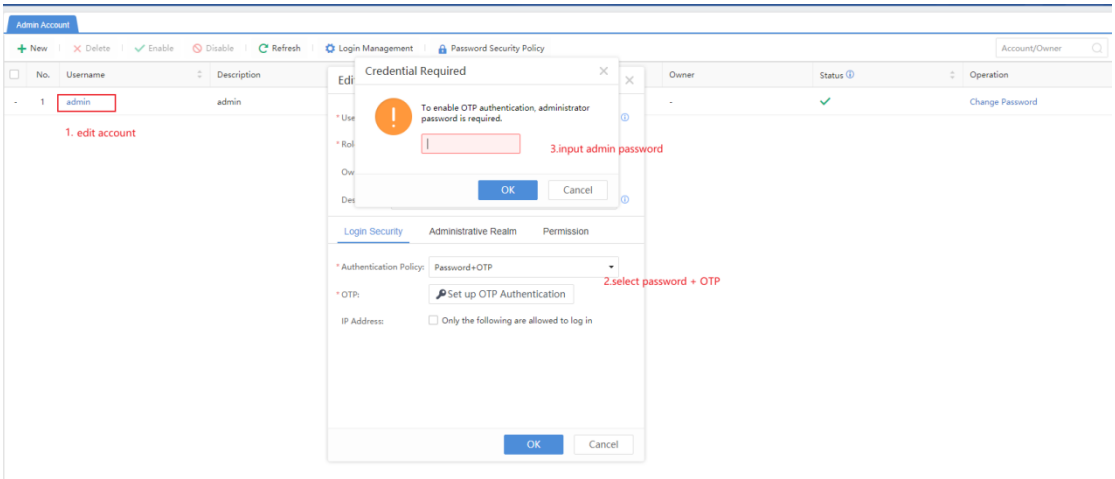
This version can be deployed on VMware EXSi by using Cyber Command 3.0.50C iso file.

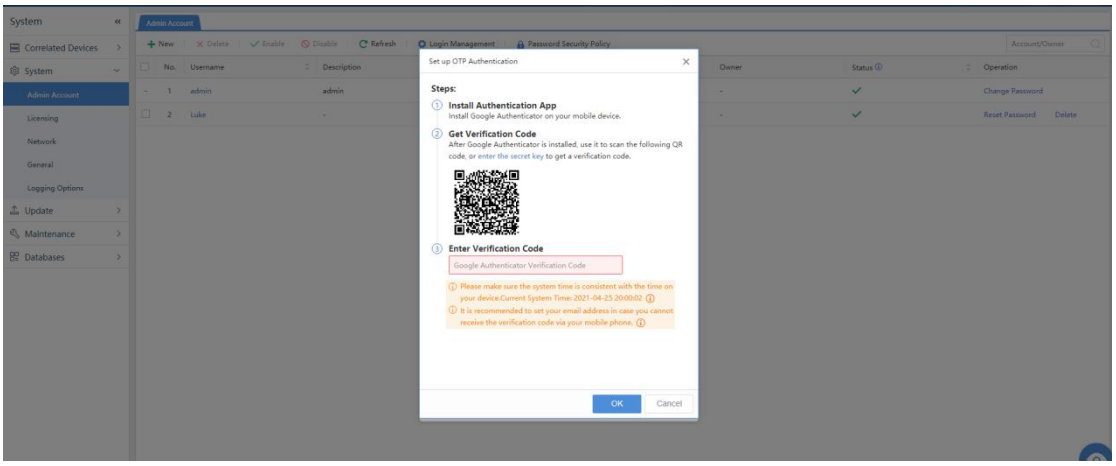
●New: Two-factor authentication

When logging in, users not only need to enter their password and CAPTCHA, but also need to verify OTP.

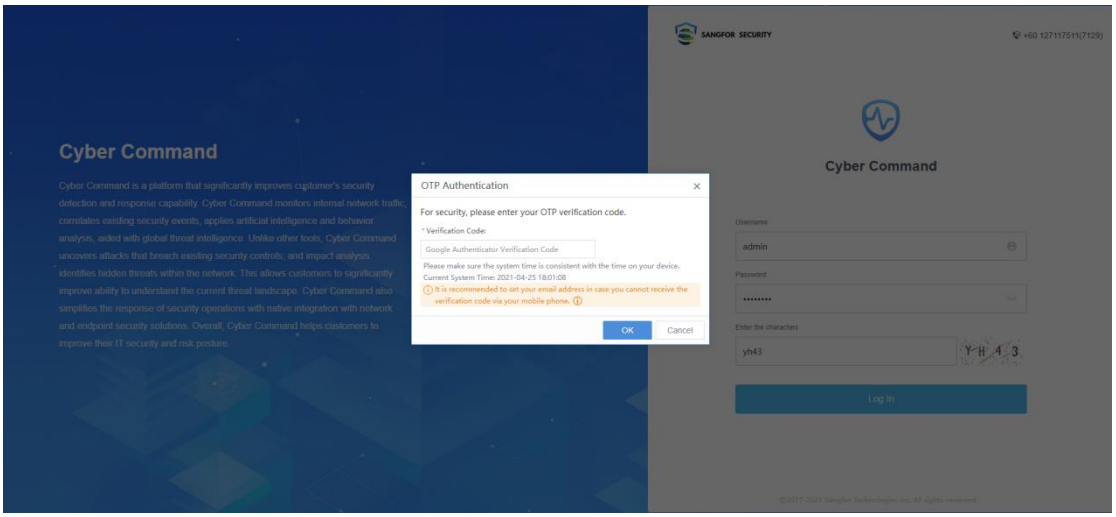
1.To set up OTP for the super admin, go to **System** > **Admin Account**, and edit the admin account.

Then, choose "Password+OTP" as the authentication policy, enter the administrator password and set up OTP authentication.



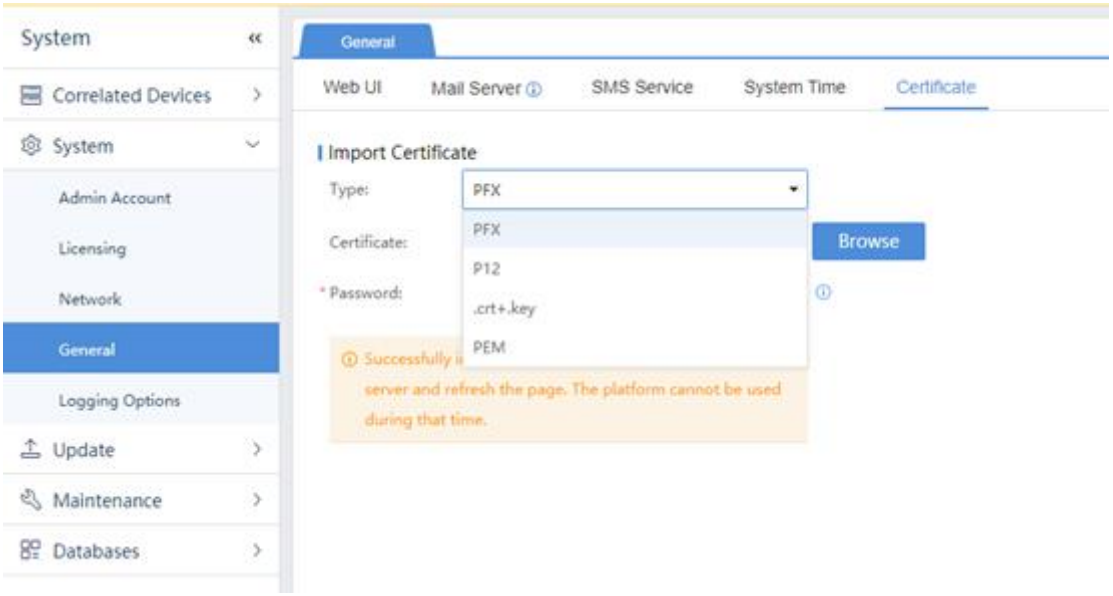


1. When logging in, a super admin not only needs to enter the password and CAPTCHA, but also needs to verify OTP generated by Google Authenticator.



●New: Import certificate

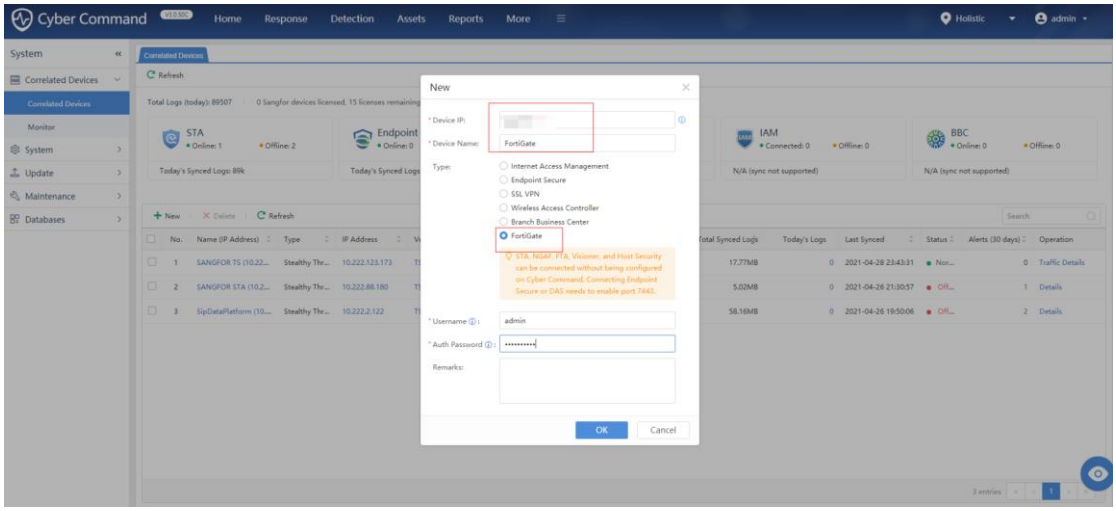
Import a certificate to solve loss and theft of the data transmitted by the browser.



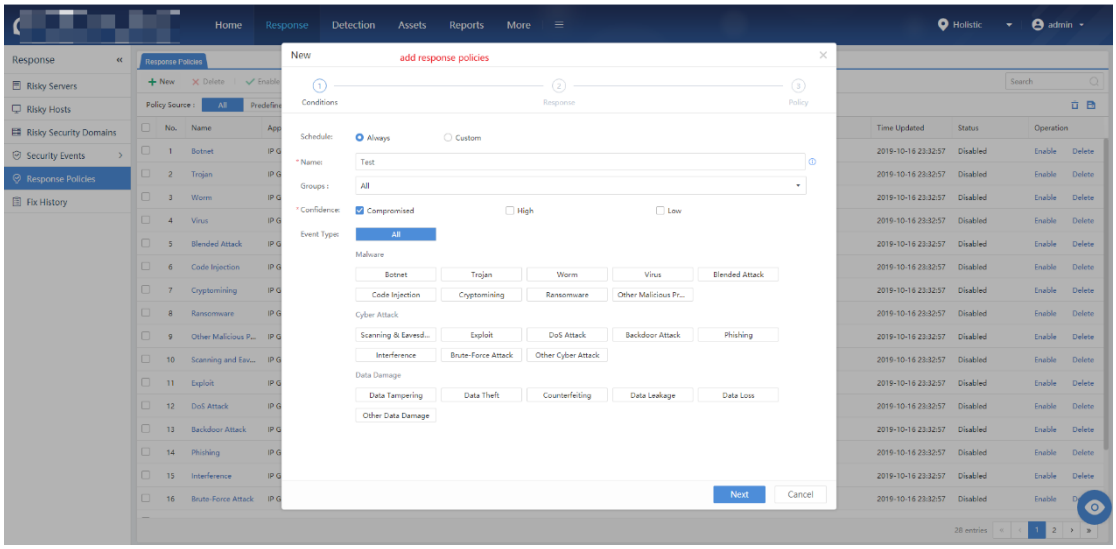
●New: Connect FortiGate

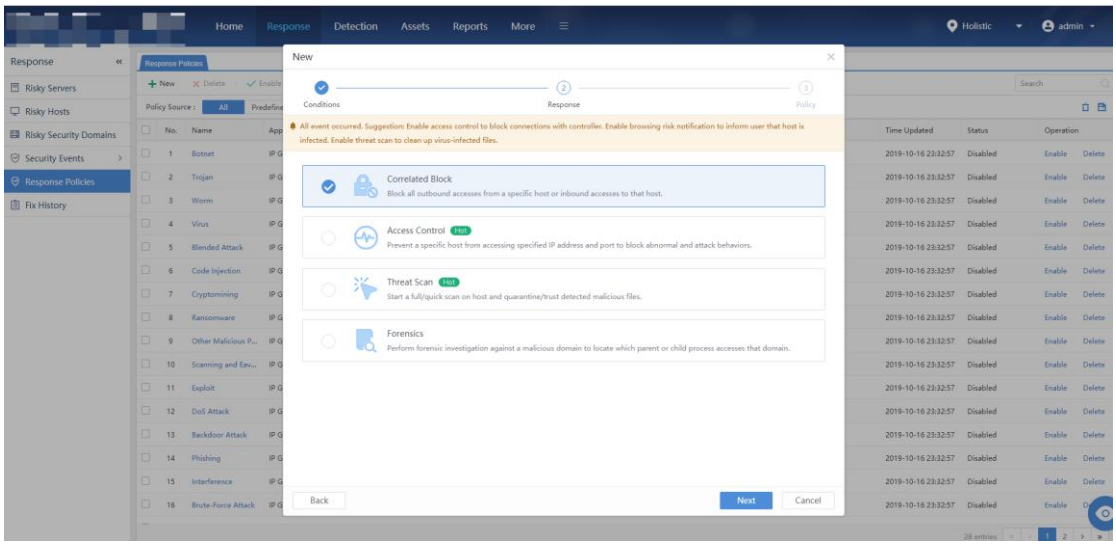
Block access from risky IP addresses for more security.

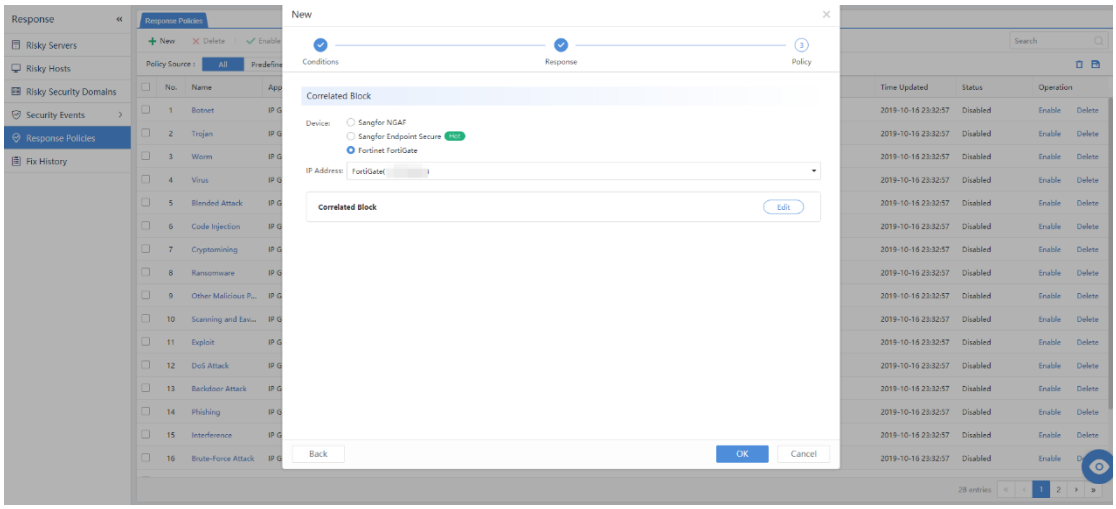
1. Go to the Correlated Devices page and add a FortiGate device.

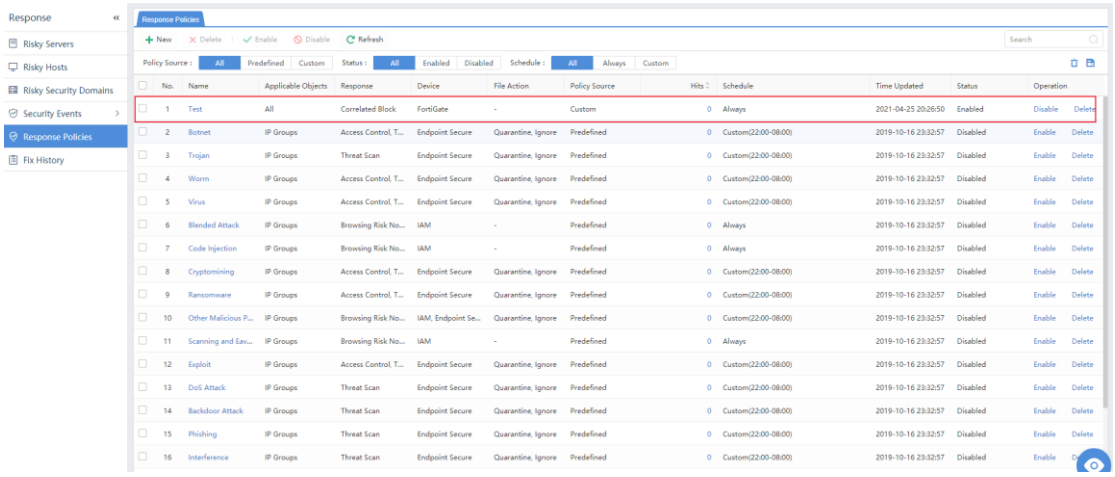


2. Go to the Response page and set response policies

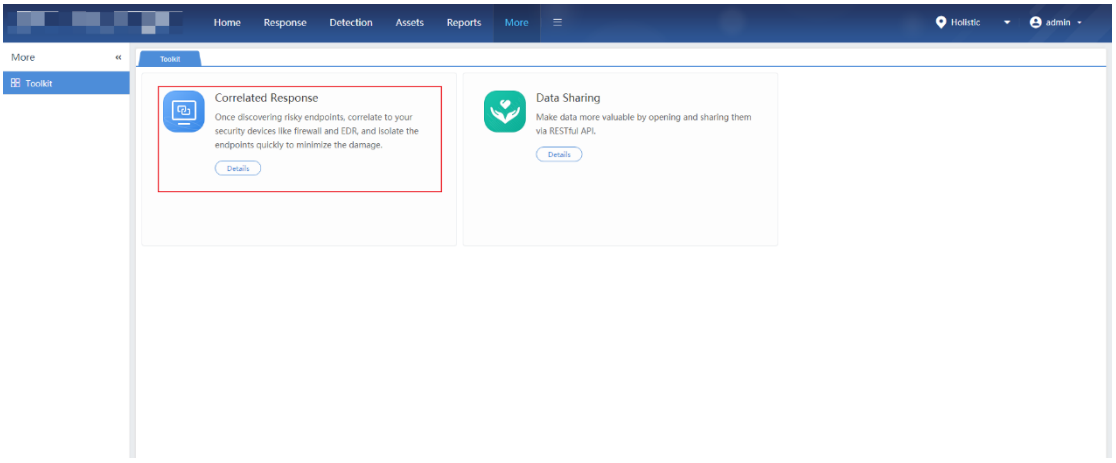

Home
Response
Detection
Assets
Reports
More
Holistic
admin
Response
Risky Servers
Risky Hosts
Risky Security Domains
Security Events
Response Policies
Fix History
New
add response policies
Conditions
Response
Policy
Schedule:
Always
Custom
Name:
Test
Groups :
All
Confidence:
Compromised
High
Low
Event Type:
All
Malware
Botnet
Trojan
Worm
Virus
Blended Attack
Code Injection
Cryptomining
Ransomware
Other Malicious Pr...
Cyber Attack
Scanning & Eavesd...
Exploit
DoS Attack
Backdoor Attack
Phishing
Interference
Brute-Force Attack
Other Cyber Attack
Data Damage
Data Tampering
Data Theft
Counterfeiting
Data Leakage
Data Loss
Other Data Damage
Next
Cancel

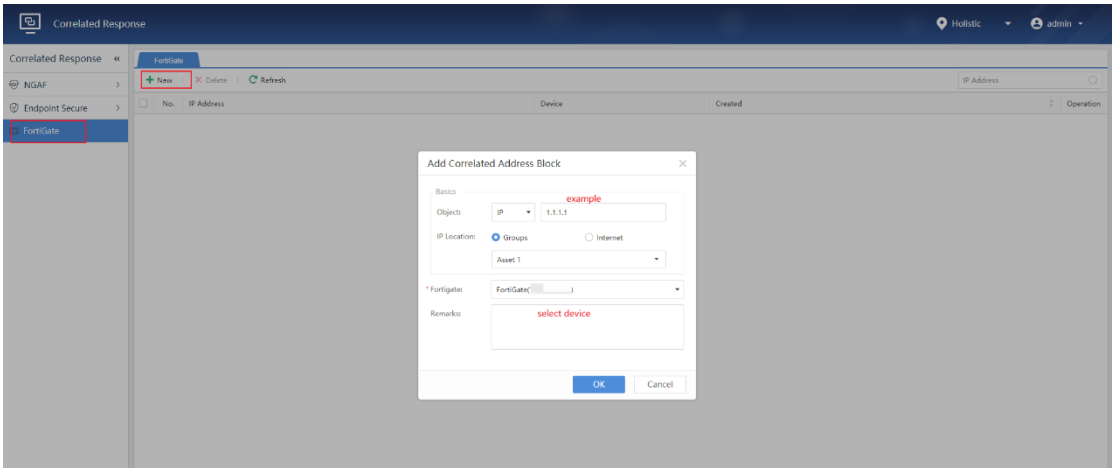

Home
Response
Detection
Assets
Reports
More
Holistic
admin
Response
Risky Servers
Risky Hosts
Risky Security Domains
Security Events
Response Policies
Fix History
New
Conditions
Response
Policy
Correlated Block
Block all outbound accesses from a specific host or inbound accesses to that host.
Access Control
Prevent a specific host from accessing specified IP address and port to block abnormal and attack behaviors.
Threat Scan
Start a full/quick scan on host and quarantine/trust detected malicious files.
Forensics
Perform forensic investigation against a malicious domain to locate which parent or child process accesses that domain.
Back
Next
Cancel

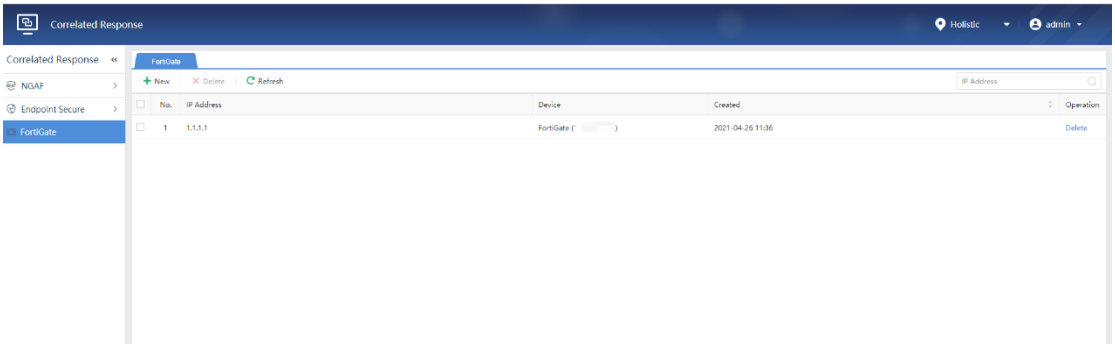

Response
Risky Servers
Risky Hosts
Risky Security Domains
Security Events
Response Policies
Fix History
New
Conditions
Response
Policy
Correlated Block
Device:
Sangfor NGAF
Sangfor Endpoint Secure
Fortinet FortiGate
IP Address:
Correlated Block
Edit
Back
OK
Cancel



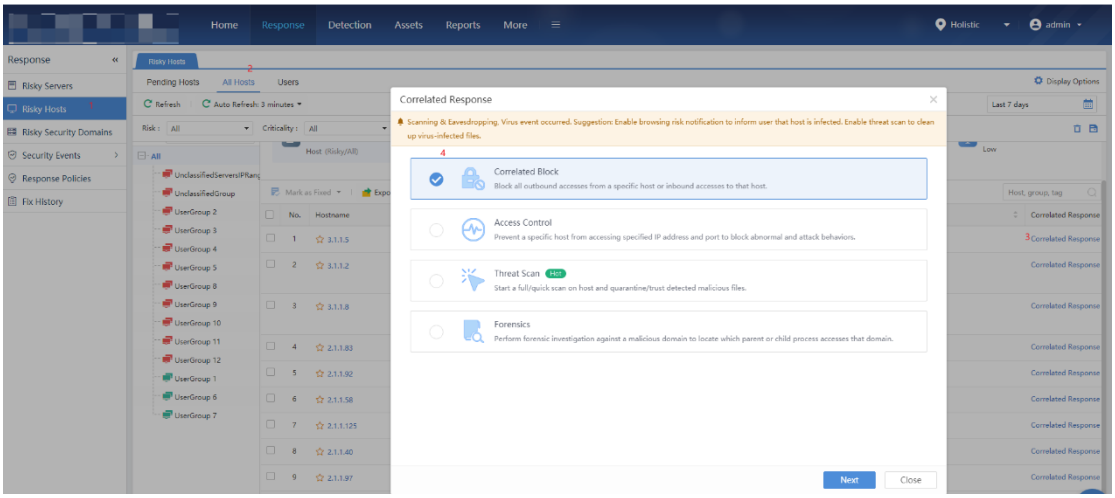
3. More > Toolkit > Correlated Response

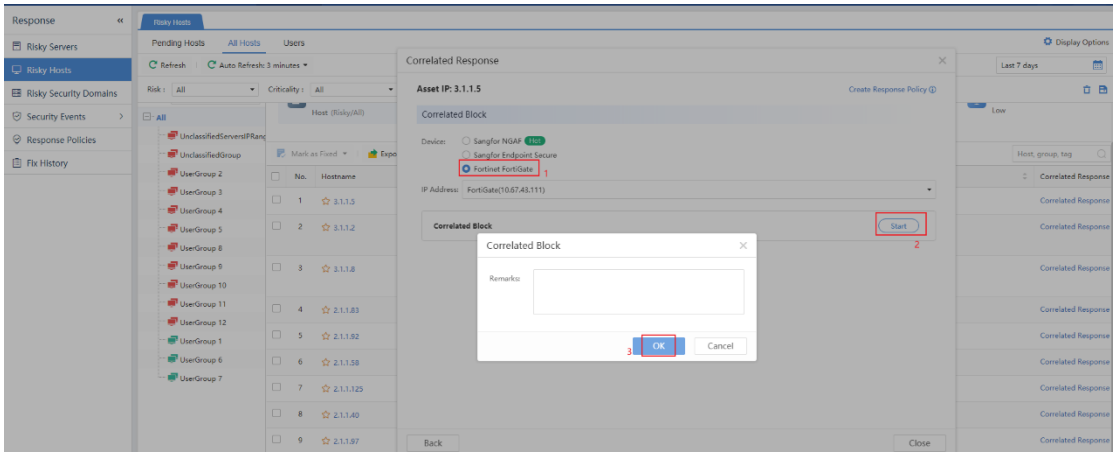


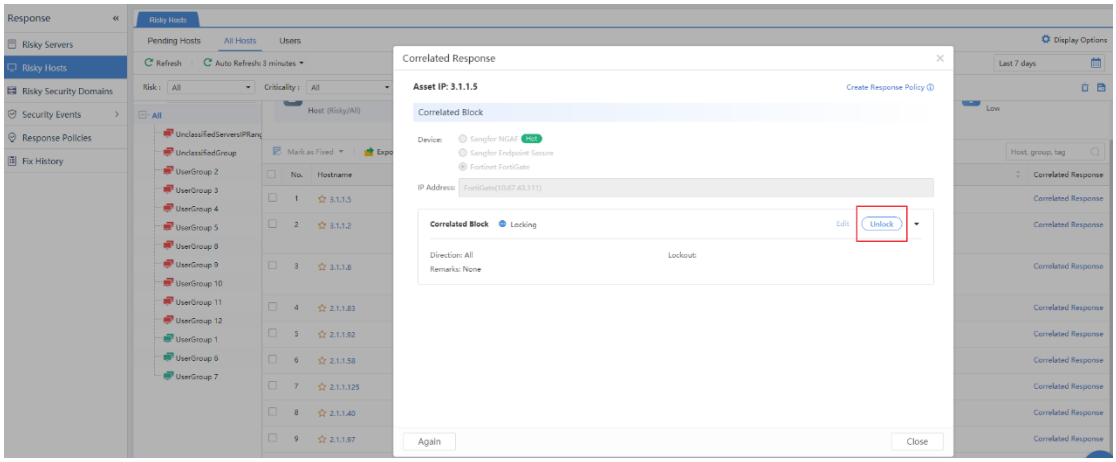




4. Enable or disable correlated response based on security events.







1.1.2. Others

None

1.1.3. Connection with Third-Party Products

Third-party products can be connected with APIs.

1.2. Deployment Impacts

The installation may take 1.5 hours.

1.2.1. Impacts on Business

None

1.2.2. Impacts on O&M

ISO installation may take 1.5 hours.

1.2.3. Impacts on Network

Deployment in bypass mode will have no impacts on network.

1.2.4. Others

None

1.3. Deployment Preparation Related to Customers

1.3.1. Resources Required for Deployment

1. You need to access to the VMware cloud environment of the customer and be familiar with the customer's network configuration.

2. Uploading the image to the cloud platform may take 50 minutes, and the entire deployment may take 1.5 hours.

3. The deployment environment should have enough resources and space (at least 8C32G+128G+4T).

1.3.2. Deployment Notification

1. The English version of 3.0.50C image can only be deployed in VMware virtual environment and cannot be deployed with physical hardware.

2. Deployment of 3.0.50C English version is only compatible with VMware ESXI5.0 \VMware ESXI 6.0\VMware ESXI 7.0

3. The following cpu models are measured: (Include but not limited): 48 CPUs x Intel(R) Xeon(R) Gold 5220R CPU @ 2.20GHz
28 CPUs x Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.40GHz
44 CPUs x Intel(R) Xeon(R) CPU E5-2699 v4 @ 2.20GHz
20 CPUs x Intel(R) Xeon(R) Silver 4210 CPU @ 2.20GHz

4. The English version of 3.0.50C can only support the following configuration:

		Configuration

Scenario	*Supported*	*Memory*	*CPU*	*Disk*	*NICs*
Virtual Environment Deployment					
VMware ESXi 5.0.0/6.0.0/7.0.0	Yes	32G	8 cores	System: 128G Data: 4T	*4*
	Yes	96G	32 cores	System: 128G Data: 4T	*4*
	Yes	128G	40 cores	System: 128G Data: 4T	*4*
	Yes	256G	40cores	System: 128G Data: 4T	*4*
Physical Hardware Deployment	*No*				

1.4. Deployment Process

- Prepare the ISO image of Cyber Command 3.0.50C.
- Import the image, configure environment and start auto installation. This may take 1.5 hours.

1.5. Business Verification After Deployment

1. Check whether you can log in normally without errors displayed.
2. If STA is connected, go to Logs page to check whether new logs are generated constantly.
3. Check as required whether customer business is normal.

1.6. Rollback

None

2. Deployment Instruction

2.1. Preparation Before Deployment

2.1.1. Deployment Tools

Prepare the ISO image of Cyber Command 3.0.50C.

2.1.2. Deployment Environment

None

2.1.3. Customer Resources

Refer to the chapter *Deployment Preparation Related to Customers*.

2.2. Confirmation Before Deployment

Refer to the chapter *Deployment Impacts*.

2.3. Deployment Procedure

2.3.1. Deployment Procedure

1. **Cyber Command 3.0.50C Deployment**

Step 1: Get the ISO image of 3.0.50C and import it to the customer's VMware cloud environment.

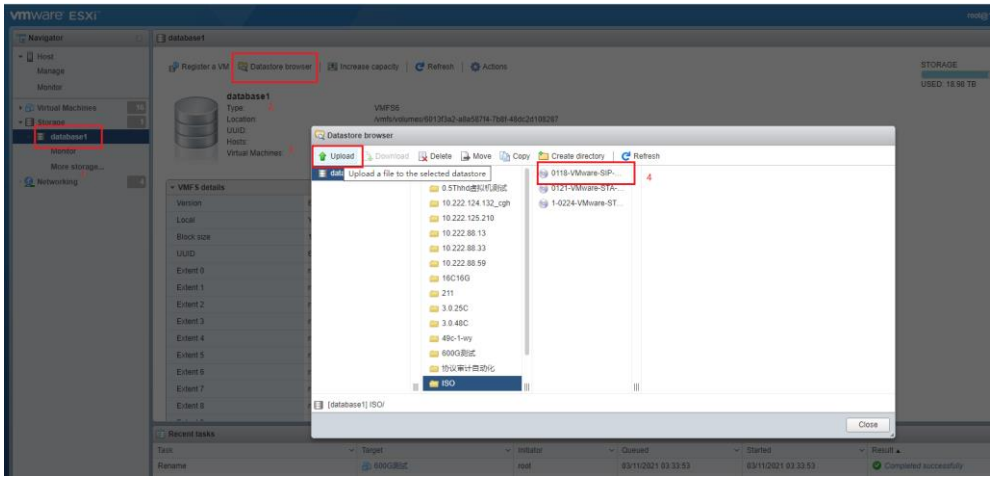
Step 2: Configure the virtual machine. Select ISO image of 3.0.50C for the virtual CD/DVD drive.

Step 3: Power on the virtual machine and select automatic installation

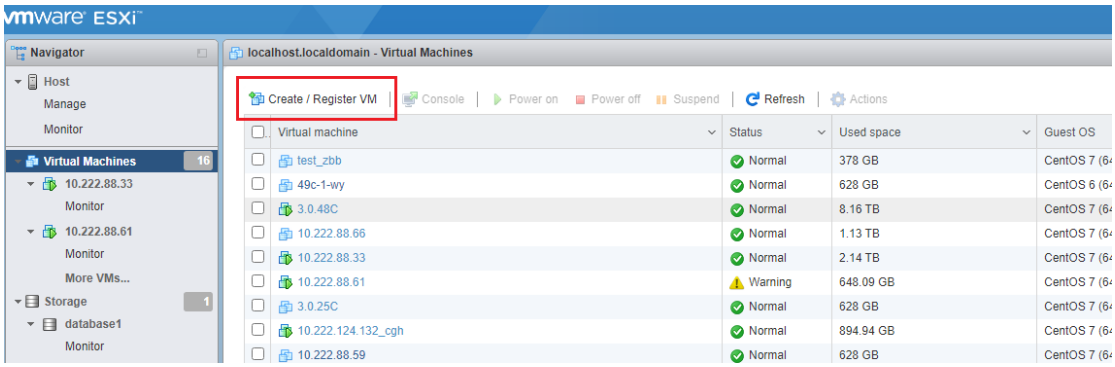
Step 4: Wait for the system to install automatically.

2. VMware esxi Deployment

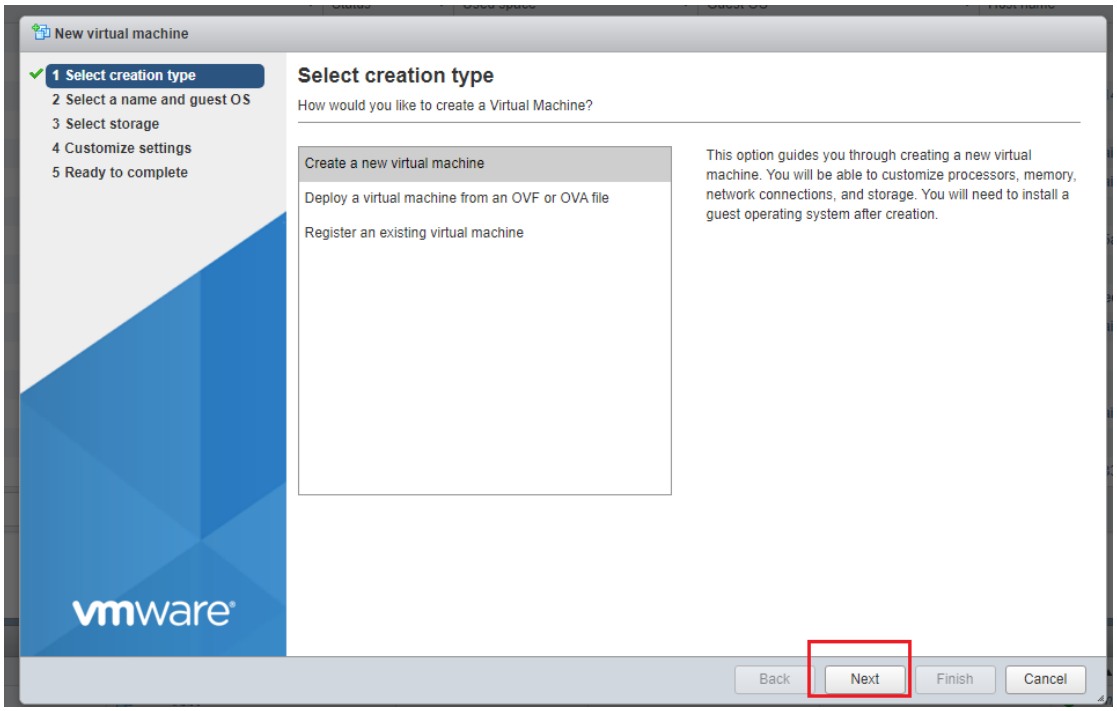
1.1 Upload the obtained image to VMware, which may take about 50 minutes.



1.2 Create a new virtual machine.

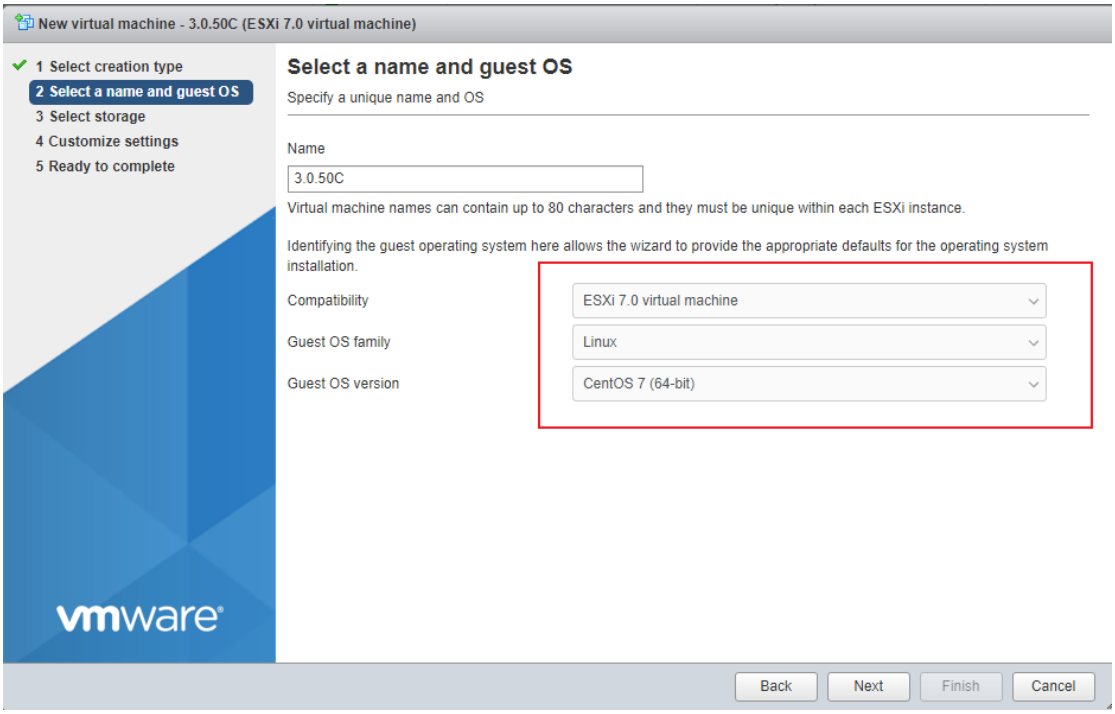


Select the option of creating a new virtual machine.

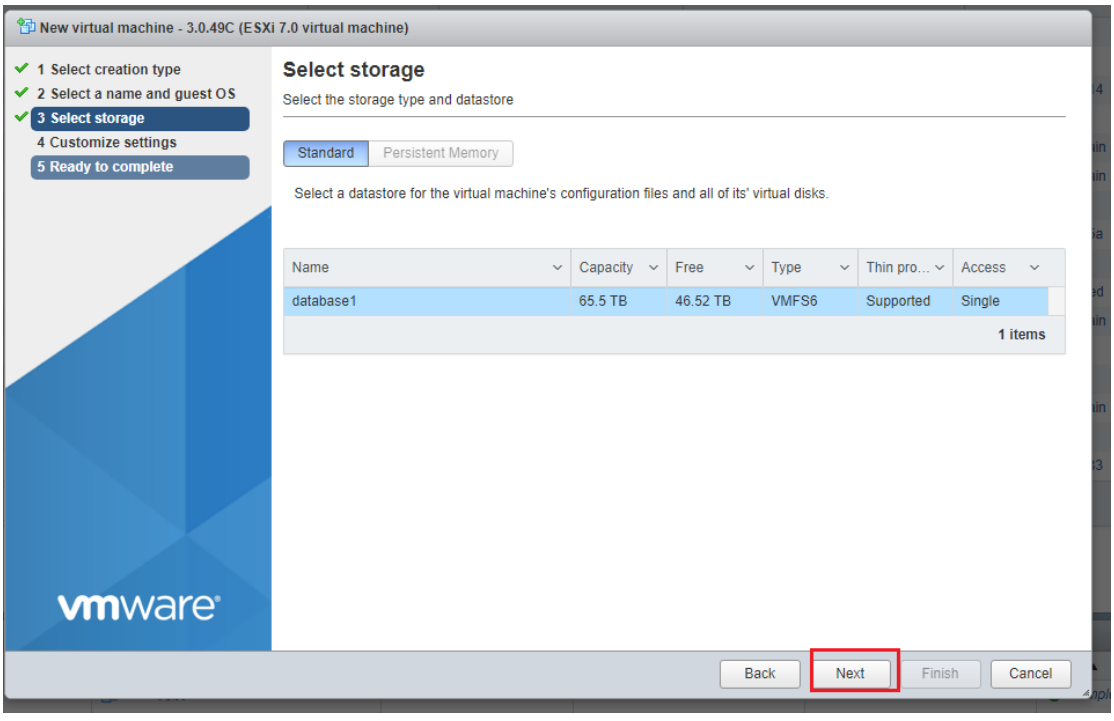


Select VMware EXSi 7.0 (you can also select VMware EXSi 5.0 or VMware EXSi 6.0).

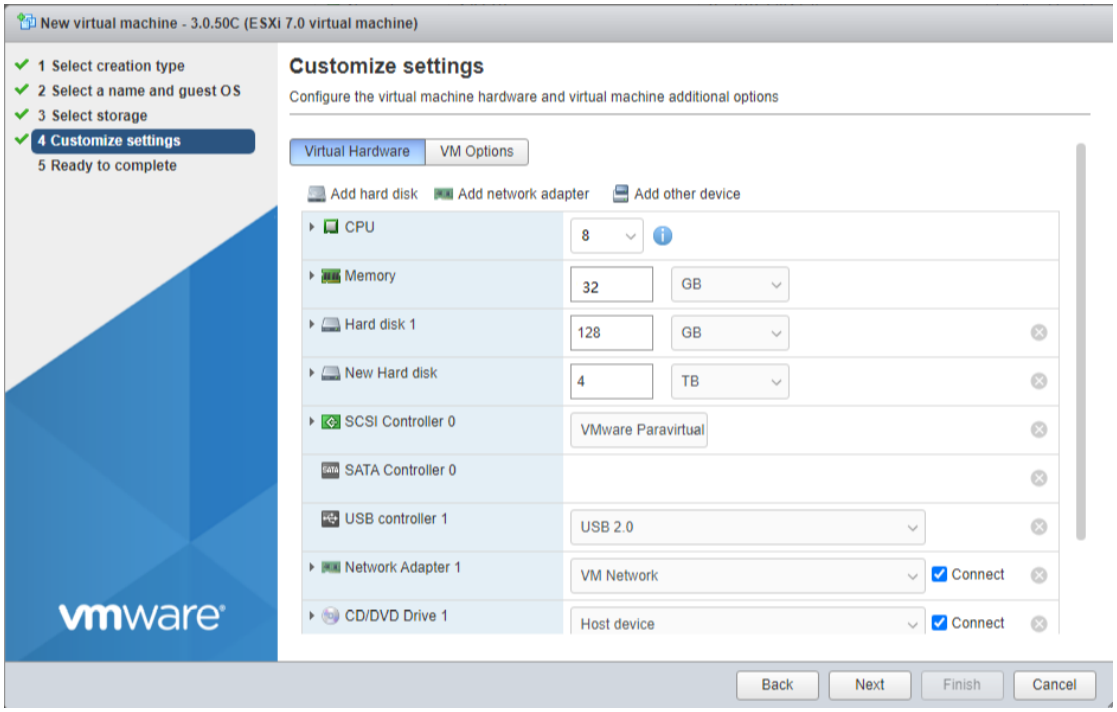
Select Linux OS and CentOS 7 (64-bit) version as below.



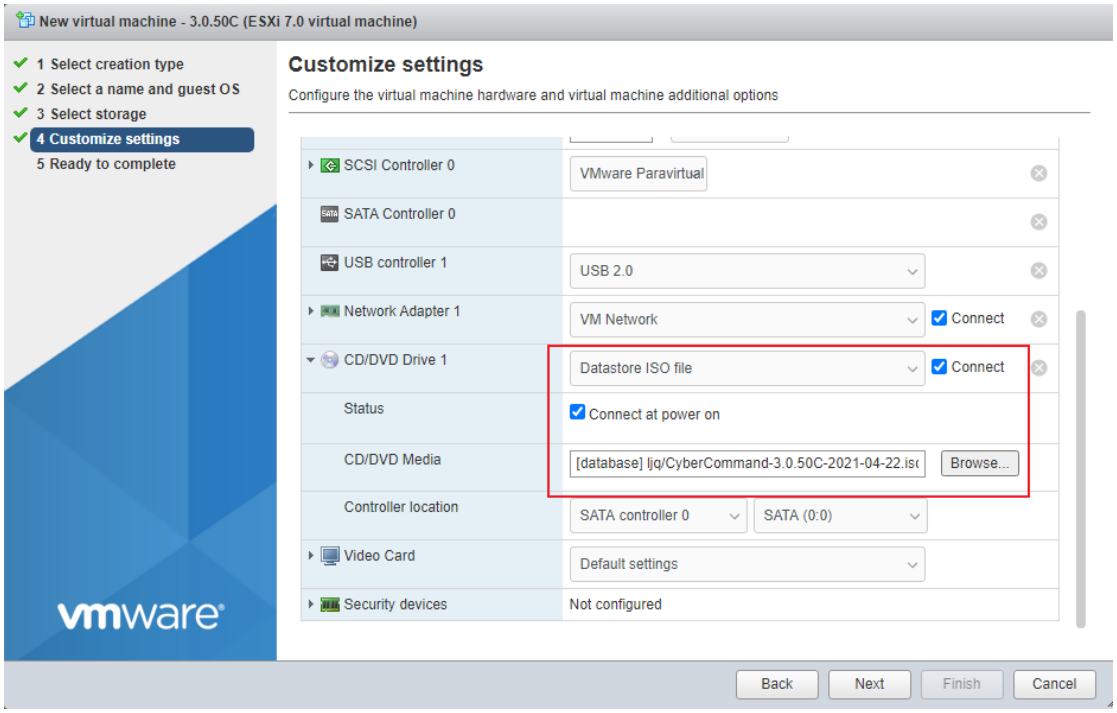
Select storage, ensuring that the environment have enough space. Then, click Next.



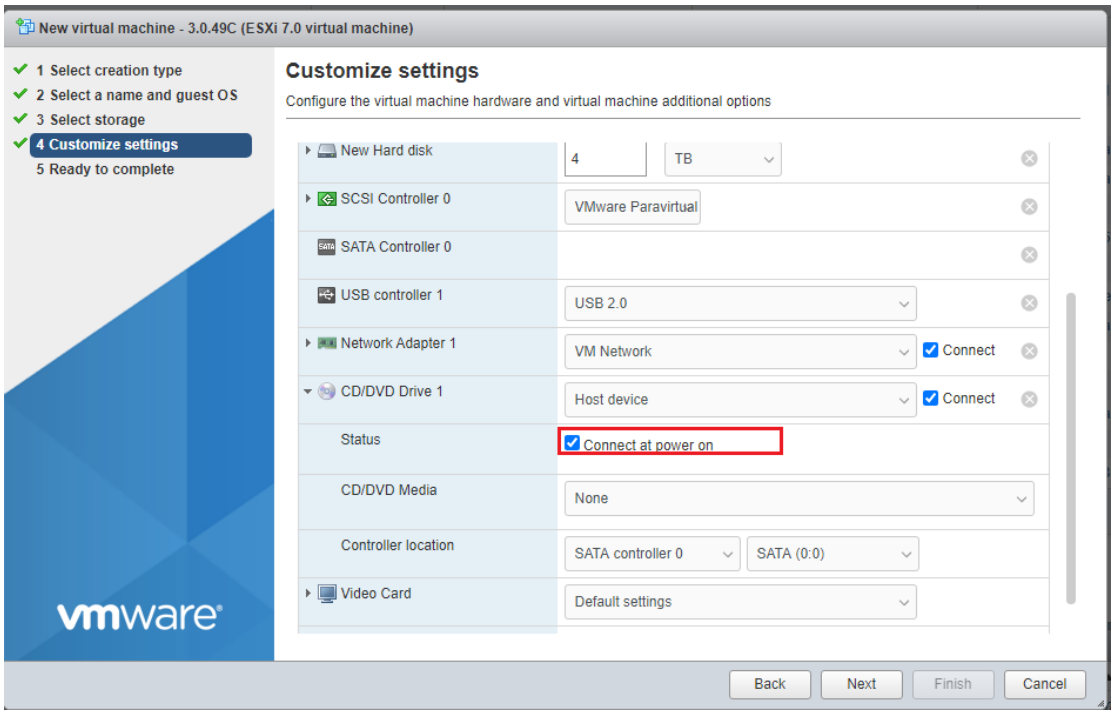
Configure the virtual machine as following: 8-core CPU, 32G memory, 128 GB system disk, and 4 TB data disk. Version 3.0.50C supports 1 to 4 NICs.



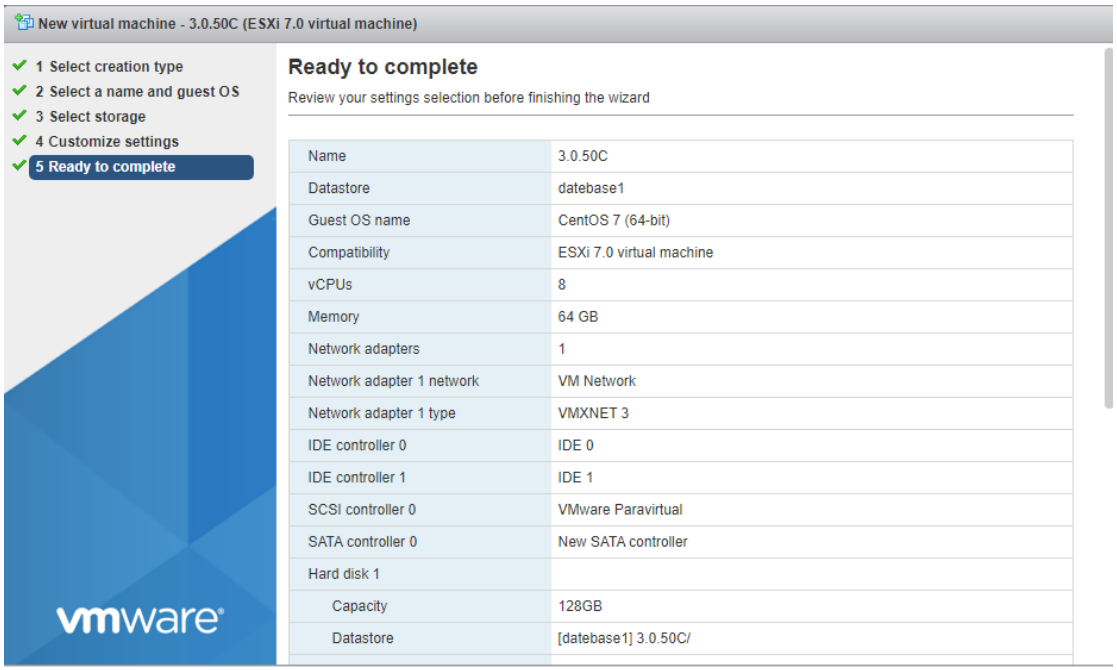
Select an image to be added to virtual CD/DVD drive.



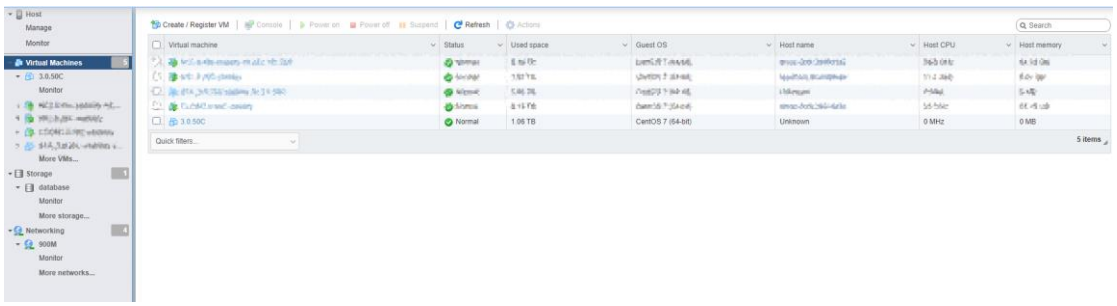
Select the option to connect at power on.



Click to finish the creation.

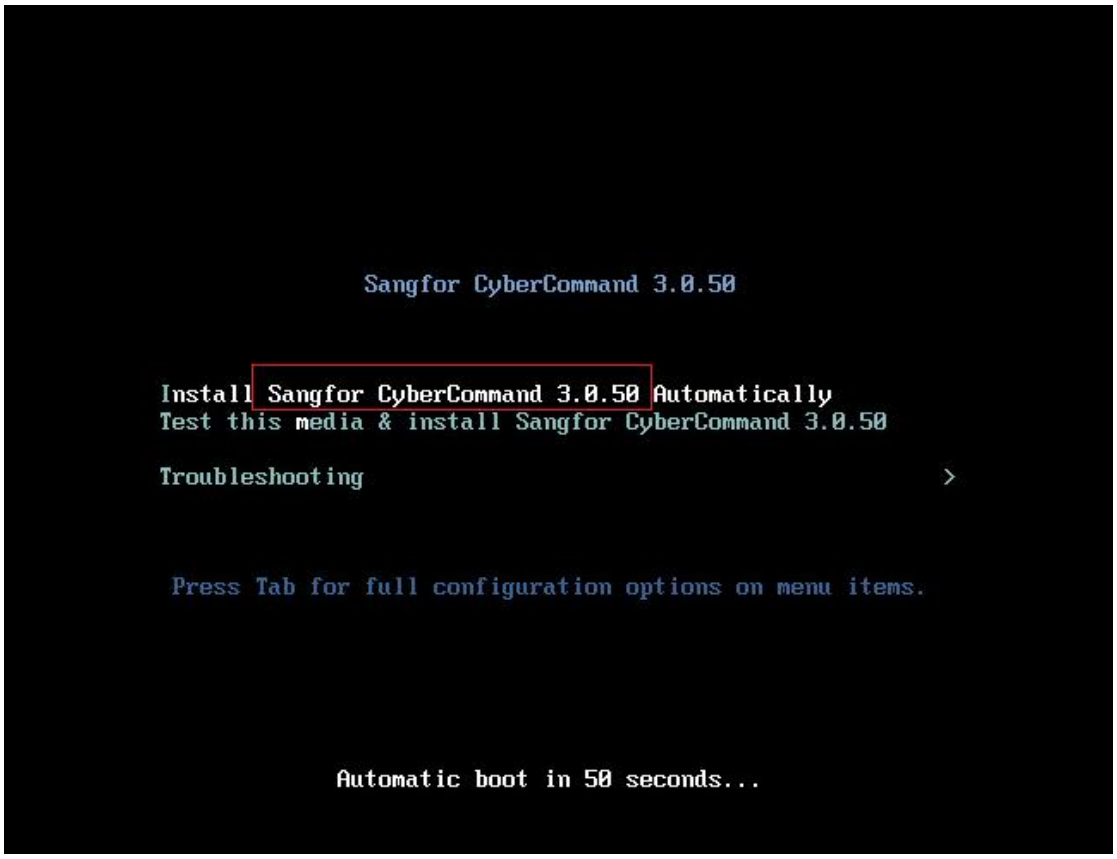


Select the created virtual machine.

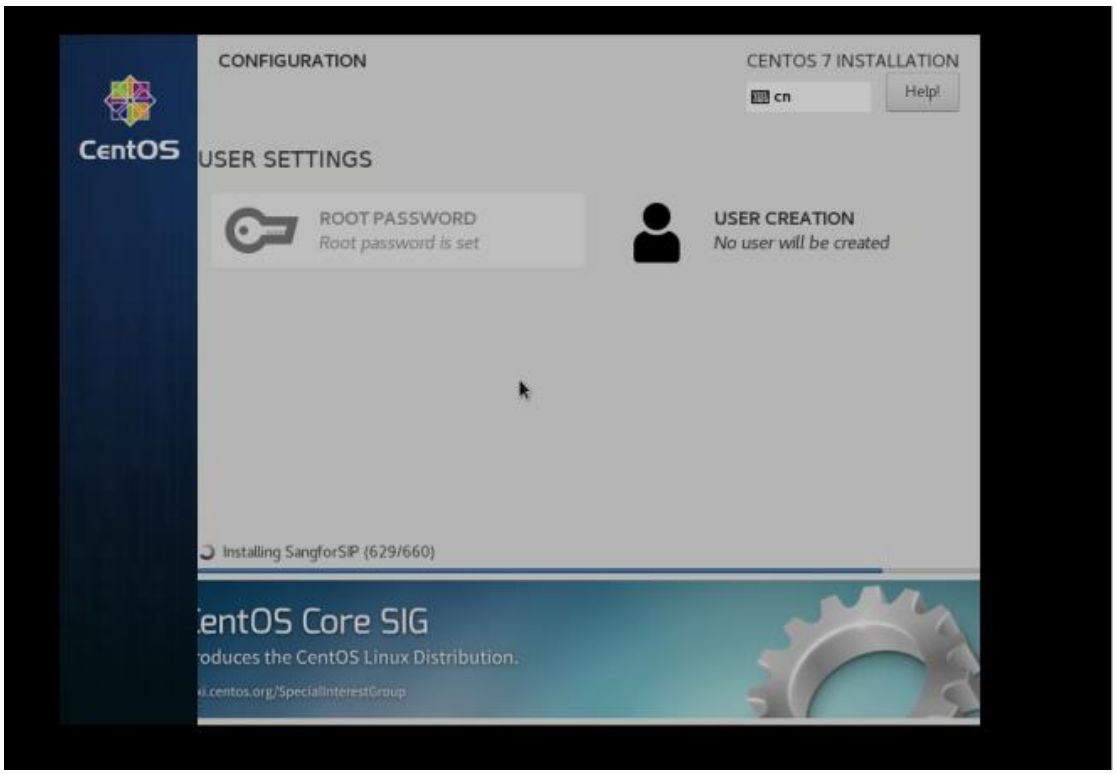


Click the button to power on the created virtual machine.

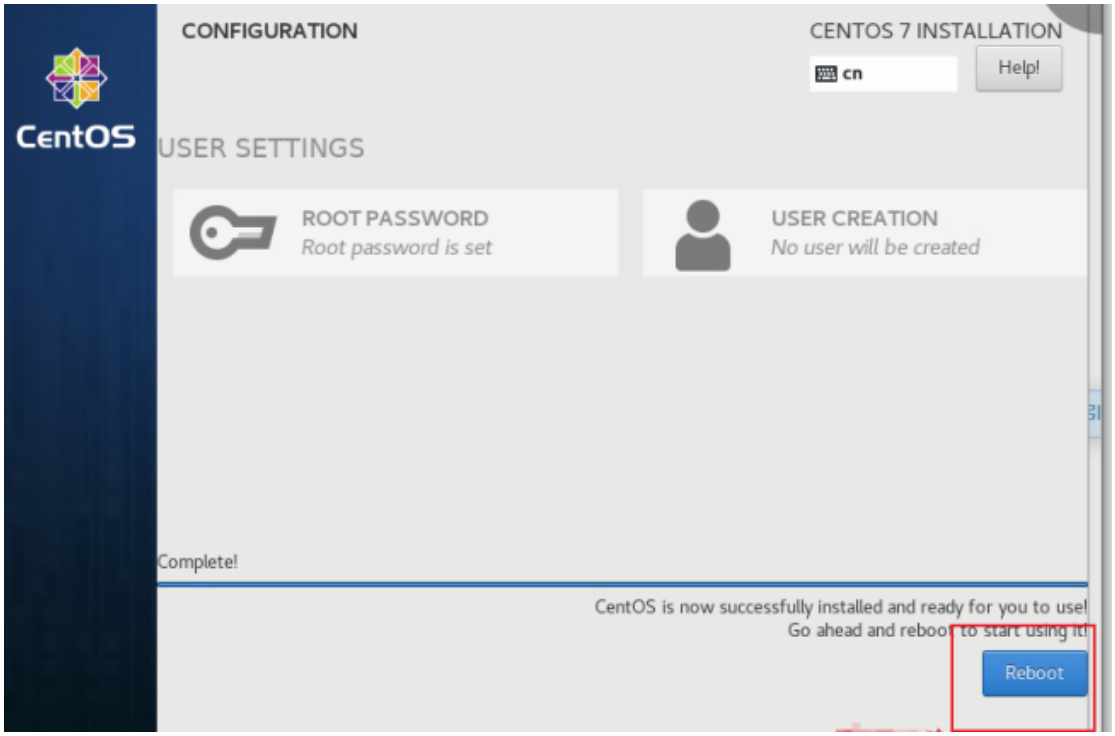
You will go to the installation page. Press Enter to select automatic installation

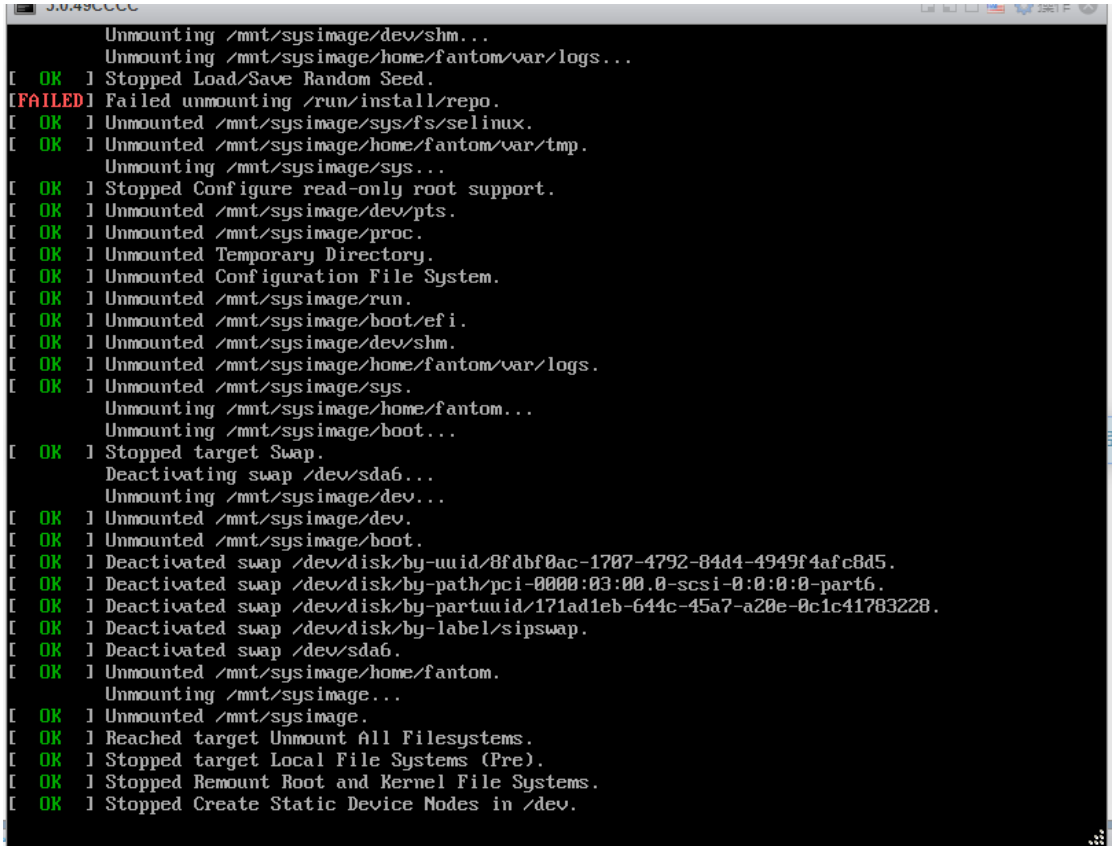


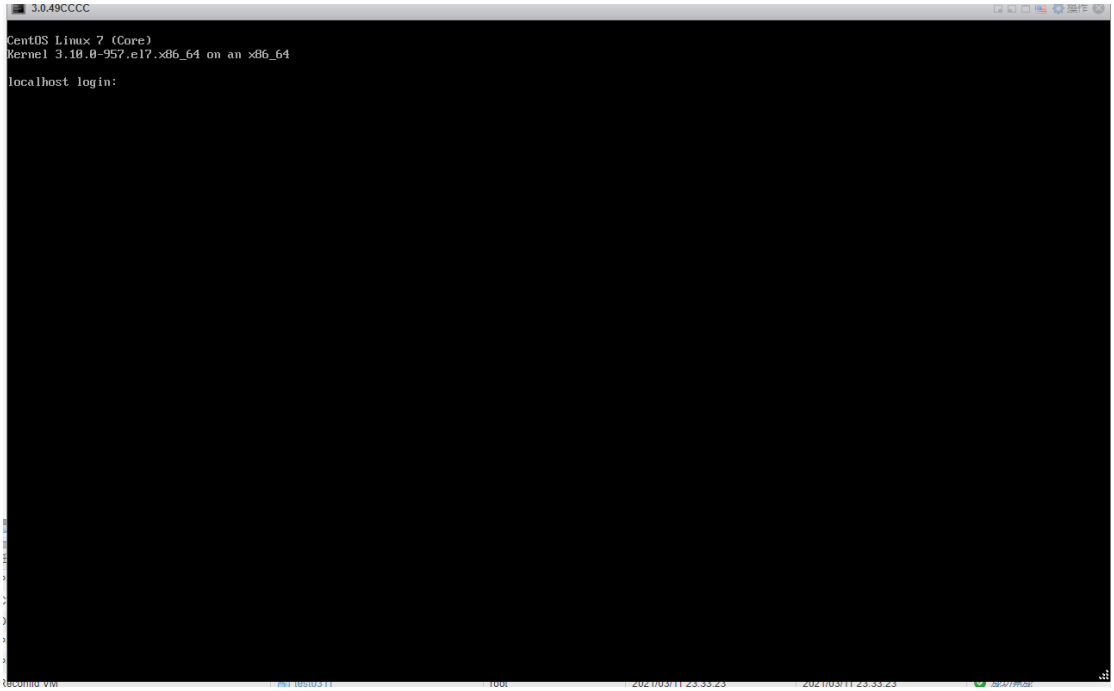
Wait during the automatic installation, which may take 1.5 hours.



After the automatic installation is complete, click Reboot.



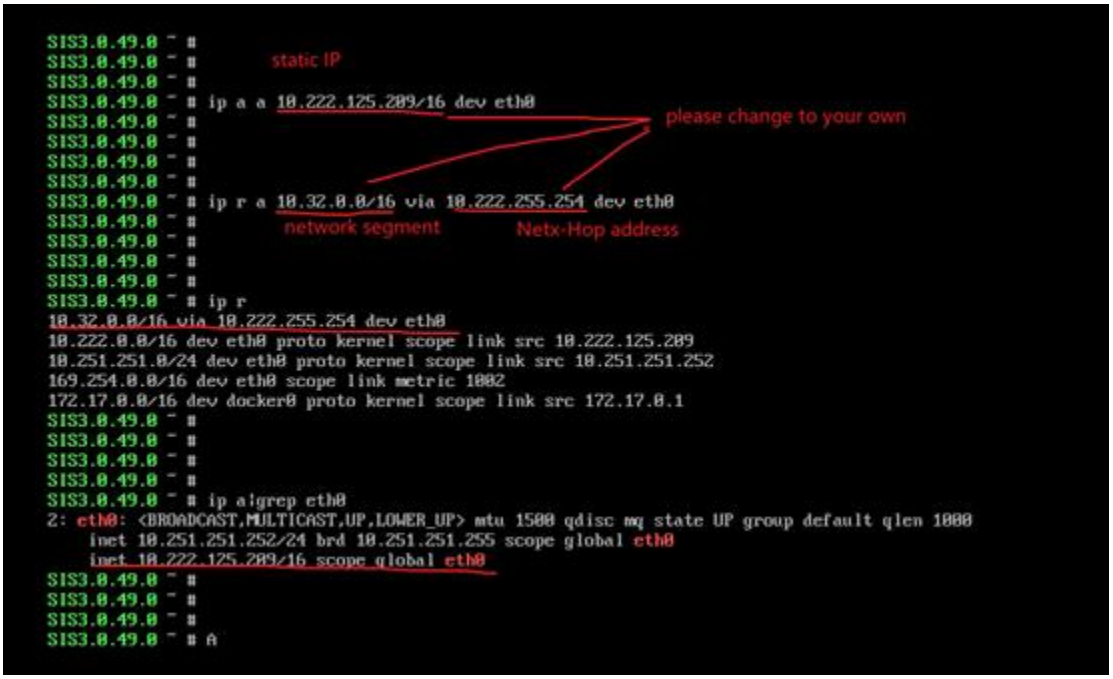




After installation, you need to enter the background to configure the IP address. The default login account is "admin" with the password "adminsangfornetwork".

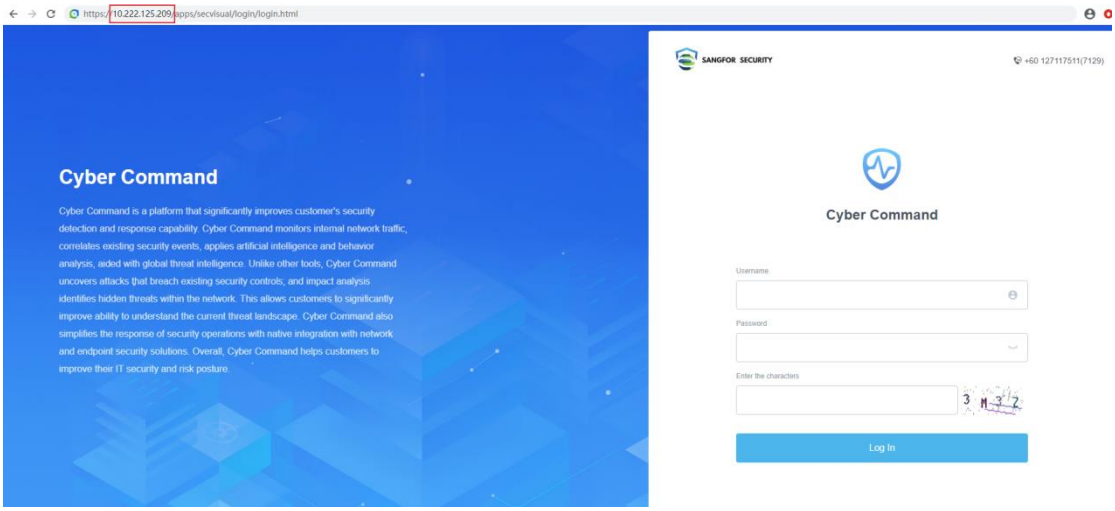
For example, if you want a PC (10.32.0.0/16) to access the web console, you need to add

the next hop address of 10.32.0.0 in the background.

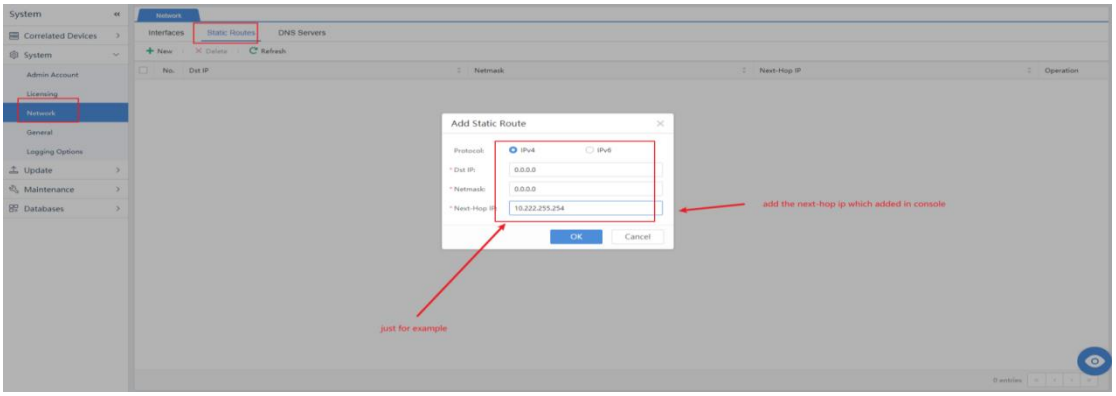


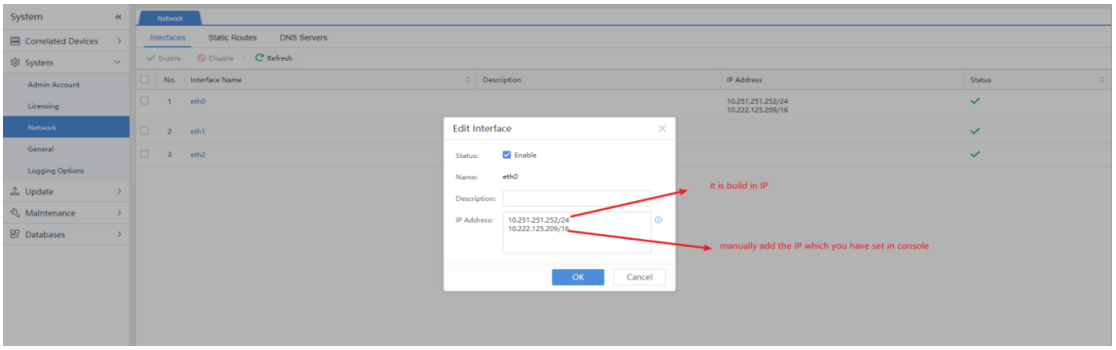
The default login account of the Web console is "admin" with the password "admin".

To use the product normally, licensing is required. Otherwise, you can only enter the page about system settings.



After entering the web console, you need to manually add the permanent route and IP address. Otherwise, the IP address information just configured will be invalid after the device restarts.





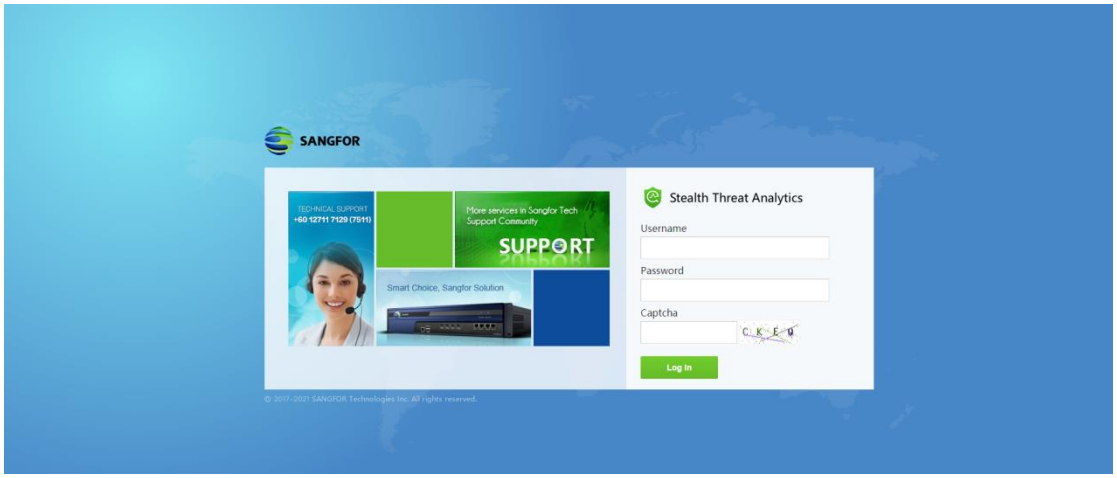
Note:

Virtualization deployment requires a basic configuration. If CPU cores, memory size, system disk and data disk size are non-standard, the system may fail to start normally or the gateway may be unreachable.

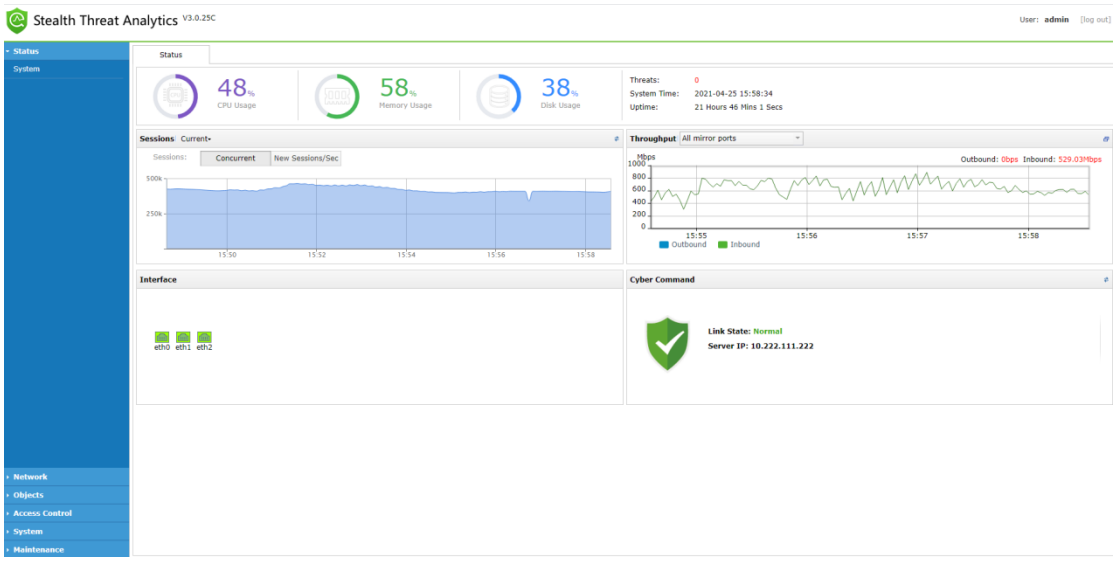
Connection with STA

Wen Cyber Command is licensed, it needs to be connected with an STA device so as to receive traffic. The following operations should be performed on STA:

1. Log in to STA.

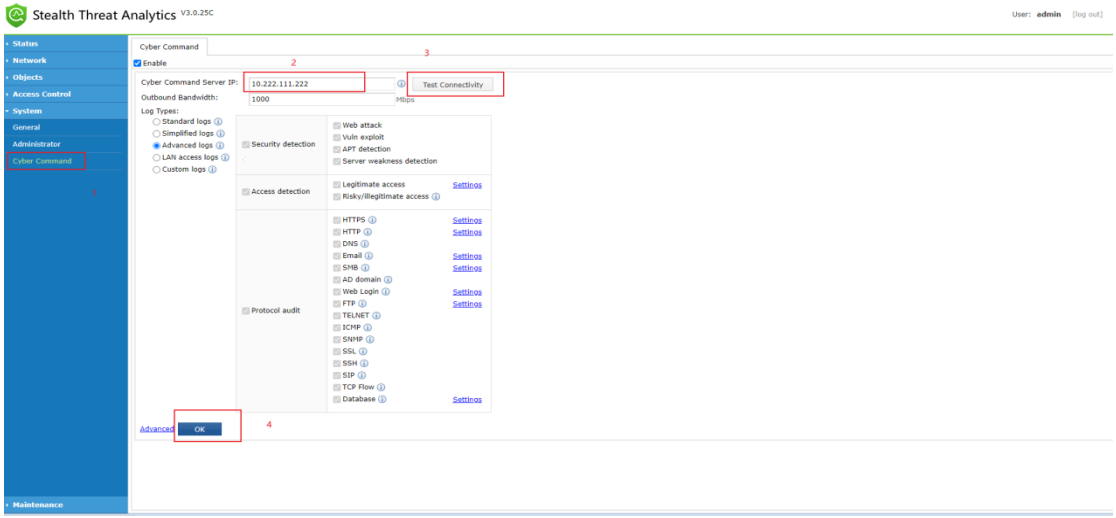


2. Ensure that the customer's traffic is connected and will be forwarded from the switch's mirror port. This also depends on the customer's network configuration.

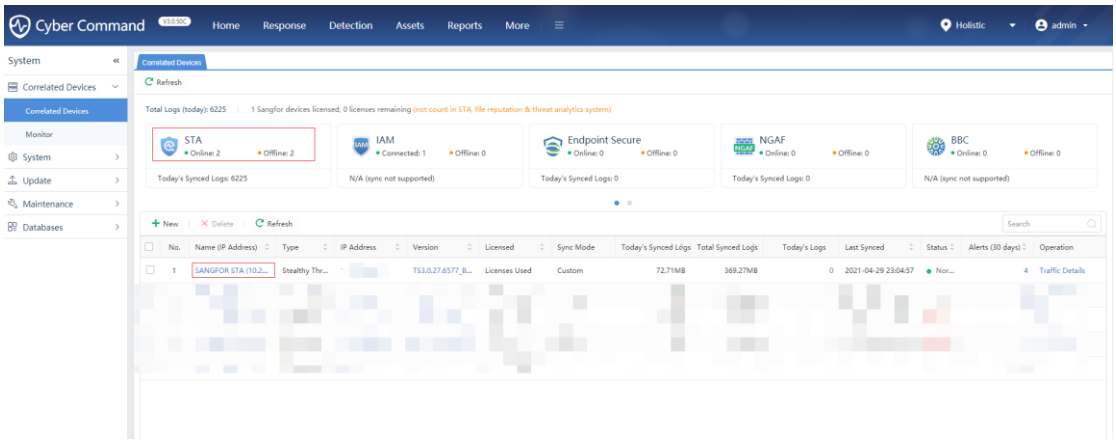


3. Go to STA and specify a Cyber Command IP address to be connected and test connectivity.

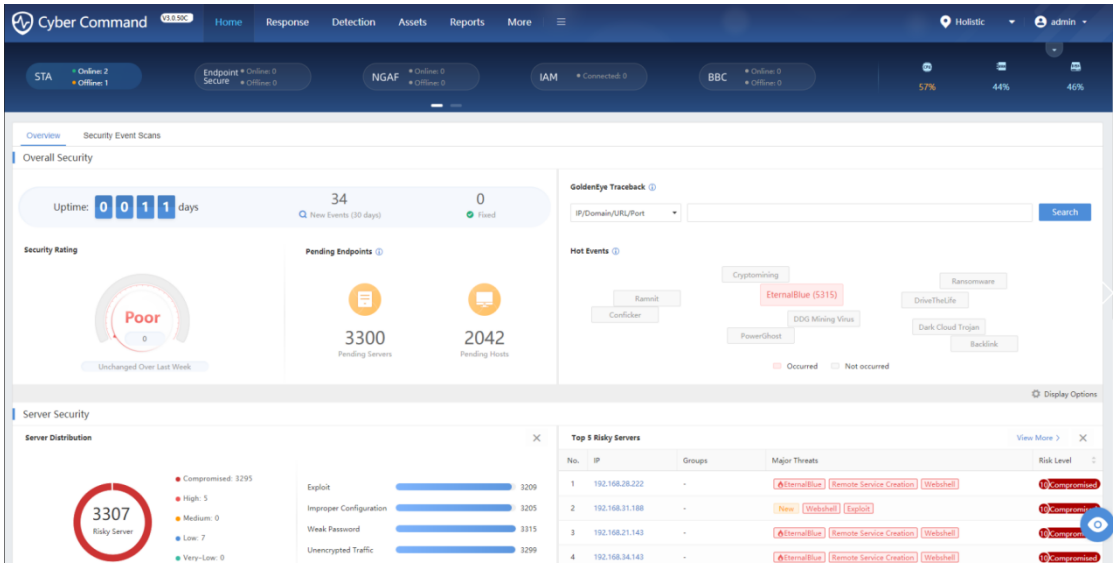
Then, choose the log transmission mode which is usually set to the "Advanced logs" mode.



4. Check the STA status on Cyber Command and ensure that STA is connected normally.

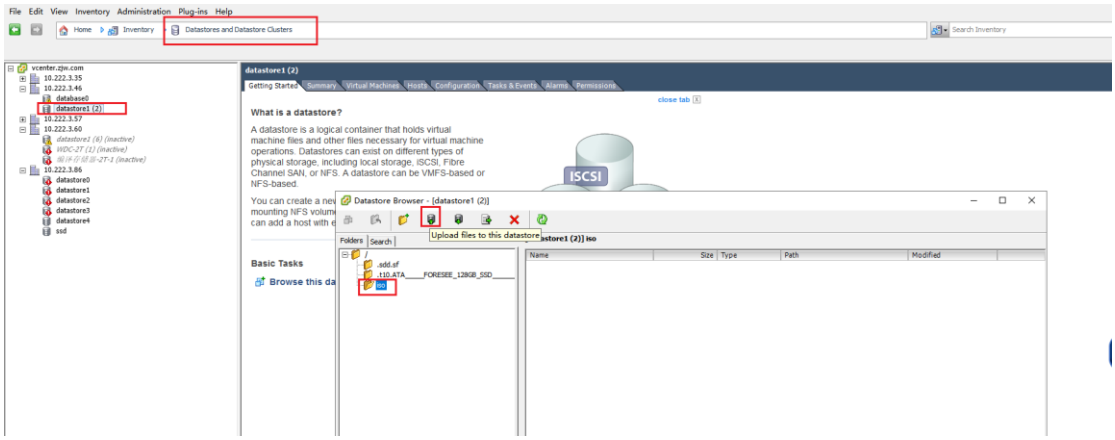


This means that Cyber Command has processed traffic normally.

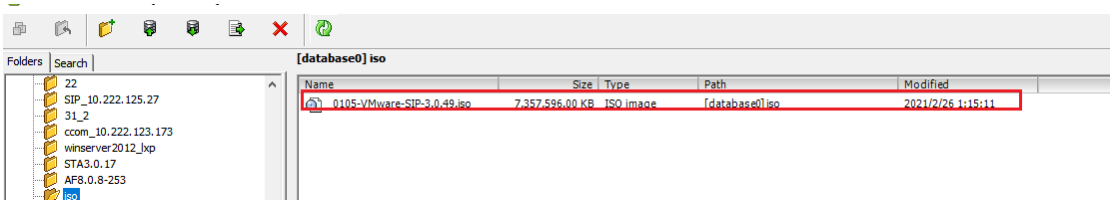


2. VMware vSphere Client Deployment

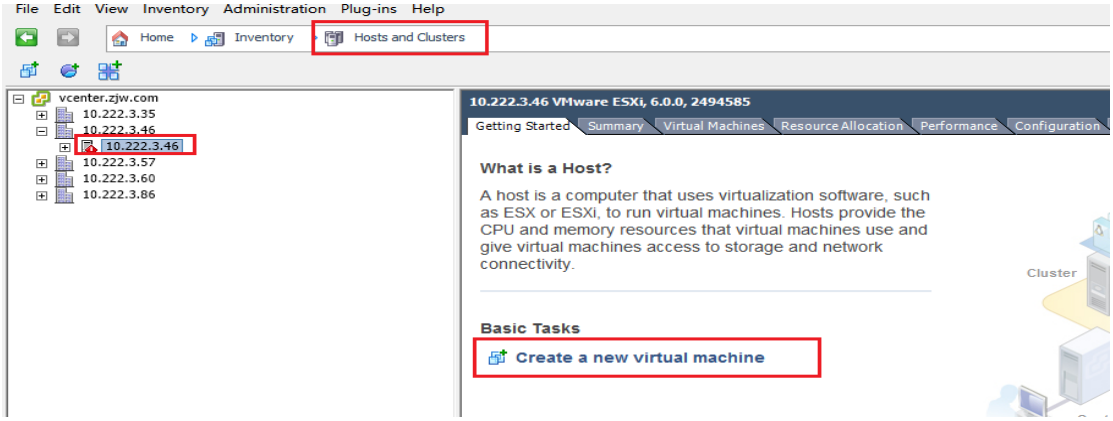
Upload ISO file to VMware datastore.



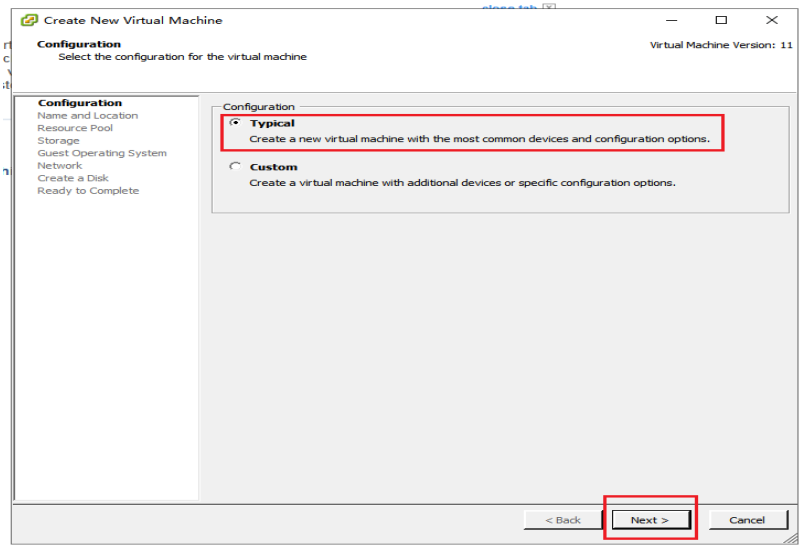
The upload may take 30 minutes. The ISO file in the following screenshot is just an example.



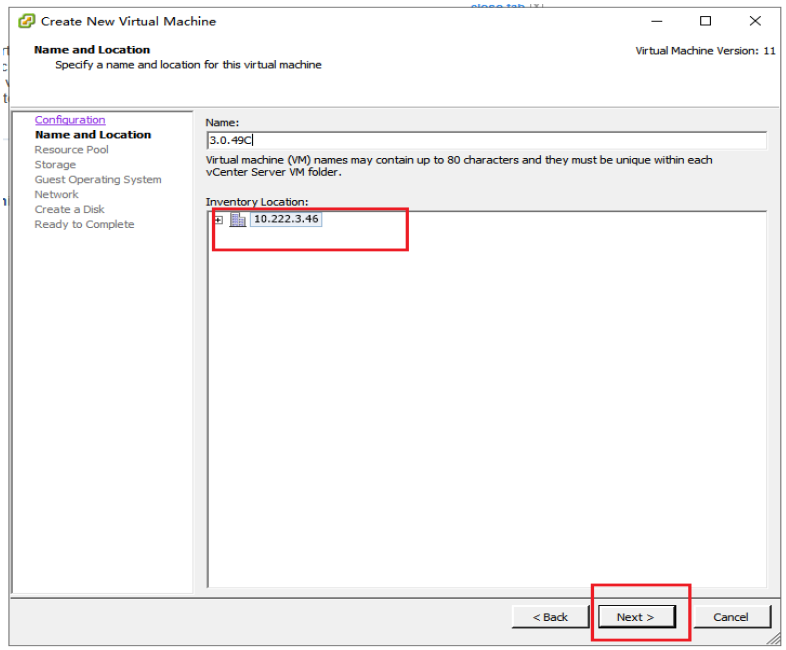
Create a new virtual machine.



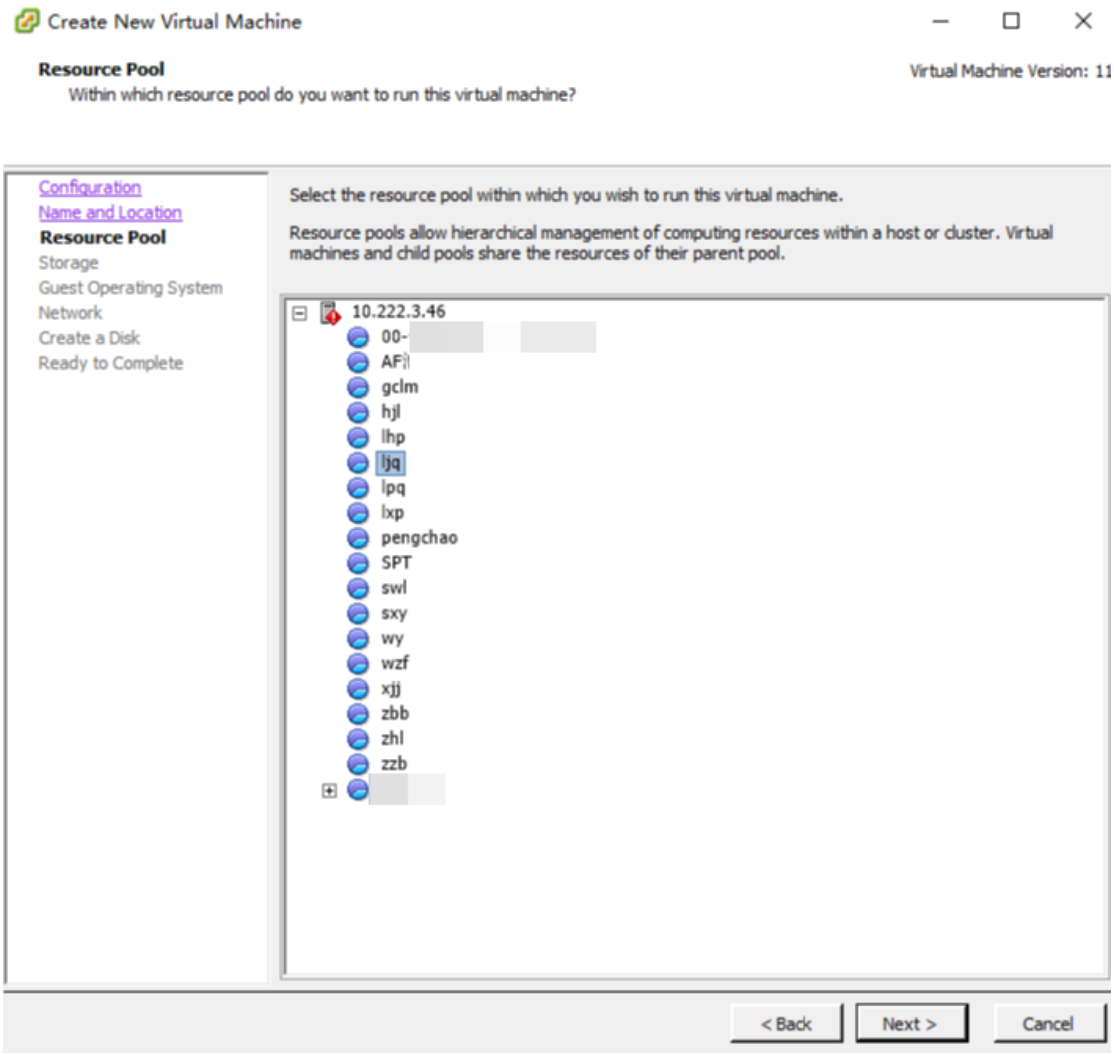
Click the button to create a new virtual machine and then click Next.



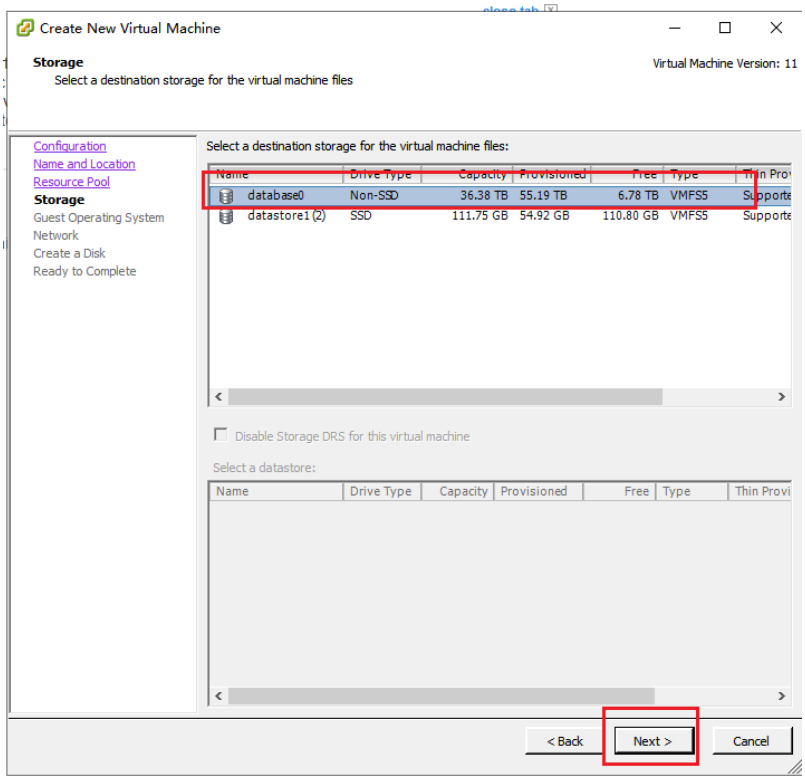
Select a host and click Next.



Select a resource pool and click Next.

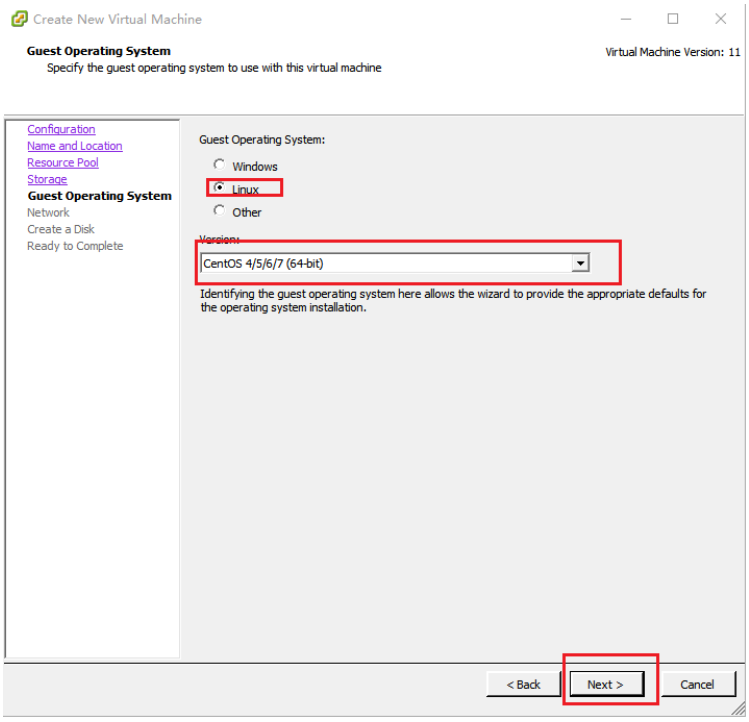


Select storage size, ensuring it is large enough.

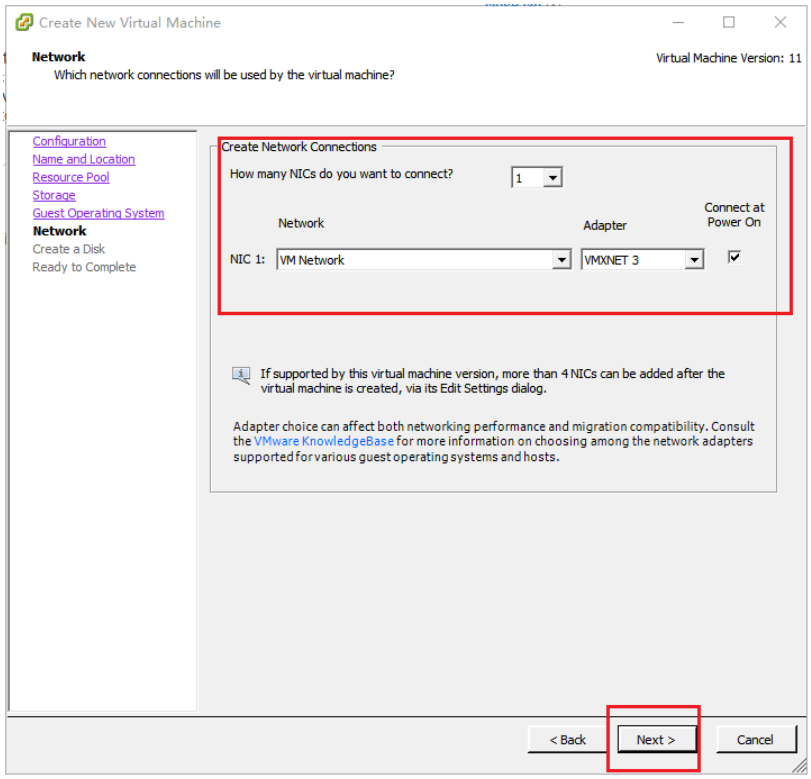


Select Linux OS and CentOs 4/5/6/7 (64-bit) version for the virtual machine.

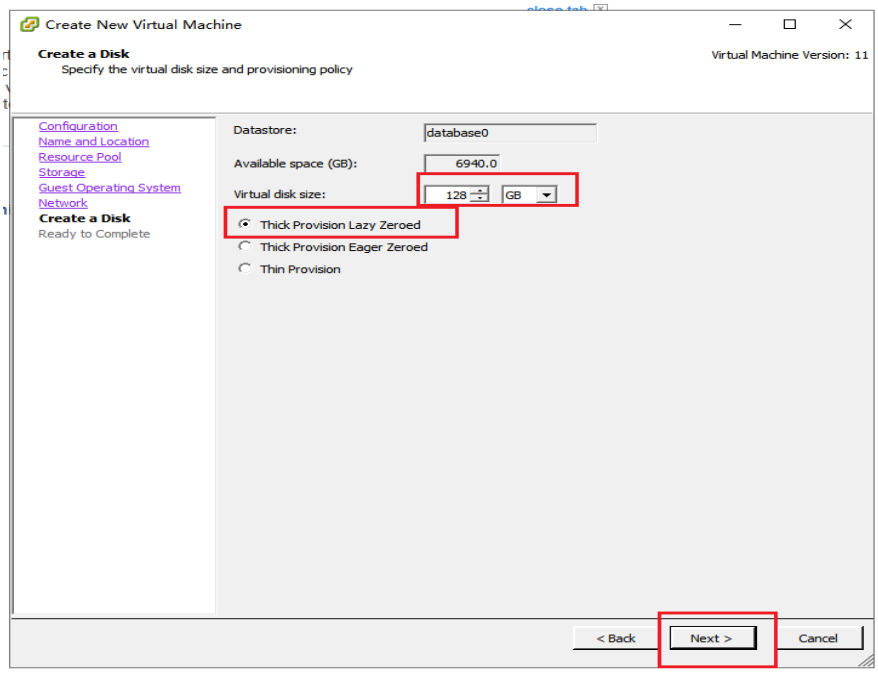
Then, click Next.



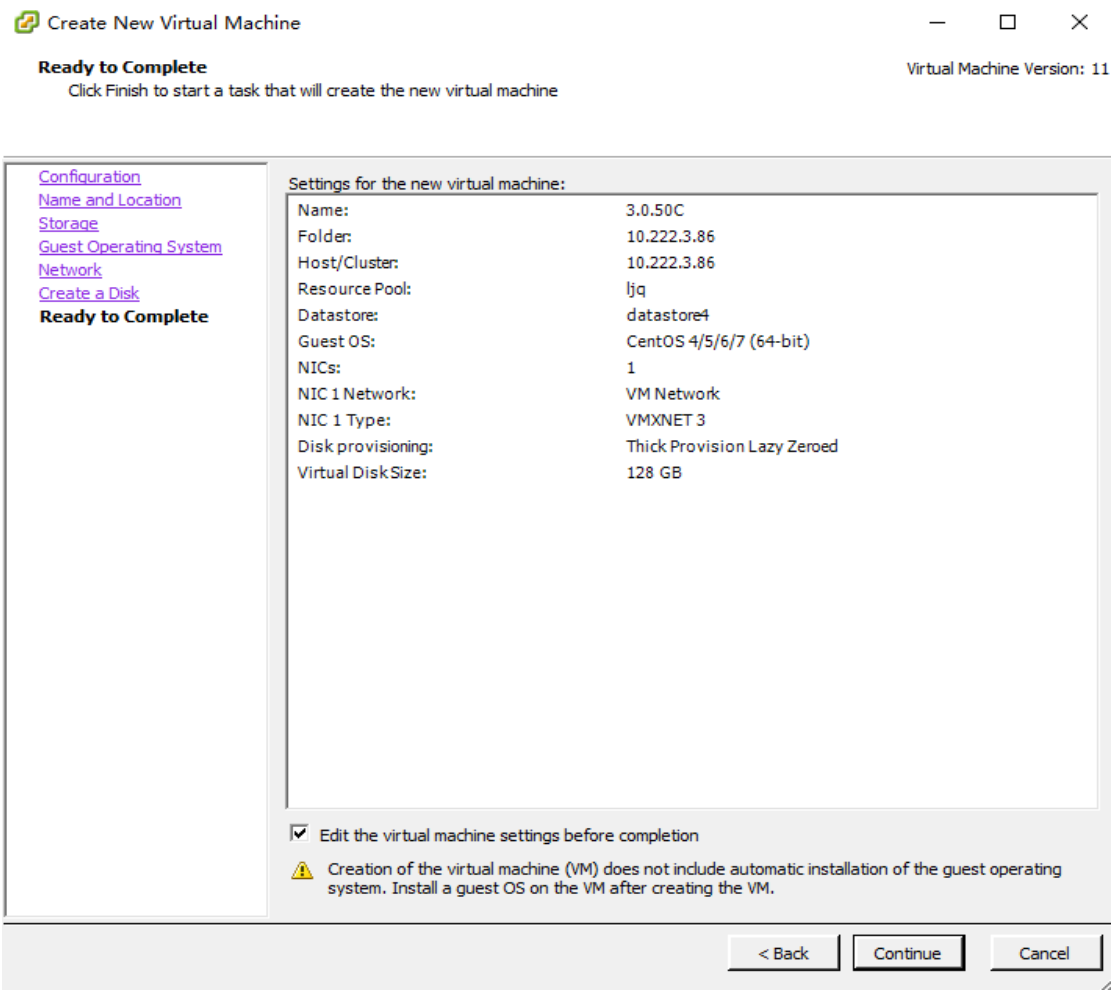
Version 3.0.50C supports 1 to 4 NICs. Supported NIC types: VMXNET3, VMXNET2 (enhanced), and e1000.



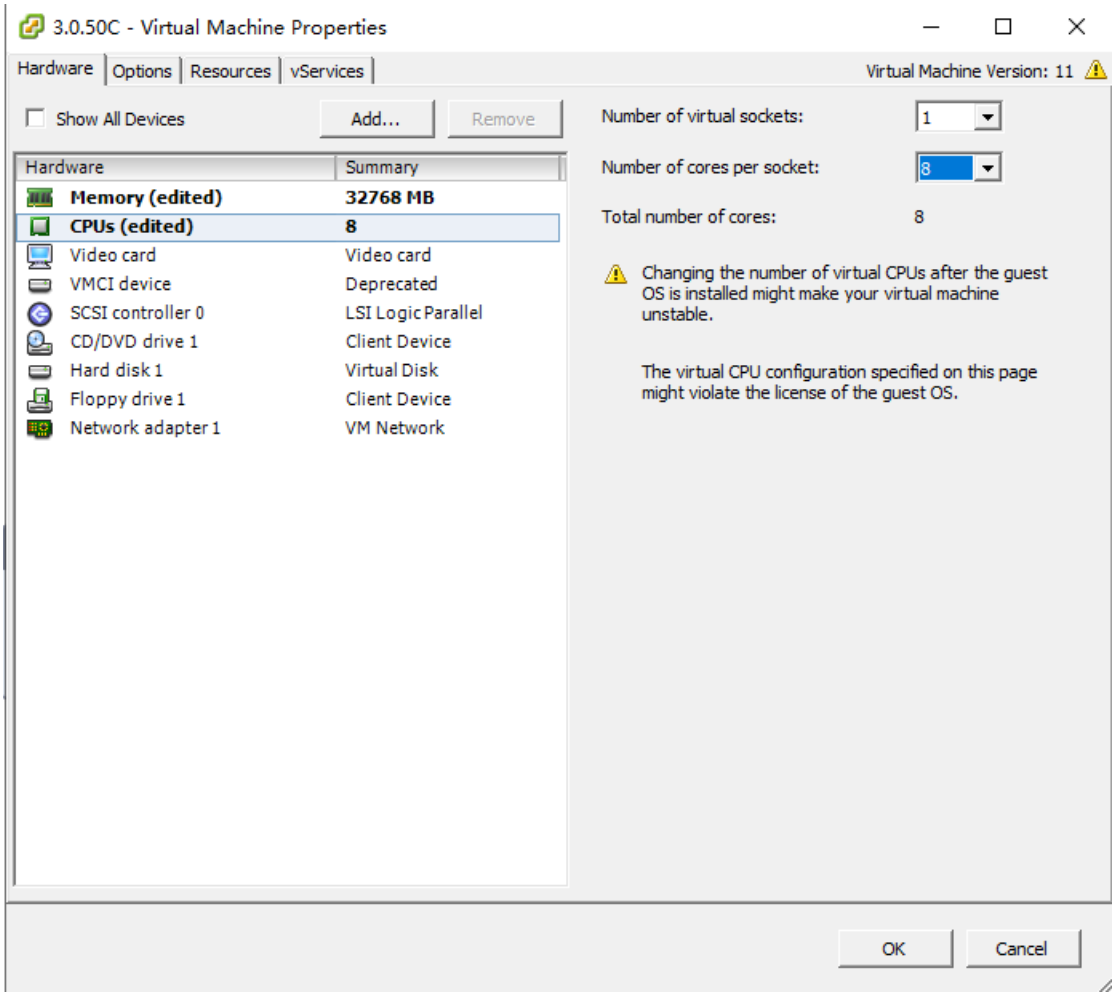
Add a 128 GB system disk. Then, click Next.



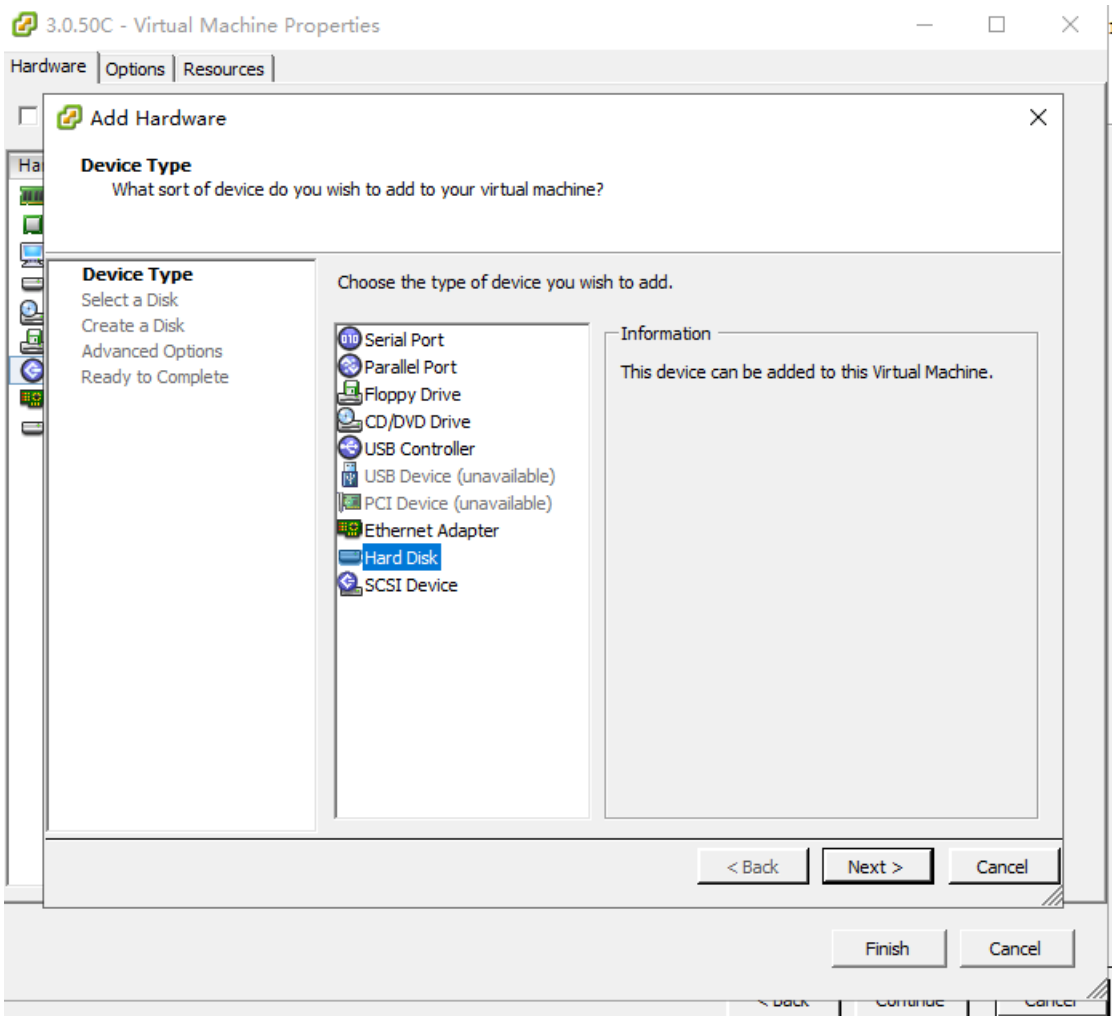
Click Continue to finish specific configurations for the virtual machine.



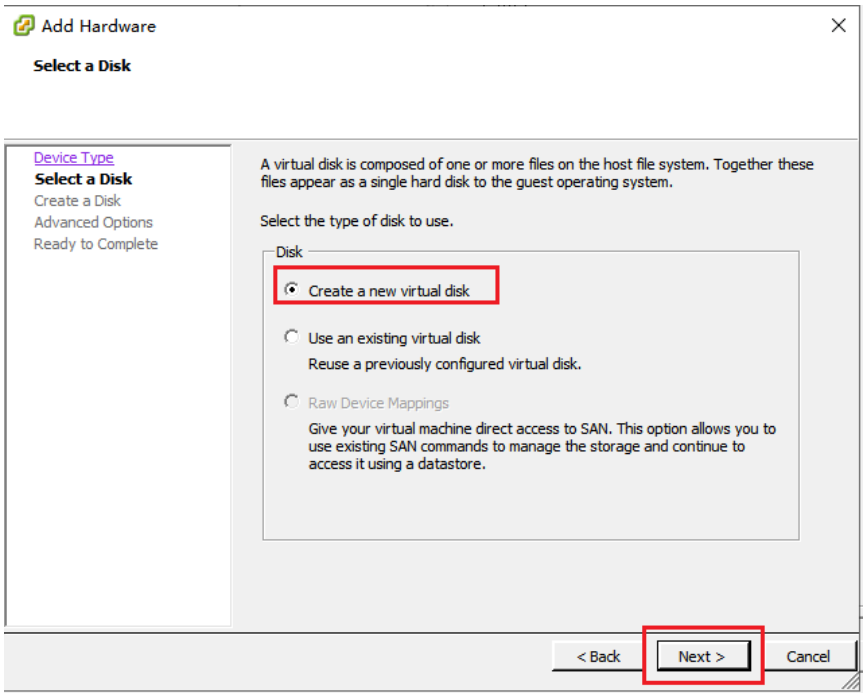
Change CPU to 8 cores and change memory size to 32G.



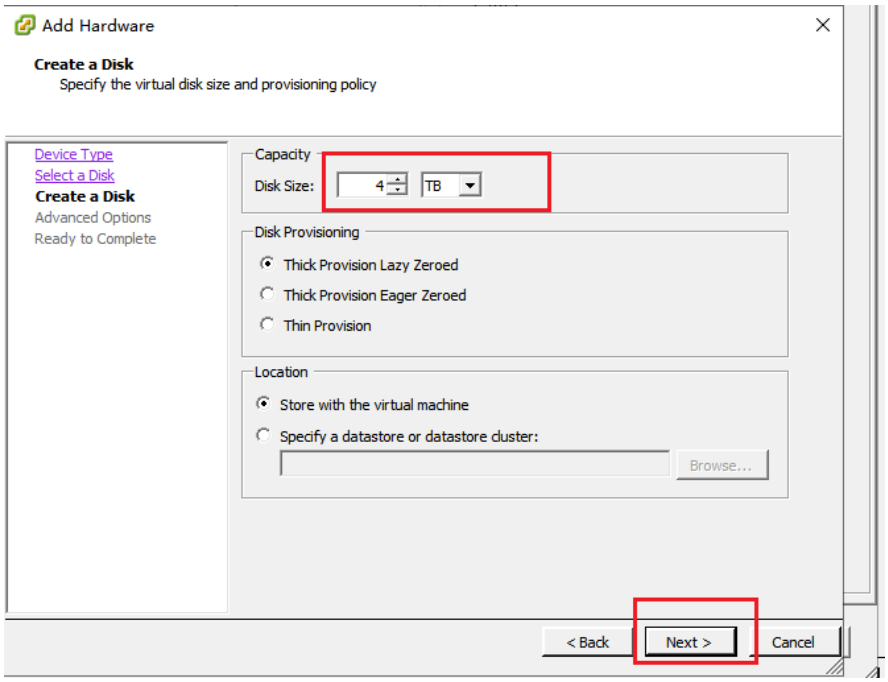
Add a 4-TB data disk, ensuring that the environment has sufficient resources.


3.0.50C - Virtual Machine Properties
Hardware
Options
Resources
Add Hardware
Device Type
What sort of device do you wish to add to your virtual machine?
Device Type
Select a Disk
Create a Disk
Advanced Options
Ready to Complete
Choose the type of device you wish to add.
Serial Port
Parallel Port
Floppy Drive
CD/DVD Drive
USB Controller
USB Device (unavailable)
PCI Device (unavailable)
Ethernet Adapter
Hard Disk
SCSI Device
Information
This device can be added to this Virtual Machine.
< Back
Next >
Cancel
Finish
Cancel

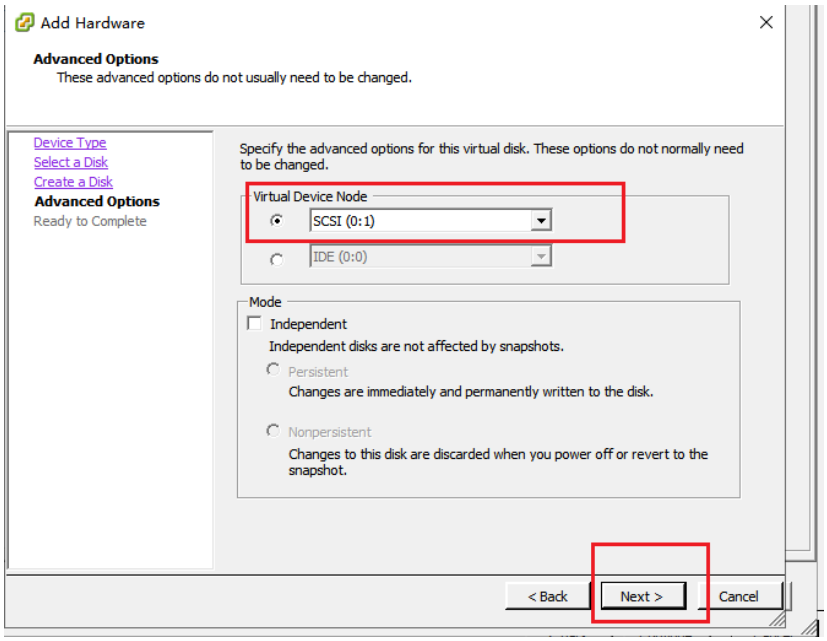
Click Next.



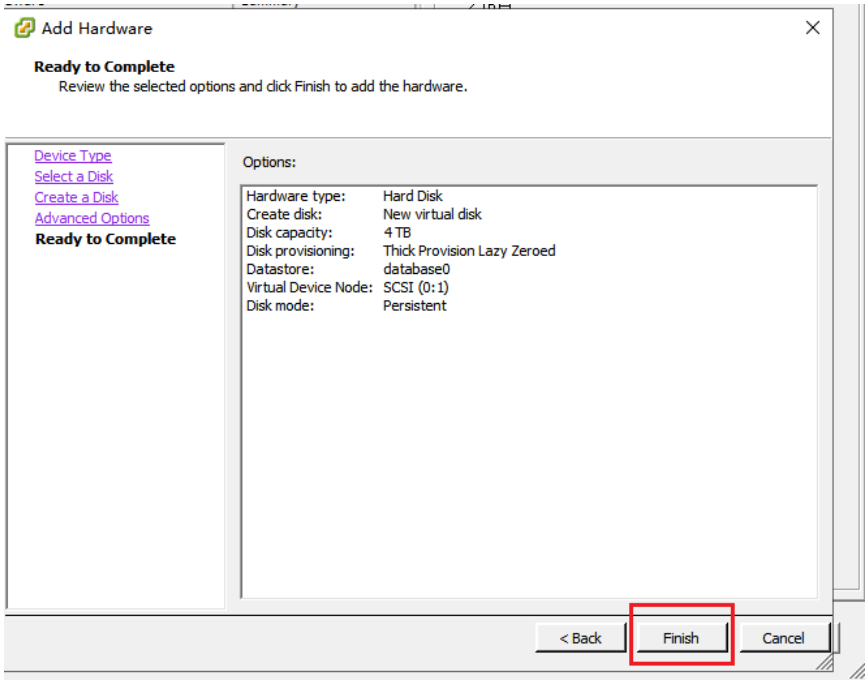
Click Next.



Click Next.

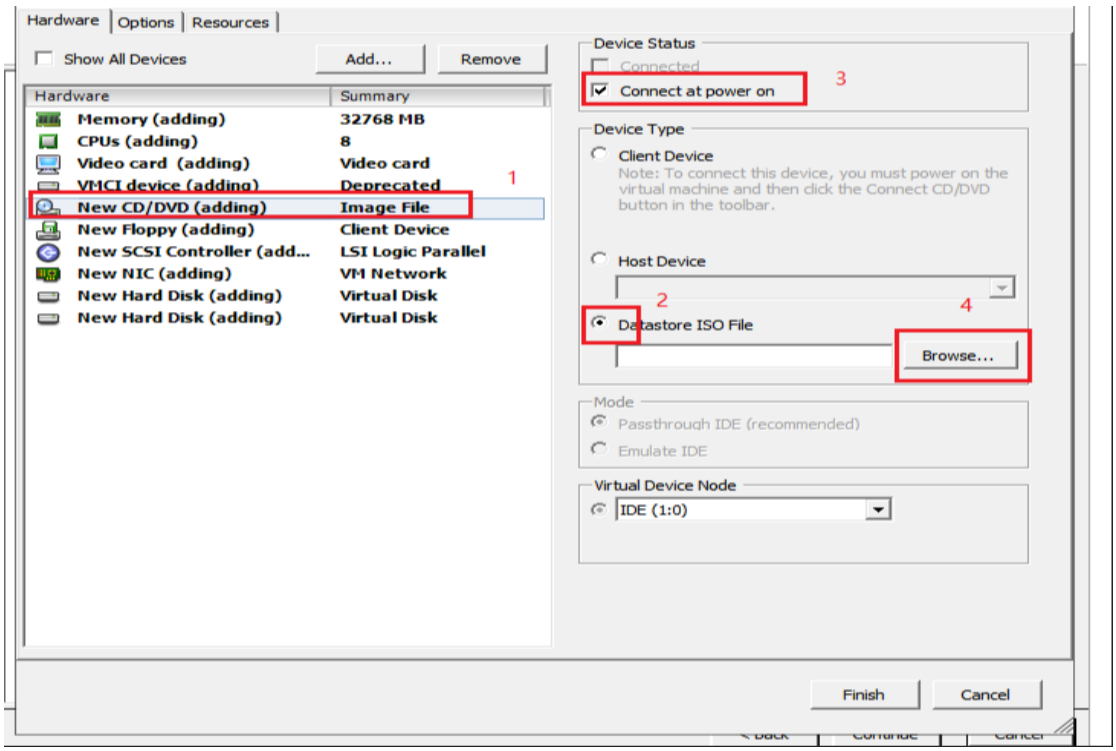


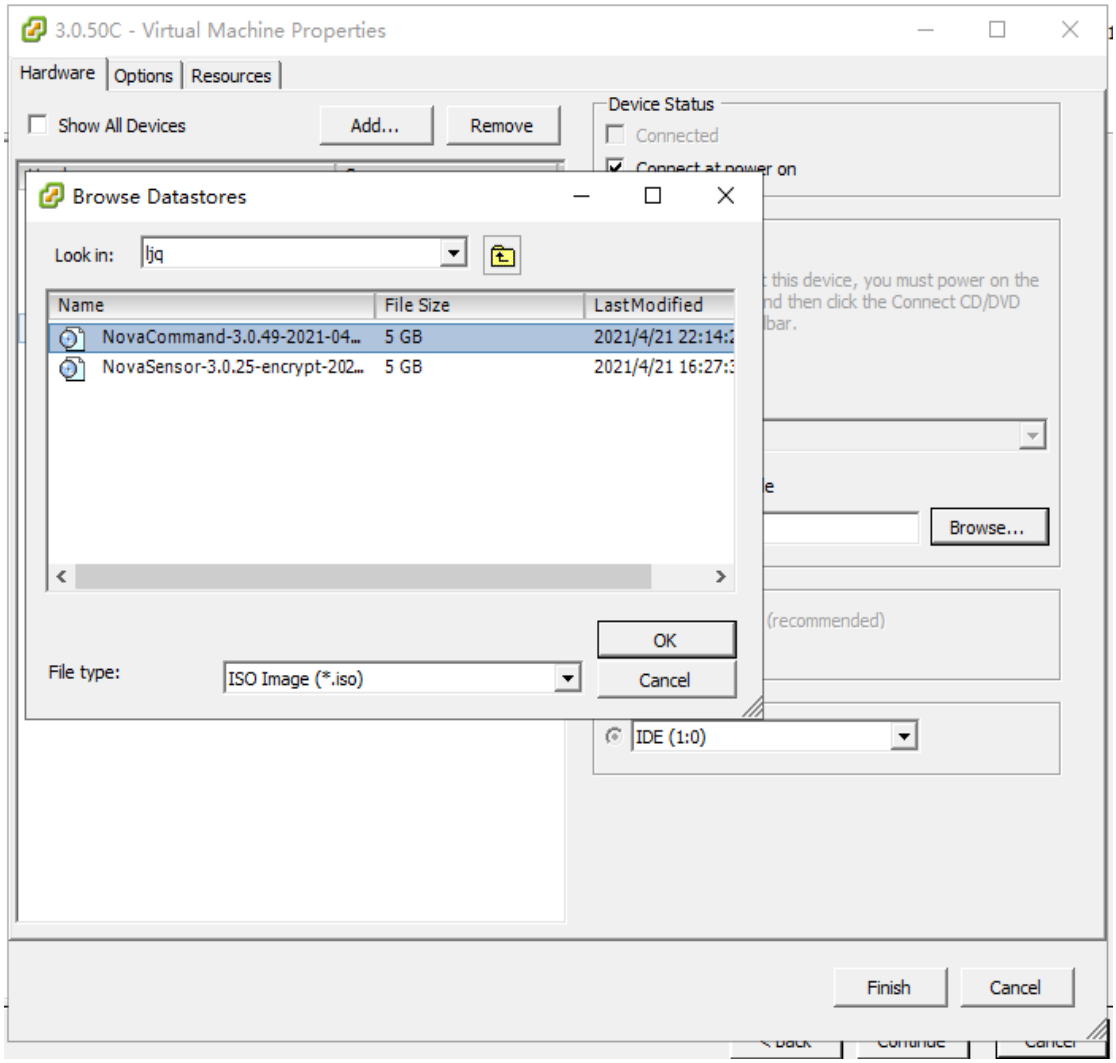
Click Finish to complete the steps to add a disk.



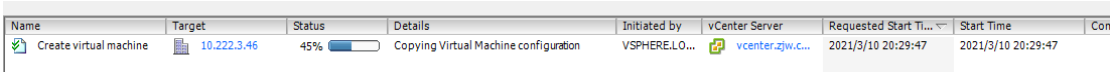
Select an image to be added to virtual CD/DVD drive. Select the option to connect at power on.

Select the directory to start uploading ISO.


Hardware
Options
Resources
Show All Devices
Add...
Remove
Hardware
Summary
Memory (adding)
32768 MB
CPUs (adding)
8
Video card (adding)
Video card
VMCI device (adding)
Deprecated
New CD/DVD (adding)
Image File
New Floppy (adding)
Client Device
New SCSI Controller (add...
LSI Logic Parallel
New NIC (adding)
VM Network
New Hard Disk (adding)
Virtual Disk
New Hard Disk (adding)
Virtual Disk
1
Device Status
Connected
Connect at power on
3
Device Type
Client Device
Note: To connect this device, you must power on the virtual machine and then click the Connect CD/DVD button in the toolbar.
Host Device
2
4
Datastore ISO File
Browse...
Mode
Passthrough IDE (recommended)
Emulate IDE
Virtual Device Node
IDE (1:0)
Finish
Cancel


3.0.50C - Virtual Machine Properties
Hardware
Options
Resources
Show All Devices
Add...
Remove
Device Status
Connected
Browse Datastores
Look in:
ljq
Name
File Size
Last Modified
NovaCommand-3.0.49-2021-04...
5 GB
NovaSensor-3.0.25-encrypt-202...
5 GB
File type:
ISO Image (*.iso)
OK
Cancel
Browse...
IDE (1:0)
Finish
Cancel

After the file is added successfully, click Finish and wait for VMware to create a new virtual machine.

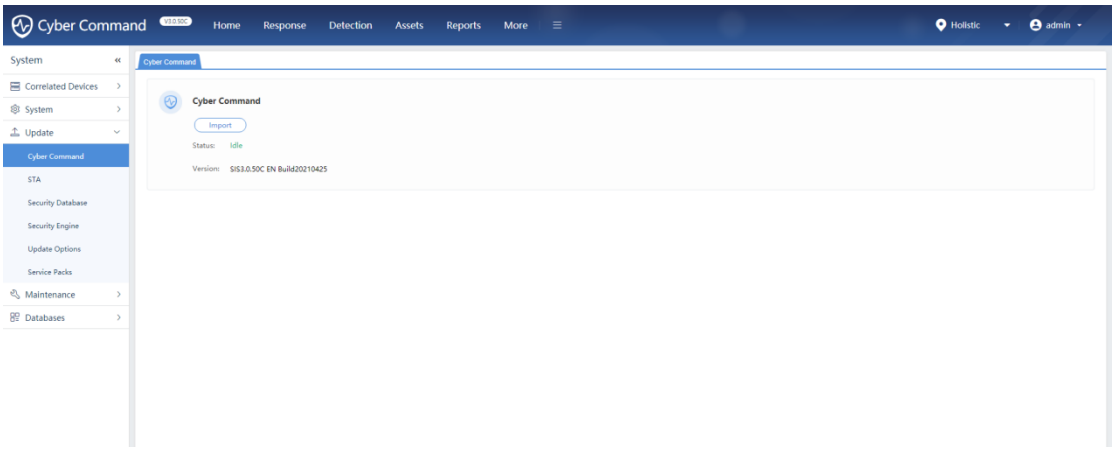


Select the newly created virtual machine and turn on the power to go to the automatic installation page. The operation steps are the same as VMware EXSi and will not be repeated here.

2.4. Check After Deployment

2.4.1. Platform Check

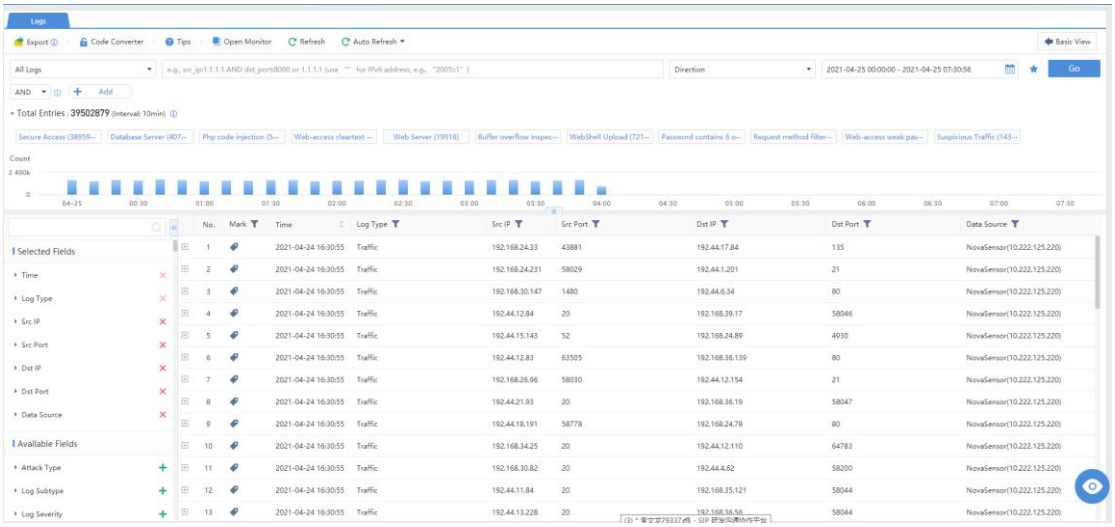
Log in to web console and go to System > Update > Cyber Command to check that the version is SIS3.0.50C.



2.4.2. Business Verification

Verify basic functions used by customers.

Log in and go to the Logs page to check whether there are new logs synchronized from STA.



2.5. Handling of Upgrade Failure

- **Scenario 1: Fail to start automatic installation.**

  Troubleshooting:

  1. Check whether the host resources on the deployment environment are sufficient

  2. Check whether the option to connect at power on is not selected when the image is selected for the added virtual CD/DVD drive.

- **Scenario 2:** Console cannot be accessed when deployment is finished and network has been configured.

  Troubleshooting:

  1. Check the resource configuration of the deployment environment. Check whether the data disk is configured and whether the data disk size is too small.

  2. Check whether the MAC address of the management interface matches the MAC address of the NIC that the virtual machine uses to access the network.

- **Scenario 3: Network error occurs after login to console**

  Troubleshooting:

1. Errors occur on pages of the console when Elasticsearch database is not started. In this case, wait for the Elasticsearch database to be started.

   Log in to the background to check the console version has been Cyber Command 3.0.50C.

2.6. Rollback

None