Introduction to proper nouns

Document Category: Product Related Experience

Management console

> Web console

The web console used for migration or disaster recovery, most related actions are performed on the management console.

It is recommended to use the Linux version management console.

Agent(Antenna)

> Source machine Agent

When migrating in agent mode, the Agent is installed on the source machine.

There is a Windows version and a Linux version. Windows Antenna and Linux Antenna are not the same version number.

Gateway (Treker)

> Role 1: transit node, target node.
>
> Role 2: Management console, when installing Windows Treker, you need to check Management during installation.
>
> No matter it is used as a transit node or a management console, cloning is not allowed! ! !

Usually acts as a transit node.

When Management is checked, it will play the role of management console.

Gateway is available in Linux and Windows versions

**When acting as a management console, the Linux version is highly recommended. **

Only the data gateway bound without VMware agent is strongly recommended to be the Windows version of the data gateway. In other scenarios, the Linux version of the data gateway is recommended.

When used as an agentless data gateway for NexaVM or NexaSphere, only the Linux version of the data gateway can be used.

BootImage (Treker Lite)

> Data gateway (target node)

It usually serves as the target node, that is, the target machine corresponding to migration or disaster recovery.

There is a Windows version and a Linux version:

- It is recommended that Windows source machines use Windows Treker Lite (WTL for short).
  - Image name: TrekerLite.qcow2 (.vhd, .iso)
- It is recommended that the Linux source machine use Linux Treker Lite (LTL for short).
  - Image name: LinuxTrekerLite.qcow2 (.vhd, .iso)

Image formats include qcow2, vhd, iso and other formats. The qcow2 format is usually uploaded to the NexaVM platform.

- **Only qcow2 format images support standard mode creation tasks. **

Offlinekit

> Source host boot image for offline migration

When the agent cannot be installed on the source host and the agentless mode cannot be used for migration, the offline migration mode can be used.

OfflineKit.iso is the image used to boot the source host during offline migration.

Protection

Protection tasks, same as synchronization tasks and replication tasks.

Provision

Provision tasks, same as recovery tasks and switching tasks.

DiagnosticsReport

> Diagnostic logs for troubleshooting analysis.

Diagnostic logs are divided into:

- Protection task diagnostic log
- Data gateway diagnostic log
- Source host diagnostic log
- TrekerLite feedback log
- Management console diagnostic log

Introduction to diagnostic logs

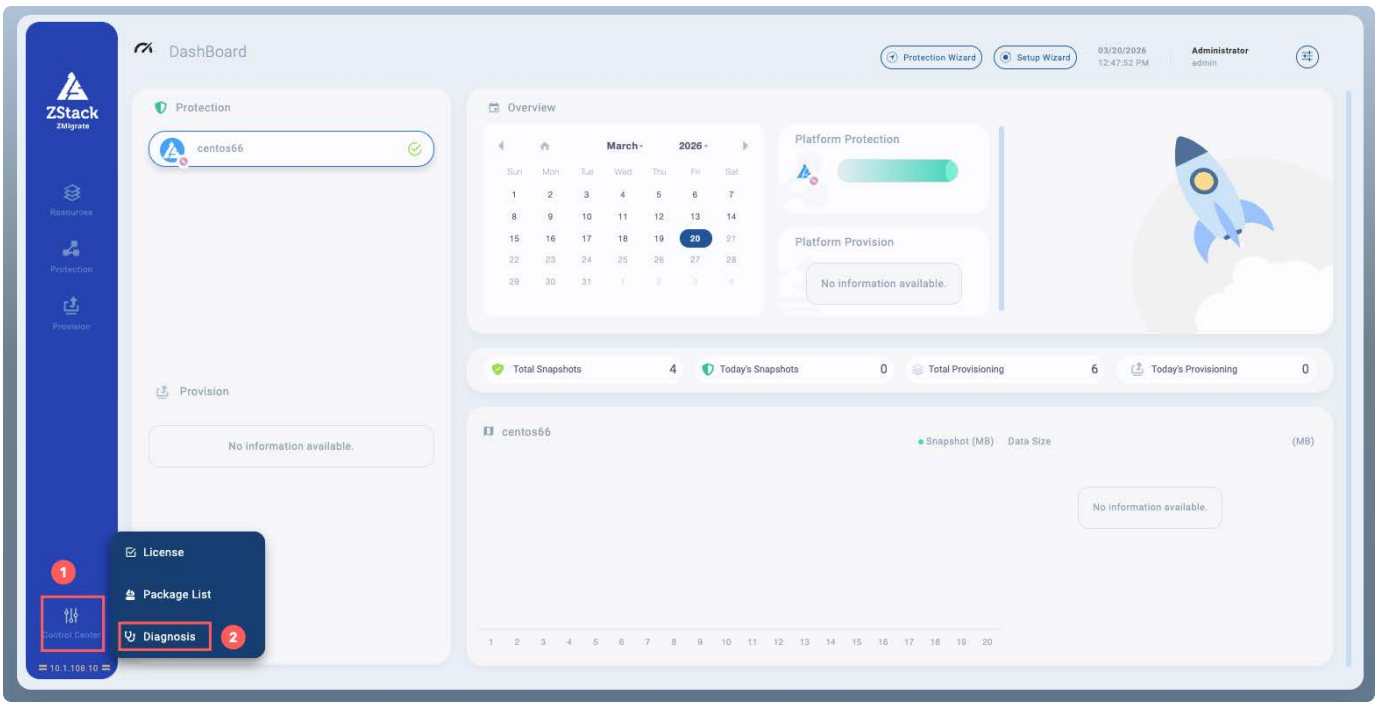
Document Category: Product Related Experience

Classification of diagnostic logs

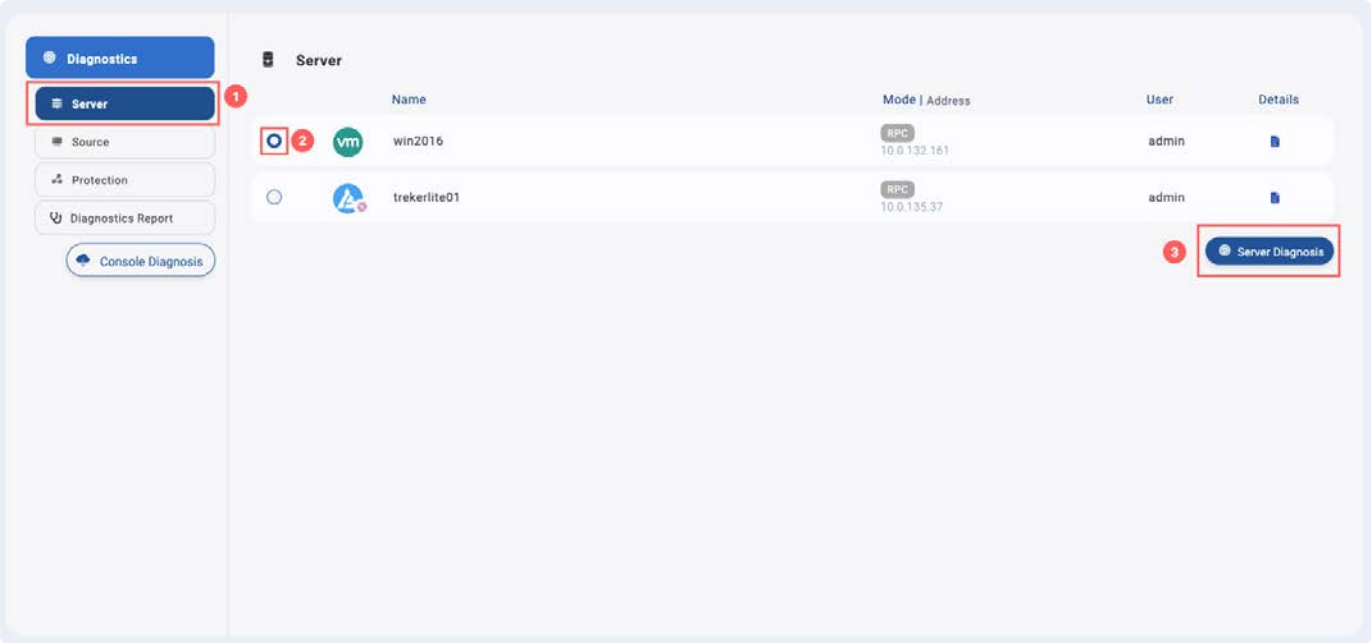
1. Management console
2. Source host
3. Gateway server
4. Protection tasks
    - The agent mode includes: source host and Treker/Treker Lite in the topology.
    - Agentless mode includes: Treker/Treker Lite in the topology.
5. TL feedback

Collect diagnostic logs

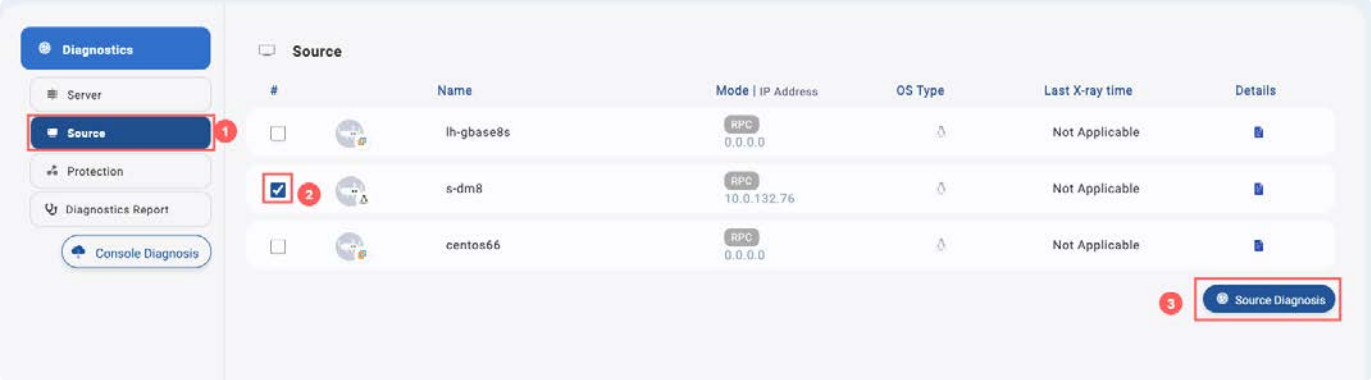
Enter the diagnostic log page



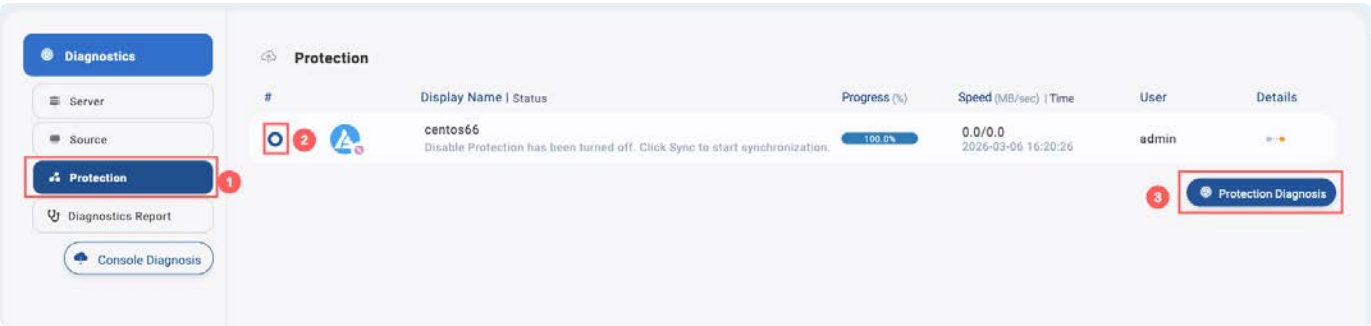
Collect data gateway diagnostic logs



Collect source host diagnostic logs



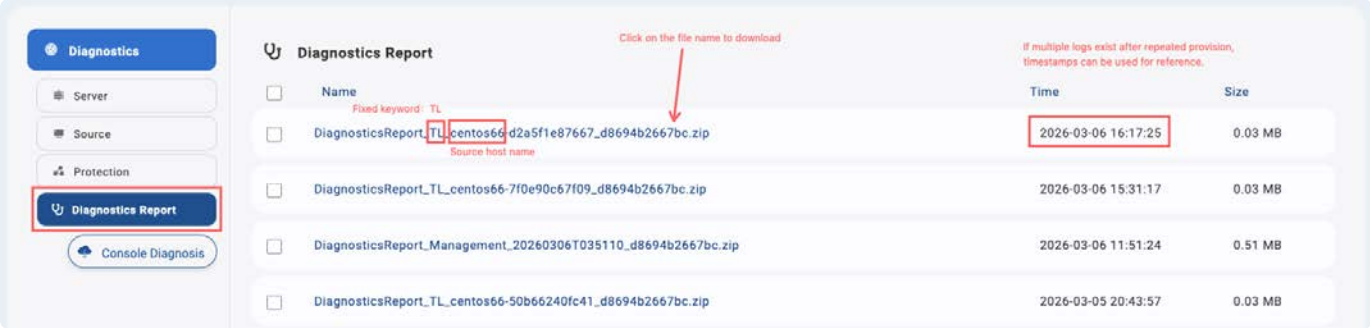
Collect protection task diagnostic logs



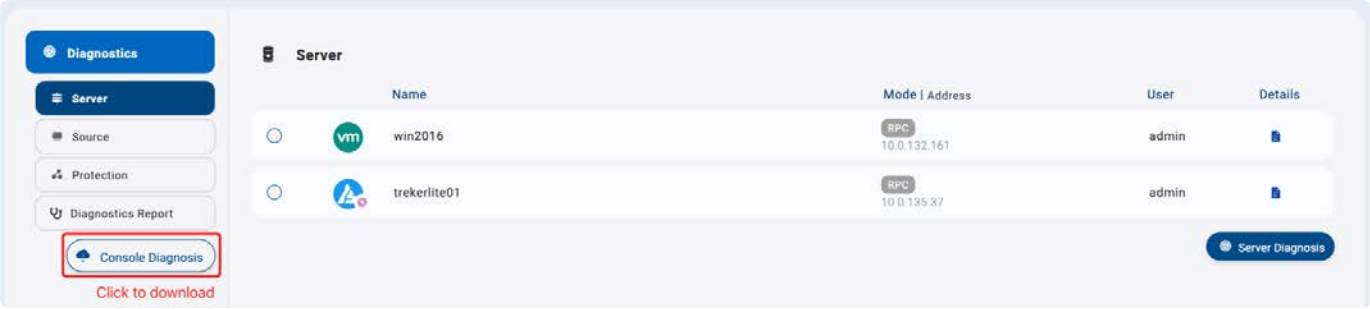
Collect TL feedback diagnostic logs

Locate the TL feedback log based on the keyword TL, host name, and log generation time.

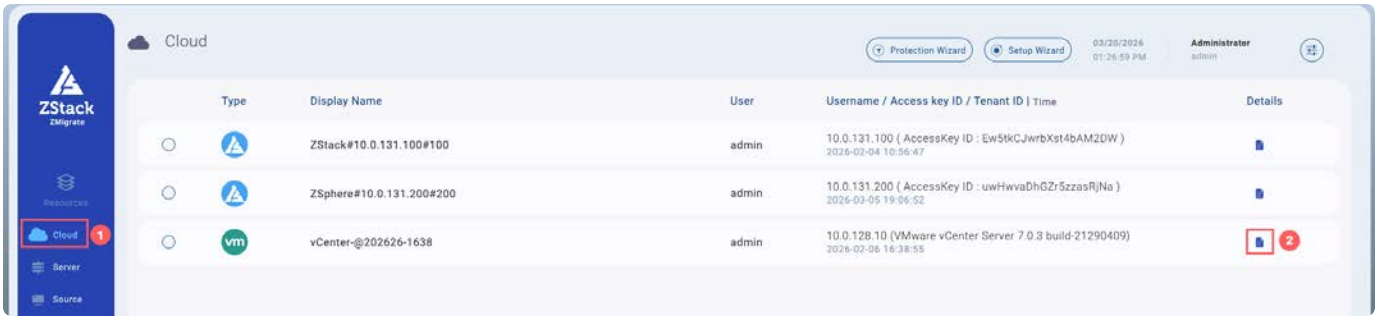
Click on the file name to download.

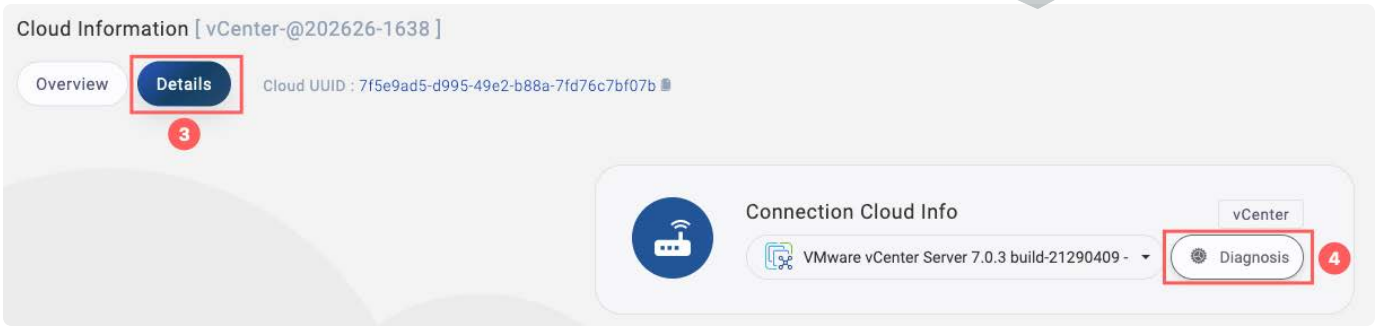


Collect management console diagnostic logs



Collect diagnostic logs of VMware cloud platform



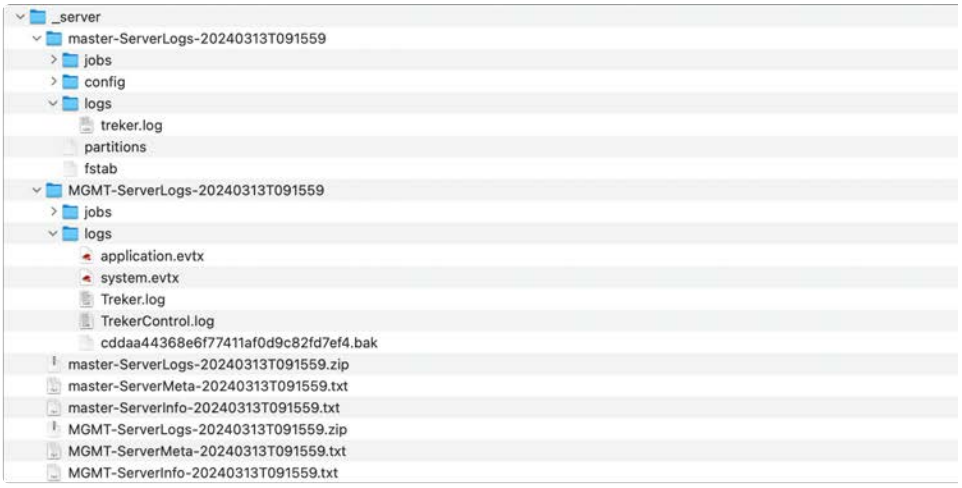


Diagnostic log structure



client: Diagnostic log of the source host.

- jobs: Stores the job information of this source host.
- logs: stores the log information of the source host.



server: Contains the transit Treker and target Treker Lite (in some architectures, the target may be Treker).

- jobs: Information about all jobs in this Treker.

- logs: All log information about this Treker.

Confirm the troubleshooting log files

An error occurred when registering the source host and data gateway server (transit node, target node) on the management console.

- **Collect management console diagnostic logs.**

The protection task shows an error when the target cloud platform automatically creates a cloud host.

- **Collect management console diagnostic logs.**

---

protection task status: The source host snapshot cannot be created. The snapshot is taken on the source host.

- **Collect the diagnostic log of the protection task.**
- Look at the client's antenna.log.

---

protection task status: Other types of errors.

- **Collect the diagnostic log of the protection task.**
- Need to analyze client's antenna.log and server's treker.log.

Provision task status: System conversion failed. The system conversion was done on the target machine.

- Select the first switching option "Provisioning by Disk".
  - **Collect the diagnostic log of the protection task.**
  - Mainly check the treker.log of the target machine of the protection task, and combine it with the antenna.log of the source host for auxiliary judgment.
- Select the second toggle option "DevTest by Snapshot"
  - **Collect the TL feedback diagnostic log and the diagnostic log of the protection task.**
  - It depends on the antenna.log of the source machine of the protection task.

- Look at the treker.log of the TL feedback log.

Task strategy parameters

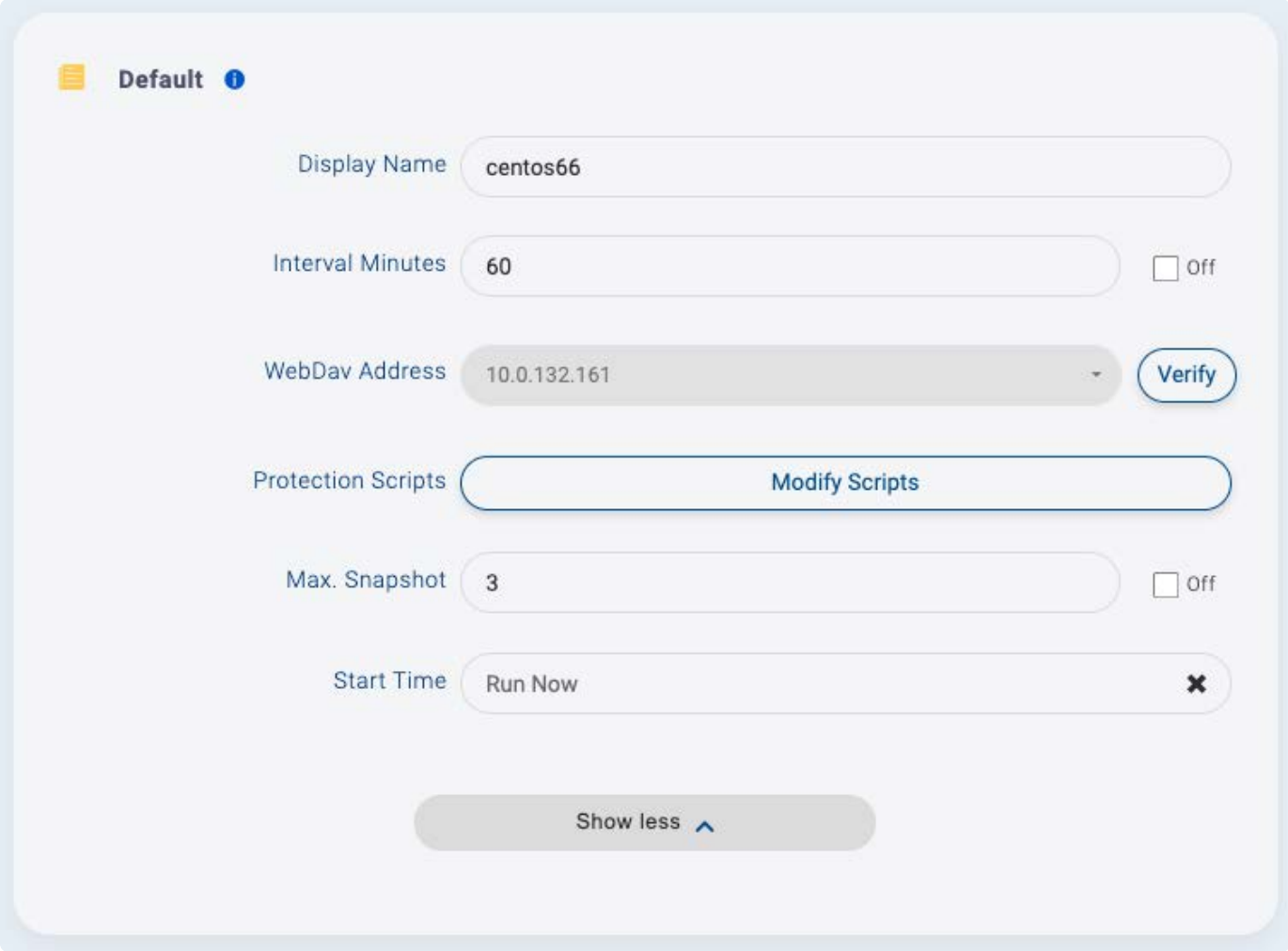
Document Category: Product Related Experience

write in front

If you don't know which parameters need to be set, just keep the default parameters.

After modifying the parameters, it will not take effect until the next synchronization takes effect.

standard



Incremental sync frequency (minutes)

Increment interval, that is, how long it takes for automatic incremental synchronization. The default is 60 minutes.

If you check `Off`, the increment will not be done automatically. You need to manually synchronize the task before the increment will be done.

Service listening address

The IP address to communicate with the target machine.

When the transit data gateway has only one IP address, no need to pay attention to it, just keep the default.

When the transfer data gateway has multiple IP addresses, please pay attention to selecting an IP address that can communicate with the target machine.

Source transfer speed limit – MB/s

This parameter is only available if the agent is installed on the source host.

Supports network QoS in the presence of a proxy. The limit unit for source machine reading rate is MB/s. Users can choose or customize it according to the actual situation.

Number of copies

The number of copies, that is, the number of snapshots of the target machine, The default value is 3;

- Migration scenario: Just select the latest snapshot when switching the migration scenario.
- Disaster recovery scenario: Combine with the `incremental synchronization frequency` and set it according to the number of historical snapshots you want to reserve.

In the mode of manually creating the target machine, there is generally no snapshot, and this parameter does not take effect.

Using the API's mounting mode or target machine mode, the migration scenario is generally set to 3 by default, and the disaster recovery scenario is set as needed.

- Some storage types only support one snapshot, so the parameter is set to 3. Only one

snapshot can be saved on some storages.

Start window

The time to start synchronization,default is to execute immediately.

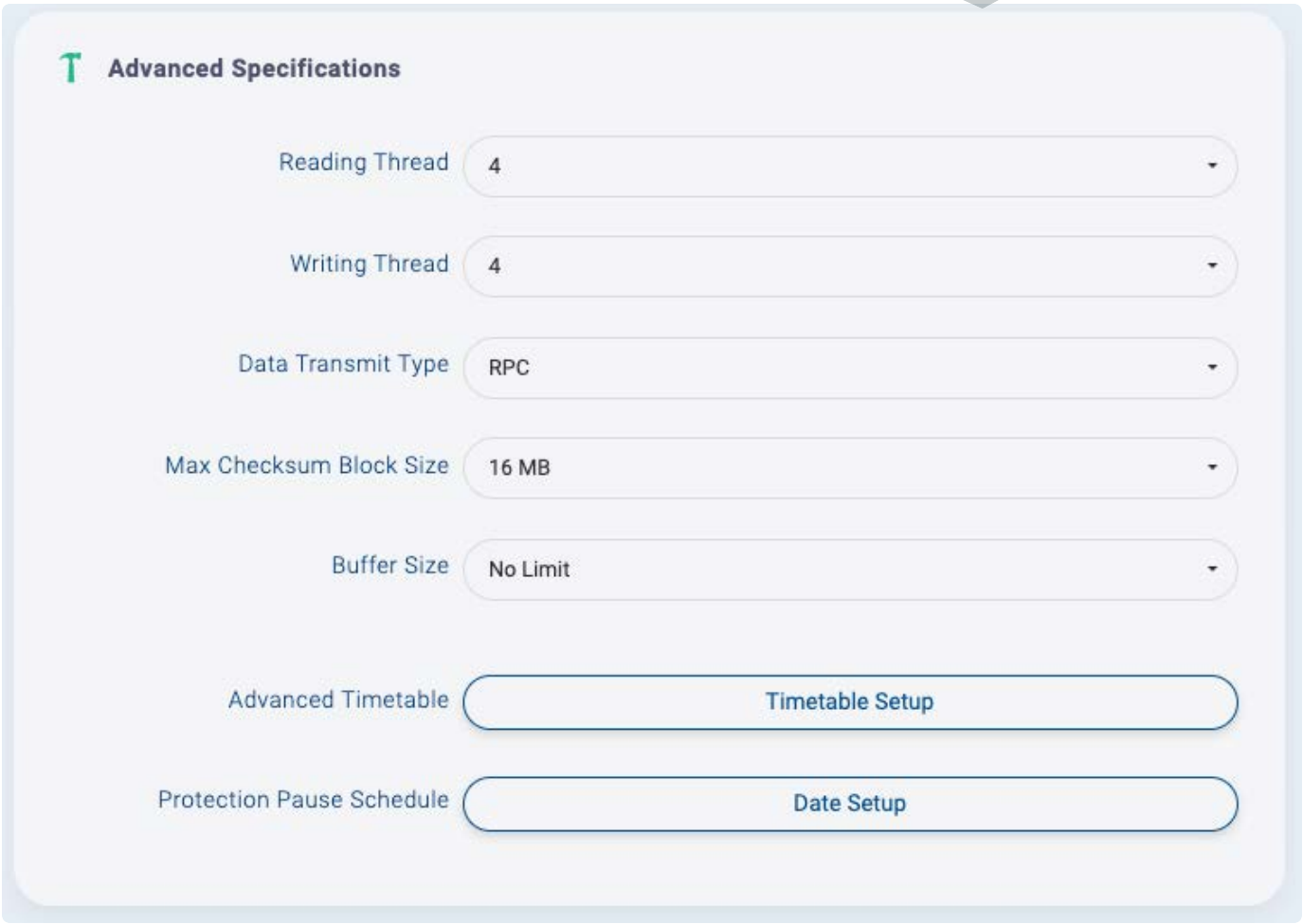
If this parameter is set when creating a task, the preparation work will be completed after the task is submitted, and the data will be transmitted at the specified time.

Modify this parameter for the created task. If synchronization is in progress, the next synchronization time will be the specified time.

Notice:

- **When the set time is in the past, it will be executed immediately. **
- **When the set time is in the future, the data will be synchronized again at the specified time. **
- **When the task is manually aborted, synchronization will not be initiated at the specified time.**

Advanced process settings



Read level

The number of threads to read data, the maximum is 8, The default is 4.

The larger the number of threads, the faster the source machine data can be read, but it will consume a little more source machine CPU resources.

Lower level

The number of threads for writing data, the maximum is 8, default is 4.

The larger the number of threads, the faster the data is written to the target machine, but it will consume a little more CPU resources of the target machine.

Transmission mode

The mode for transmitting data, default is RPC.

NEXAVM

RPC_SSL encrypted transmission is optional. Since encryption and decryption are required, the transmission efficiency will be lower.

Optional HTTPS transmission is reserved for compatibility with some older versions and is generally not used.

Check unit

The difference compares the block size during transmission, whichdefaults to 16M.

When the amount of data is large, it is recommended to change it to 32M.

When doing differential transfer:

- The larger the block, the faster the target block information is calculated, but the amount of difference transmitted will be greater.
    - Taking 32M as an example, if the source machine has a 1KB data change, it will also transmit 32M.
- The smaller the block, the slower it is to calculate the target block information, but the amount of difference transmitted will be smaller.
    - Taking 4M as an example, if the source machine has a 1KB data change, only 4M will be transmitted.

cache

The size of space used to cache block data, is unlimited by default.

Migration projects, general use without restrictions;

The size of the disaster recovery project can be planned based on the number of parallel tasks and the disk size of the transit data gateway.

- If you don't want to worry about planning, you can directly choose 30G.

Advanced strategy window

You can choose the time at which synchronization is initiated.The selected time is the time when synchronization is allowed.

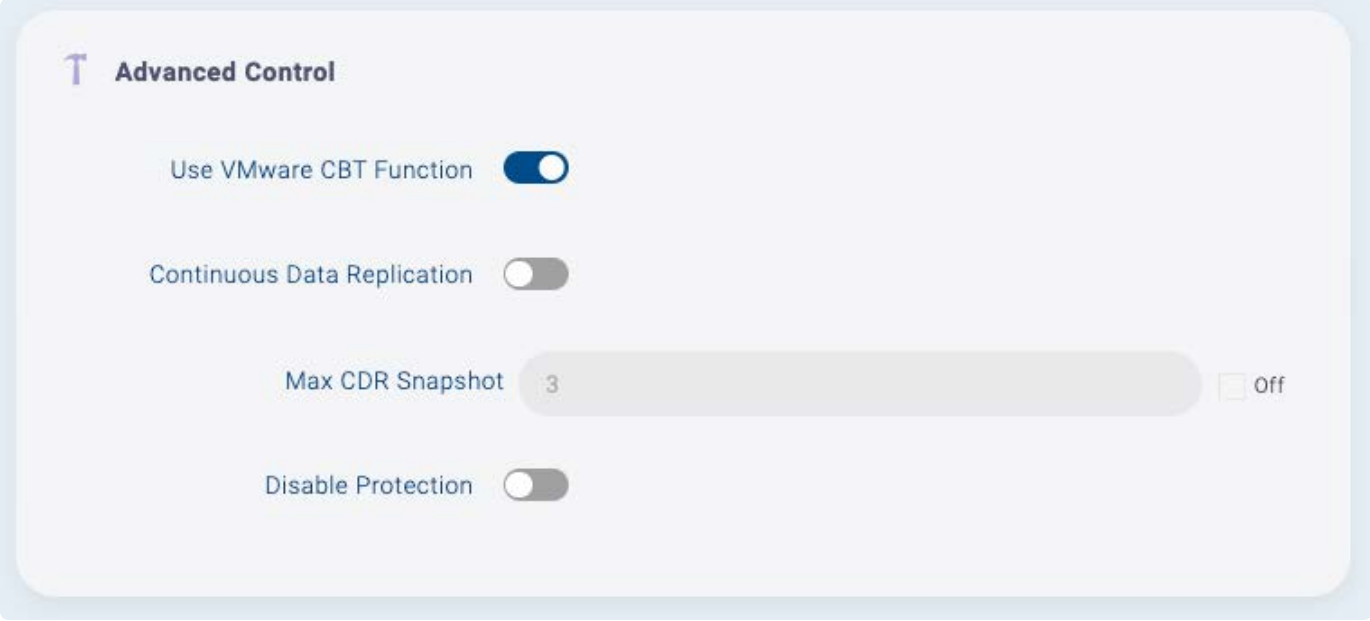
Note: It only controls the time when synchronization is initiated. When synchronization takes a long time, the synchronization end time may not be within the selected time window.

Skip policy date

You can specify which dates do not want to be synchronized.

Advanced control





Exclude files/folders

This parameter is only available if the agent is installed on the source host.

You can choose which files or folders you don't want to sync to the target.

Using the VMware CBT feature

This parameter is available only because the source host is VMware agentless.

VMware CBTis a VMkernel feature that tracks changes in a virtual machine's storage blocks over time. The default is on.

Enable: VMware CBT records blocks with data changes and only transmits blocks with data changes. The transmission efficiency is relatively high.

Close: Skip VMware CBT and record the hash value of the data at the transit data gateway. Compared with differential transmission, the transmission efficiency is lower and is suitable for VMware CBT errors.

Notice:

- The single scope of VMware CBT is the VMDK disk file. One virtual machine may use CBT normally, while another virtual machine may use CBT abnormally.

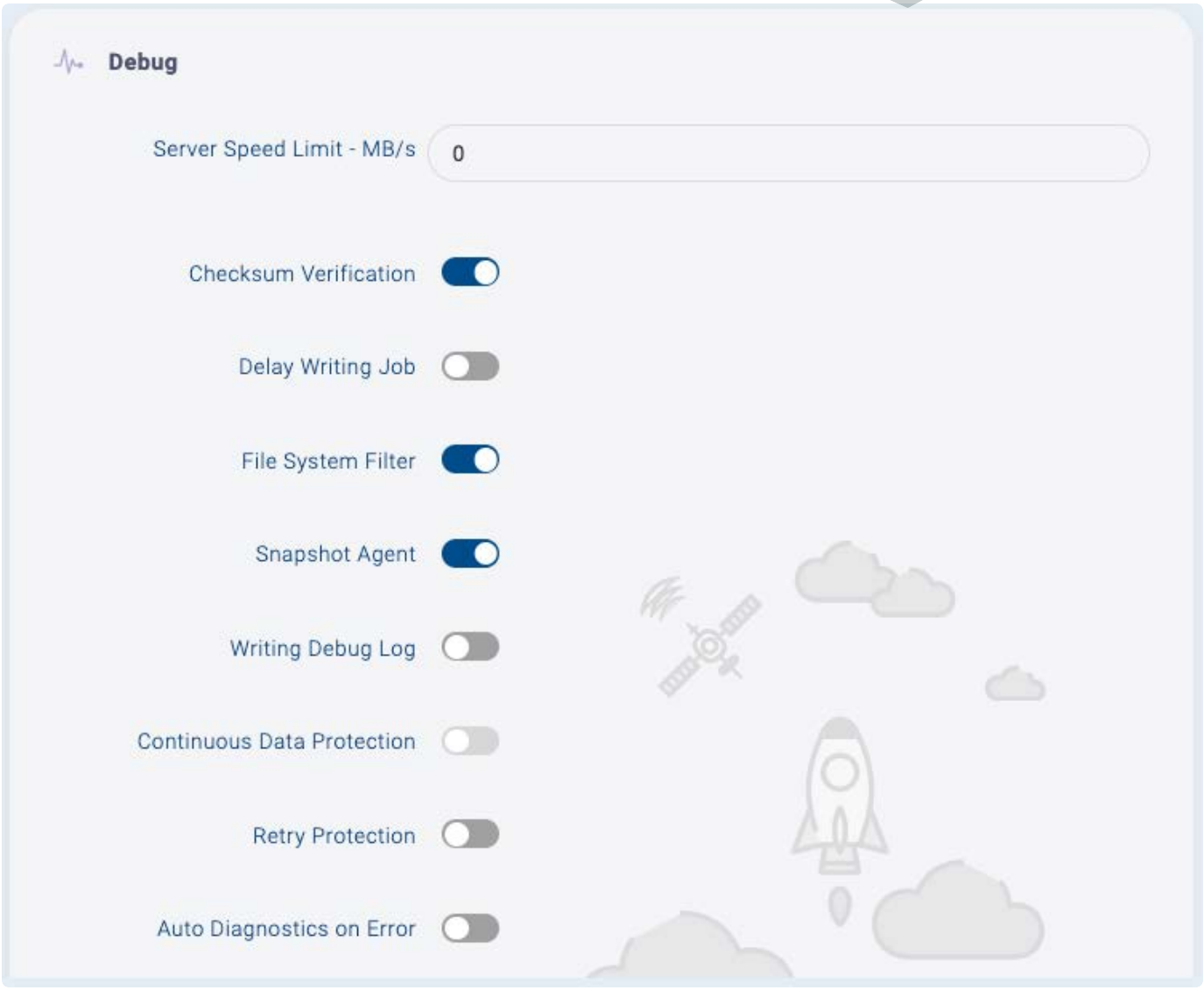
client compression

The source host compresses the data before transmitting it. is turned off by default.

Compression requires very little CPU resources on the source host. However, when the source host's CPU resources are tight, it is recommended to turn off this function.

The compression of text data is relatively high; the compression of pictures and videos is relatively low.

Troubleshooting



snapshot agent

Synchronize using snapshot mode, enabled by default.

Windows source machine:

- When the snapshot agent is enabled, the system's VSS will be called to take snapshots for synchronization tasks during synchronization.
- Turn off the snapshot agent, and the checkpoint function of the software will be called during synchronization to perform synchronization tasks.

Linux source machine:

- Turn on the snapshot agent, and during synchronization, the software's Driver will be called to take snapshots for synchronization tasks.
- Turn off the snapshot agent. During synchronization, the driver's snapshotless mode will be

called to perform synchronization tasks.

- This feature is still in closed beta.

Intelligent filtering of client data

File filtering, is enabled by default.

Enabling it will filter deleted files, virtual memory, SWAP and other files, and synchronize data based on the block information provided by the disk header information.

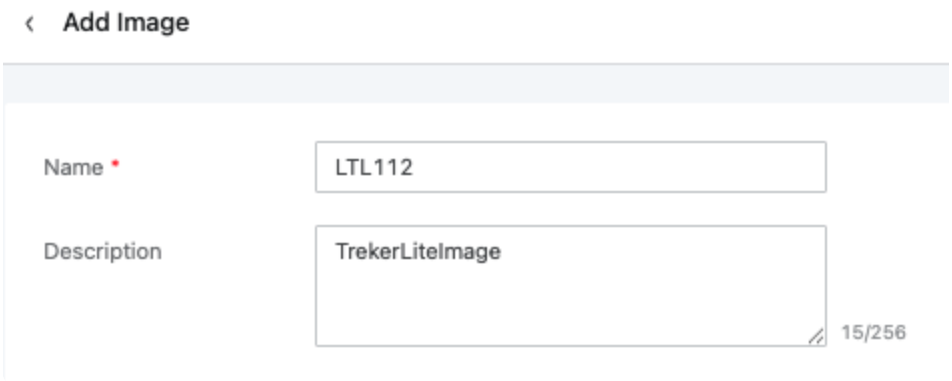
Turning it off will synchronize deleted files, virtual memory, SWAP and other files to the target machine, and will copy the block files of the entire disk, resulting in longer synchronization time.

If the source host's disk has a superblock error and chkdsk has not been performed for a long time, resulting in a switch failure or abnormal switch, this function can be turned off.

Upload the image of BootImage (Treker Lite)

Operation steps

1. It is recommended that the image enable virtio.
2. It is recommended to upload two images each of LTL (Linux Treker Lite) and WTL (Windows Treker Lite), and set the BIOS mode to UEFI and Legacy respectively.
3. Platform and system versionDo not select Other.
4. The image format must be qcow2, and ISO can be used in full manual mode.
5. Fill in the introduction correctly: TrekLiteImage, **case sensitive**.

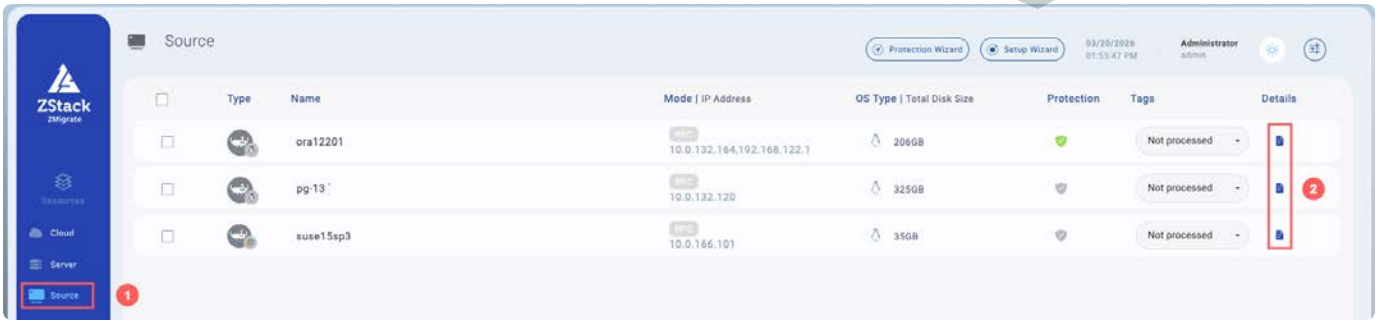


Things to note

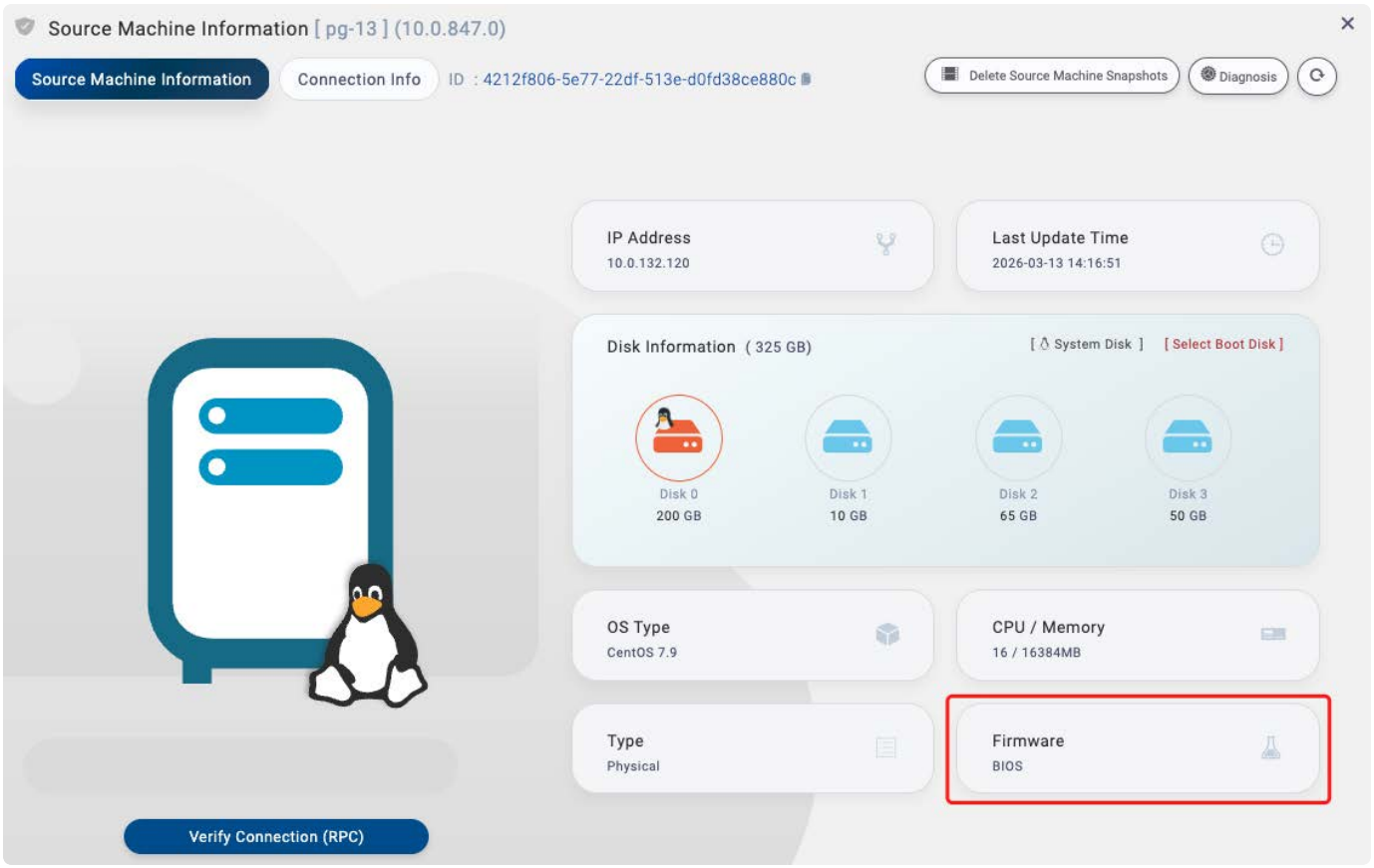
When creating a synchronization task, **filter images with the same BIOS mode based on the BIOS mode of the source host**.

Check the BIOS mode of the source host

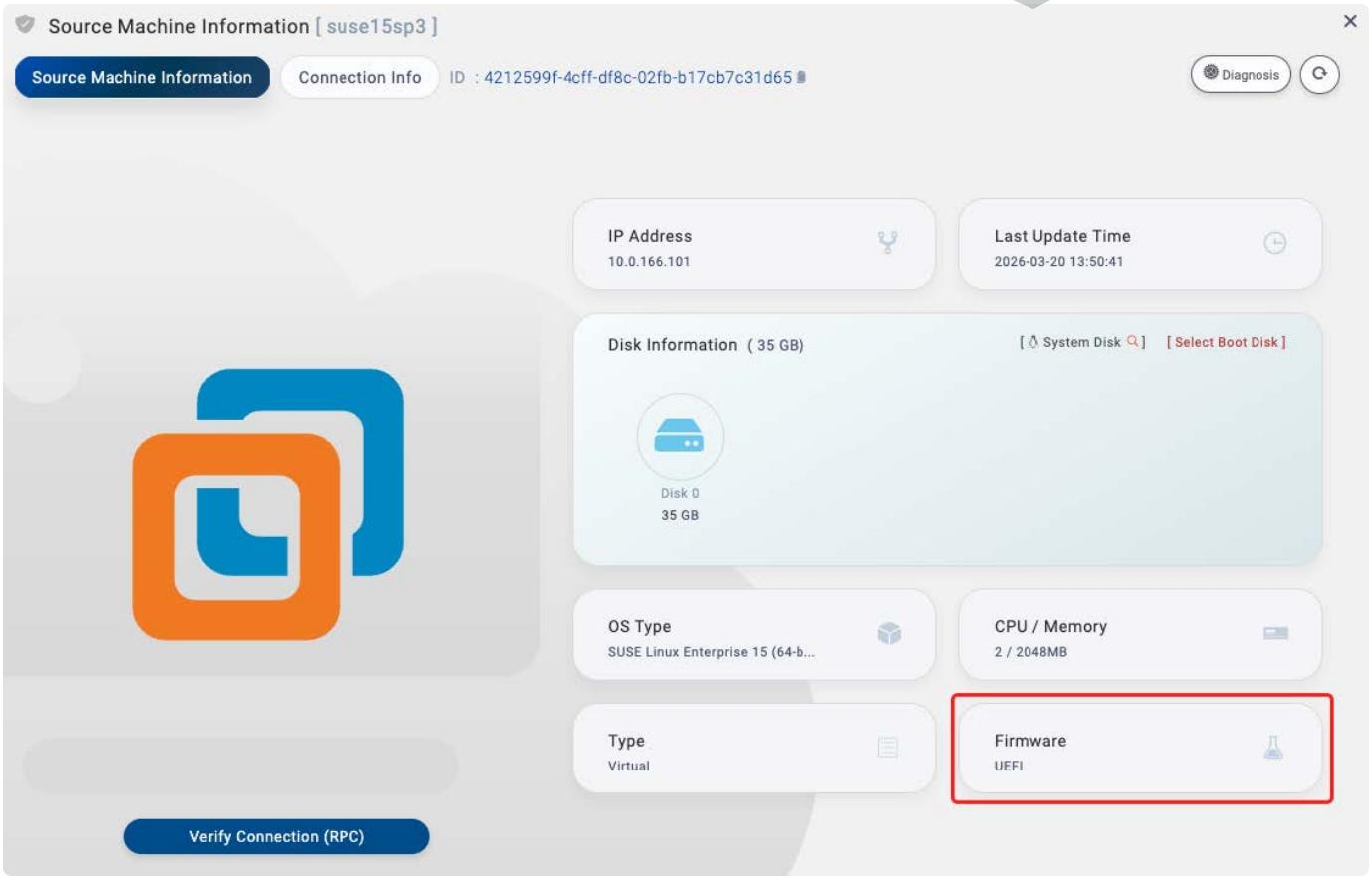
The BIOS mode of the source host can be viewed in the management console --> Resources --> Source host --> Details.



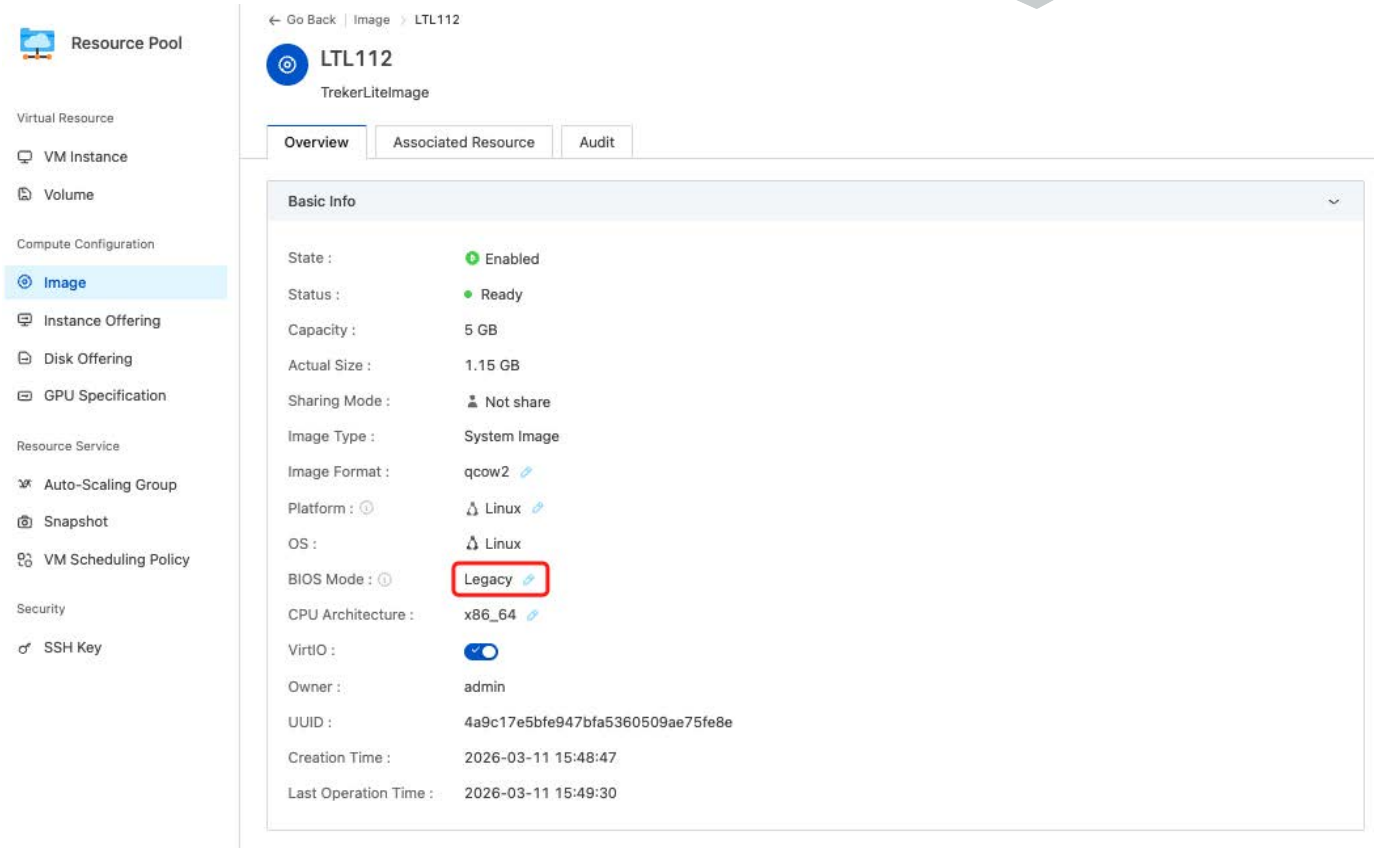
- BIOS=Legacy, requires using legacy mode target image.

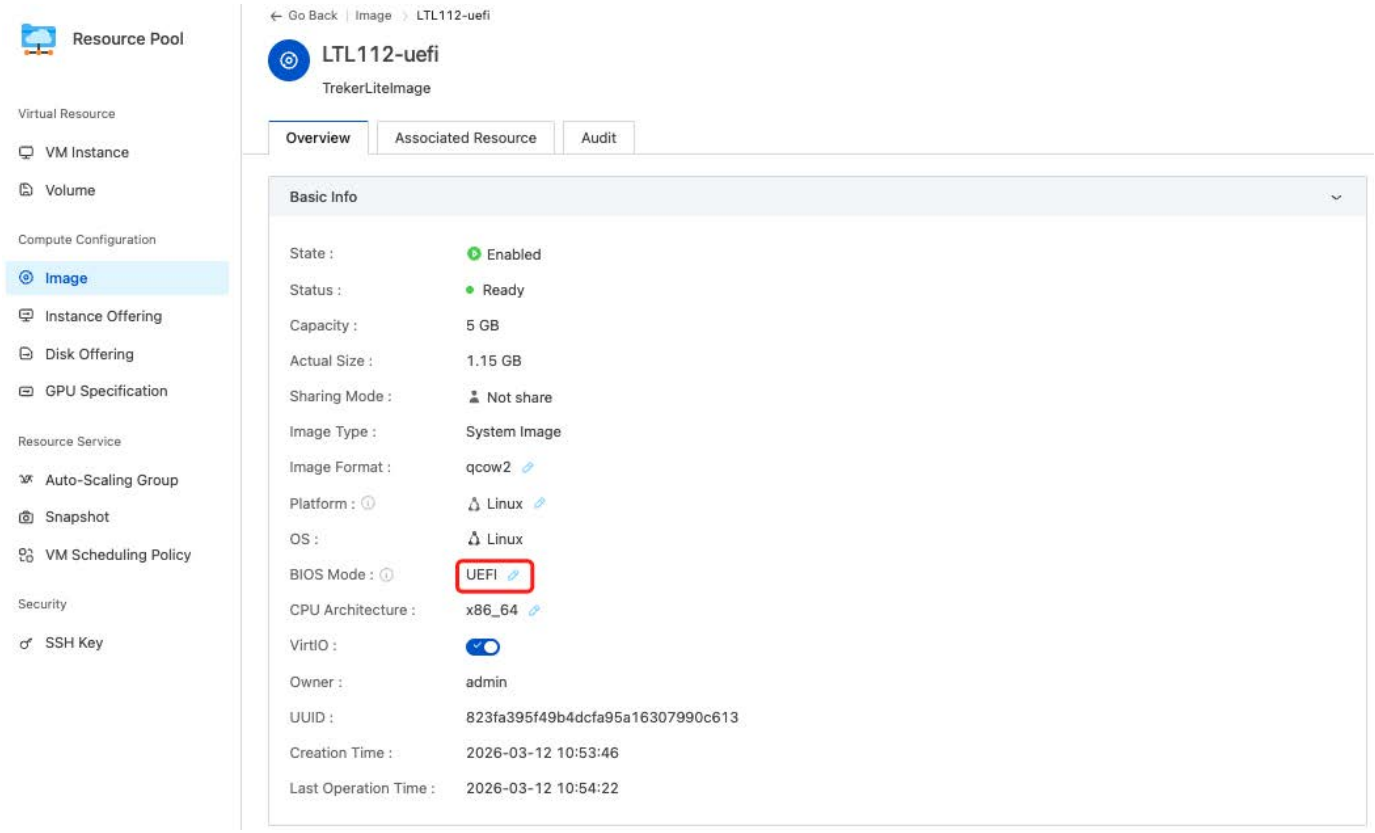


- UEFI=UEFI, you need to use the target image in UEFI mode.



Check the BIOS mode of the target image


Resource Pool
Virtual Resource
VM Instance
Volume
Compute Configuration
Image
Instance Offering
Disk Offering
GPU Specification
Resource Service
Auto-Scaling Group
Snapshot
VM Scheduling Policy
Security
SSH Key
Go Back | Image | LTL112
LTL112
TrekerLiteImage
Overview
Associated Resource
Audit
Basic Info
State : Enabled
Status : Ready
Capacity : 5 GB
Actual Size : 1.15 GB
Sharing Mode : Not share
Image Type : System Image
Image Format : qcow2
Platform : Linux
OS : Linux
BIOS Mode : Legacy
CPU Architecture : x86_64
VirtIO :
Owner : admin
UUID : 4a9c17e5bfe947bfa5360509ae75fe8e
Creation Time : 2026-03-11 15:48:47
Last Operation Time : 2026-03-11 15:49:30


Resource Pool
Virtual Resource
VM Instance
Volume
Compute Configuration
Image
Instance Offering
Disk Offering
GPU Specification
Resource Service
Auto-Scaling Group
Snapshot
VM Scheduling Policy
Security
SSH Key
Go Back | Image | LTL112-uefi
LTL112-uefi
TrekerLiteImage
Overview
Associated Resource
Audit
Basic Info
State : Enabled
Status : Ready
Capacity : 5 GB
Actual Size : 1.15 GB
Sharing Mode : Not share
Image Type : System Image
Image Format : qcow2
Platform : Linux
OS : Linux
BIOS Mode : UEFI
CPU Architecture : x86_64
VirtIO :
Owner : admin
UUID : 823fa395f49b4dcfa95a16307990c613
Creation Time : 2026-03-12 10:53:46
Last Operation Time : 2026-03-12 10:54:22

Migrate One-Page-Guide Streamline

Agentless scenario

1. Download the server media and target machine image.
2. Upload the target machine image to NexaVM.
3. Install the Migration Management Console (Admin Console).
4. Register the relay to the management console.
5. Register NexaVM to the management console.
6. Register VMware to the management console.
7. Register the source host on the management console (multiple choices available).
8. Create a synchronization task.
9. Incremental sync on demand.
10. Create a switching task.
11. Verify system operations.

Agent installation scenario

1. Download agent software media, server media, and target machine image.
2. Upload the target machine image to NexaVM.
3. Install the Migration Management Console (Admin Console).
4. Register the relay to the management console.
5. Register NexaVM to the management console.
6. The source machine installs agent software.
7. Register the source host on the management console.
8. Create a synchronization task.
9. Incremental sync on demand.
10. Create a switching task.
11. Verify system operations.

Migrate One-Page-Guide Details

Agentless scenario

1. Download the server media and target machine image.
    - Server media: TrekerInstall.exe, LinuxTreker.qcow2
        - The Windows version is an exe installation package.
        - The Linux version is a mirror of qcow2. After installation, the IP is configured and used out of the box.
    - Target machine image：
        - Windows version: Treker**Lite**.qcow2
        - Linux version: LinuxTreker**Lite**.qcow2
        - It can be used cross-wise, but it is recommended to use the Win target image for the Win source host and the Linux target image for the Linux source host.
2. Upload the target machine image to NexaVM.
    - Mirrors are available in Linux and Windows versions
        - WTL: Treker**Lite**.qcow2 (uploaded twice, configure Legacy and UEFI respectively)
        - LTL: LinuxTreker**Lite**.qcow2 (uploaded 2 times, configure Legacy and UEFI respectively)
3. Install the migration management console.
    - Choose Linux version or Windows version as needed.
        - Windows: Double-click TrekerInstall.exe in Windows 2016 system and check Management.
        - Linux: Upload LinuxTreker.qcow2 and create a cloud host. Set the system disk size as needed. It is recommended to be larger than 100G.
4. Register the relay to the management console.
    - Register the data gateway in the resources of the management console
        - A management console can be added natively to the data gateway. (not recommended)
        - You can create a new server (uncheck Management) and add it to the data gateway. (Recommended👍)

5. Register NexaVM to the management console.
    - Register the NexaVM cloud platform information in the target end of the management console.
6. Register VMware to the management console.
    - Register VMware ESXi or VMware vCenter on the target side of the management console.
    - **When registering VMware to the management console, please select the Windows version to bind the data gateway**.
7. Register the source host on the management console (multiple choices available).
    - Select **VMware Agentless** in the source host of the management console, select the transit node bound to VMware, and check the VM to be migrated.
8. Create a synchronization task.
9. Incremental sync on demand.
10. Create a switching task.
11. Verify system operations.

Agent installation scenario

1. Download agent software media, server media, and target machine image.
    - Agent software media:
        - Windows version: AntennaInstall.exe.
        - Linux version: all_antenna–..tar.gz
    - Server media: TrekerInstall.exe, LinuxTreker.qcow2
        - The Windows version is an exe installation package.
        - The Linux version is a mirror of qcow2. After installation, the IP is configured and used out of the box.
    - Target machine image:
        - Windows version: Treker**Lite**.qcow2
        - Linux version: LinuxTreker**Lite**.qcow2
        - It can be used cross–wise, but it is recommended to use the Win target image for the Win source host and the Linux target image for the Linux source host.
2. Upload the target machine image to NexaVM.

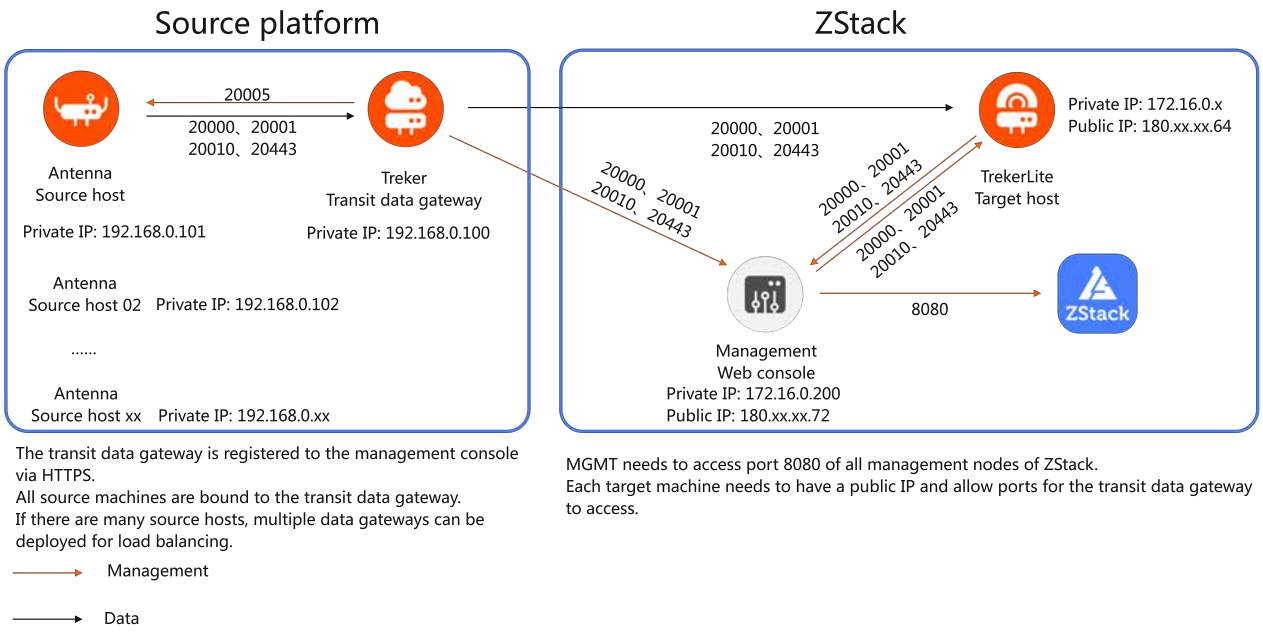
- Mirrors are available in Linux and Windows versions
  - WTL: Treker**Lite**.qcow2 (uploaded twice, configure Legacy and UEFI respectively)
  - LTL: LinuxTreker**Lite**.qcow2 (uploaded 2 times, configure Legacy and UEFI respectively)

3. Install the Migration Management Console (Admin Console).
   - Choose Linux version or Windows version as needed.
     - Windows: Double-click TrekerInstall.exe in Windows 2016 system and check Management.
     - Linux: Upload LinuxTreker.qcow2 and create a cloud host. Set the system disk size as needed. It is recommended to be larger than 100G.
4. Register the relay to the management console.
   - Register the data gateway in the resources of the management console
     - A management console can be added natively to the data gateway. (not recommended)
     - You can create a new server (uncheck Management) and add it to the data gateway. (Recommended👍)
5. Register NexaVM to the management console.
   - Register the NexaCloud platform information in the target end of the management console.
6. The source host installs agent software.
   - Install the corresponding agent software on the source machine.
7. Register the source host on the management console.
   - Select the corresponding operating system in the source host of the management console, enter the source host IP, and verify the addition.
8. Create a synchronization task.
9. Incremental sync on demand.
10. Create a switching task.
11. Verify system operations.

[HTTPS Registration]-Network architecture for public network migration and disaster recovery

Document Category: Product Related Experience

Topology map



network planning

The transit data gateway uses HTTPS mode to register, and the management console and each target machine need to use public IP.

Number of public IPs required: 1 (management console) + N (number of target machines)

Serial number	Role	Deployment location	Registration method	Intranet IP	Public IP	Release port
1	Source Host	Source Platform	RPC	192.168.0.101	–	20005
2	Data Gateway	Source Platform	HTTPS	192.168.0.100	–	20000, 20001, 20010, 20443.
3	Management Console	Target Cloud Platform	–	172.16.0.200	180...72	20000, 20001, 20010, 20443.
4	Target Cloud Platform	–	–	–	–	8080
5	Target host	Target cloud platform	RPC	172.16.0.*	180...64	20000, 20001, 20010, 20443.

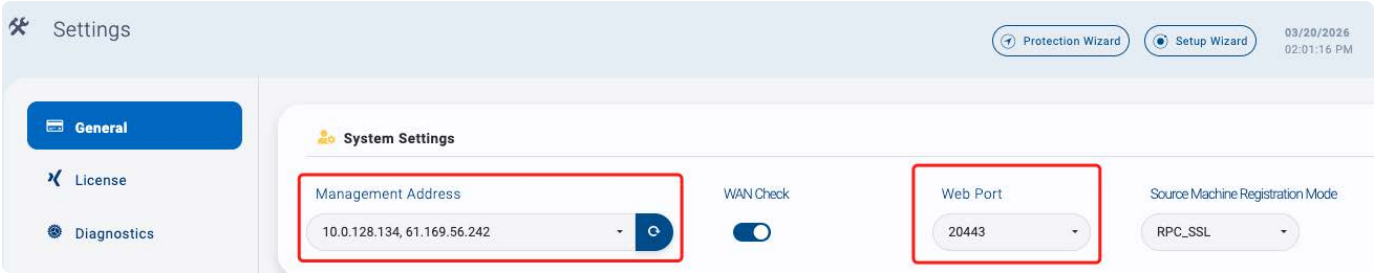
Confirm that the preparation environment is ready

1. The management console has been assigned a public IP.
2. The NexaCloud platform has been configured with a shared network.
3. The corresponding ports have been released.
    - Refer to the topology diagram for the release direction.

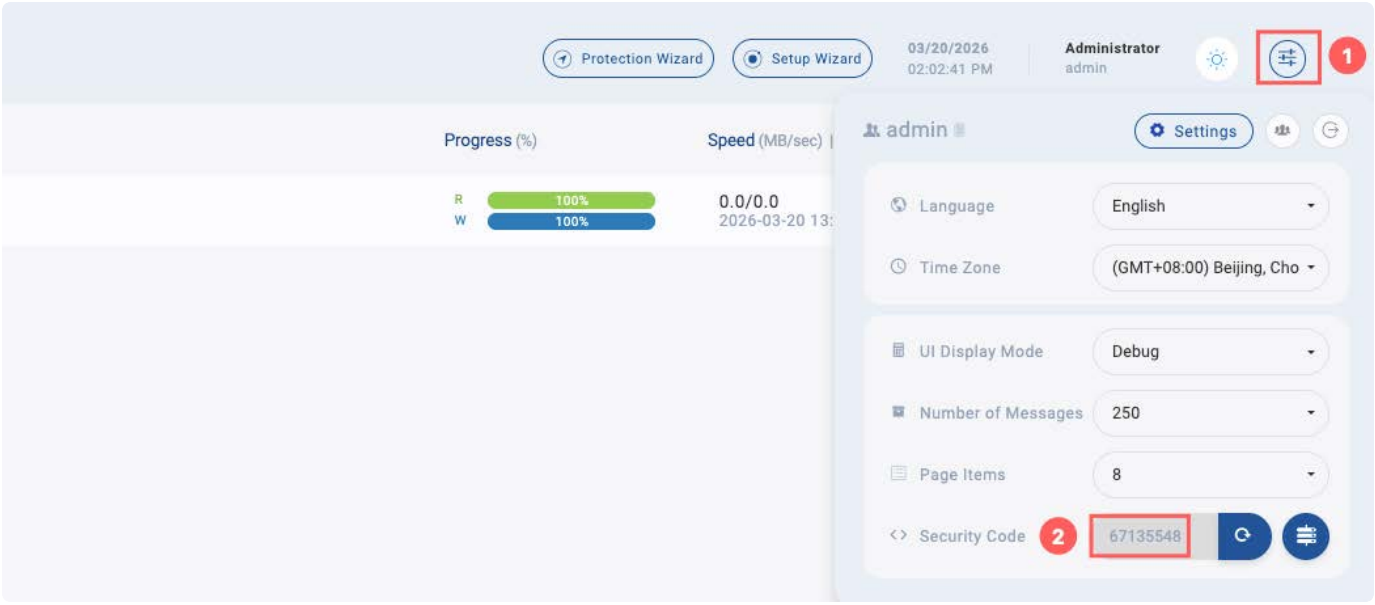
Operation steps

1. Configure the management console and confirm that the central control IP and port have been set correctly.

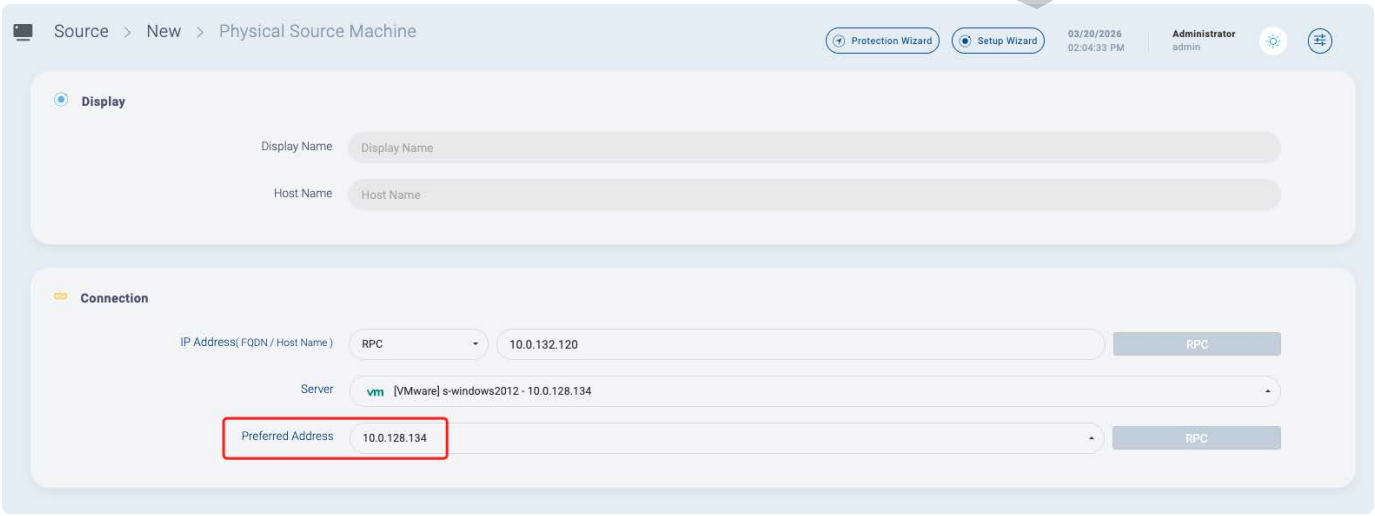
- Check at least the internal IP and public IP in the central control IP.
- The port is set to 20443.



2. Record the public IP, central control port, and security verification code of the management console.
   - **Example public IP:**180.xx.xx.72
   - **Example central control port:**20443
   - **Example security verification code: **72421233



3. Add a transit data gateway.
   - HTTPS mode, connecting to the management console from within the data gateway's system.
   - The HTTPS registration steps for Windows data gateway and Linux data gateway are different. Please refer to `HTTPS registration data gateway` at the end of this knowledge base.
4. Add the source host.
   - In RPC mode, you can add the source host directly from the management console.
   - In Data Gateway IP, select an IP address that can communicate with the source host.

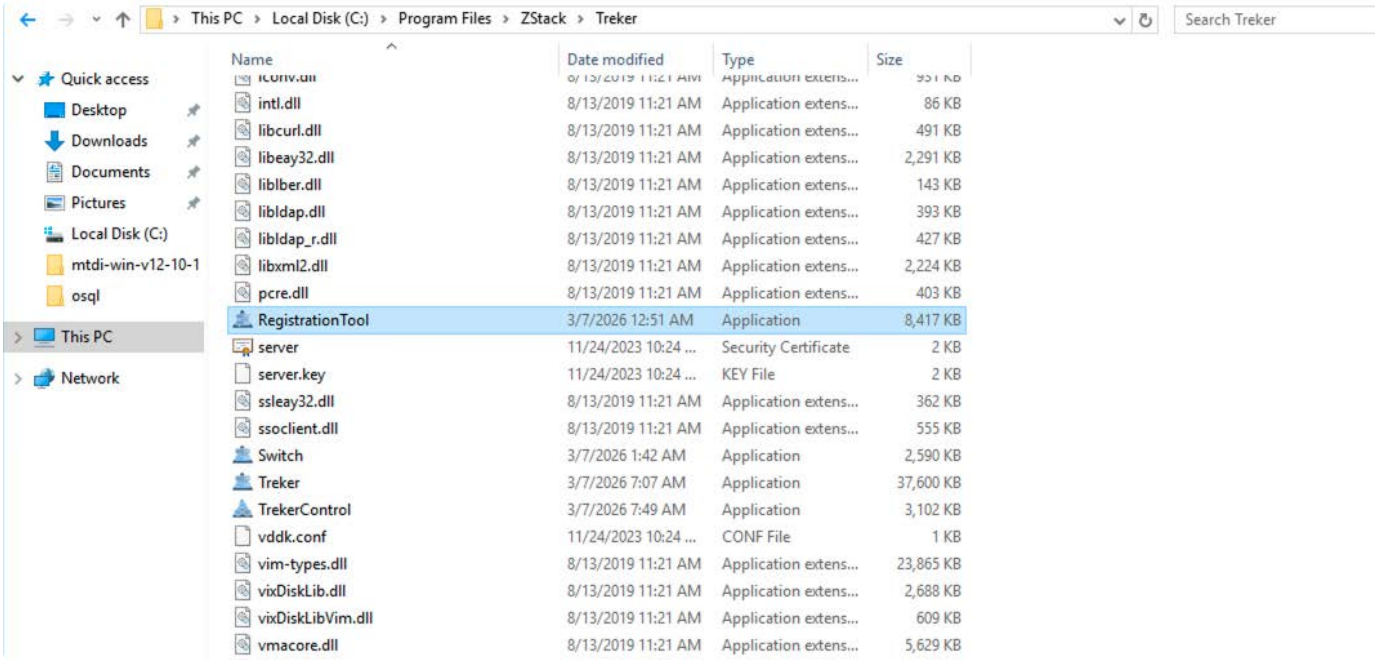


5. Add a cloud platform.
6. Create a synchronization task.
7. Create a switching task.

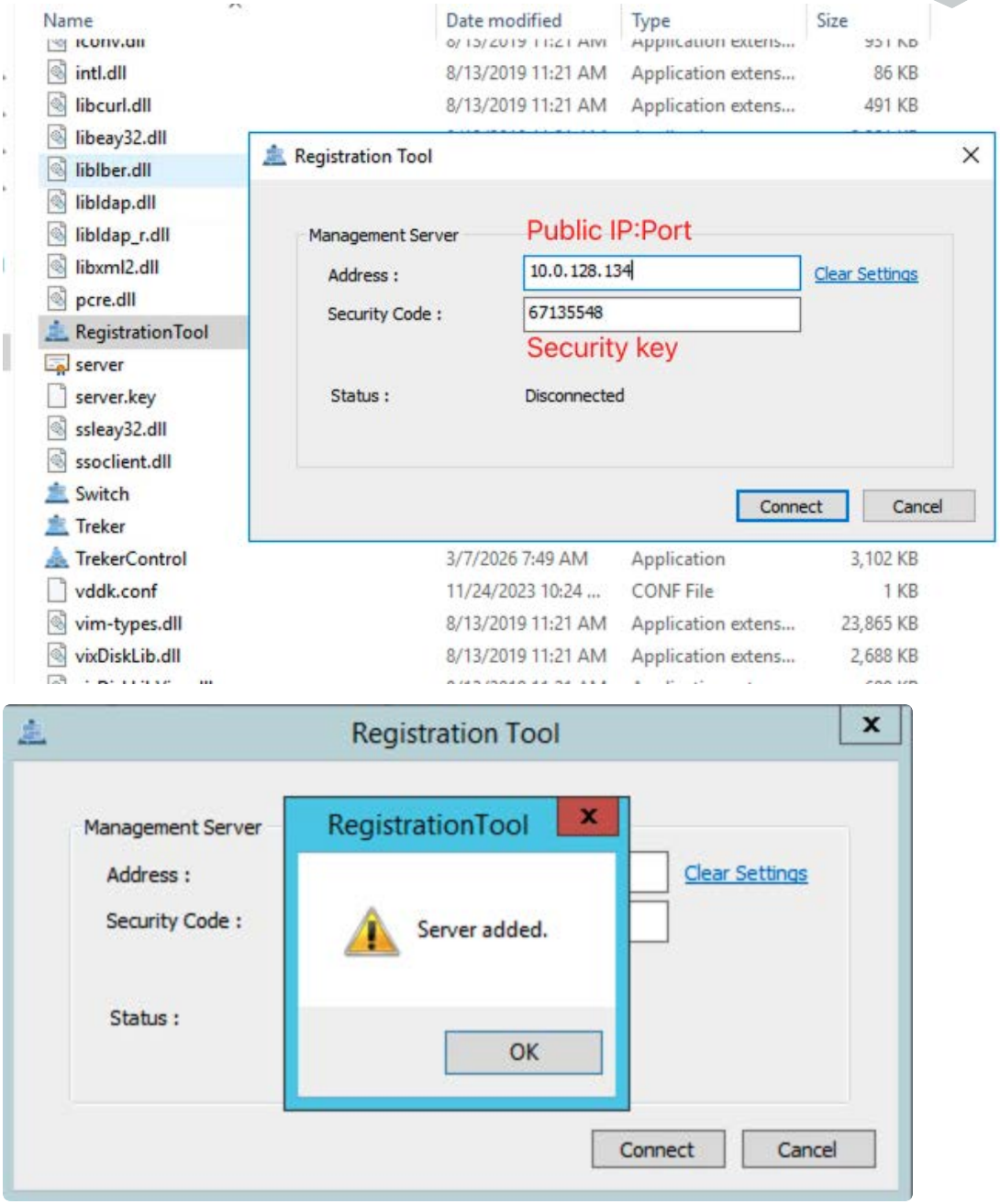
HTTPS registration data gateway

Windows version data gateway registers to the management console in HTTPS mode

Find `RegistrationTool` in the installation path (default path: C:\Program Files\ZStack\Treker) and double-click to run it.

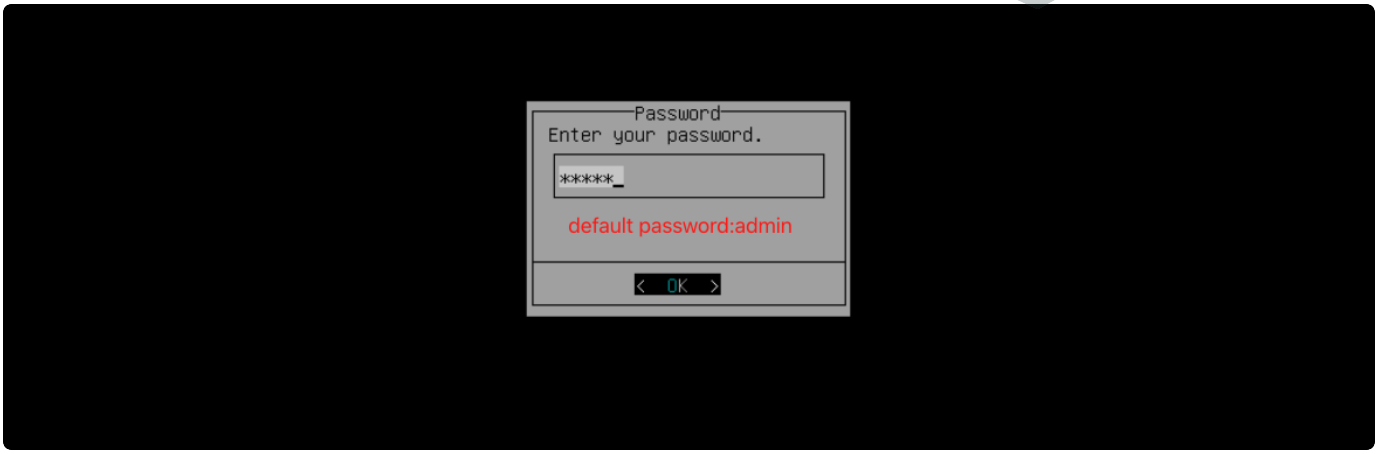


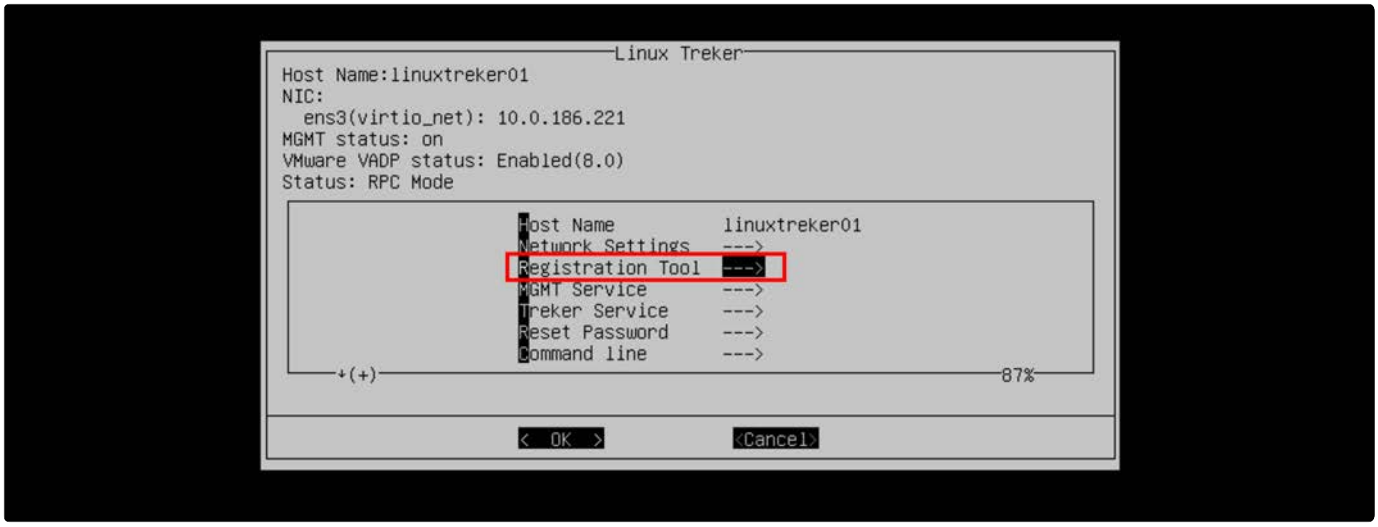
Fill in based on the actual information in the management console!



The Linux version data gateway is registered to the management console in HTTPS mode

Enter the UI console of the Linux data gateway. The default password is admin.


Password
Enter your password.
*****_
default password:admin
< OK >


Linux Treker
Host Name:linuxtreker01
NIC:
ens3(virtio_net): 10.0.186.221
MGMT status: on
VMware VADP status: Enabled(8.0)
Status: RPC Mode
Host Name linuxtreker01
Network Settings --->
Registration Tool --->
MGMT Service --->
Treker Service --->
Reset Password --->
Command line --->
+(+)
87%
< OK >
<Cancel>

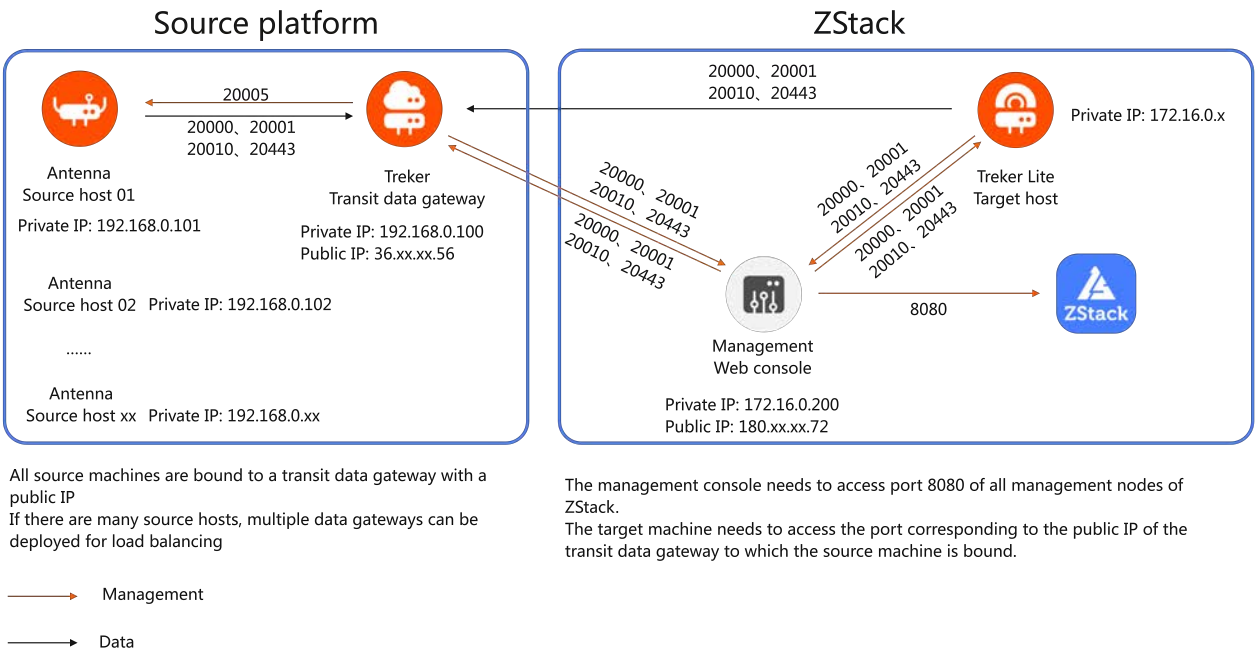

Registration Tool
: disconnected
:
public ip:port
Host Name/ IP Address: 10.0.128.134
Security Code: ********_ security code
<Connect>
<Cancel >


Registration Tool
Server added.
< OK >

[RPC Registration]-Network architecture for public network migration and disaster recovery

Document Category: Product Related Experience

Topology map



network planning

The transit data gateway is registered using RPC mode, and the management console and data gateway need to use public IP.

Number of public IPs required: 1 (management console) + N (number of transit data gateways)

Serial number	Role	Deployment location	Registration method	Intranet IP	Public IP	Release port
1	Source Host	Source Platform	RPC	192.168.0.101	–	20005
2	Data Gateway	Source Platform	RPC	192.168.0.100	36...56	20000, 20001, 20010, 20443.
3	Management Console	Target Cloud Platform	–	172.16.0.200	180...72	20000, 20001, 20010, 20443.
4	Target Cloud Platform	–	–	–	–	8080
5	Target Host	Target Cloud Platform	RPC	172.16.0.*	–	20000, 20001, 20010, 20443.

Confirm that the preparation environment is ready

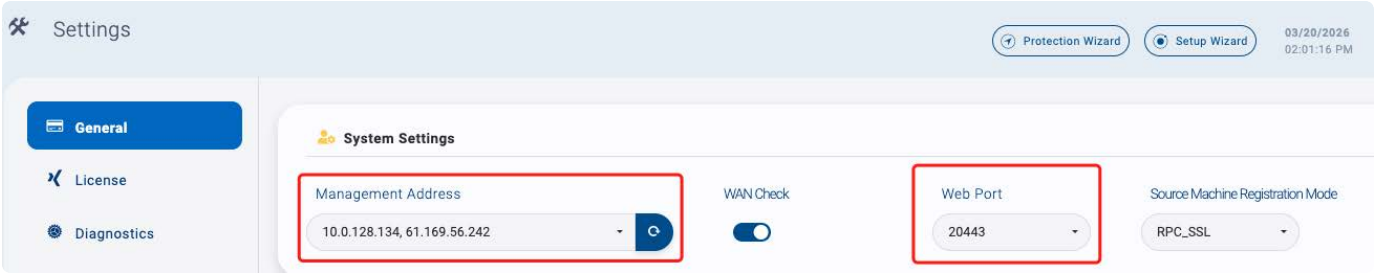
1. The management console has been assigned a public IP.
2. The transit data gateway has been assigned a public IP.
3. The corresponding ports have been released.
    - Refer to the topology diagram for the release direction.

Operation steps

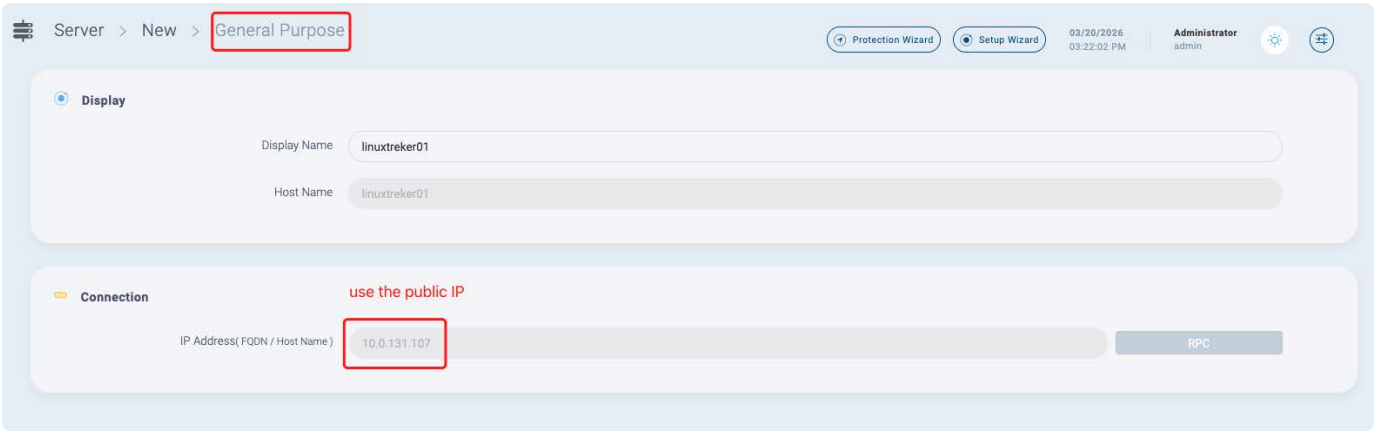
1. Configure the management console and confirm that the central control IP and port have

been set correctly.

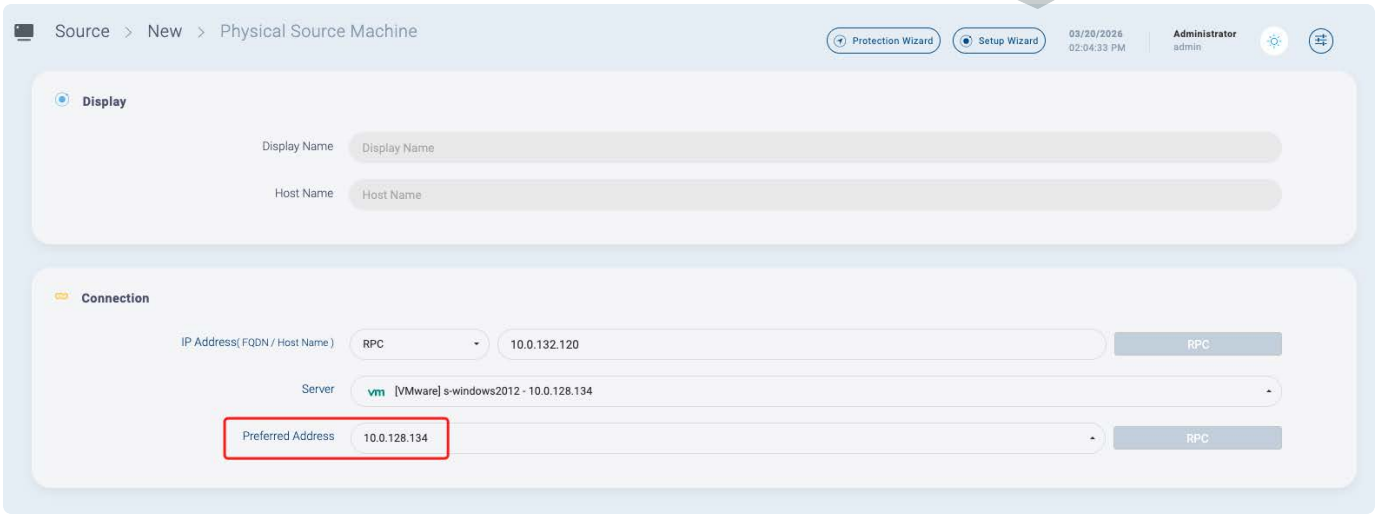
- Check at least the internal IP and public IP in the central control IP.
- The port is set to 20443.



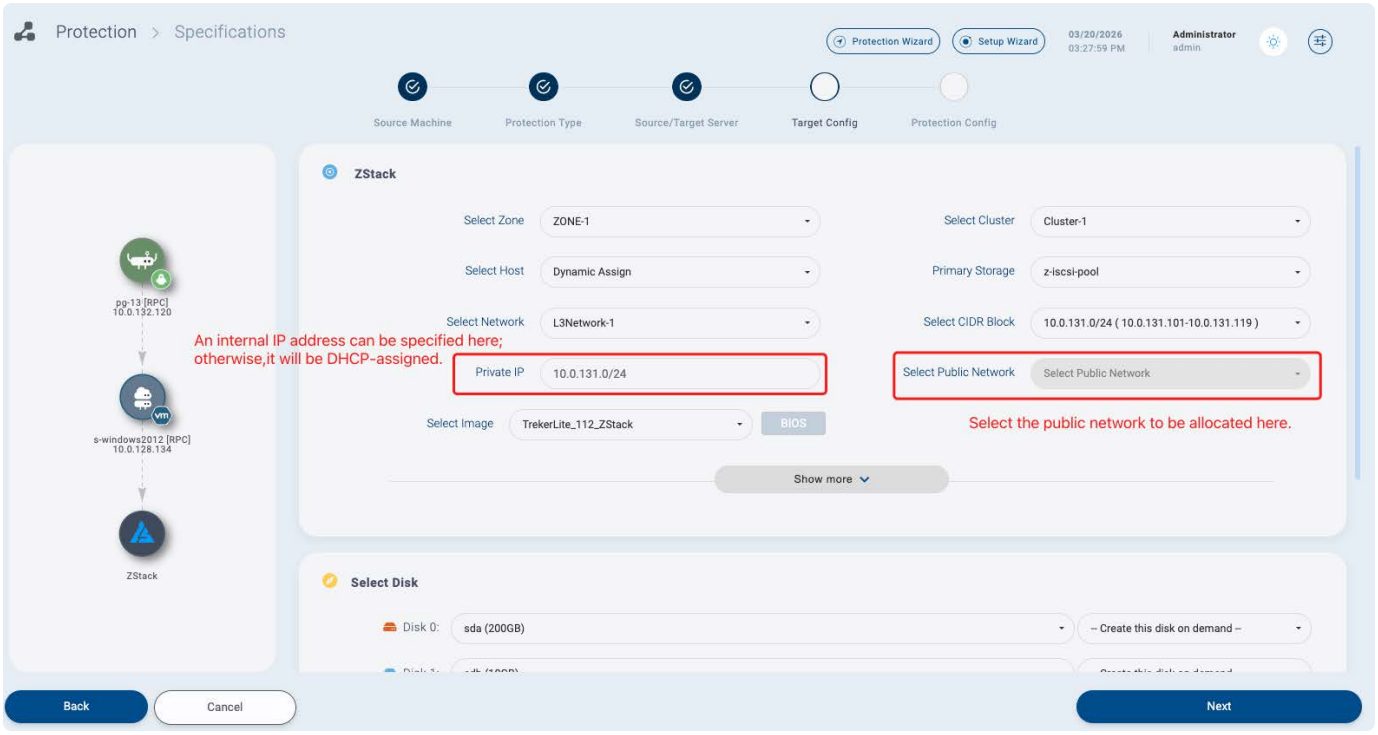
2. Add a transit data gateway.
   - In RPC mode, just enter the transit data gateway and add it directly from the management console.
   - Use the public IP to add, and manually add the internal IP (separated by English commas).



3. Add the source host.
   - In RPC mode, you can add the source host directly from the management console.
   - In Data Gateway IP, select an IP address that can communicate with the source host.



4. Add a cloud platform.
5. Create a synchronization task.
    - When creating a task, you need to assign a public IP to the target machine.



6. Create a switching task.

Use NexaVM API for migration when the target network does not have DHCP

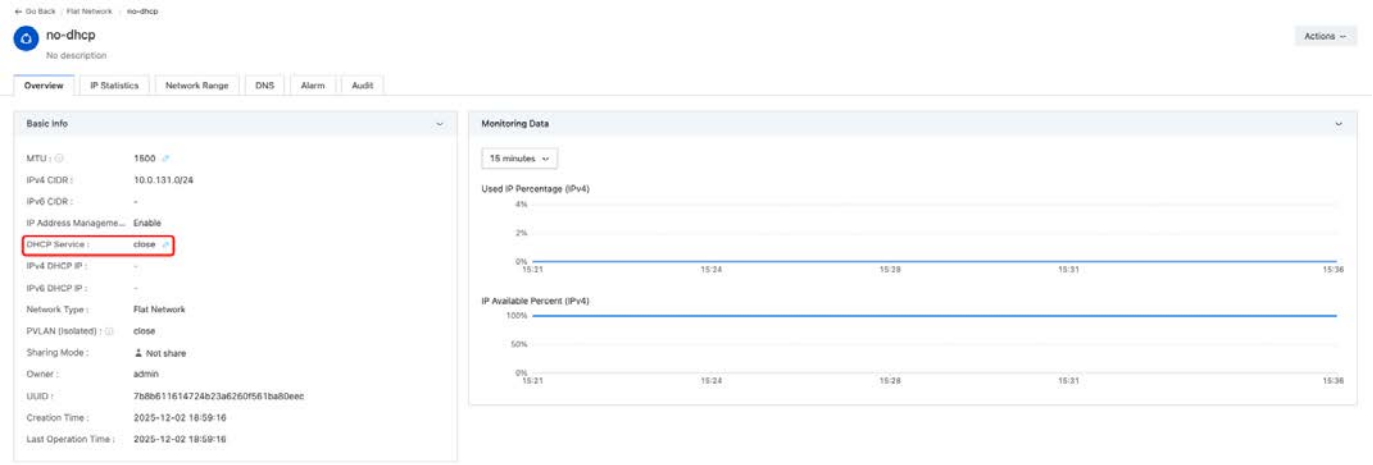
Document Category: Product Related Experience

Write in front

**This solution is an emergency solution and is not recommended as a regular implementation solution. **

Applicable scenarios

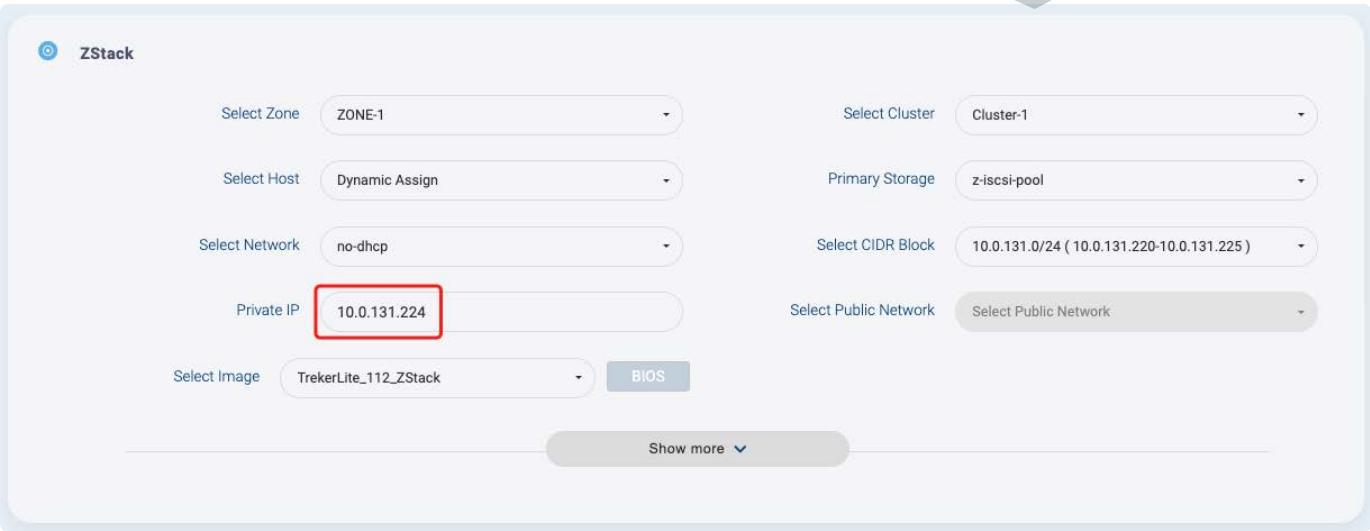
The subnet of the NexaVM platform does not have DHCP enabled and is not allowed to create a temporary migration network with DHCP enabled.



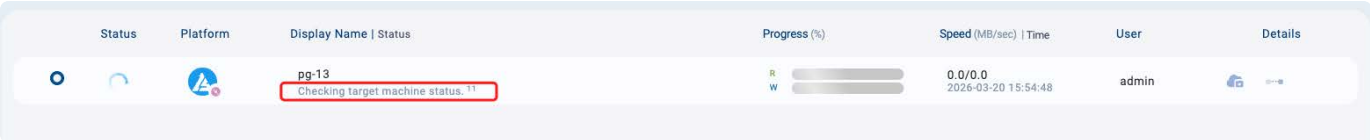
Operation steps

1. Create a synchronization task and specify an IP address when configuring the target machine parameters.

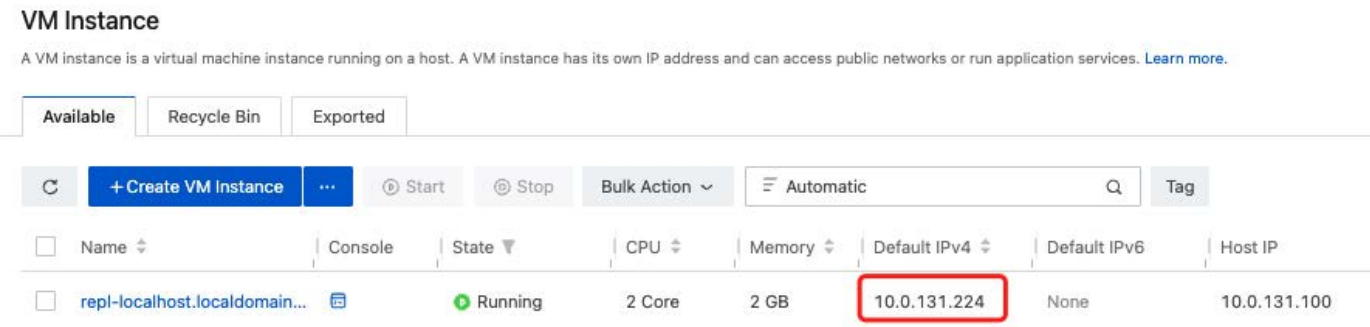
- Take 10.0.131.224 as an example.



2. Observe the information progress of the synchronization task.
3. When the information progress reaches "Checking the status of the target machine.", switch the browser page to the NexaVM cloud platform.

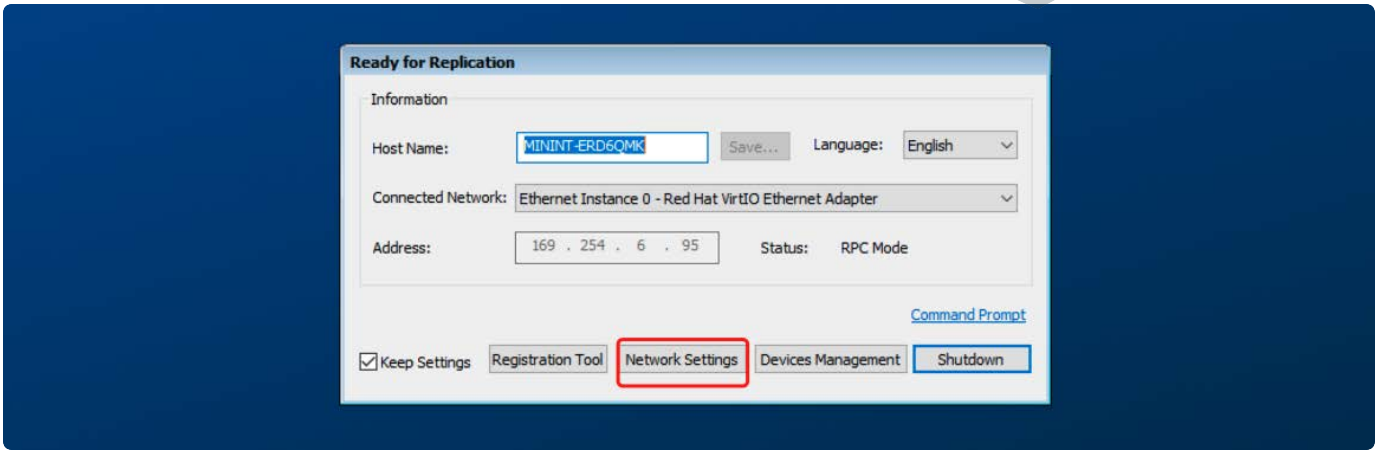


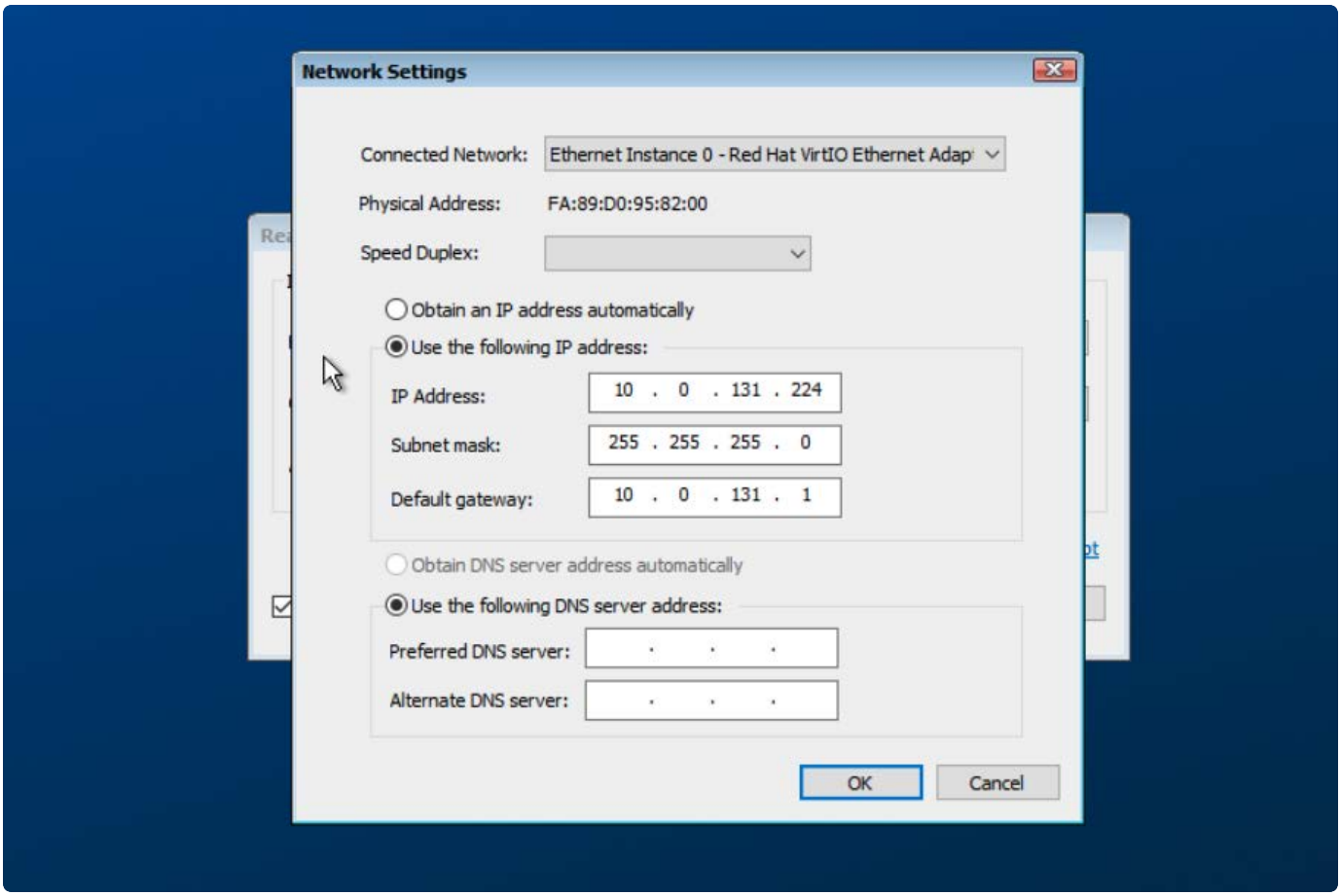
4. Locate which cloud host is the target machine based on the cloud host name and IP address.

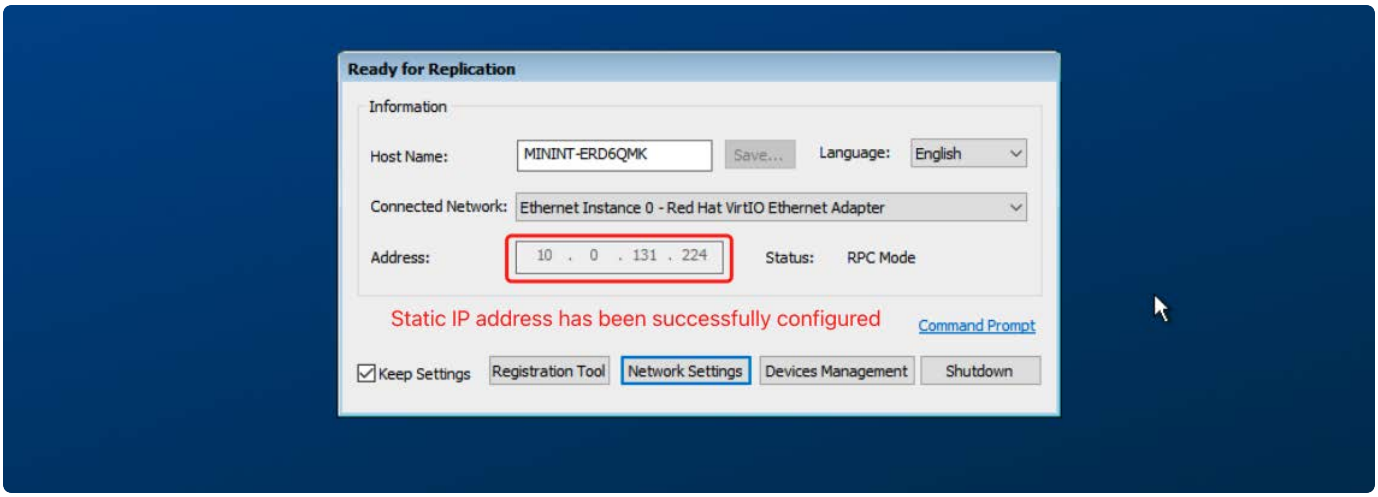


5. Open the management console, observe the startup status of WTL/LTL, enter the graphical interface, and configure a static IP.

- You may observe an automatic restart, just wait.
- Configuration interface after the Windows target machine starts normally

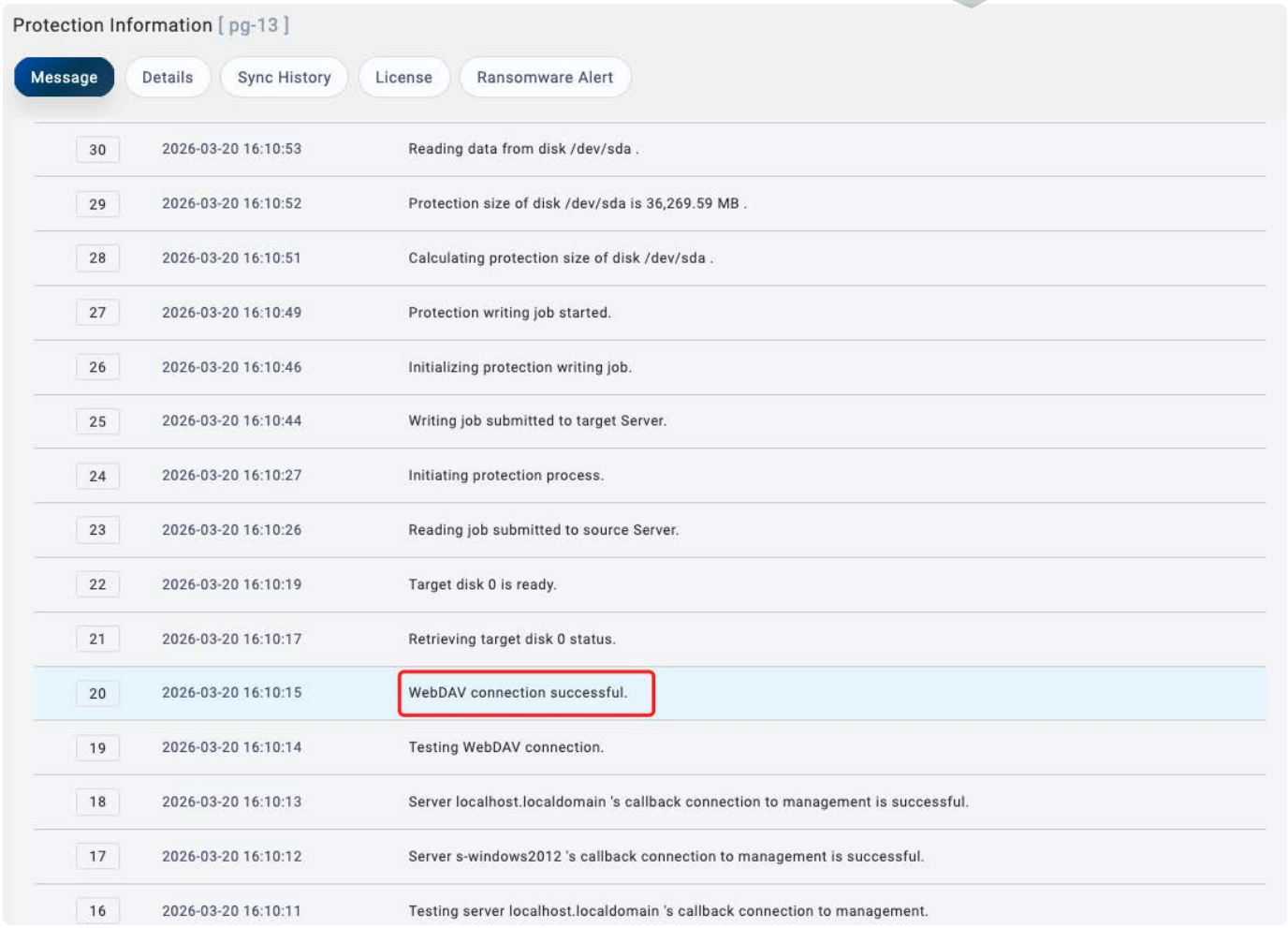

Ready for Replication
Information
Host Name:
MININT-ERD6QMK
Save...
Language:
English
Connected Network:
Ethernet Instance 0 - Red Hat VirtIO Ethernet Adapter
Address:
169 . 254 . 6 . 95
Status:
RPC Mode
Command Prompt
Keep Settings
Registration Tool
Network Settings
Devices Management
Shutdown


Network Settings
Connected Network:
Ethernet Instance 0 - Red Hat VirtIO Ethernet Adap
Physical Address:
FA:89:D0:95:82:00
Speed Duplex:
Obtain an IP address automatically
Use the following IP address:
IP Address:
10 . 0 . 131 . 224
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
10 . 0 . 131 . 1
Obtain DNS server address automatically
Use the following DNS server address:
Preferred DNS server:
Alternate DNS server:
OK
Cancel

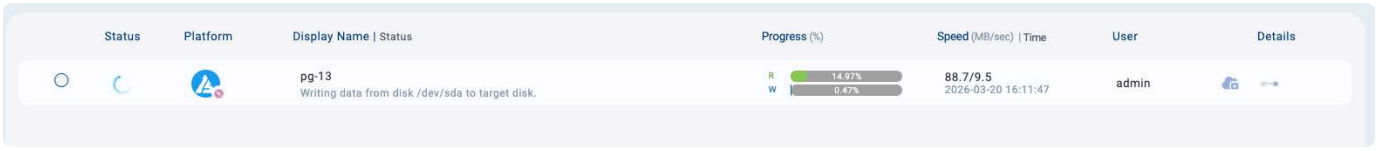

Ready for Replication
Information
Host Name:
MININT-ERD6QMK
Save...
Language:
English
Connected Network:
Ethernet Instance 0 - Red Hat VirtIO Ethernet Adapter
Address:
10 . 0 . 131 . 224
Status:
RPC Mode
Static IP address has been successfully configured
Command Prompt
Keep Settings
Registration Tool
Network Settings
Devices Management
Shutdown

- Extended supplement: Linux target machine configuration interface after normal startup.

6. Switch to the synchronization task and wait for the WebDAV connection to be successful.



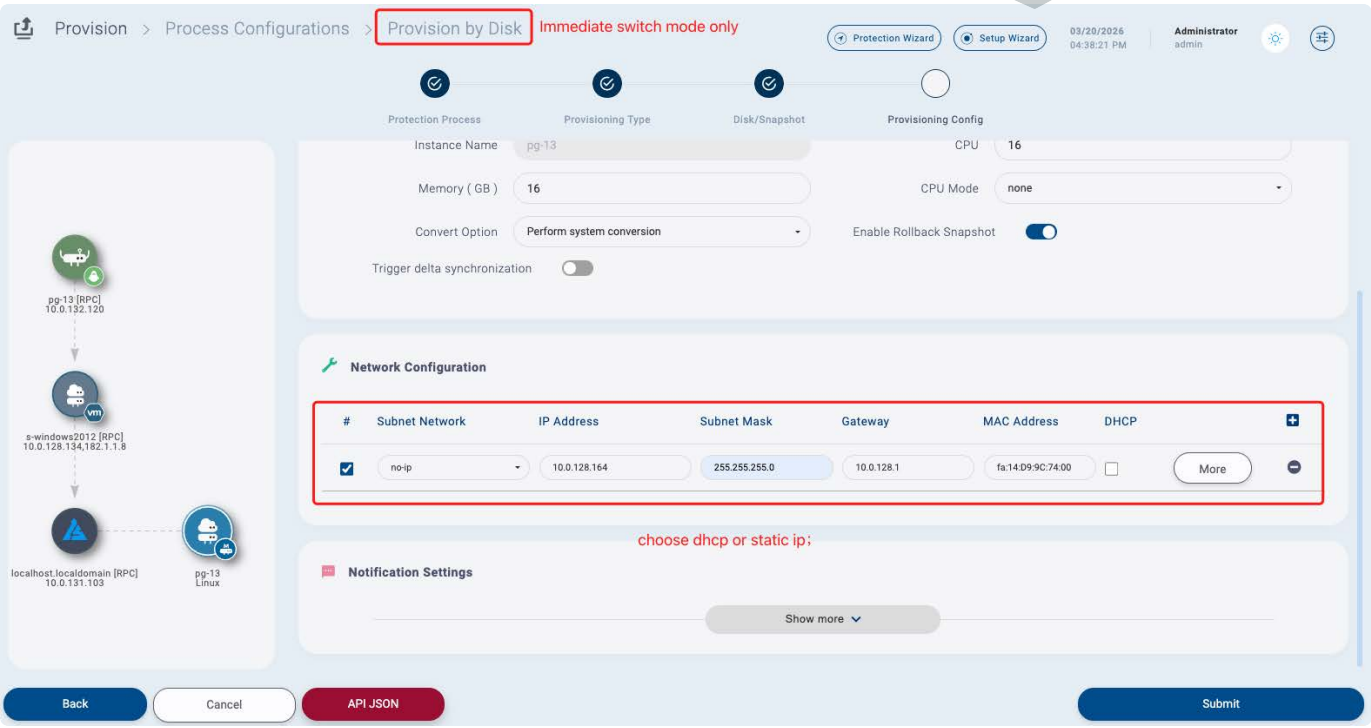
7. The synchronization task synchronizes normally.



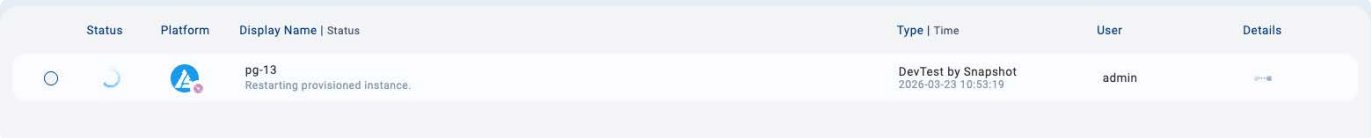
8. Just wait for the synchronization task to complete.



9. When performing a switching task (immediate switching), confirm that the IP address is automatically loaded or manually set in the `network card configuration` .



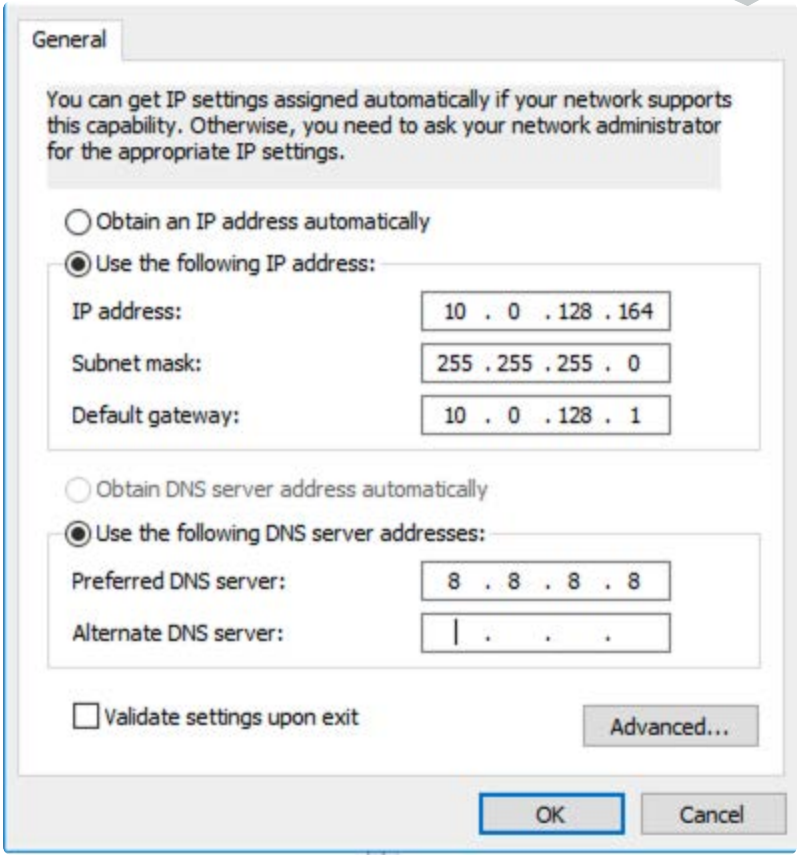
10. Just wait for the activation task to complete.
    - When the message reads "Restart the target to enable the host", the recovery has been completed and the target machine is being powered on and pre-configured.
    - At this time, you may observe that the target machine restarts once, which is normal.



    - When the message reads "Operating system started successfully", the recovery has been completed and the target machine has been pre-configured.
    - A few systems may not have this information, which is normal.



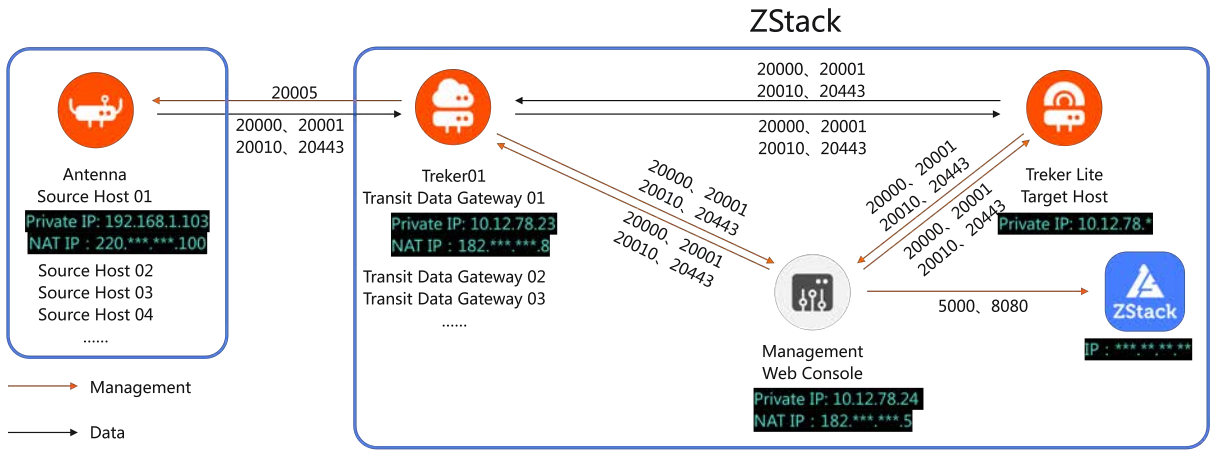
11. Check the network card configuration of the target machine. Generally, the IP will be written to the system network card configuration as a static IP.


General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 0 . 128 . 164
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 0 . 128 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 8 . 8 . 8 . 8
Alternate DNS server: . . .
Validate settings upon exit
Advanced...
OK
Cancel

Management console and Treker gateway server in NAT IP architecture

Document Category: Product Related Experience

Topology map



- If multiple transit data gateways are deployed, a NAT IP must be configured for each gateway;
- The private IP of the migration console must be able to communicate with port 8080 on all ZStack management nodes, including the VIP.
- It is recommended that the private IP of the migration console can communicate with port 5000 on the ZStack Web Console.
  - In other words, the ZStack Web Console should be accessible from within the migration console system.

network planning

When the source host uses RPC mode to register, the source host needs to use NAT IP;

The source host uses HTTPS mode to register, and the source host does not need to use NAT IP.

- If you don't understand the difference between RPC and HTTPS registration, you can refer

NEXAVM

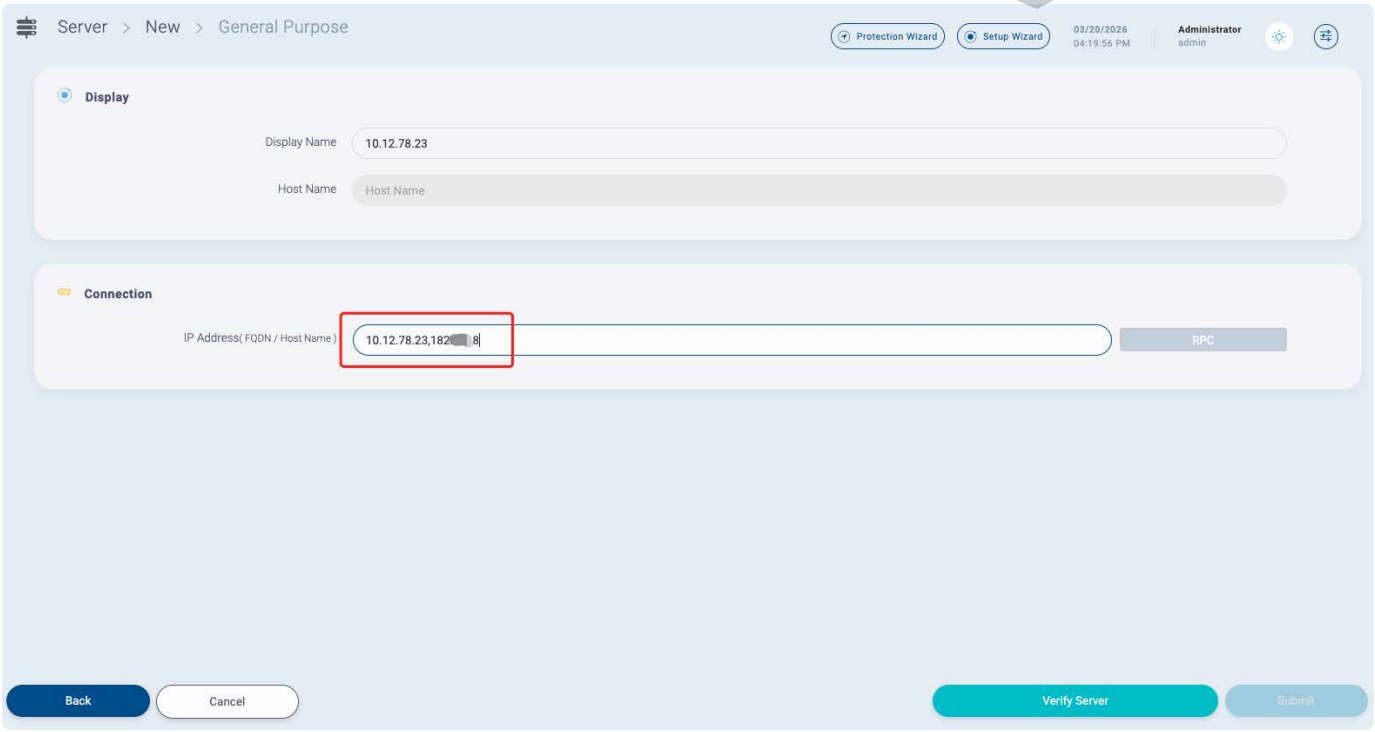
to the knowledge base "Concepts and Comparison of HTTPS and RPC Modes".

Serial number	Role	Deployment location	Intranet IP	NAT IP	NAT port
1	Source host	Source platform	192.168.1.103	220...100	20005
2	Data Gateway	Target Cloud Platform	10.12.78.23	182...8	20000, 20001, 20010, 20443.
3	Management Console	Target Cloud Platform	10.12.78.24	182...5	20000, 20001, 20010, 20443.
4	Target Cloud Platform	–	–	–	–
5	Target Server	Target Cloud Platform	10.12.78.*	–	–

Data gateway configuration NAT address

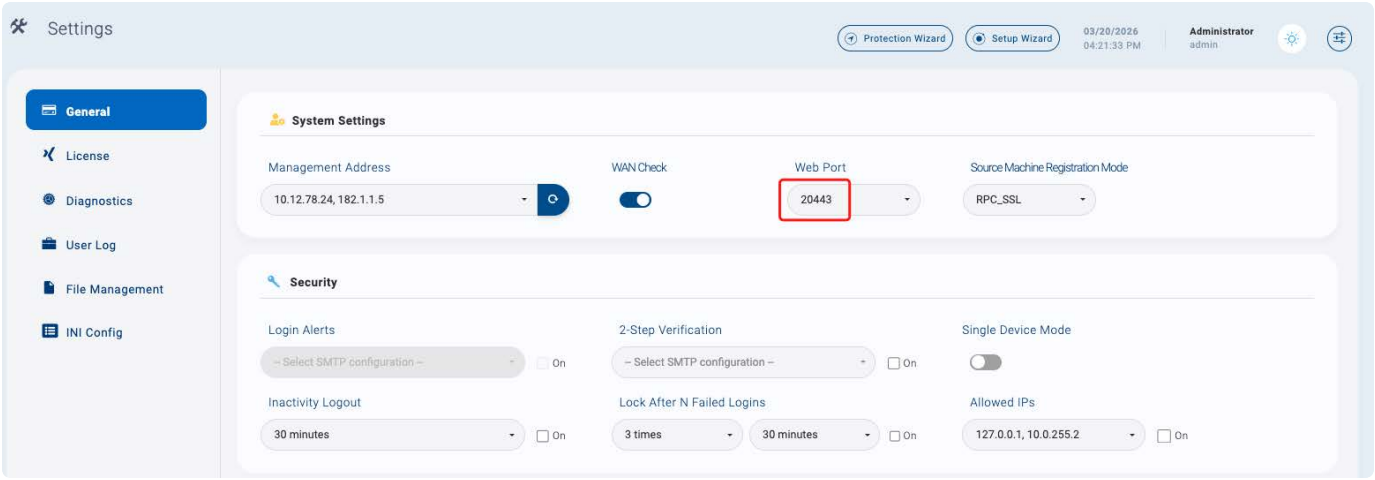
When adding a data gateway, fill in the intranet IP address and NAT IP address, separated by **English commas**.

- `10.12.78.23` , `182...8` .
- If there are multiple data gateways, just add them in the same way as `Intranet IP, NAT IP` .



Configure NAT address and port on the management console

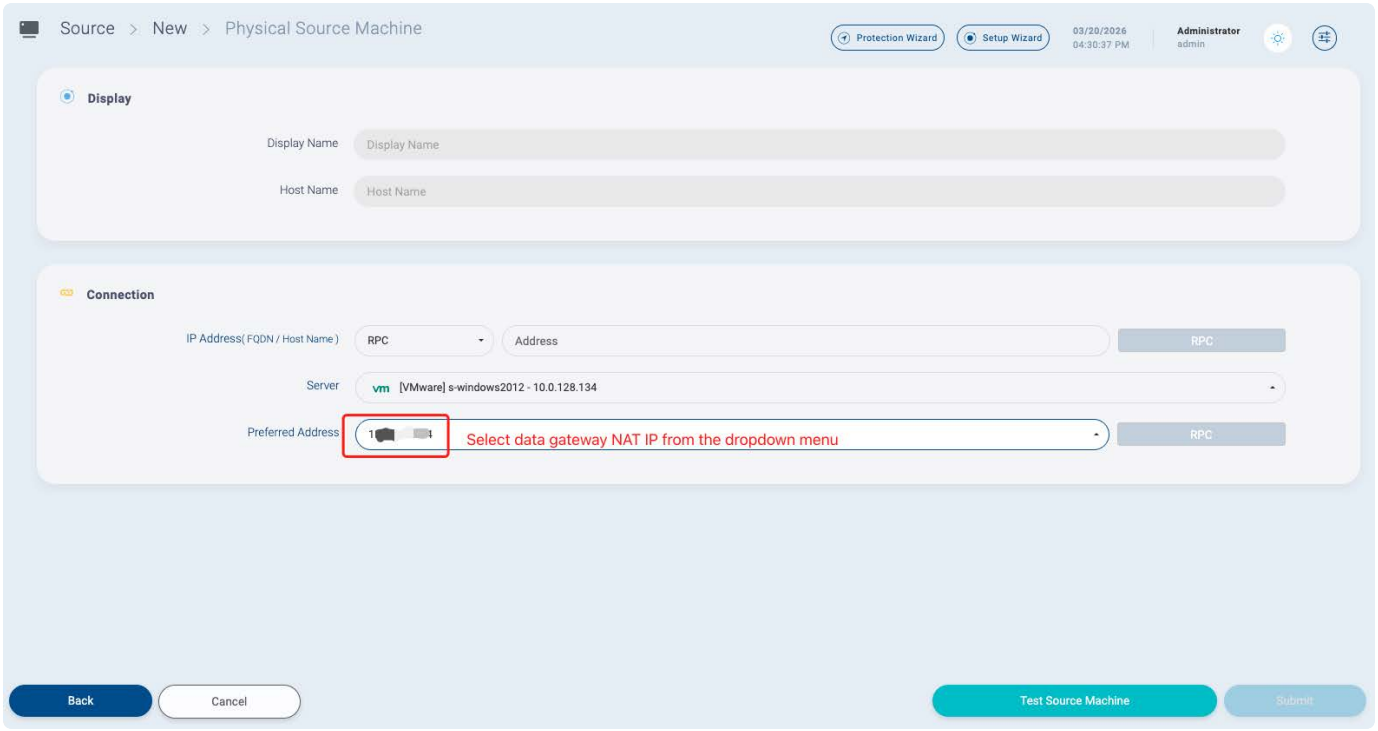
**In the central control address setting, you need to manually add the NAT IP address of the management console and set the central control port to 20443. **



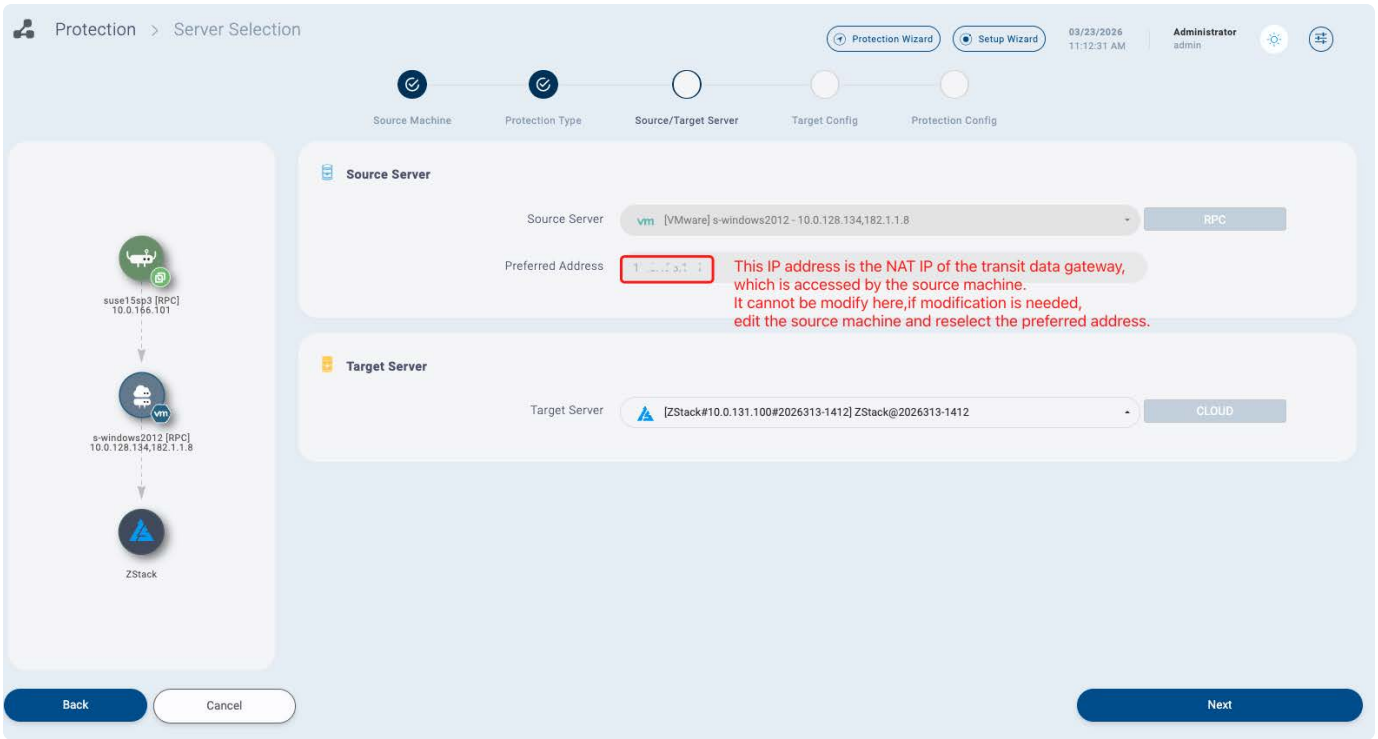
Add the source host on the management console

- **Pre-step: Configure the NAT address for the data gateway. **
- How to choose the data gateway IP here mainly depends on which IP address of the data

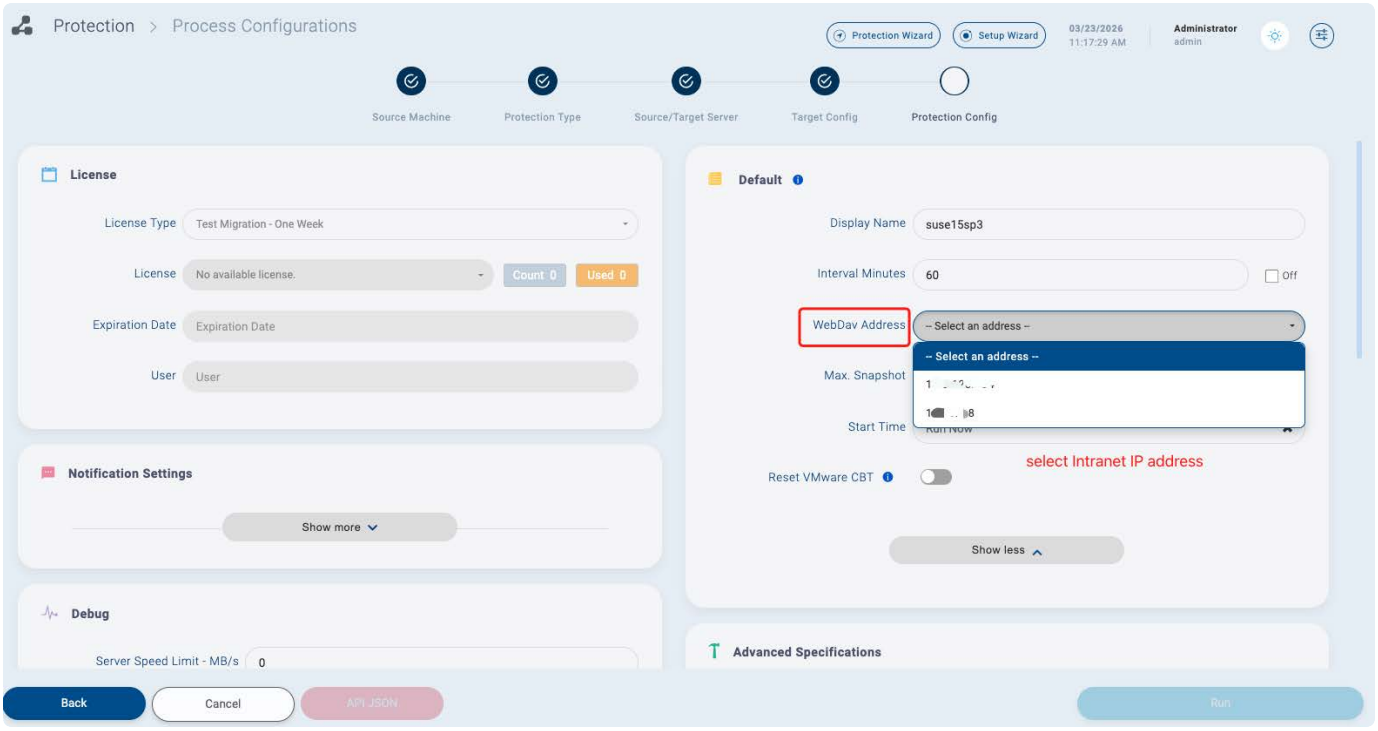
gateway the source host wants to communicate with. The source host can only communicate with the NAT IP of the data gateway, so you must choose the NAT IP.



Create a synchronization task



Service monitoring address. The target machine and the transit machine communicate on the intranet. Here you need to select the intranet IP address of the transit data gateway.



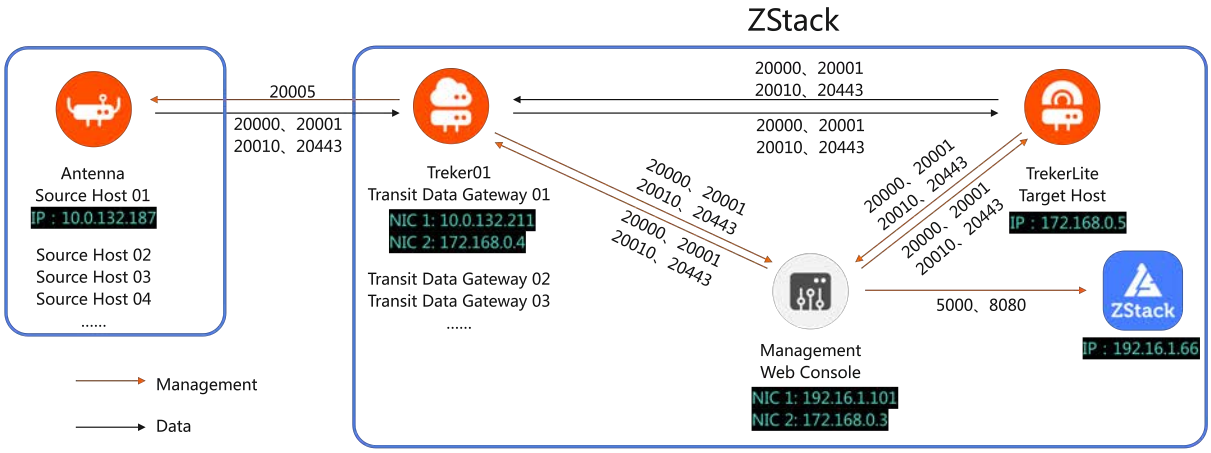
Management console and Treker gateway server in dual network card architecture

Document Category: Product Related Experience

Applicable scenarios

1. The user environment requires separation of read and write networks.
2. The subnet of the NexaVM platform doesn't have DHCP enabled and needs to be migrated using the NexaVM API.
3. Other scenarios that fit this architecture.

Topology map



- If multiple transit data gateways are deployed, each gateway must be configured with dual NICs;
- The IP address of NIC 1 on the transit data gateway can be on a different subnet from the source host, as long as connectivity is available.
- The IP of NIC 1 on the migration console must be able to communicate with port 8080 on all ZStack management nodes, including the VIP.
- It is recommended that the IP of NIC 1 on the migration console can communicate with port 5000 on the ZStack Web Console.
  - In other words, the ZStack Web Console should be accessible from within the migration console system.

network planning

Serial Number	Role	IP	Remarks
1	Source host (Antenna)	10.0.132.187	
2	Transit data gateway (Treker)	Network card 1: 10.0.132.211 Network card 2: 172.168.0.4	Configuring dual network cards Network card 1 needs to be configured with a gateway to communicate with the source machine; Network card 2 needs to be configured with a gateway to communicate with the target machine.

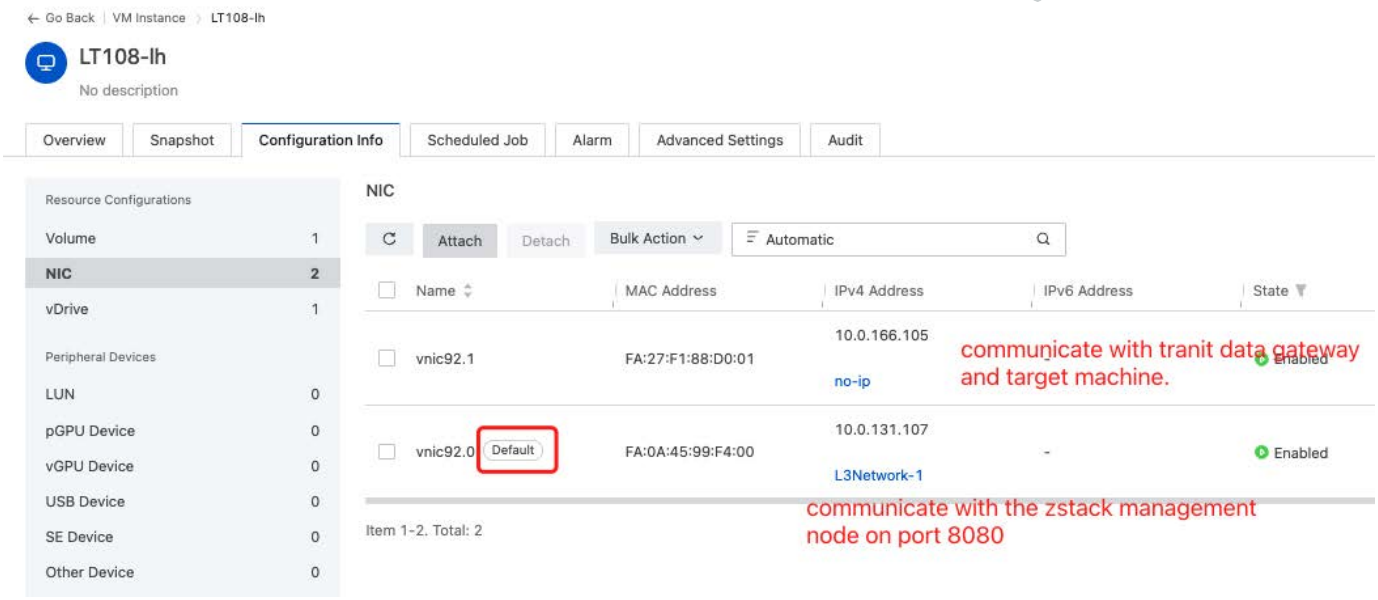
3	Migration Console (Management Console)	Network Card 1: 192.16.1.101 Network Card 2: 172.168.0.3	Network card 1: To communicate with port 8080 of all NexaVM management nodes (including VIP), a gateway needs to be configured. Network card 2: communicates with the target machine and the transit data gateway, without configuring a gateway.
4	Target machine (BootImage)	172.168.0.5	Specified when creating a task, or automatically assigned by DHCP.

- In the case, the 172.168.0.0 network segment is the temporary migration subnet configured on the NexaVM platform, and DHCP (ipv4) is enabled.
  - Please refer to the last paragraph of this knowledge base "[On demand] Create a NexaVM temporary migration subnet".
- If multiple transit data gateways are deployed, dual network cards must be configured.
- The IP address of the transit data gateway network card 1 and the source machine can be across network segments, as long as they can communicate.
- The IP of the migration console network card 1 needs to communicate with the 8080 port of all NexaVM management nodes (including VIP).
- It is recommended that the IP of the migration console network card 1 communicate with the 5000 port of the NexaVM Web console.
  - That's the NexaVM Web console can be accessed in the system where the console is migrated.

Deploy the management console and transit data gateway (the installation steps are omitted)

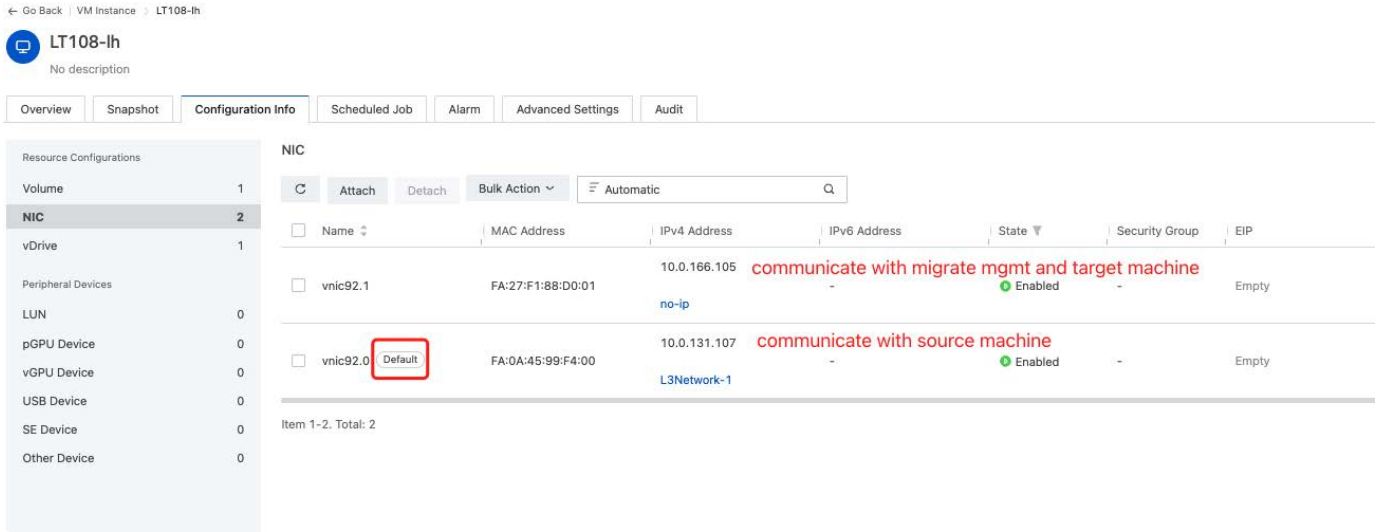
Management console

The deployment process is omitted. For installation steps, please refer to the quick manual.



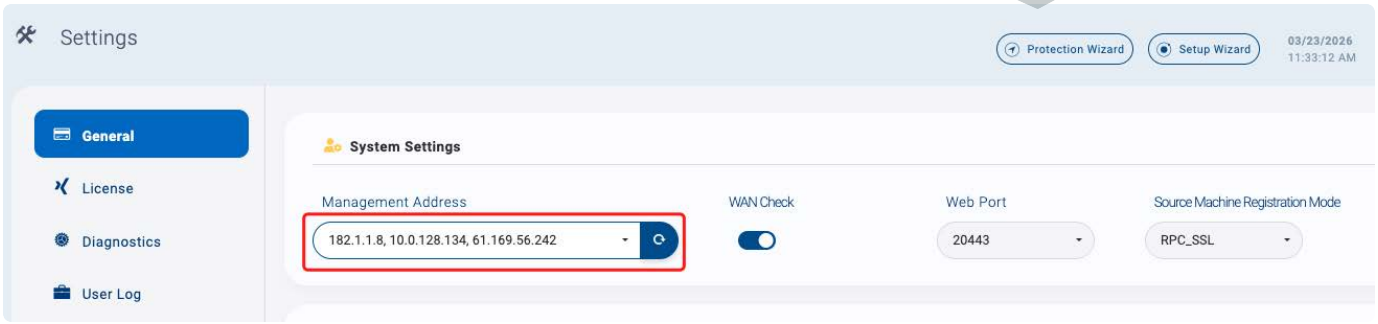
Transit data gateway

The deployment process is omitted. For installation steps, please refer to the quick manual.

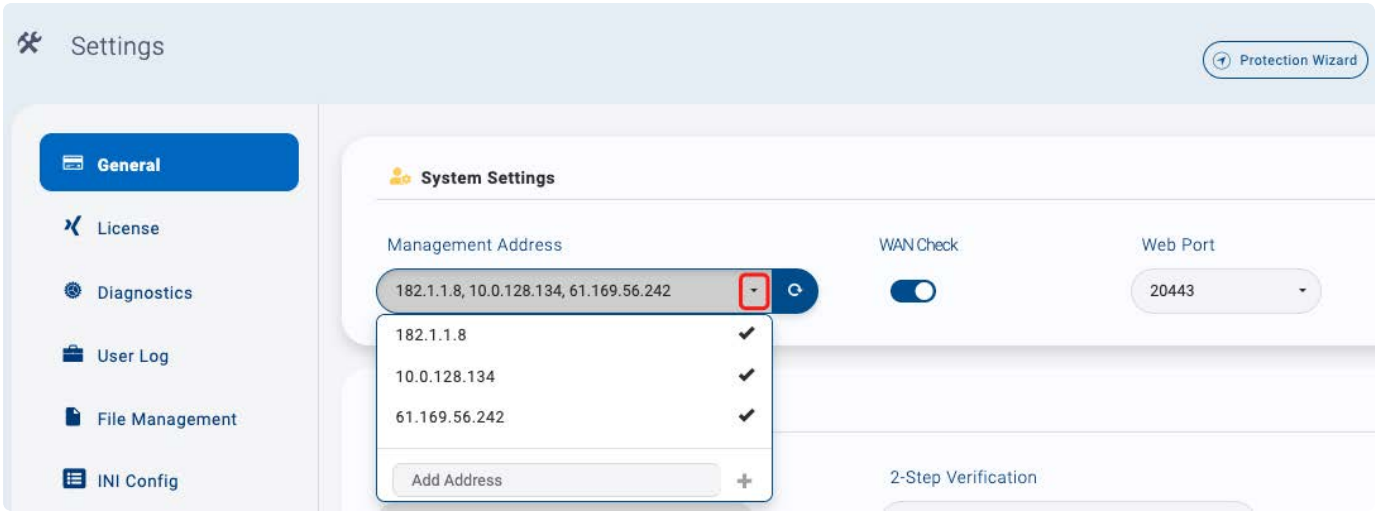


Configure multiple IPs for the management console

Confirm that the IP addresses of the two network cards are displayed in the central control address.



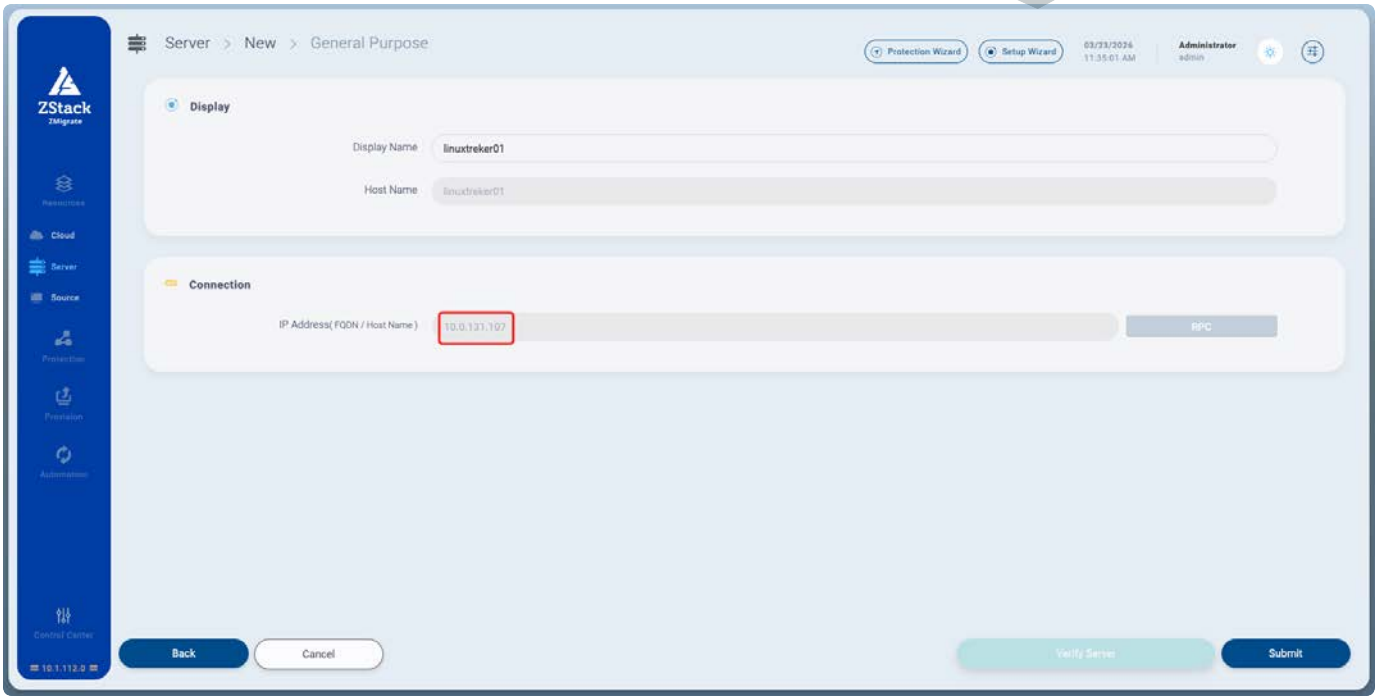
If the IP addresses of the two network cards are not displayed, you can drop down the check box or add them manually.



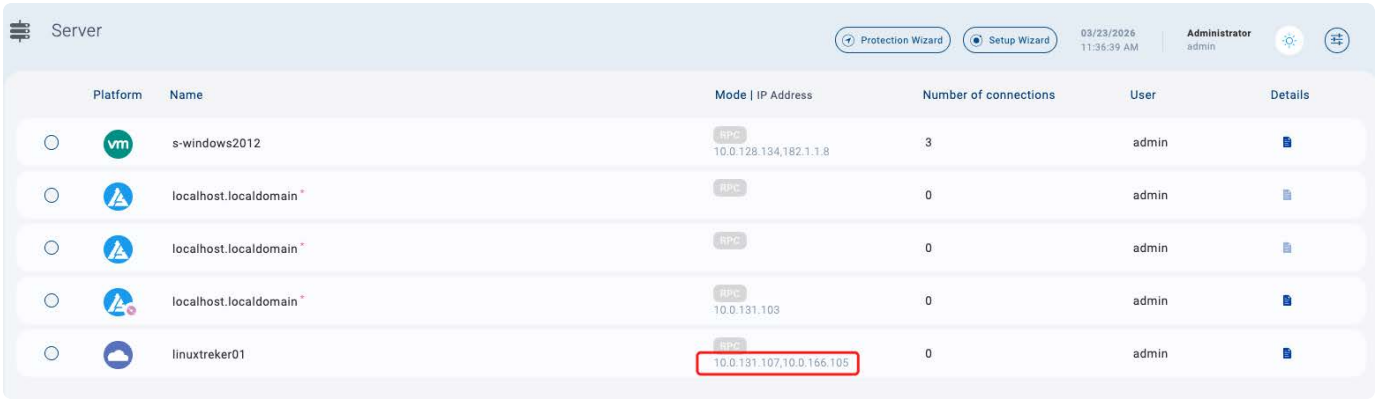
Add a transit data gateway on the admin console

When adding a data gateway, fill in the IP address on the same network segment as the management console.

- In this case, `10.0.131.107` should be filled in.

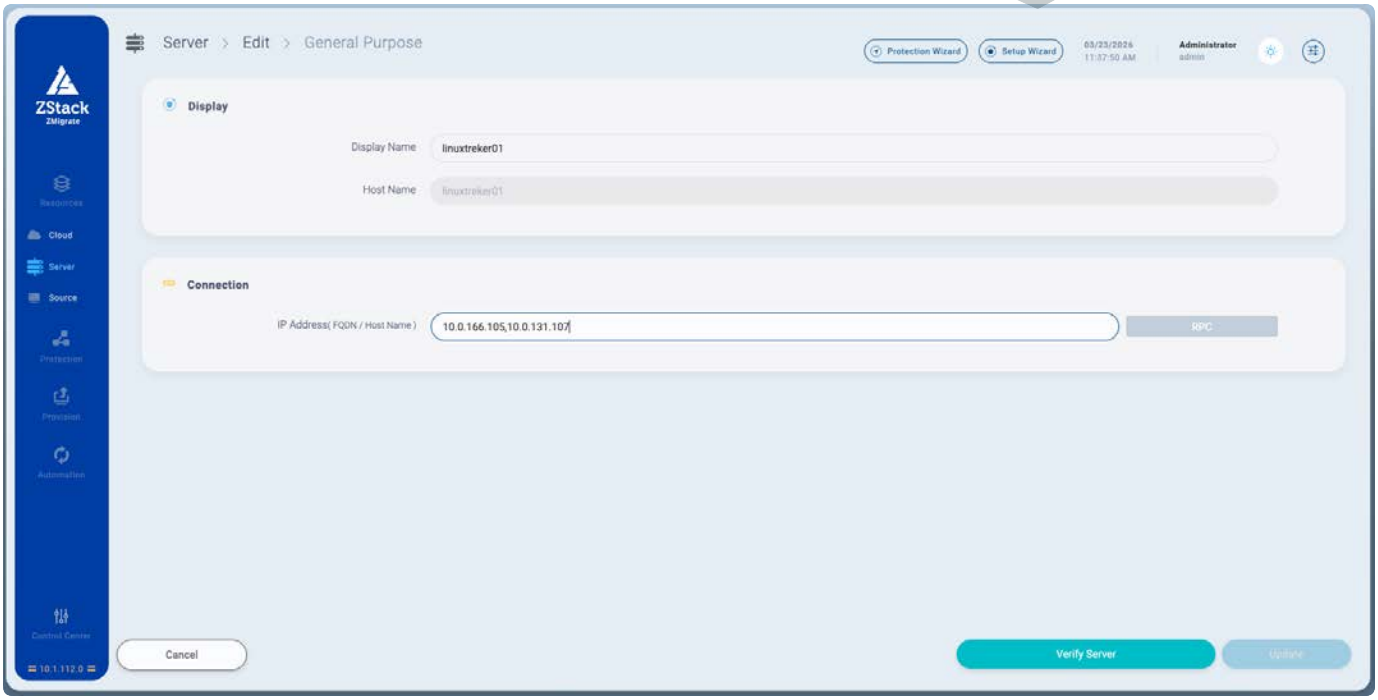


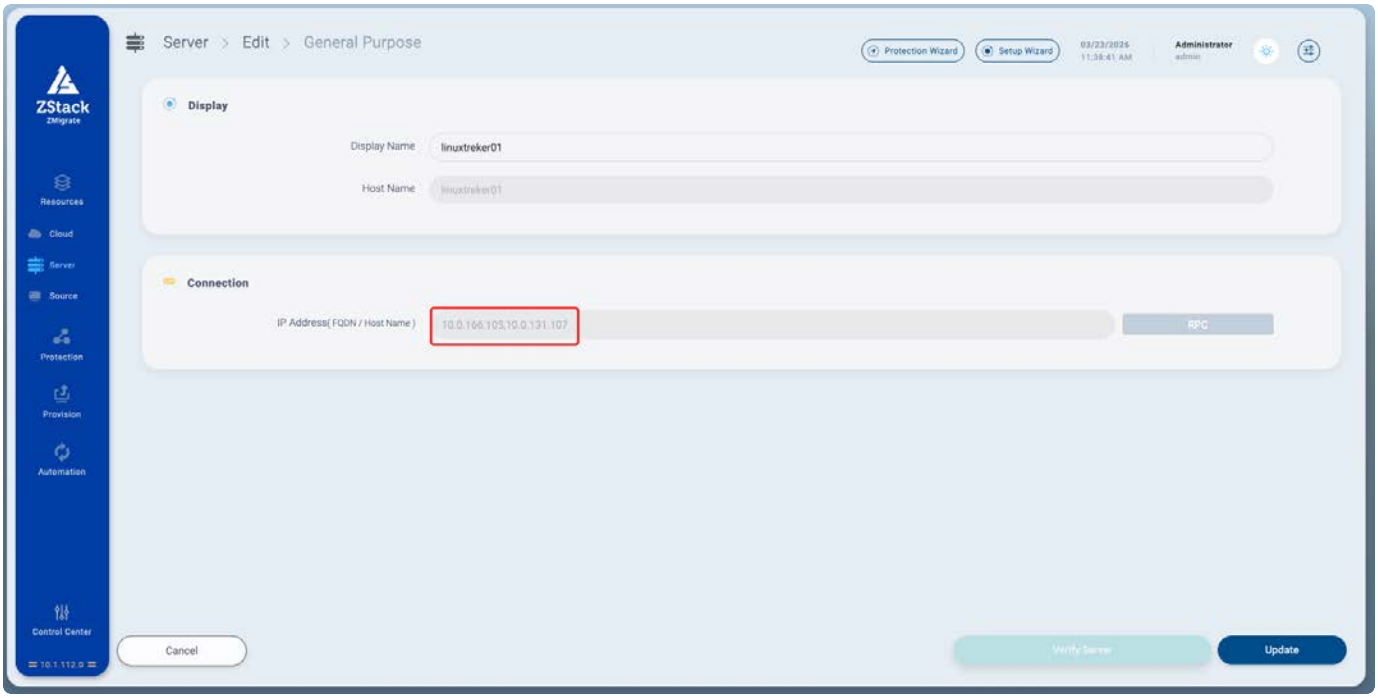
After the addition is successful, the IP addresses of the two network cards will be automatically identified.

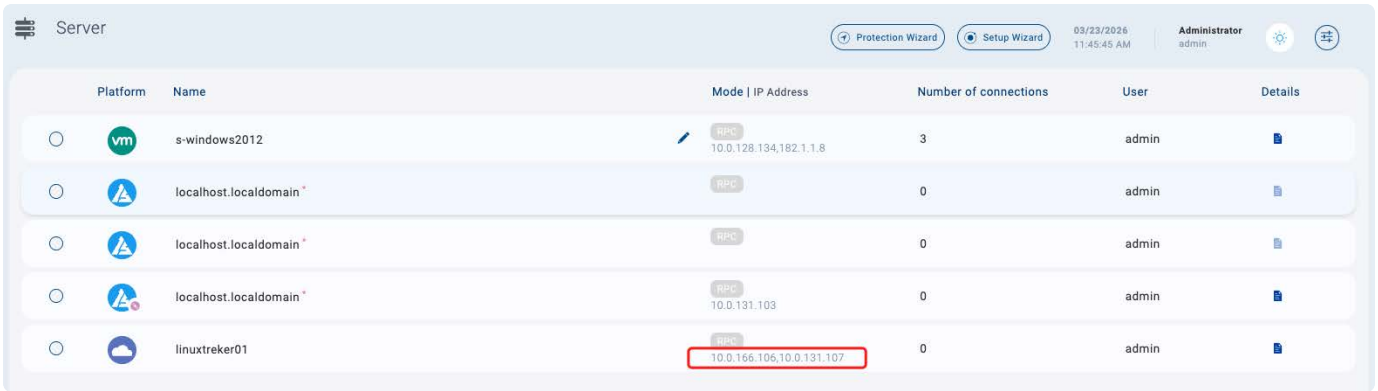


**If you fail to successfully identify the two network card IPs, you can delete them and add them again. 2 IPs have been successfully identified and you can proceed to the next step (add the source host). **

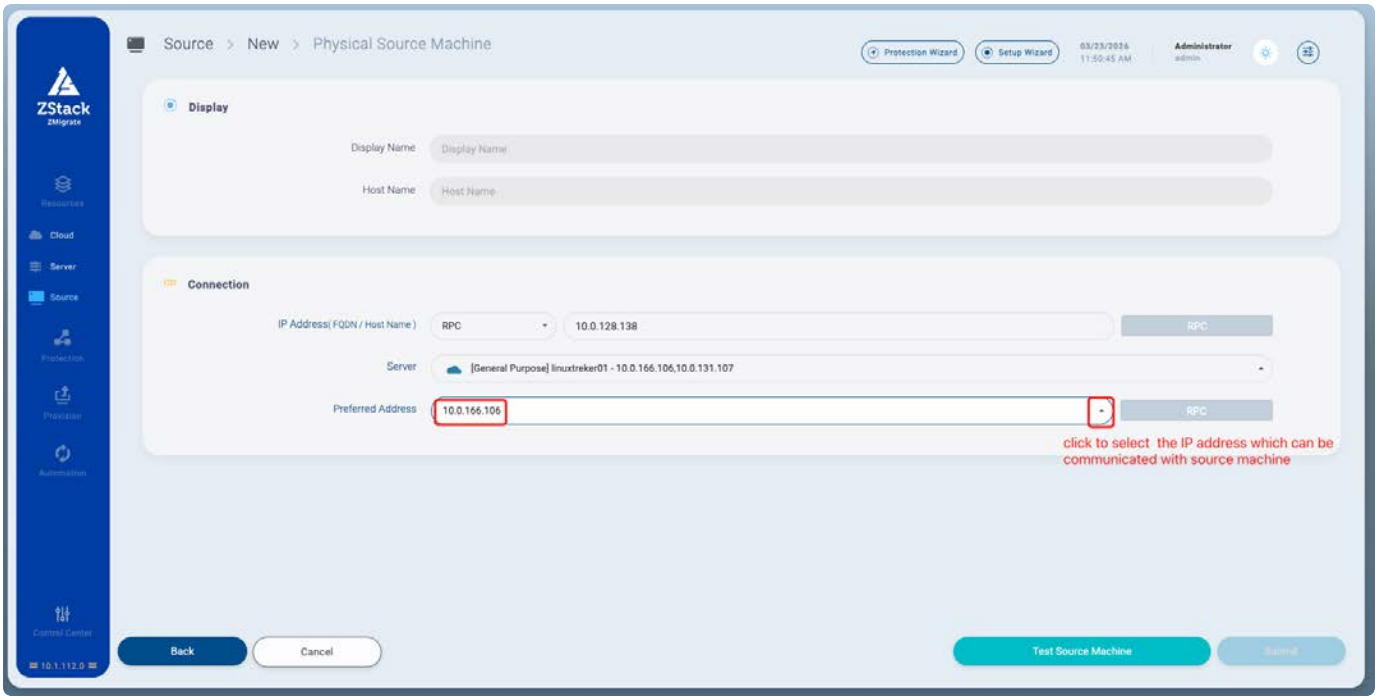
When adding, separate them with English commas and enter multiple IP addresses. **The IP that can communicate with the management console is written first**.


Server > Edit > General Purpose
Protection Wizard
Setup Wizard
Administrator
admin
ZStack
ZMigrate
Resources
Cloud
Server
Source
Protection
Provision
Automation
Control Center
Display
Display Name
linuxtreker01
Host Name
Connection
IP Address(FQDN / Host Name)
10.0.166.105,10.0.131.107
RPC
Cancel
Verify Server
Update


Server > Edit > General Purpose
Protection Wizard
Setup Wizard
Administrator
admin
ZStack
ZMigrate
Resources
Cloud
Server
Source
Protection
Provision
Automation
Control Center
Display
Display Name
linuxtreker01
Host Name
Connection
IP Address(FQDN / Host Name)
10.0.166.105,10.0.131.107
RPC
Cancel
Update


Server
Protection Wizard
Setup Wizard
Administrator
admin
Platform
Name
Mode | IP Address
Number of connections
User
Details
s-windows2012
RPC
10.0.128.134,182.1.1.8
3
admin
localhost.localdomain
RPC
0
admin
localhost.localdomain
RPC
0
admin
localhost.localdomain
RPC
10.0.131.103
0
admin
linuxtreker01
RPC
10.0.166.106,10.0.131.107
0
admin

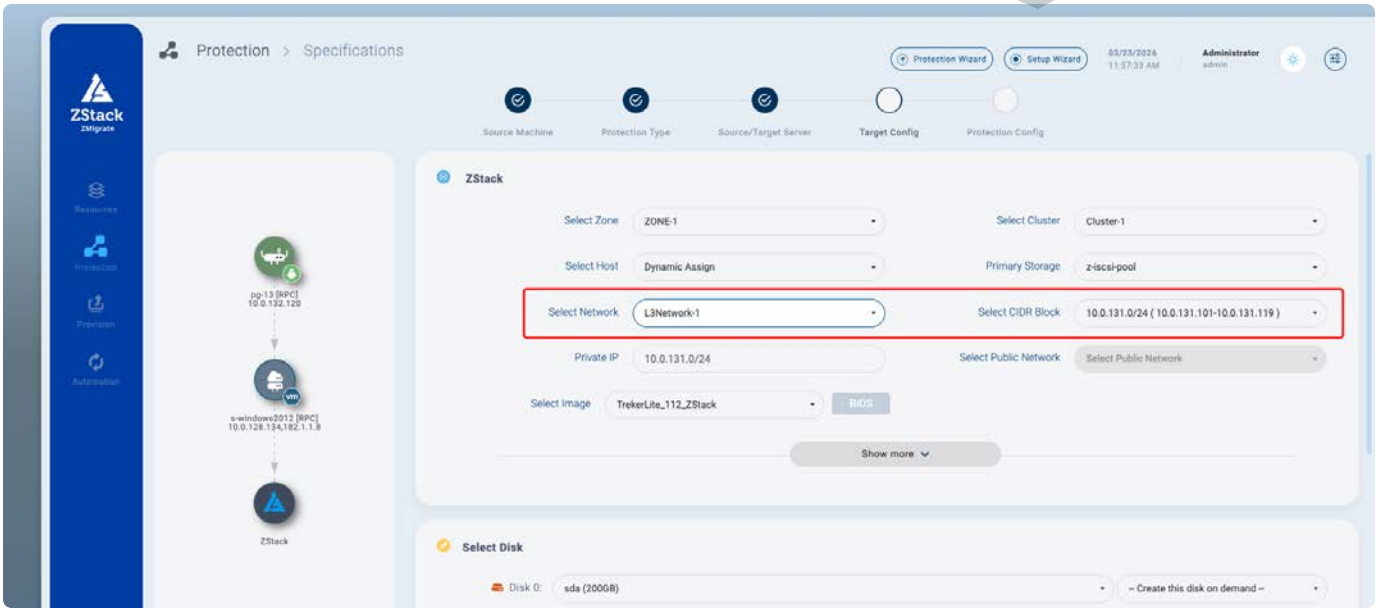
Add the source host on the management console



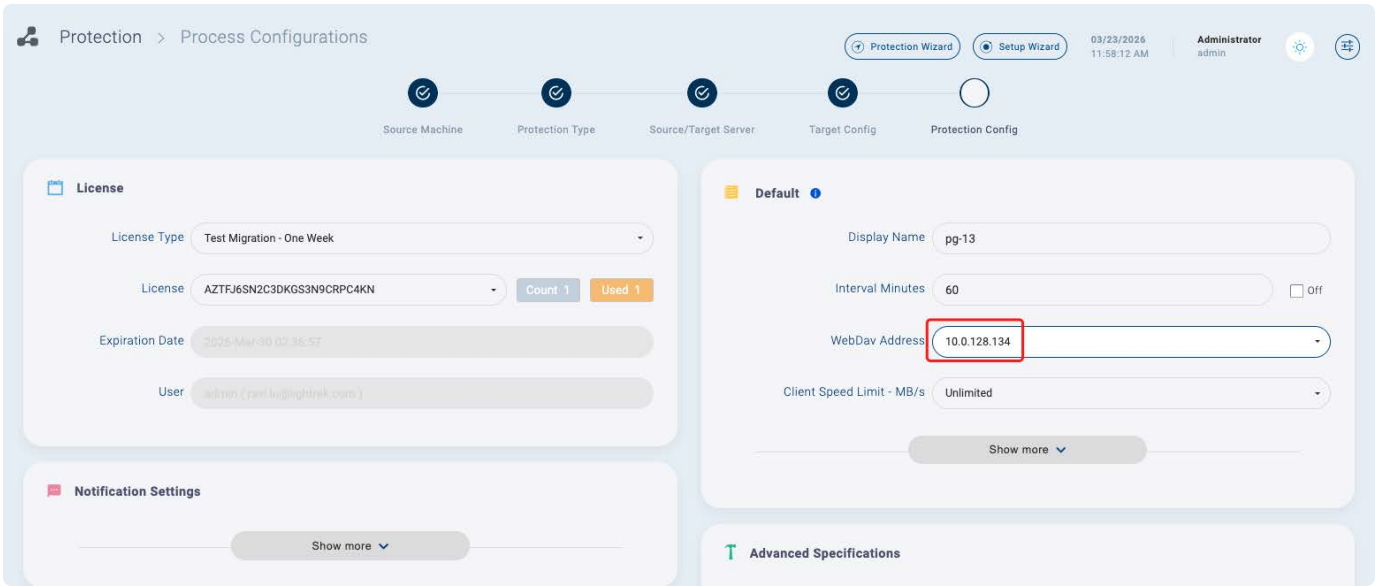


Create a synchronization task

Select the created "Configure DHCP Temporary Migration Subnet" for the synchronization task.

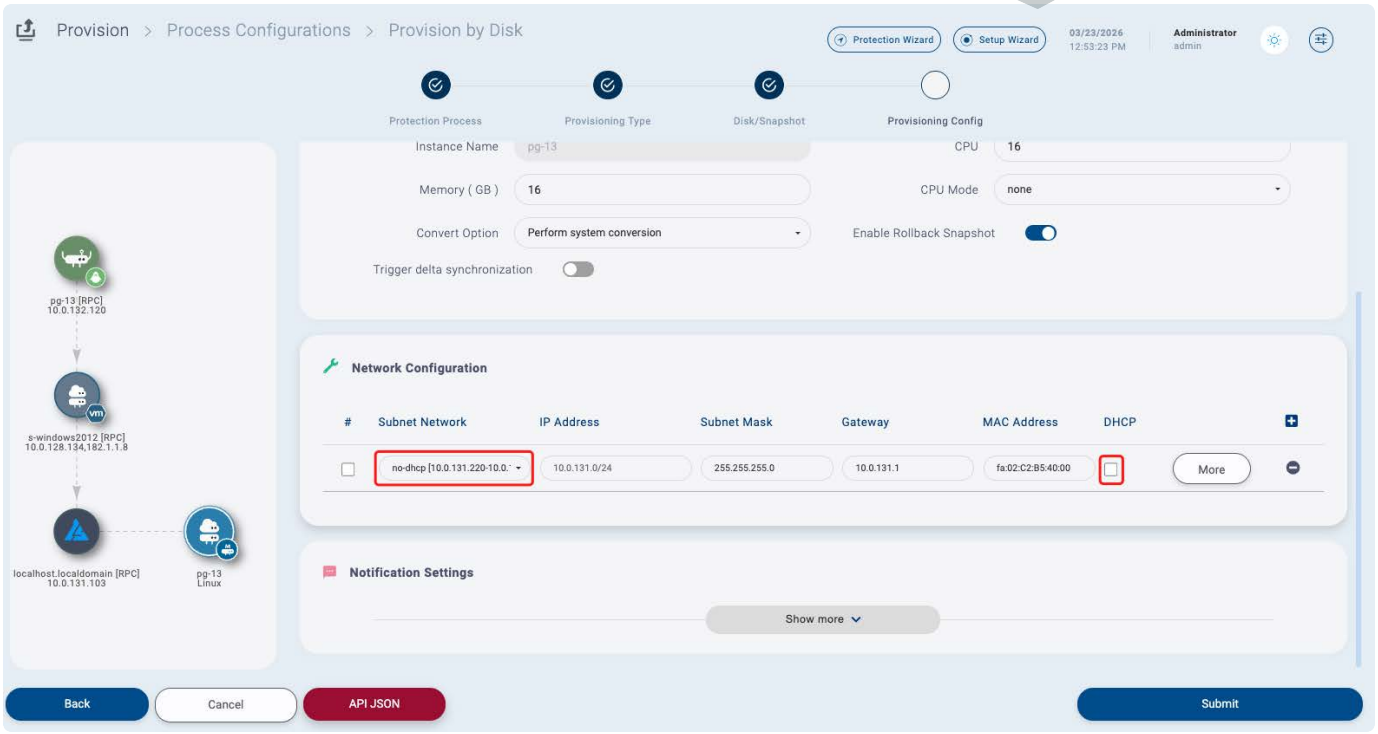


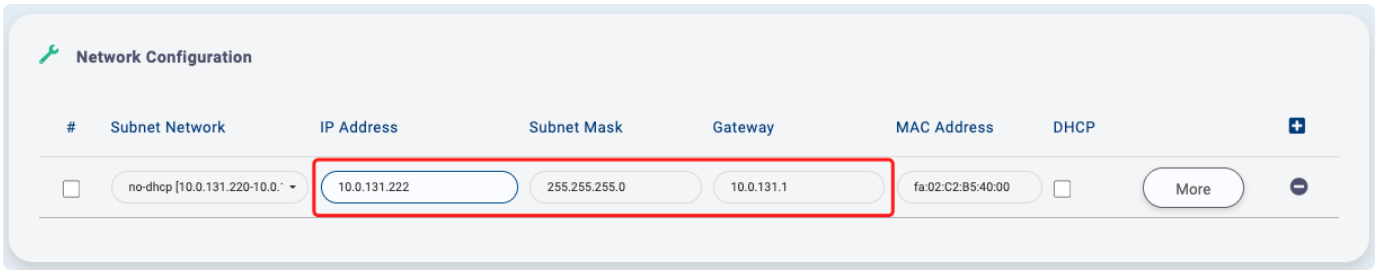
Select the IP `172.168.0.4` in the data gateway that can communicate with the target machine.



Create a switching task

1. Modify the subnet to the desired subnet. In the case, "subnet without DHCP enabled" is used after switching.
2. Since there is no DHCP, the IP address needs to be assigned manually.

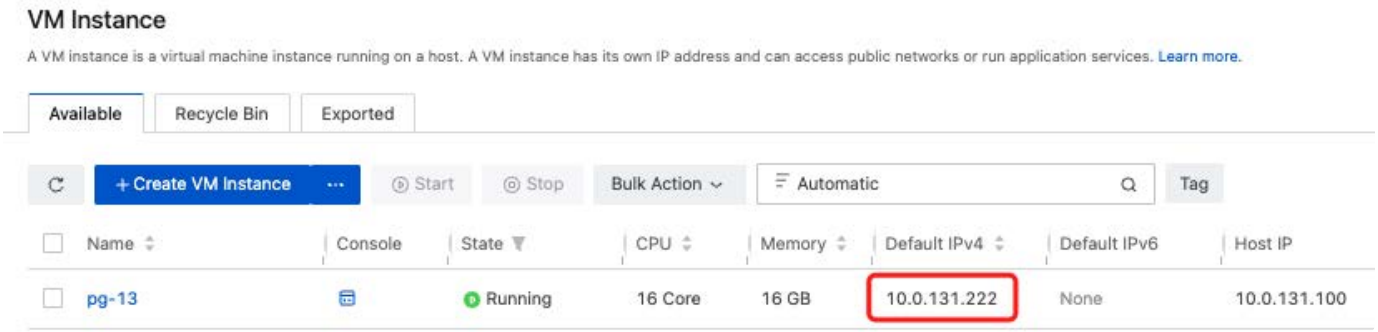




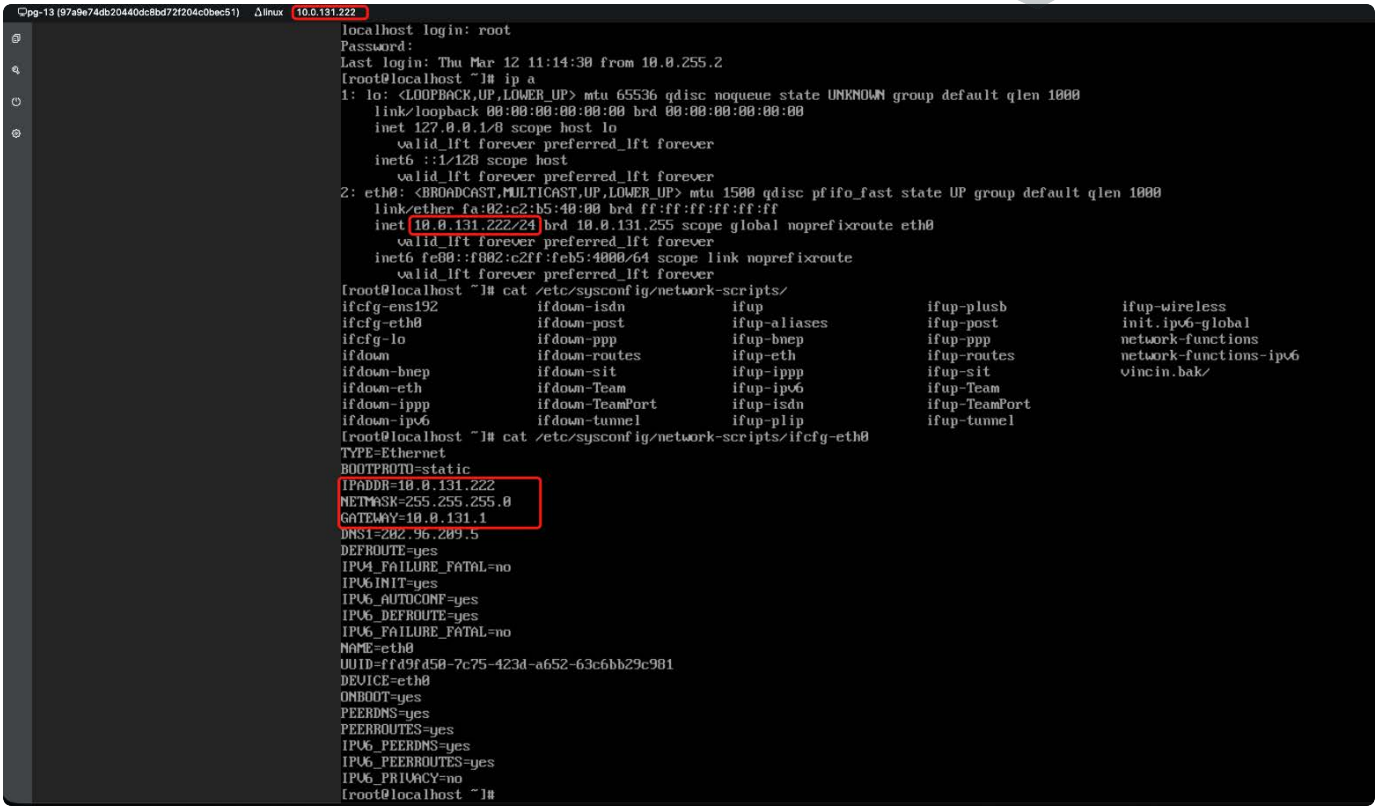
Switching task completed



The IP displayed on the NexaVM platform web page has been changed to the specified IP.



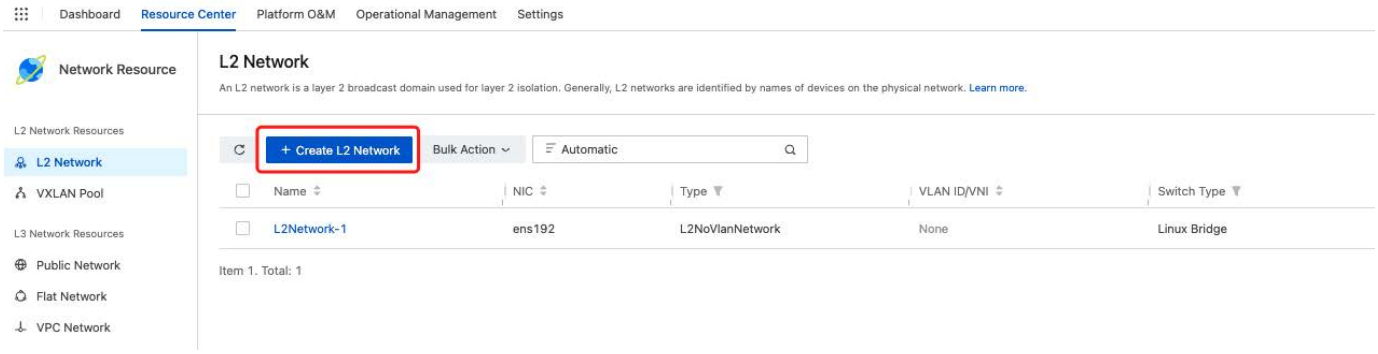
Set the specified IP as the system's static IP.



[On demand] Create NexaVM temporary migration subnet

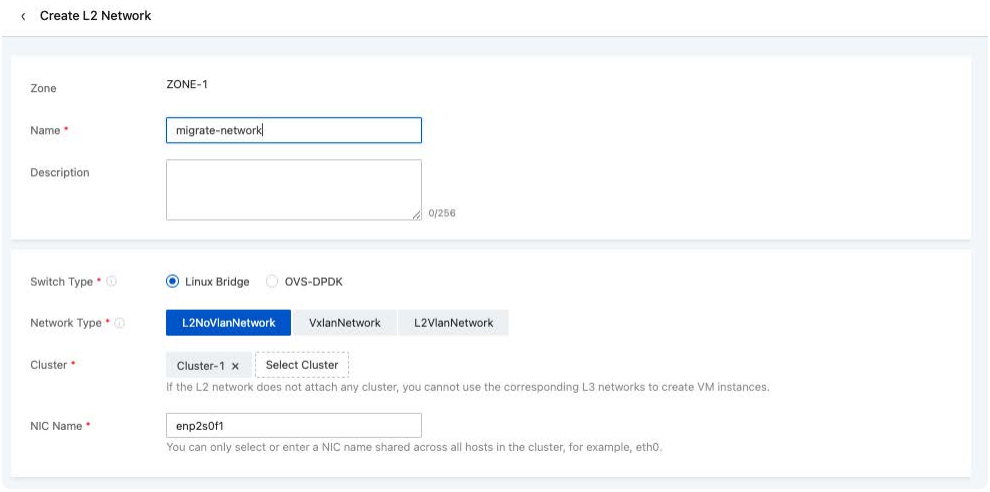
Create and migrate a Layer 2 network

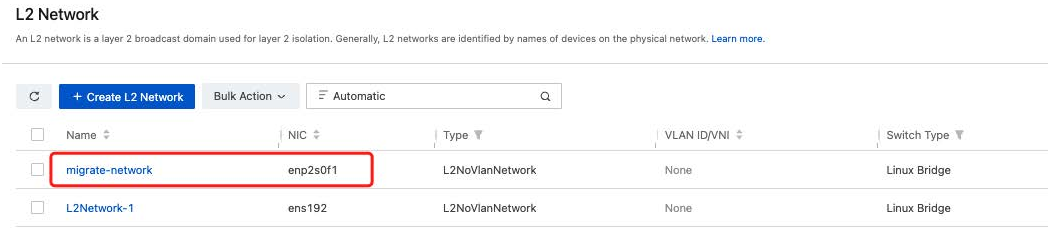
Resource Center --> Network Resources --> Layer 2 Network --> Create Layer 2 Network



Network card name: Fill in the name according to the actual situation. Generally, choose an unused network port.

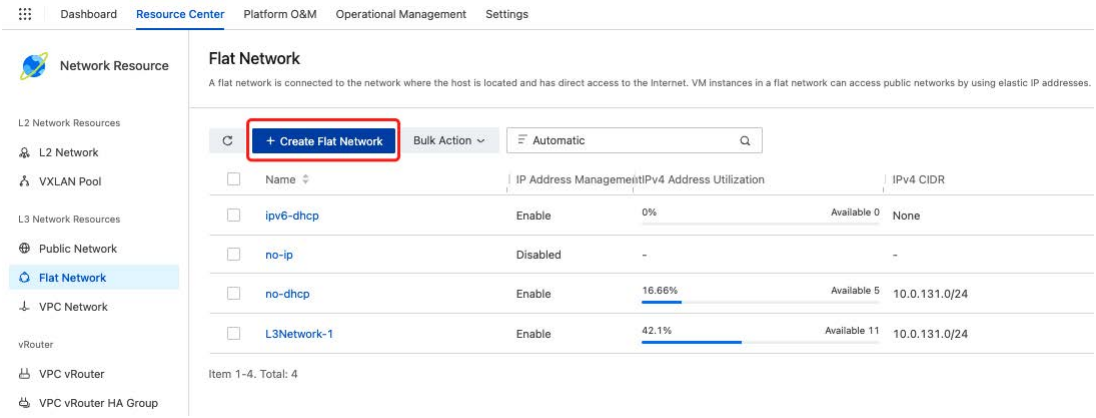
If you have other needs, please modify it as needed.





Create a migration flat network (three layers)

Resource Center --> Network Resources --> Flat Network --> Create a Flat Network



For the Layer 2 network, select the newly created migration subnet.

CIDR should not conflict with existing network segments.

The DHCP service needs to be turned on.

‹ Create Flat Network

Name * Migrate-L3

Description for migrate 11/256

L2 Network * migrate-network ×

IP Address Manage... ⓘ

If you turn on the switch, you can add network ranges and enable the DHCP service.

Network Address Type * IPv4 IPv6

Network Range M... * ⓘ IP Range CIDR

CIDR * 10.0.166.0/24

Gateway 10.0.166.1

DHCP Service ⓘ

IP Allocation Policy ⓘ Random Allocate in Order Allocate in Cycle

1. The system assigns all available IP addresses from the network range in ascending order.
2. Released IP addresses are assigned in the next allocation.

DHCP IP ⓘ

If not specified, the system uses the start IP address in the network range as the DHCP IP.

DNS ⓘ

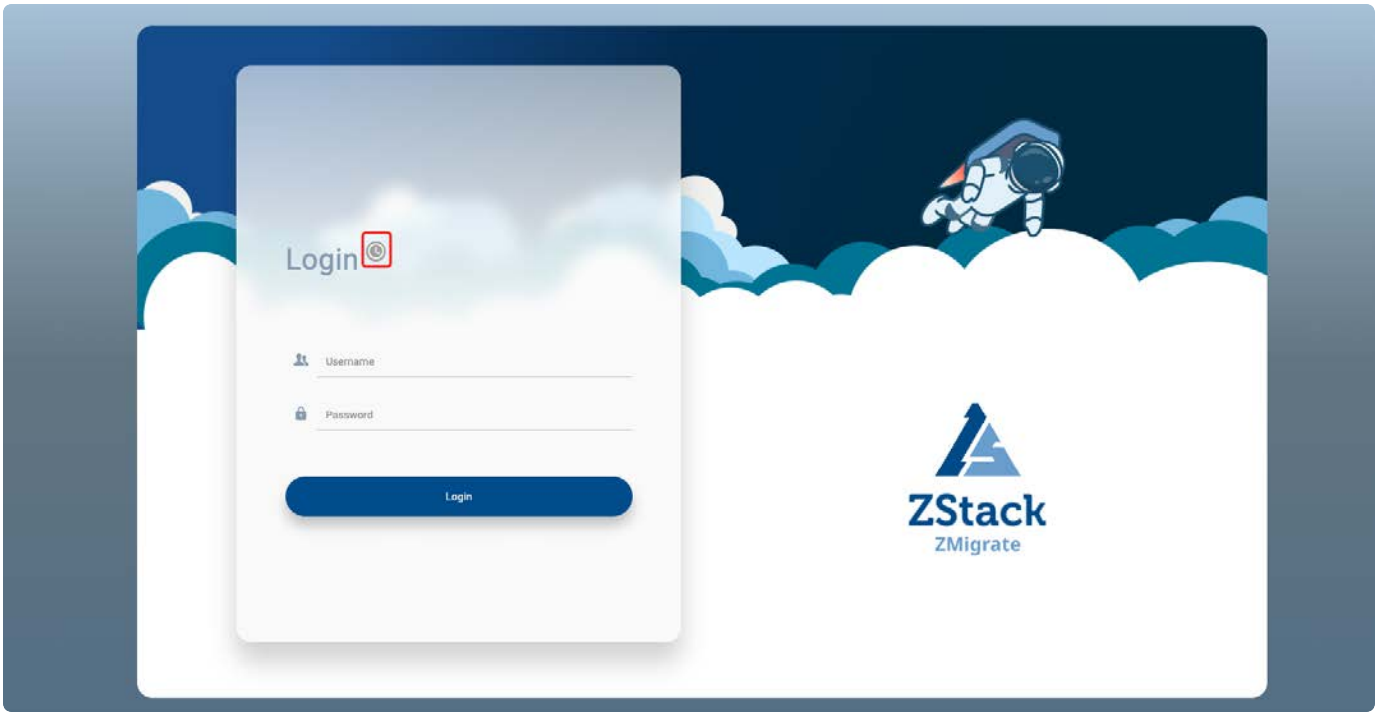
Flat Network

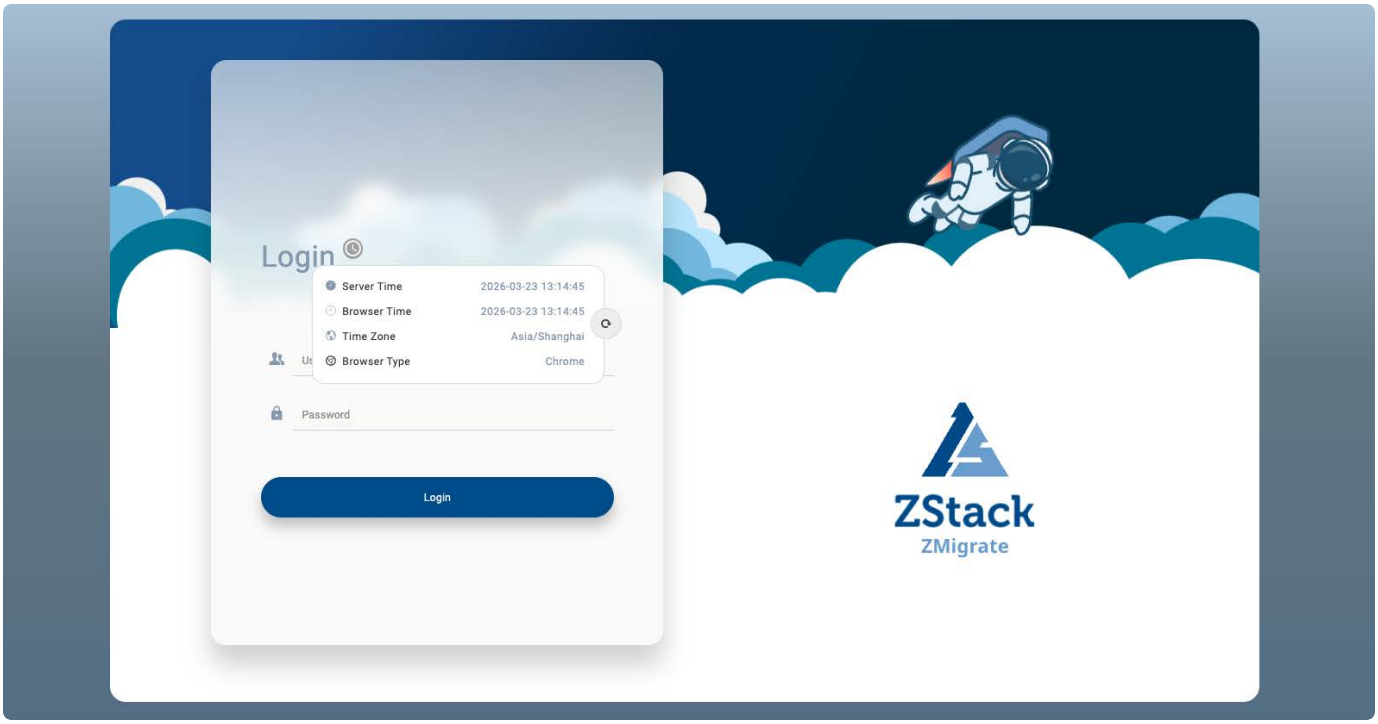
A flat network is connected to the network where the host is located and has direct access to the Internet. VM instances in a flat network can access public networks by using elastic IP addresses. Learn more.

+ Create Flat Network | Bulk Action | Automatic

Name	IP Address Management	IPv4 Address Utilization	IPv4 CIDR	IPv6 CIDR	Sharing Mode	Creation Time	Actions
Migrate-L3	Enable	0.39% Available 252	10.0.166.0/24	None	Not share	2026-03-23 13:09:50	...

Login interface





Server time: The system time of the management console will be automatically converted from UTC to the time in the corresponding time zone.

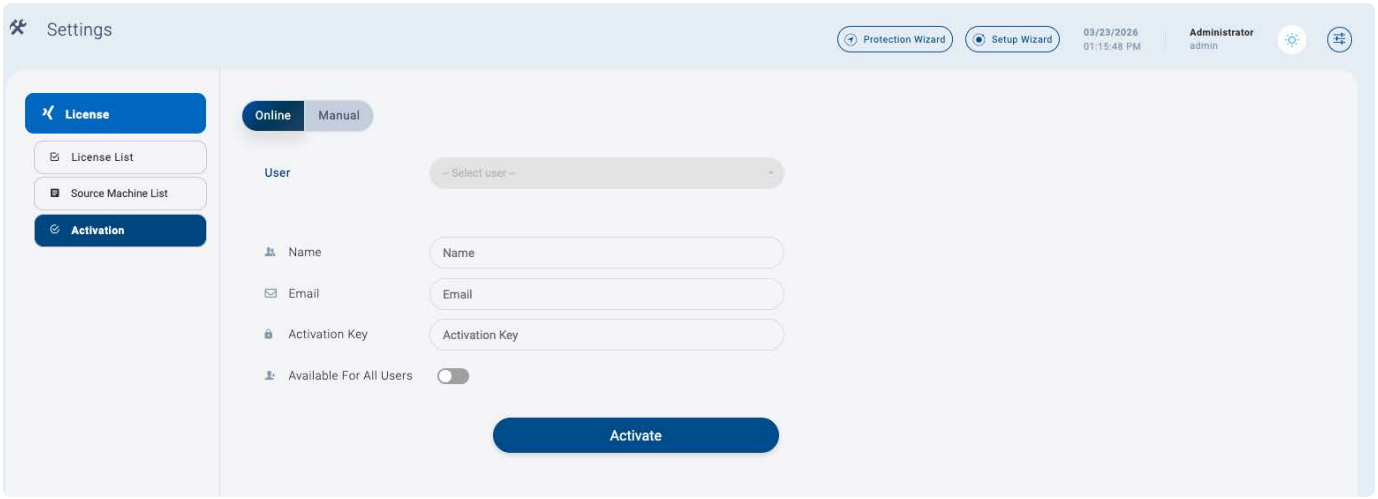
Browser time: The computer system time currently logged into the browser.

Time requirement: The difference cannot exceed 15 seconds.

Licensing interface

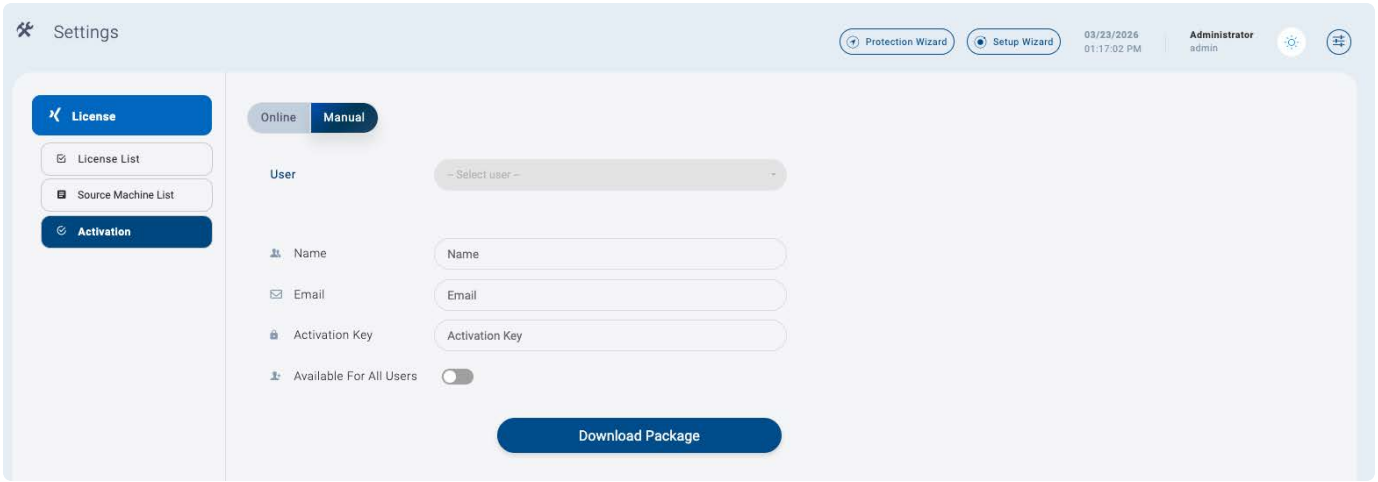
Online activation

In the MGMT network state, enter the `display name`, `email address`, `activation key`, and click `Register (valid)` to activate.



Offline activation

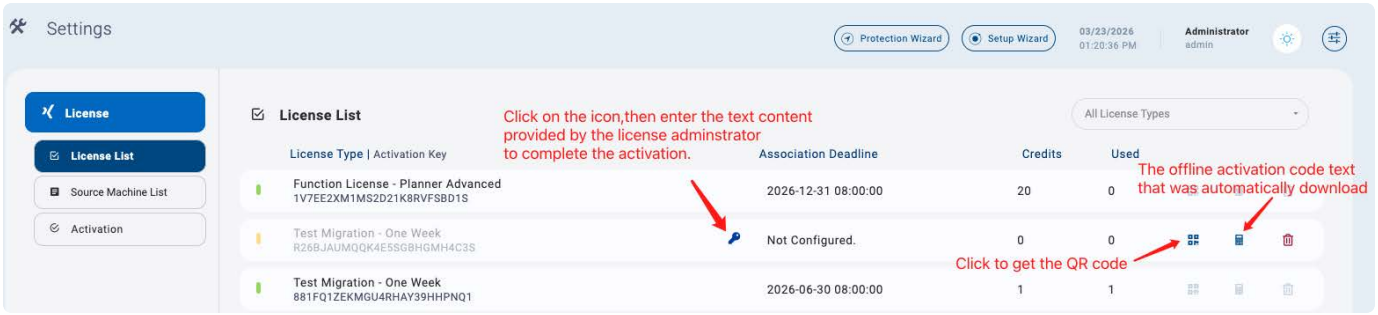
When online activation is not possible, enter the `display name`, `email address`, and `activation key`, and click `Download offline activation file` to automatically jump to the "Authorization Key" page and automatically download the offline activation code.

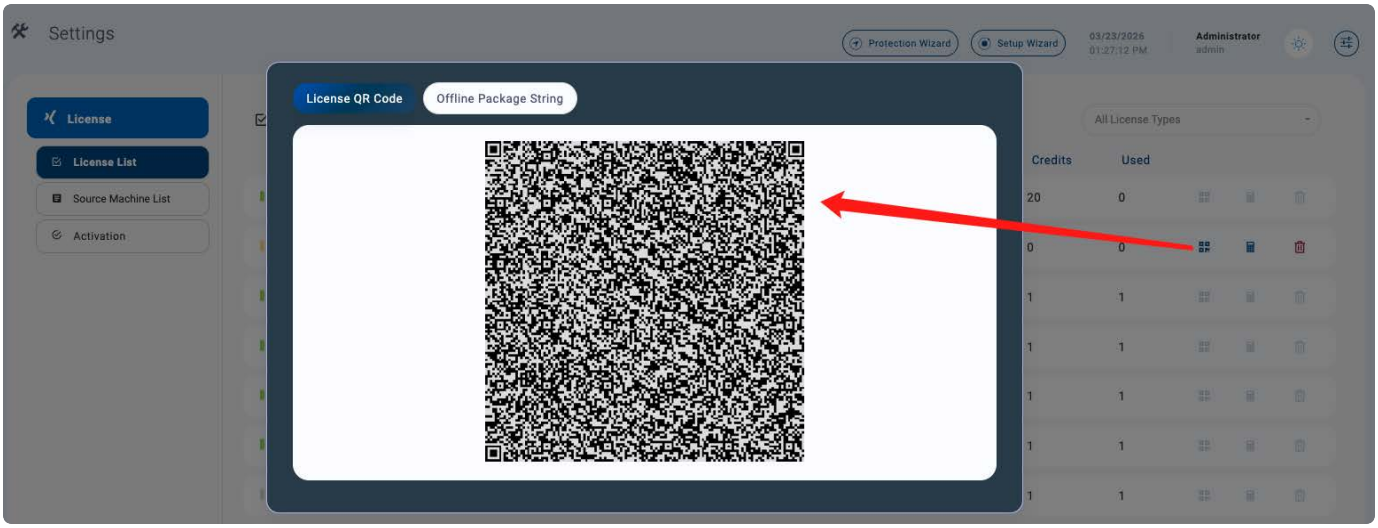


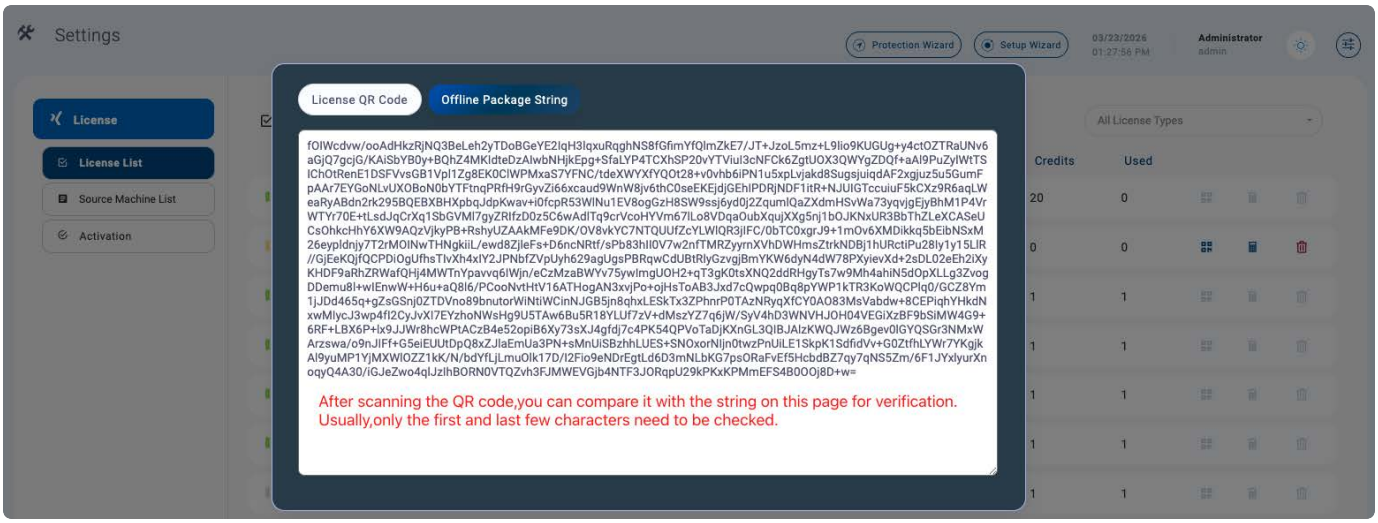
"Authorization Key" page

- The QR code of the offline activation code has the same content as the text of the offline

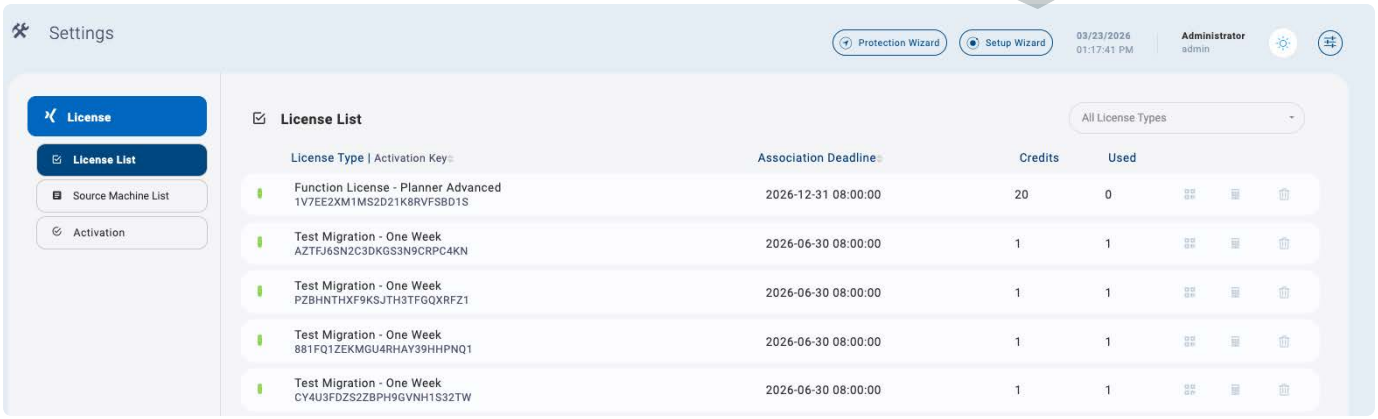
activation code. The QR code is suitable for scenarios where it is inconvenient to take out the text.





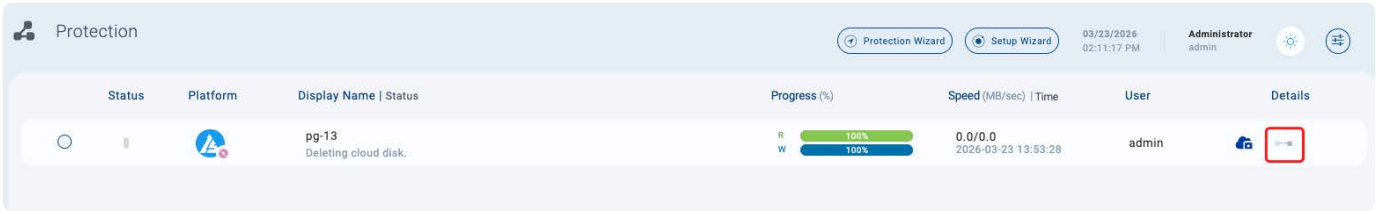


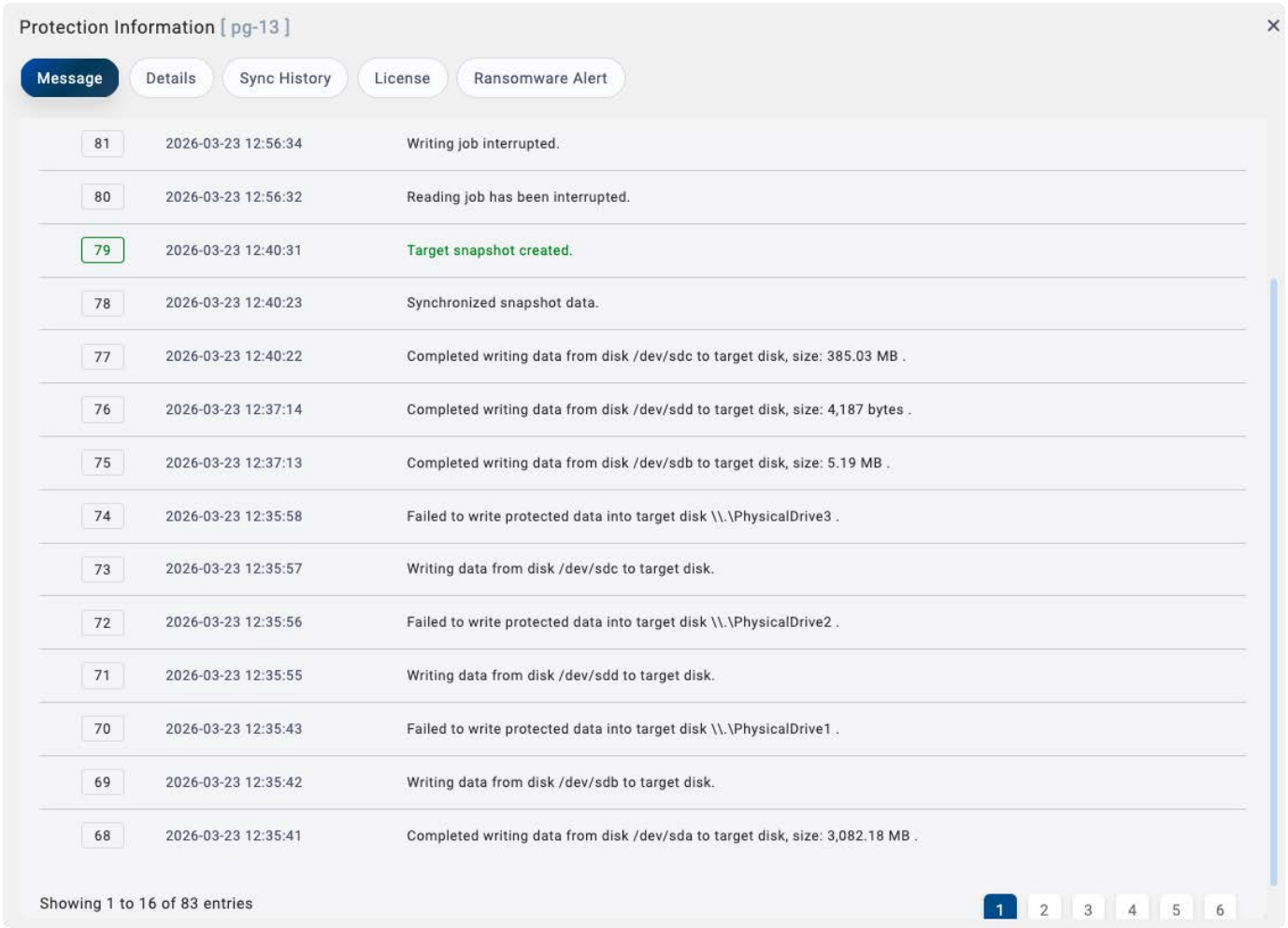
License activated status


Settings
Protection Wizard
Setup Wizard
03/23/2026
01:17:41 PM
Administrator
admin
License
License List
Source Machine List
Activation
License List
All License Types
License Type | Activation Key
Association Deadline
Credits
Used
Function License - Planner Advanced
1V7EE2XM1MS2D21K8RVFSBD1S
2026-12-31 08:00:00
20
0
Test Migration - One Week
AZTFJ6SN2C3DKGS3N9CRPC4KN
2026-06-30 08:00:00
1
1
Test Migration - One Week
PZBHNTHXF9KSJTH3TFGQXRFZ1
2026-06-30 08:00:00
1
1
Test Migration - One Week
881FQ1ZEKMGU4RHAY39HHPNQ1
2026-06-30 08:00:00
1
1
Test Migration - One Week
CY4U3FDZS2ZBPH9GVNH1S32TW
2026-06-30 08:00:00
1
1

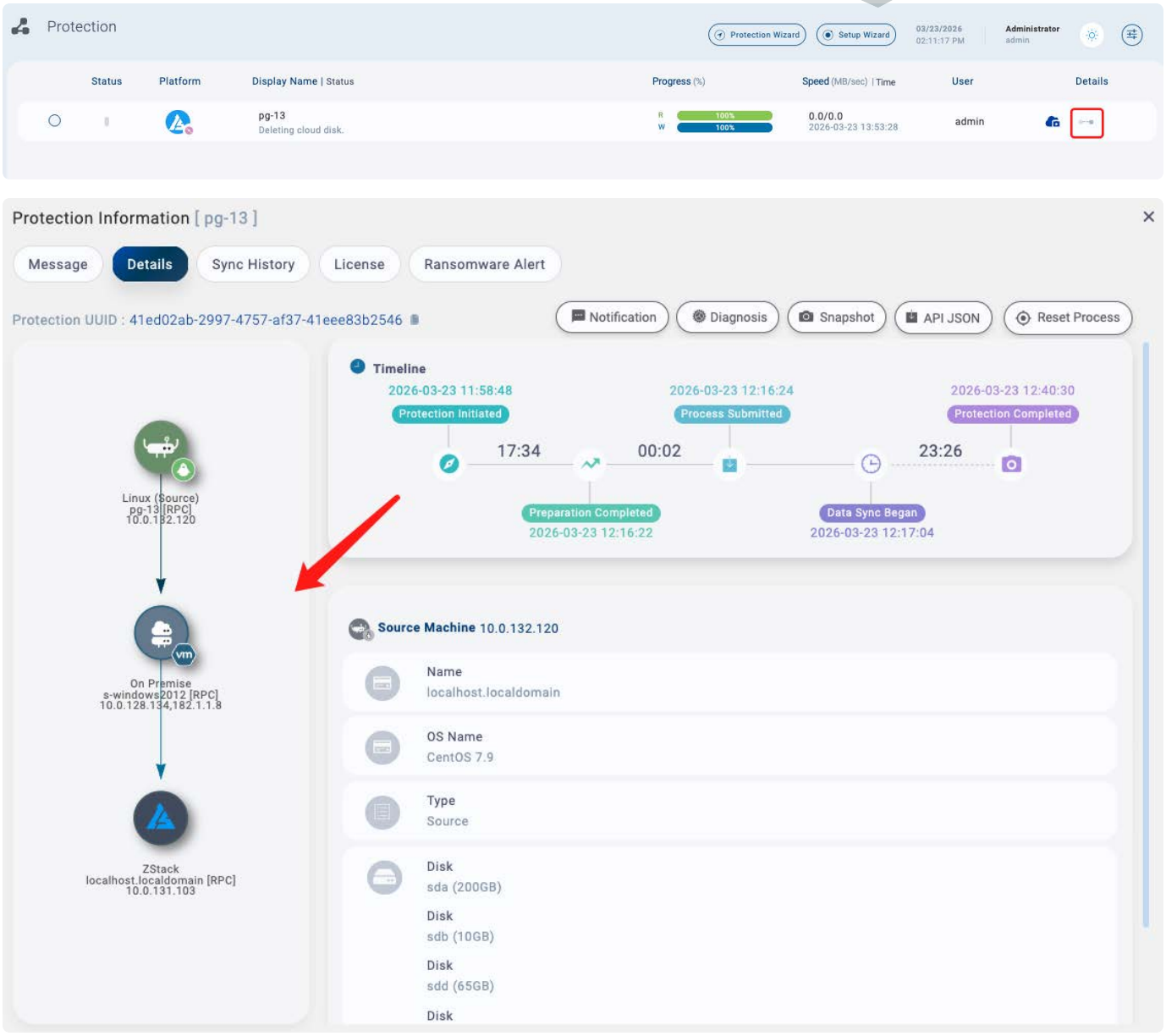
Common operation guide chart of ZMigrate console

View error message

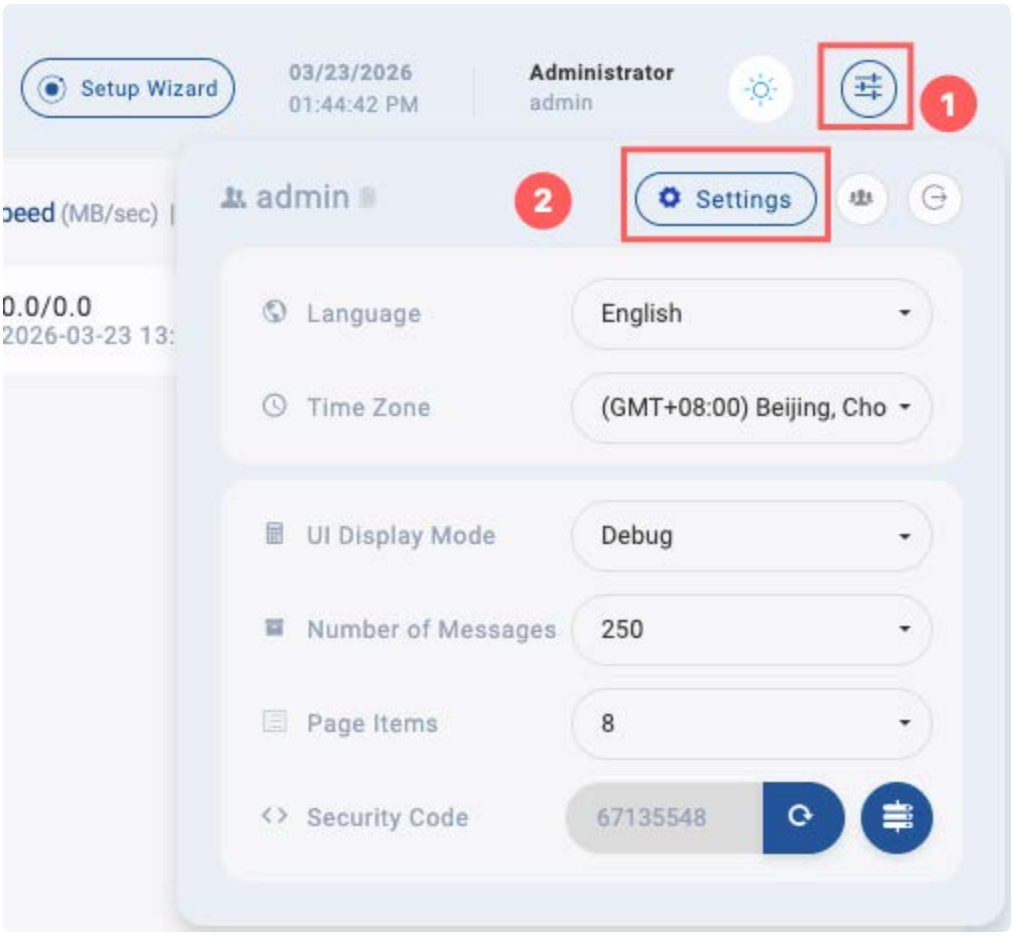


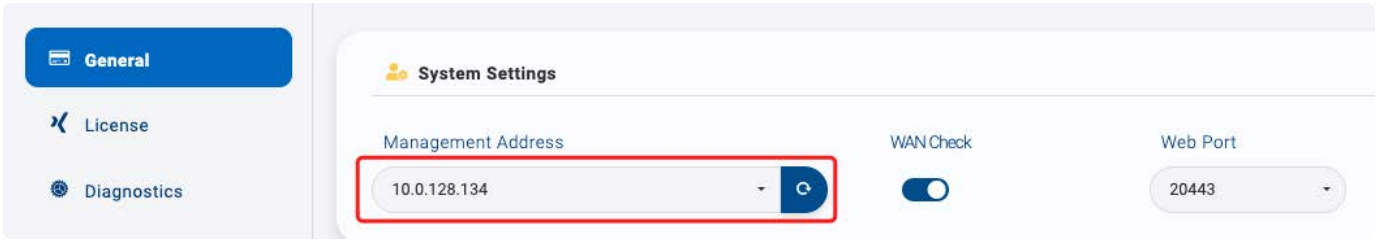


View the replication topology diagram



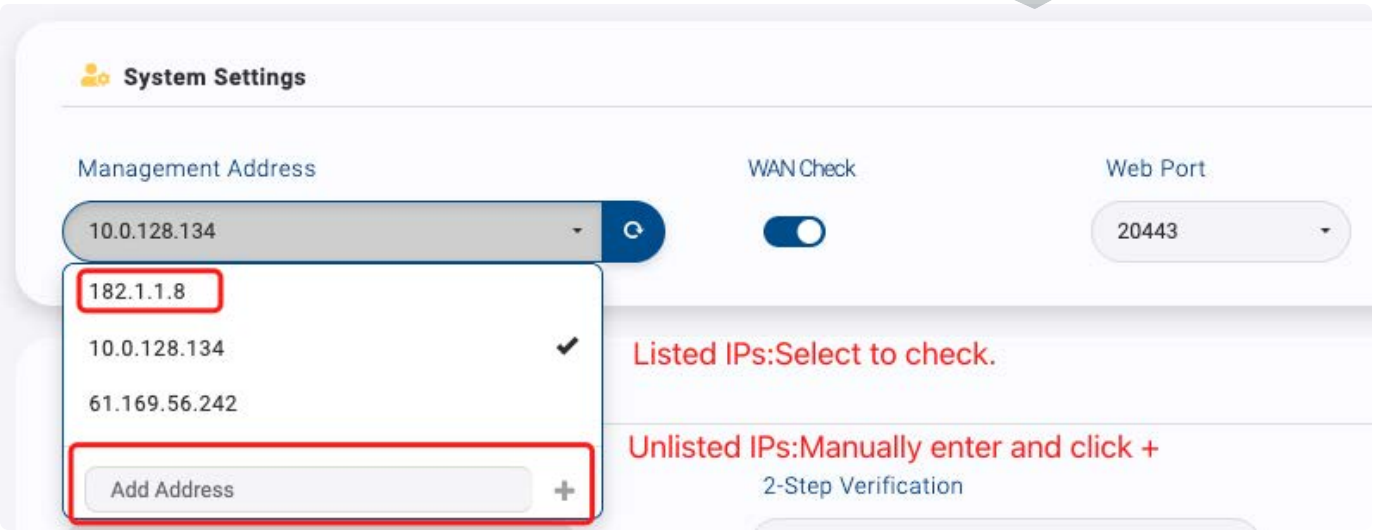
Check the management console IP





Increase/decrease management console IP

Uncheck to reduce the management console IP.

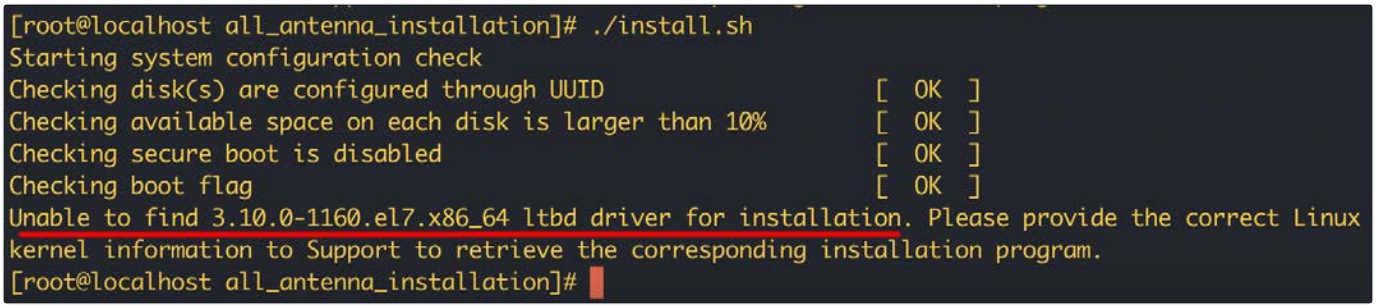

System Settings
Management Address
WAN Check
Web Port
10.0.128.134
20443
182.1.1.8
10.0.128.134
61.169.56.242
Add Address
Listed IPs:Select to check.
Unlisted IPs:Manually enter and click +
2-Step Verification

Linux Antenna installation issues

Document Category: Product Related Experience

The Agent corresponding to the kernel version is missing

```
Unable to find <kernel> ltd driver for installation.
Please provide the correct Linux kernel information to Support to retrieve
the corresponding installation program.
```



reason

No advance research was done.

solution

The Agent installation package for this kernel version is missing, **Please open a Linux Antenna compilation work order**.

- You can go to the after-sales group to obtain the work order address, account password.

Need to provide:

1. Error screenshot to confirm this is the problem.
2. **Required items**: Kernel version and system version, preferably screenshots + text.
    - like:
        - System version: CentOS7.9

NEXAVM

- Kernel version: 3.10.0–1160.el7.x86_64

```
[root@localhost all_antenna_installation]# uname -r
3.10.0-1160.el7.x86_64
[root@localhost all_antenna_installation]# cat /etc/redhat-release
CentOS Linux release 7.9.2009 (Core)
[root@localhost all_antenna_installation]#
```

Port 20005 is occupied by services

```
1  Checking service port status          [FAILED]
2  Service port is occupied by :
3  tcp LISTEN users:(("sshd",pid=1135,fd=3)) tcp LISTEN users:(("sshd",pid=113
   5,fd=4))
4  Failed to install Antenna for Linux. Please copy the installation log file
   and provide it to your support window.
```

```
[root@localhost all_antenna_installation]# ./install.sh
Starting system configuration check
Checking disk(s) are configured through UUID                  [  OK  ]
Checking available space on each disk is larger than 10%      [  OK  ]
Checking secure boot is disabled                              [  OK  ]
Checking boot flag                                            [  OK  ]
Checking service port status                                  [  FAILED  ]
Service port is occupied by :
tcp LISTEN users:(("sshd",pid=1135,fd=3)) tcp LISTEN users:(("sshd",pid=1135,fd=4))
Failed to install Antenna for Linux. Please copy the installation log file and provide it to your support window.
[root@localhost all_antenna_installation]#
```

reason

A business in the user environment is using port 20005, which conflicts with antenna's default port.

solution

NEXAVM

```
#Using disable-listen option to disable 20005 port listening during instal
lation
./install.sh disable-listen

#!!!installation with disable-listen option,the antenna is in a non-runnin
g state by default.

#Usage steps
1.register agent to mgmt by HTTPS mode.
2.start antenna service.
cd /usr/local/antenna/
./antenna --restart
3.create sync task.
```

```
[root@localhost all_antenna_installation]# ./install.sh disable-listen
Starting system configuration check
Checking disk(s) are configured through UUID                    [  OK  ]
Checking available space on each disk is larger than 10%        [  OK  ]
Checking secure boot is disabled                                [  OK  ]
Checking boot flag                                              [  OK  ]
Installing snapshot driver module                               [  OK  ]
Installing Antenna service                                      [  OK  ]
Checking snapshot driver status                                 [  OK  ]
Checking Antenna service status                                 [  OK  ]
Installation completed.
[root@localhost all_antenna_installation]#
```

Installation error rpmdb: BDB0113 Thread/process

```
rpmdb: BDB0113 Thread/process <数字>/<数字> failed: BDB1507 Thread died in B
erkeley DB library
error: db5 error(-30973) from dbenv->failchk: BDB0087 DB_RUNRECOVERY: Fata
l error, run database recovery
error: cannot open Packages index using db5 -  (-30973)
error: cannot open Packages database in /var/lib/rpm
```

```
error: rpmdb: BDB0113 Thread/process 19863/140400656549952 failed: BDB1507 Thread died in Berkeley DB library
error: db5 error(-30973) from dbenv->failchk: BDB0087 DB_RUNRECOVERY: Fatal error, run database recovery
error: cannot open Packages index using db5 -  (-30973)
error: cannot open Packages database in /var/lib/rpm
error: rpmdb: BDB0113 Thread/process 19863/140400656549952 failed: BDB1507 Thread died in Berkeley DB library
error: db5 error(-30973) from dbenv->failchk: BDB0087 DB_RUNRECOVERY: Fatal error, run database recovery
error: cannot open Packages database in /var/lib/rpm
```

reason

The rpm of the user environment is abnormal.

solution

The error reported is rpmdb error, and the user's operation and maintenance needs to solve the rpm problem before installing the Agent.

```
#Check the processes related to RPM;it is possible that some RPM processes are hung.
ps -ef |grep rpm
```

Use any rpm-related command to check whether the rpm can be executed normally:

```
#Use rpm command to query which kernels are installed.
rpm -qa |grep kernel
```

- If the output can be normal, the rpm problem can be eliminated.
- If the output cannot be normal, the user needs to solve the rpm problem before installing the Agent.
  - According to the experience of a certain project, after restarting the server, rpm will return to normal.
  - According to a certain project, the experience provided by the NexaVM implementation engineer (no restart required):
    - For reference only, users are asked to decide whether to use this method after internal evaluation.

```
#The RPM database is corrupted; rebuild the RPM database.

#backup
tar zcvf /var/lib/rpmbak.tar.gz  /var/lib/rpm
rm -f /var/lib/rpm/__db.[0-9][0-9]*
rpm --quiet -qa

#rebuild
rpm --rebuilddb
yum clean all
```

Checking available space on each disk is larger than 10% during installation [FAILED]

```
[root@webtools all_antenna_installation]# ./install.sh
Starting system configuration check
Checking available space on each disk is larger than 10%        [FAILED]
Please correct the above configuration error after installation... Press any key to continue.
Checking secure boot is disabled                                [  OK  ]
Checking default boot kernel                                    [  OK  ]
Checking service port status                                    [  OK  ]
Installing snapshot driver module                               [  OK  ]
Installing Antenna service                                      [  OK  ]
Checking snapshot driver status                                 [  OK  ]
Checking Antenna service status                                 [  OK  ]
Installation completed.
[root@webtools all_antenna_installation]#
```

reason

If there is only this error and everything else is OK, it means the Agent was successfully installed, but the free space at a mount point in the user environment is less than 10%, which is not enough to meet the default size requirement for creating a snapshot.

Solution 1. Clean up or make space

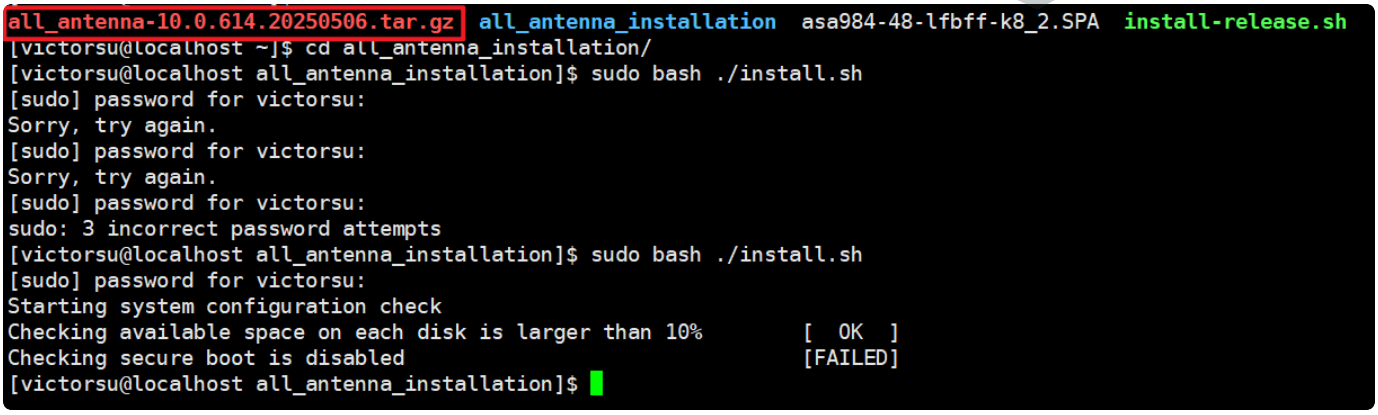
Please operate and maintain personnel to free up 10% or more space at the designated mount point.

Solution 2. Modify ratio

Refer to the knowledge base "Linux Modification Ratio (Snapshot Size)".

Checking secure boot is disabled during installation [FAILED]

NEXAVM




```
file /usr/local/antenna/antenna conflicts between attempted installs of antenna-10.8.612-1.x86_64 and antenna-18.8.614-1.x86_64
```

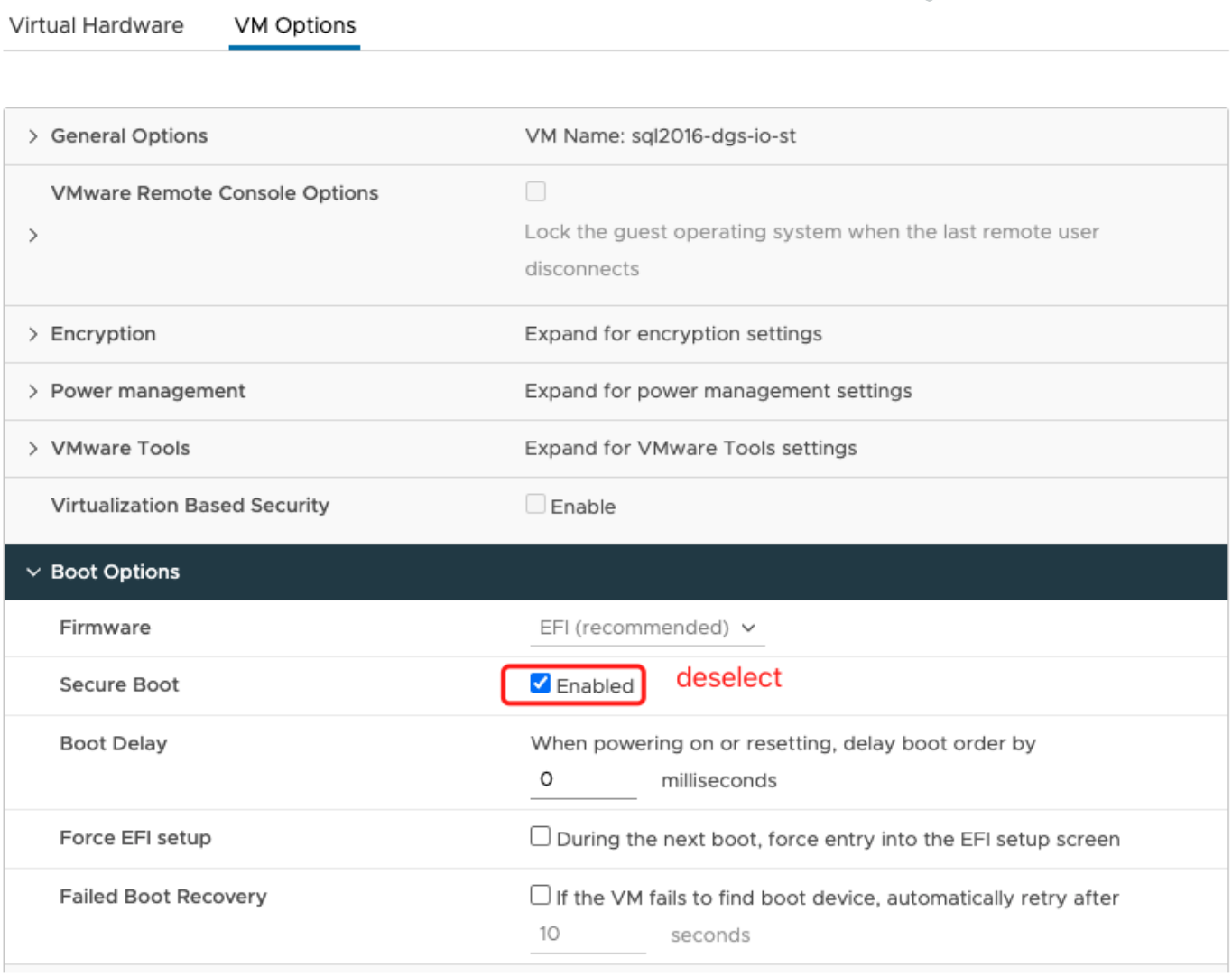
reason

Secure boot is not turned off on the source host.

solution

Turn off secure boot on the source host.

Operation to turn off secure boot (take VMware virtual machine as an example):



Checking antenna boot entry [FAILED]

Reason

When installing the Agent, the grub.cfg of the source machine will be backed up and a disable driver boot item will be added. When an error is reported, it means that this boot item was not successfully added, which generally does not affect synchronization and switching.

But if the system is CentOS6 series or Redhat6 series, please contact Support for processing. These two versions of the system have been optimized and theoretically will not encounter this problem.

When installing the Agent, I wait for a long time at a certain step.

Complete installation steps (for comparison and reference)

```
[root@localhost all_antenna_installation]# ./install.sh
Starting system configuration check
Checking disk(s) are configured through UUID                    [  OK  ]
Checking available space on each disk is larger than 10%        [  OK  ]
Checking secure boot is disabled                                [  OK  ]
Checking boot flag                                              [  OK  ]
Checking service port status                                    [  OK  ]
Installing snapshot driver module                               [  OK  ]
Installing Antenna service                                      [  OK  ]
Checking snapshot driver status                                 [  OK  ]
Checking Antenna service status                                 [  OK  ]
Installation completed.
[root@localhost all_antenna_installation]#
```

reason

The rpm of the user environment is abnormal.

solution

If you wait for a long time at a certain step, there is probably a problem with rpm.

You can use any rpm-related commands to troubleshoot:

```
rpm -qa |grep kernel
```

- If the output can be normal, the rpm problem can be eliminated.
- If the output cannot be normal, the user needs to solve the rpm problem before installing the Agent.
    - According to the experience of a certain project, after restarting the server, rpm will return to normal.
    - According to a certain project, the experience provided by the NexaVM implementation engineer (no restart required):
        - For reference only, users are asked to decide whether to use this method after

internal evaluation.

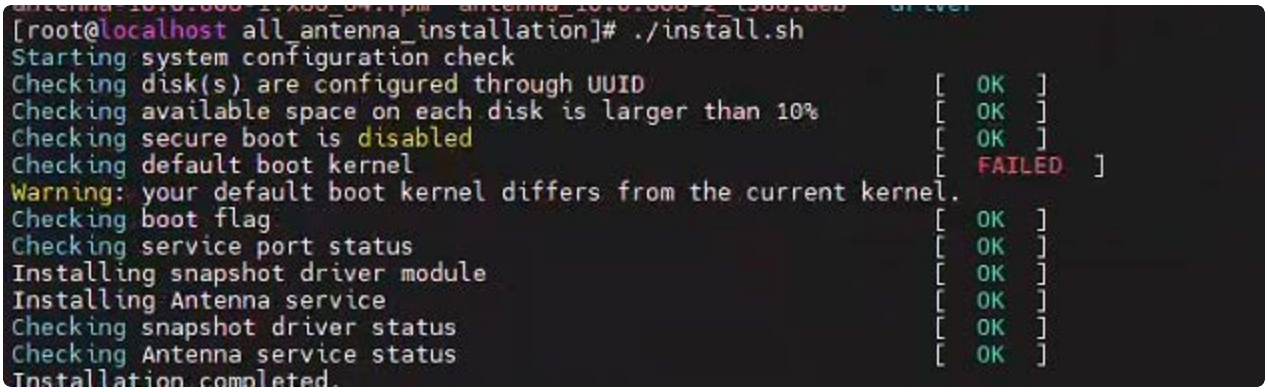
```
#The RPM database is corrupted; rebuild the RPM database.

#backup
tar zcvf /var/lib/rpmbak.tar.gz  /var/lib/rpm
rm -f /var/lib/rpm/__db.[0-9][0-9]*
rpm --quiet -qa

#rebuild
rpm --rebuilddb
yum clean all
```

Checking default boot kernel FAILED during installation

```
Checking default boot kernel          [FAILED]
```



reason

The currently running kernel is inconsistent with the next boot kernel.

```
#Check the currently running kernel.
uname -r

#Check the kernel for the next boot (using CentOS 7 as an example).
cat /boot/grub2/grubenv
```

solution

NEXAVM

> Users are asked to evaluate which core they expect to run on, and use this as a baseline to confirm which solution to use.

Option 1

- Modify the next boot kernel to the current kernel.

Option 2

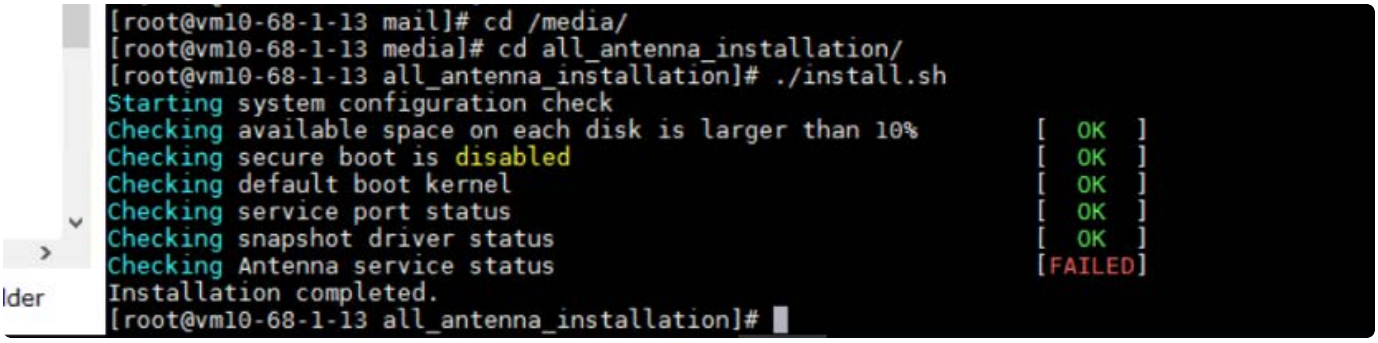
- Uninstall antenna, reboot to the next boot kernel and reinstall antenna.

Option three

- Do the migration normally. After migrating to the target platform, manually select the currently running kernel to start.

When installing the Agent, Checking Antenna service status FAILED

```
1   Checking Antenna service status         [FAILED]
```



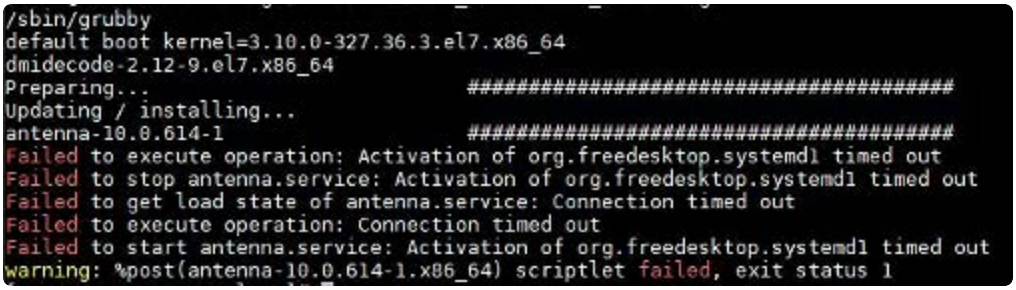
reason

The systemd (systemctl) of the user environment is abnormal, causing the installation to fail.

Error log: logs/install.log

```
1   Failed to execute operation: Activation of org.freedesktop.systemd1 timed o
    ut
2   Failed to antenna.service: Activation of org.freedesktop.systemd1 timed out
```

NEXAVM



Use systemctl to check the status of any service. If an error is reported, it is confirmed to be a systemd (systemctl) exception.

```
#check sshd service status
systemctl status sshd
```

solution

This problem is caused by the user environment. Please repair the systemd (systemctl) of the source host.

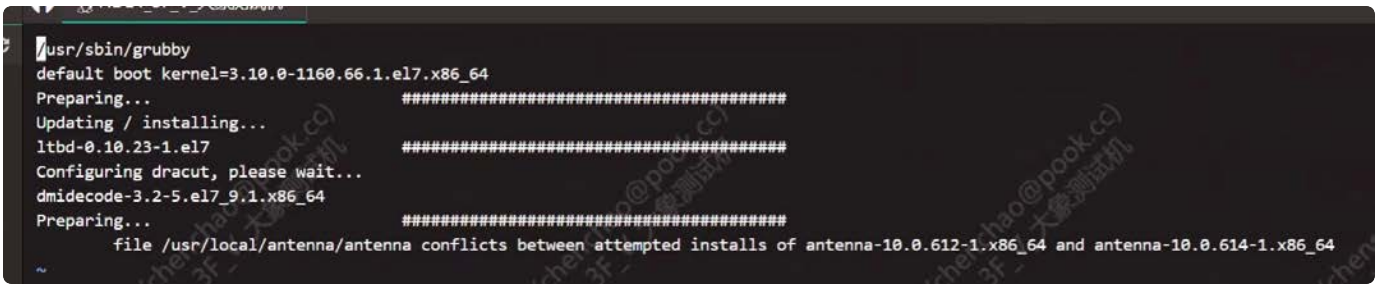
Reference plan 1 (please evaluate the operation carefully): Force restart

```
reboot -f
```

Reference plan 2:

1. Upgrade systemd.

An error occurs when installing Agent. Checking the installation log shows that there are multiple versions of Agent.




```
file /usr/local/antenna/antenna conflicts between attempted installs of ant
enna-10.8.612-1.x86 64 and antenna-18.8.614-1.x86 64
```

reason



The user decompresses the installation packages of multiple versions and decompresses them to the same folder. The installation packages of multiple versions are in the same folder.

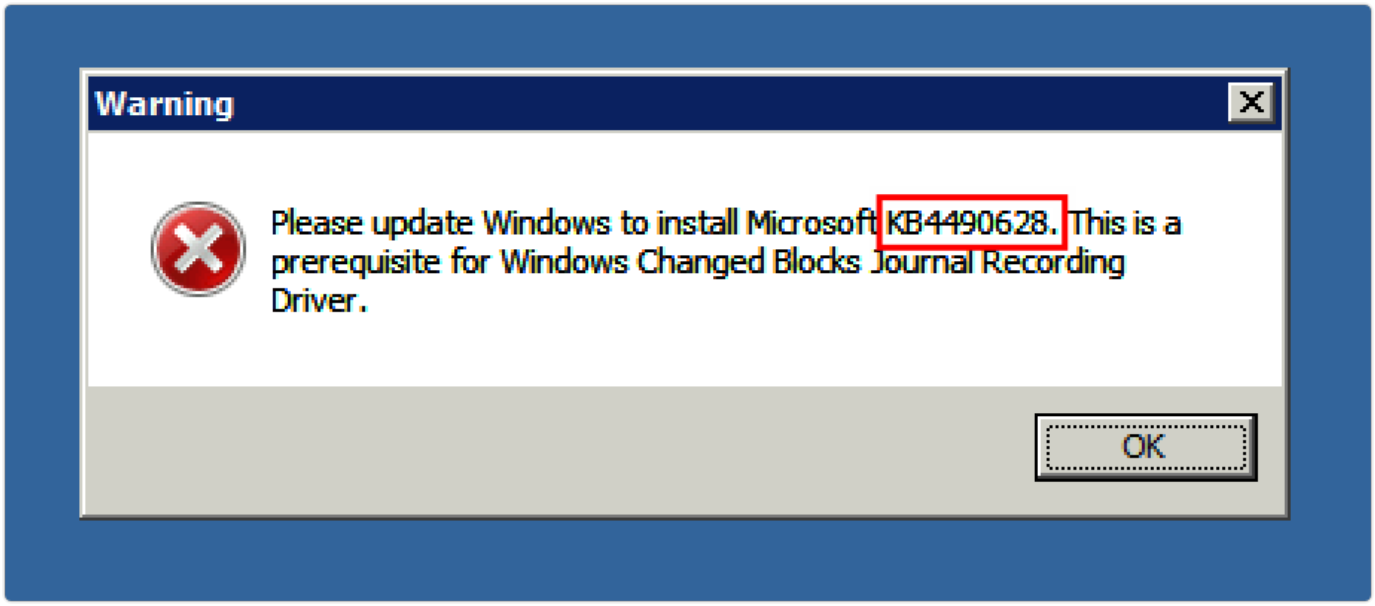
solution

Delete the decompressed installation package folder and decompress it again.

Windows Antenna installation issues

Document Category: Product Related Experience

Installing agent prompts that KB is missing



Official Website Download Link：Microsoft Update Catalog

Serial number	System version	Required KB
1	Win7 64-bit	kb4490628, kb4474419
2	Windows 2008 32-bit	kb4493730, kb4474419
3	Windows 2008 64-bit	kb4493730, kb4474419
4	Windows 2008 R2 64-bit	kb4490628, kb4474419

reason

The user system has not been updated with the security patches provided by Windows.

Solution 1

NEXAVM

Install the corresponding KB according to the prompt information. After installing the KB, install the agent.

- When installing kb4474419, you will be asked to restart the server, so you need to arrange the time to install KB appropriately.

Solution 2

If the user does not agree to install the KB, or cannot install the KB, please refer to the knowledge base "Manual Installation of Windows Antenna".

- **Note: Without installing the required KB, migration cannot be performed normally in increments. Each synchronization is a checksum (compared with differential data transmission), which is slower than increments. **

Possible problems

The KB installation prompt does not apply to your system version

- Please confirm that the downloaded KB matches the operating system type. 32-bit and 64-bit KB are not compatible with each other.
- If it is confirmed that the KB is downloaded correctly, it may be caused by a Microsoft bug.
  - Computer Manager has a knowledge base for reference: When installing msu patch, it shows that the computer is not applicable
  - Please **evaluate carefully** whether to use the method provided by Computer Manager to install KB.
    - The source host is a virtual machine. You can consider cloning one and trying the above method to install the KB.

Windows Treker installation issues

Document Category: Product Related Experience

System requirements for installing Treker

Windows Server2016 and above

- Windows Server 2016 or 2019 is recommended.
- Be sure to install performance optimization tools and enable virtio.
- It is recommended to use **Legacy mode** of Windows for installing Treker.
    - A Win2016.qcow2 image is provided.

Do I need to check management during installation?

- Must be checked when used as a management console.
- When used as a transit server, you can uncheck it, and checking it will not affect the use.

Unable to open management console after installation

reason

The system has IIS installed or other services occupying port 80. It is recommended to use a clean system to install Treker.

solution

1. Check whether the apache service is running normally.
2. Check whether port 80 is occupied.

NEXAVM

3. Uninstall and disable services and applications that occupy port 80.

Reference command

```
#check port
pid: netstat -ano|findstr "80"

#Check the program corresponding to the PID,assuming the PID for port 80 fr
om the previous check is 1076.
tasklist|findstr 1076

#Terminate the process and its child processes(F:force,T:child-processes)
#Assuming the PID for port 80 is 1076.
taskkill /T /F /PID 1076
```

HTTPS registration source machine failed

Document Category: Product Related Experience

Problem analysis

Reason 1

The user's source host time is too different from the management console time.

Reason 2

Generally, it is mostly caused by the user's network problems. In a few cases, it is due to storage abnormalities on the source machine.

Check whether it is a timing issue

Log in to the source host to check the time and compare it with the time on the management console.

Check if there is a network problem

Windows

- Open a browser on the source machine to access the management console.
  - Can be accessed normally and the network is normal.
  - If you cannot access it normally, troubleshoot the network problem.

Linux

- There is a graphical interface to install, open the browser to access the management console.

    - Can be accessed normally and the network is normal.
    - If you cannot access it normally, troubleshoot the network problem.
- No graphical interface is installed, use telnet to test the port of the management console.
    - General situation:
        - If the 20000, 20001, and 20443 ports of the telnet management console can be connected, the network problem can be eliminated.
    - Special circumstances:
        - Linux has a network proxy configured, so telnet can work, but registration may not be successful. Please turn off the network proxy before registering.

Troubleshoot whether it is a storage issue

Windows

Open Disk Manager and check whether the status of each disk is normal.

Linux

Execute the command and check whether the output can be normal.

```
1   lshw -c disk
```

Failed to register source machine in RPC mode

Document Category: Product Related Experience

Problem analysis

Reason 1

The user's source host time is too different from the management console time.

Reason 2

Generally, it is mostly caused by the user's network problems. In a few cases, it is caused by storage abnormalities on the source host.

solution

Option 1

Modify the source host time to be consistent with the management console.

- If it is inconvenient to modify the source host, please modify the time of the management console (Not recommended).

Option 2

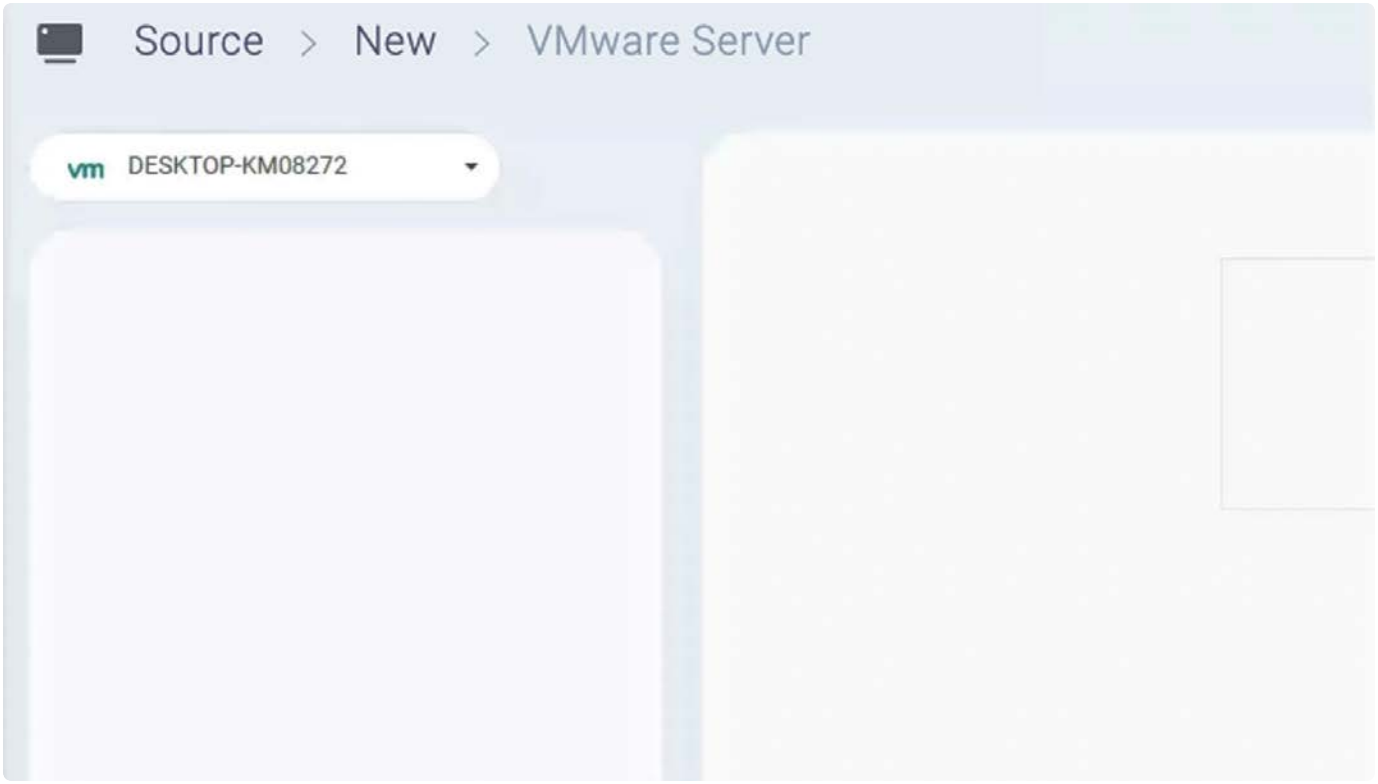
Refer to the knowledge base "Unable to connect to the source host".

Can not display the VMware agentless source VM when adding Resource

Document Category: Third Party Related Experience

Error screenshot

**Some virtual machines may be listed here, or none of the virtual machines may be listed. **



Problem analysis

Refer to "Introduction to Diagnostic Logs" to collect VMware diagnostic logs. You can see that the UUID of ESXi is a string of 0s. View the source host you want to add in `vms`.

So far, such problems have occurred only when ESXi is deployed on physical servers of HP and Inspur, and are caused by BIOS bugs or hard settings of HP and Inspur servers.

NEXAVM



Solution 1. Modify the serial number of the HP server

> Thanks to Man Haoxuan for the solution.
>
> If the serial number is not written in the bios, it will default to 0000000. Even if you enter the bios and write it casually, you have to synchronize it with a non-zero value.

If you have physical access to the server, then you can find the serial number on the service tag. It is located in the front side of the server, check this link: HPE ProLiant DL380 Gen9 Server QuickSpecs to locate it.

Then from UEFI (F9 during POST) follow the below steps in order to enter again the serial number and the product ID:

From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced System ROM Options > Serial Number

From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced System ROM Options > Product ID

NEXAVM

via. https://community.hpe.com/t5/proliant-servers-ml-dl-sl/uuid-and-serial-number-issue/td-p/7034202

Solution 2. Migrate the virtual machine to non-local storage

> Thanks to Liang Zhengde for the information.
>
> VMs on the same ESXi local storage cannot be listed, but VMs in centralized storage can be listed.

Migrate virtual machines to non-local storage, such as shared storage.

Solution 3. Use a proxy instead

Install Antenna and use agent migration.

Add NexaVM to the cloud platform and report an error

Document Category: Product Related Experience

network problems

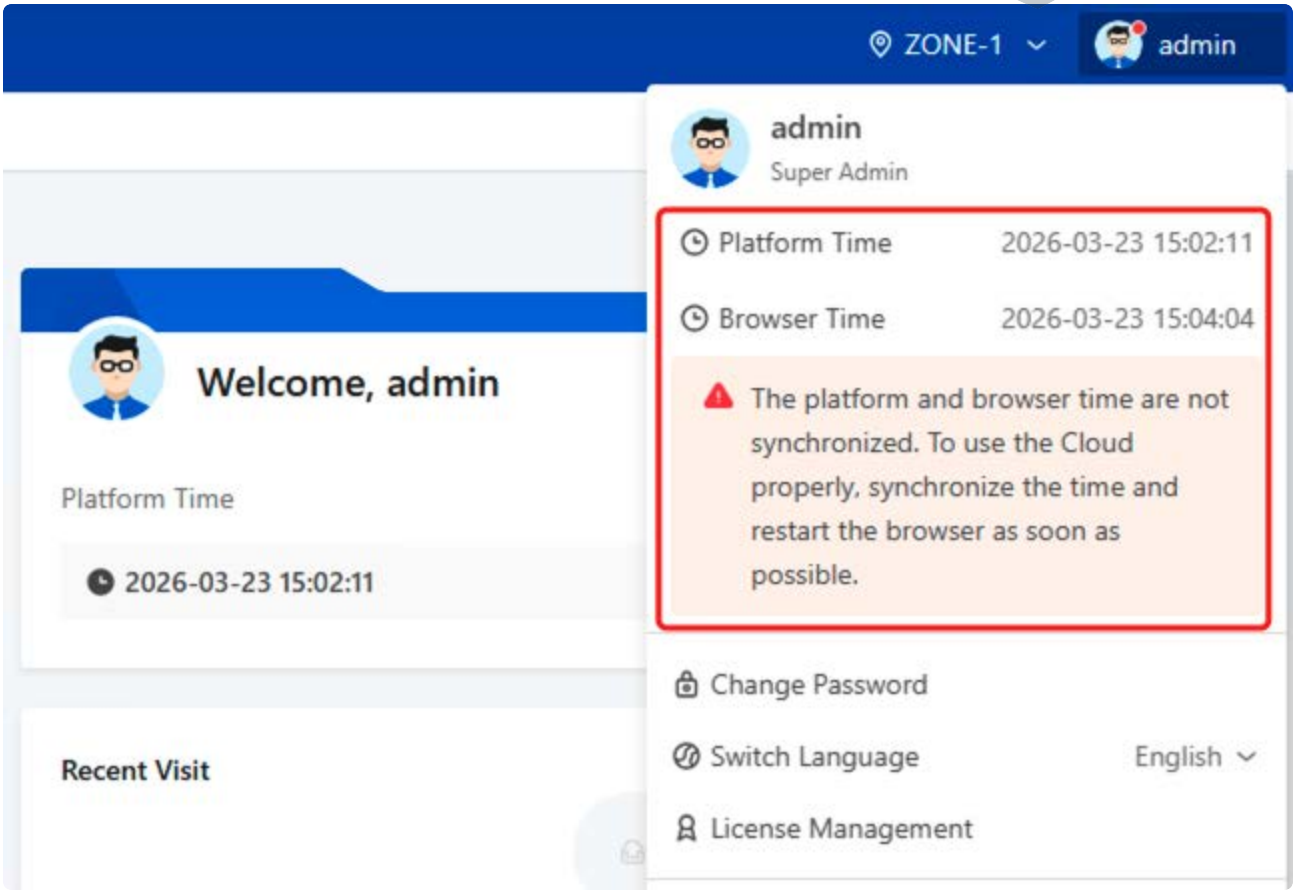
Confirm that the management console can communicate with the 8080 of all NexaVM management nodes (including VIP).

a matter of time

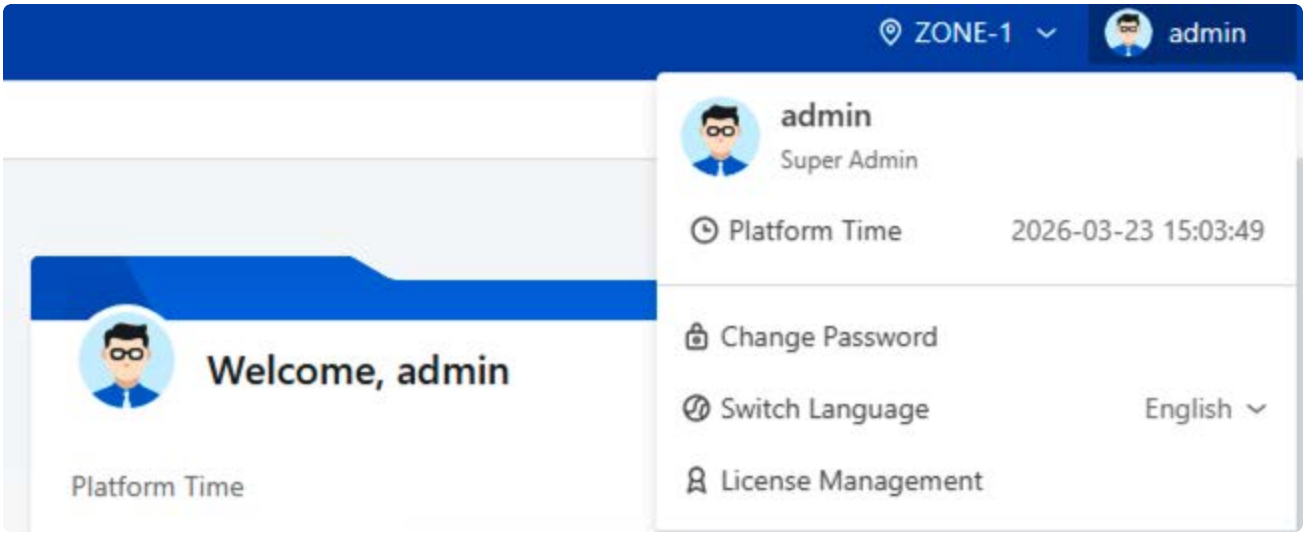
Confirm that the time difference between the management console and NexaVM does not exceed 15 minutes.

- Use a browser to access NexaVM management console in the management console system, click admin to view the cloud platform time.

Screenshot example of inconsistent time



Example of time-consistent screenshots



The NexaVM information filled in is incorrect

Confirm that the NexaVM information filled in is correct.

- Protocol: HTTP
- Address: IP of the web console

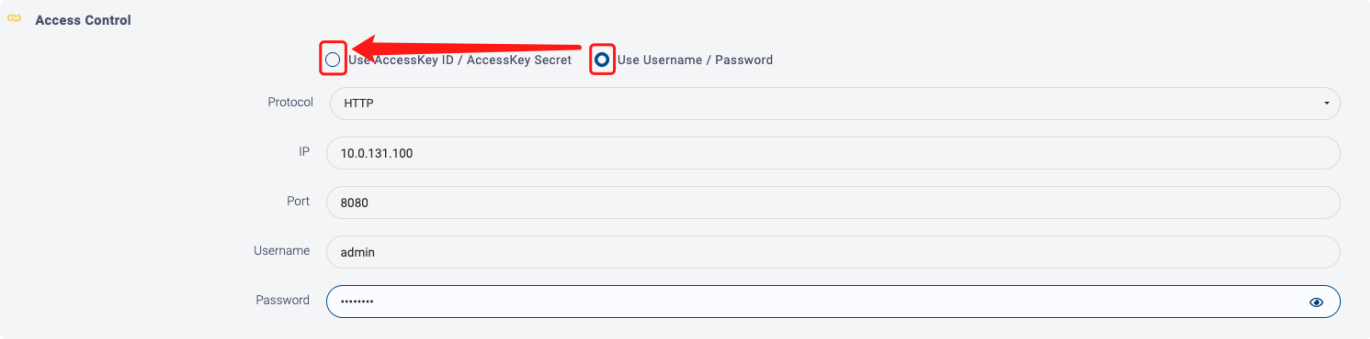
- Port: 8080
- AccessKey ID: Fill in the obtained
- AccessKey Secret: Fill in the obtained
    - For lower versions of NexaVM you must open to see the plain text Key and then copy it! ! !

The filled-in AccessKey has been deleted

Please go to NexaVM to check whether the AccessKey used has been deleted by other maintainers.

The account and password verification method is abnormal.

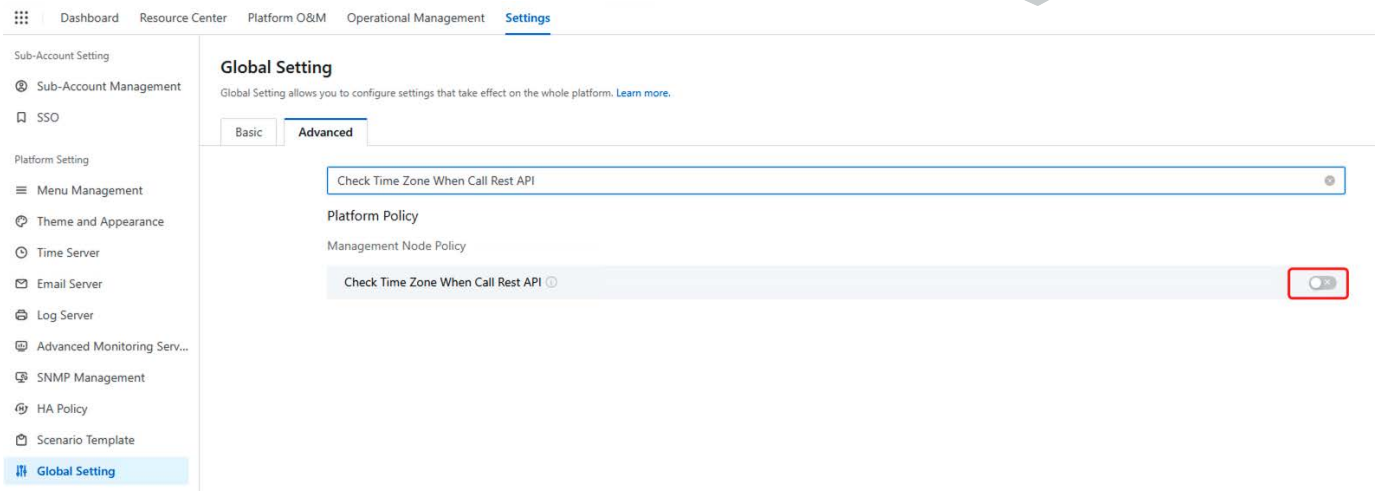
Modify the NexaVM authentication method in the cloud platform: change the `account password` to `AK, SK`.



NexaVM setup issues

Turn off "Call Rest API to check time zone switch" in global settings.

- If this option is turned off, try turning it on.


Dashboard
Resource Center
Platform O&M
Operational Management
Settings
Sub-Account Setting
Sub-Account Management
SSO
Platform Setting
Menu Management
Theme and Appearance
Time Server
Email Server
Log Server
Advanced Monitoring Serv...
SNMP Management
HA Policy
Scenario Template
Global Setting
Global Setting
Global Setting allows you to configure settings that take effect on the whole platform. Learn more.
Basic
Advanced
Check Time Zone When Call Rest API
Platform Policy
Management Node Policy
Check Time Zone When Call Rest API

The IP address is not displayed after adding the source host

Document Category: Product Related Experience

Error screenshot



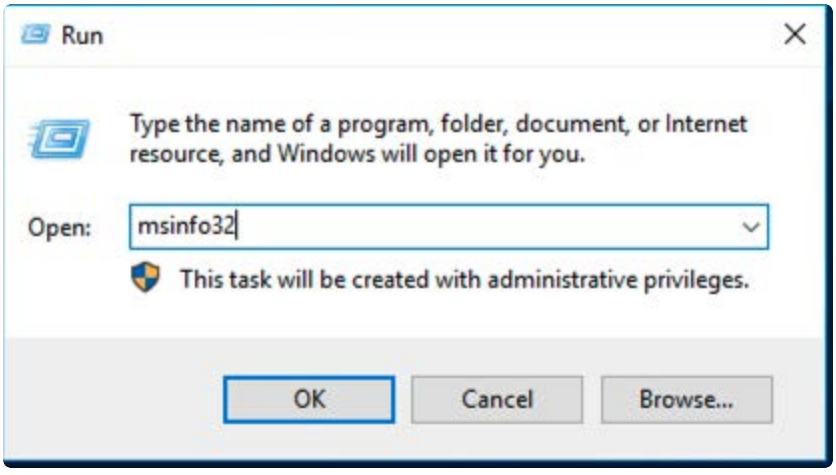
Problem analysis

There is an error in the system environment of the source machine.

Troubleshooting steps

Windows

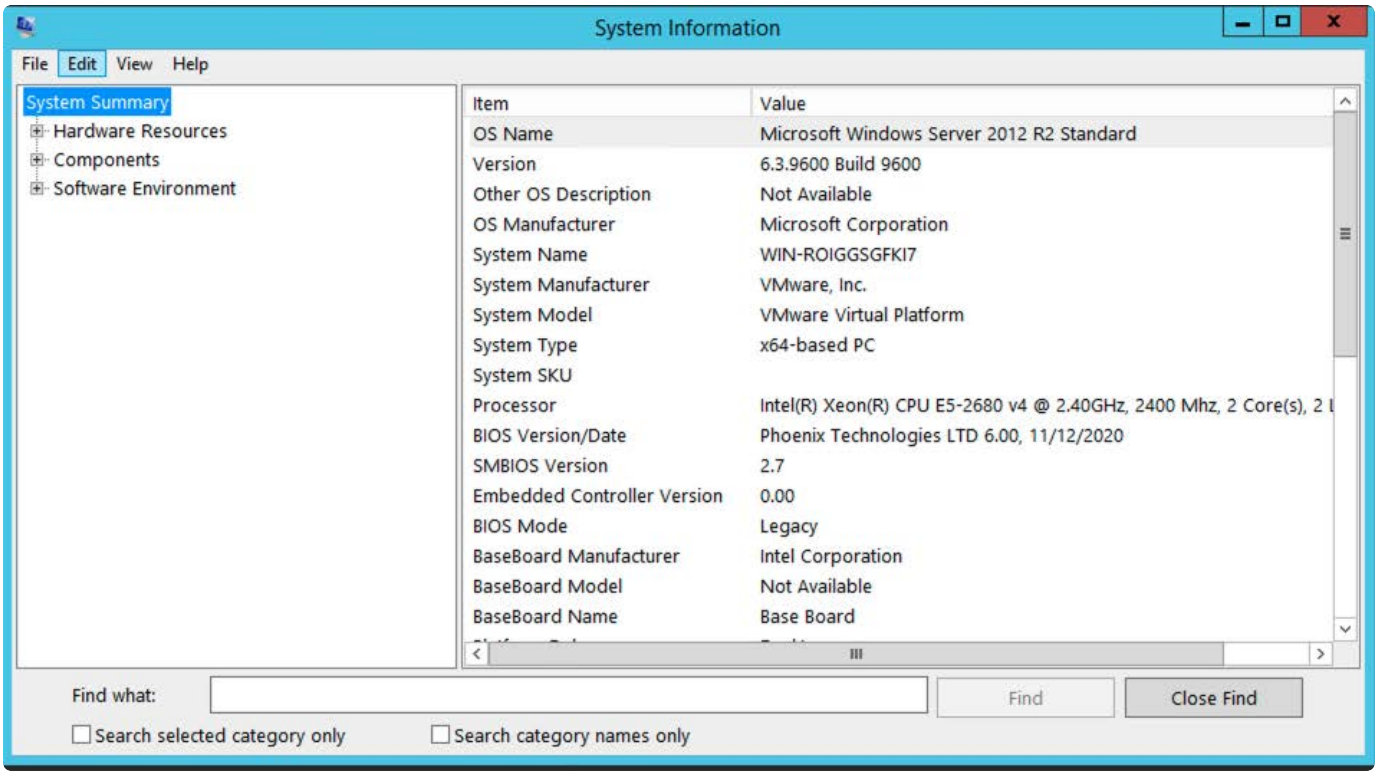
1. run –msinfo32

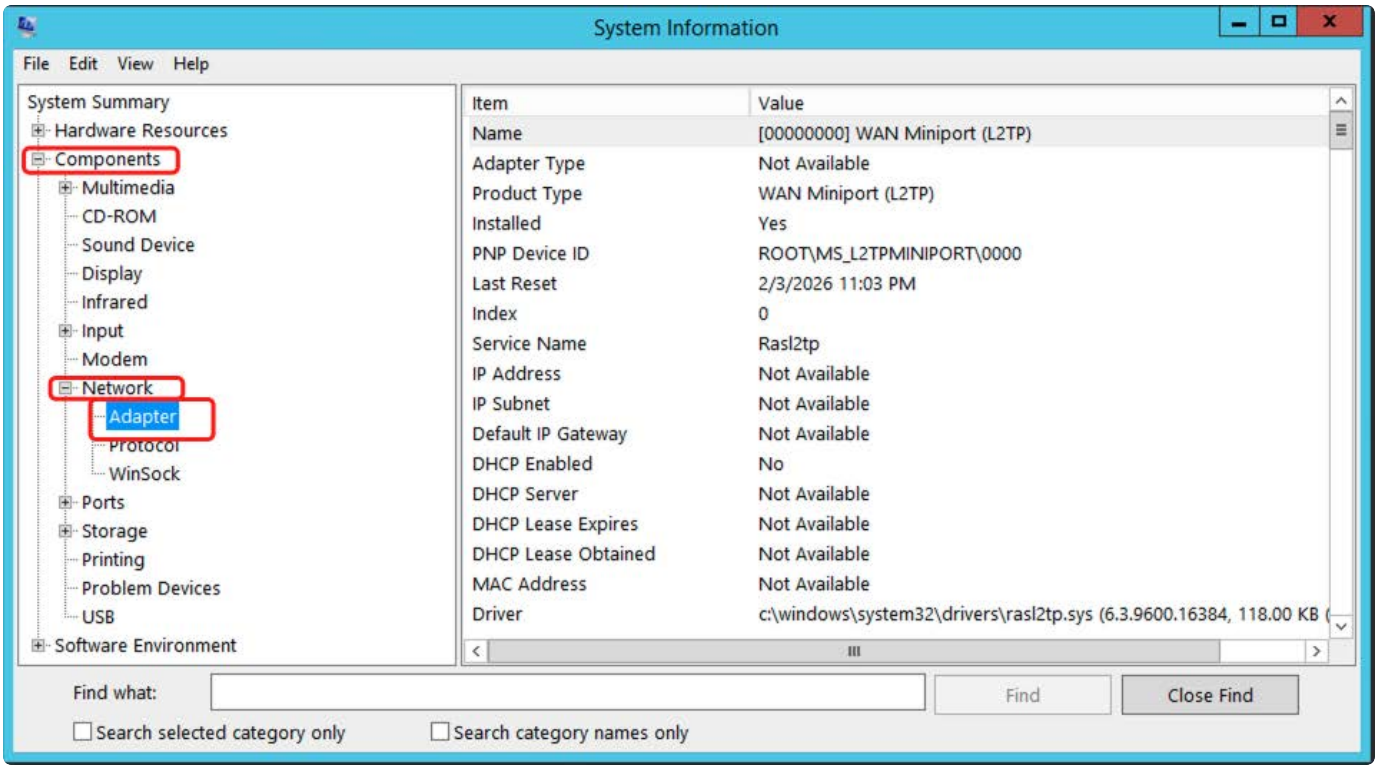


2. Check whether the system information can be loaded normally and whether the IP address is

displayed normally.

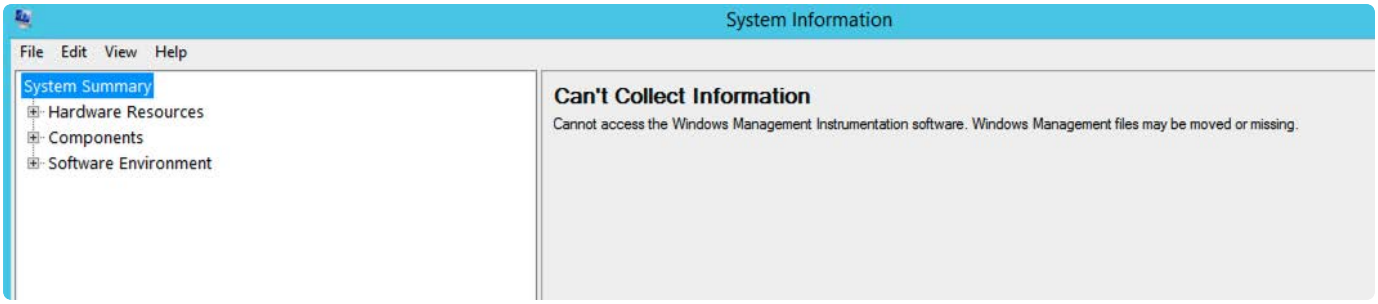
a. It can be loaded normally, excluding errors in the system environment.

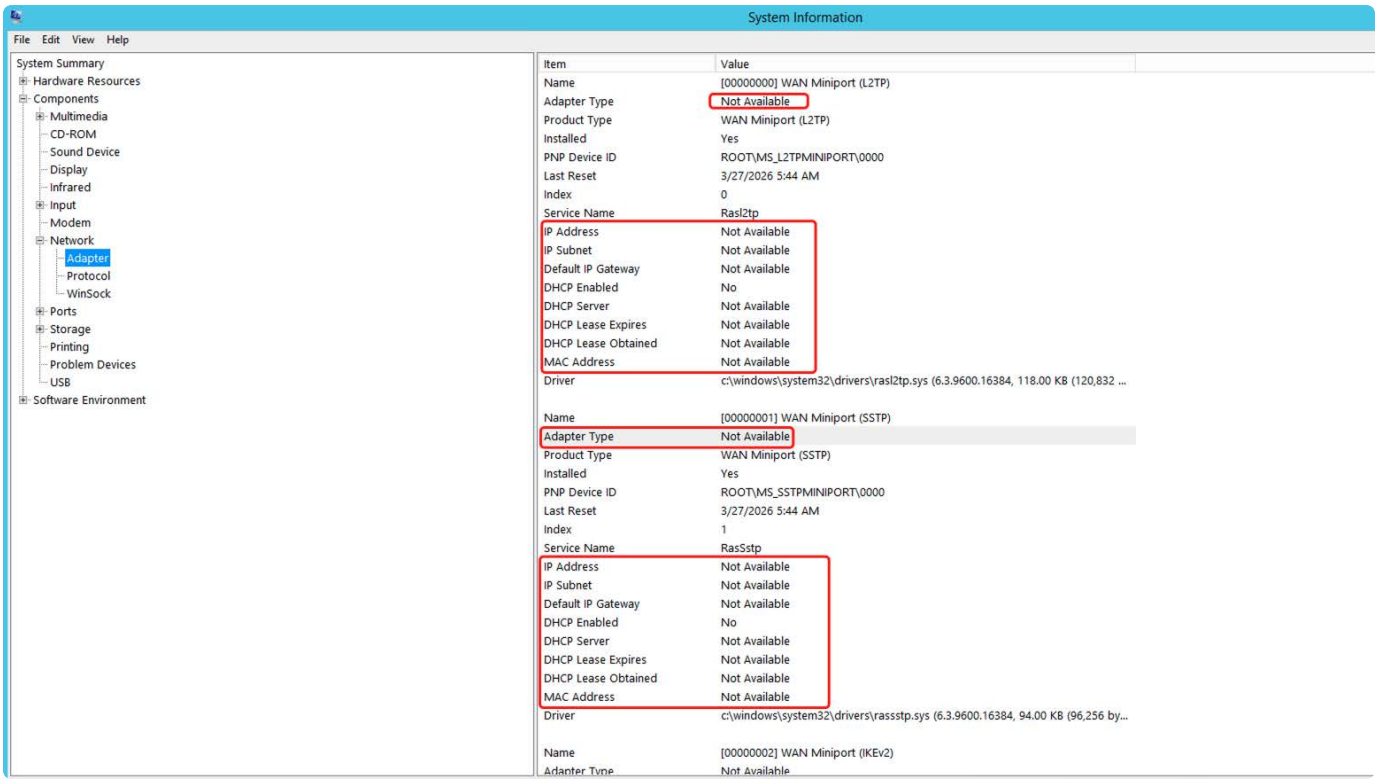




NEXAVM

```
2. It cannot be loaded normally. Please fix the system problem before migrating.
- Fix:
    * Refer to the knowledge base "Windows source machine reports error when executing msinfo32"
    * You can also try to restart the source machine.
```





Linux

1. Log in to the source machine's system.
2. Check out antenna's services.

```
systemctl status antenna
```

3. Observe the output information of antenna.

NEXAVM

```
[root@localhost ~]# systemctl status antenna
● antenna.service - Lightrek antenna
   Loaded: loaded (/etc/systemd/system/antenna.service; enabled; vendor preset: disabled)
   Active: active (running) since 二 2024-03-12 23:42:43 EDT; 1h 23min ago
 Main PID: 6909 (antenna.sh)
   CGroup: /system.slice/antenna.service
           ├─6909 /bin/bash /usr/local/antenna/antenna.sh
           └─6956 /usr/local/antenna/antenna

3月 12 23:42:43 localhost.localdomain systemd[1]: Started Lightrek antenna.
3月 12 23:42:44 localhost.localdomain antenna.sh[6909]: Initializing firewall successful
3月 12 23:42:44 localhost.localdomain antenna.sh[6909]: Starting the server...
[root@localhost ~]#
```

4. Relevant error reports will be reflected in antenna's service status output.

Adding Win 2003 to the management console fails to connect to the source host

Document Category: Product Related Experience

Problem Description

After installing Antenna on Windows Server 2003, adding this Win 2003 machine to the Management Console reports an inability to connect to the source host.

Problem Analysis

1. Other services on the source machine are using port 20005.
2. The SSL version on the source machine is too low to authenticate with the Management Console.
3. The time difference between the source machine and the Management Console exceeds 3 days.

Solution 1: Port 20005 Occupied and SSL Version Too Low

Register the source machine to the Management Console using HTTPS. Please refer to "Registering the Source Host to the Management Console via HTTPS".

Solution 2: Significant Time Difference

Modify the time on the source machine so that the difference with the Management Console does not exceed 3 days.

Legacy booting source host with 2T system disk cause target machine restarts repeatedly

Document Category: Product Related Experience

Fault phenomenon

The target machine restarts repeatedly and cannot enter the IP configuration interface.

Problem analysis

1. Under normal circumstances, Legacy's system disk supports up to 2T.
2. For standard mode migration, the system disk of the target machine needs to be 5G larger than the system disk of the source machine.
3. When the system disk of the Legacy target machine is larger than 2T, this problem will occur after repeated restarts.

Solution 1. Use mount mode

The system disk of the target machine in mount mode does not need to be 5G large. The system disk is still 2T and can be migrated normally.

Solution 2. Split the partitions of the source machine

The source host is a Windows system

Refer to the knowledge base "Windows partition (separate C drive) migration" and "Windows source machine migration using partition script".

The source host is a Linux system

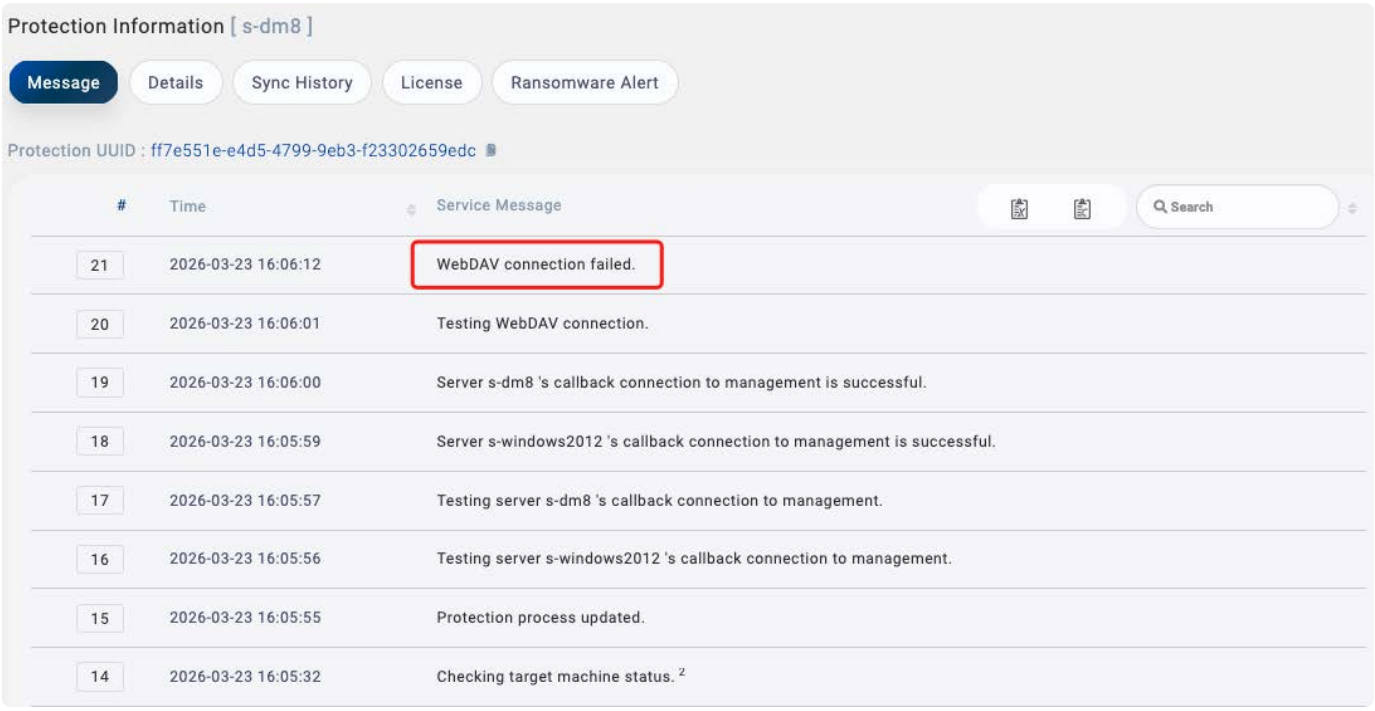
The Linux scenario is more complicated. Please collect the `df -hT` lsblk `fdisk -l /dev/system disk` of the source machine and provide it to Support. Support will determine whether the partitions of the system disk can be split based on the above information.

WebDav connection failed

Document Category: Product Related Experience

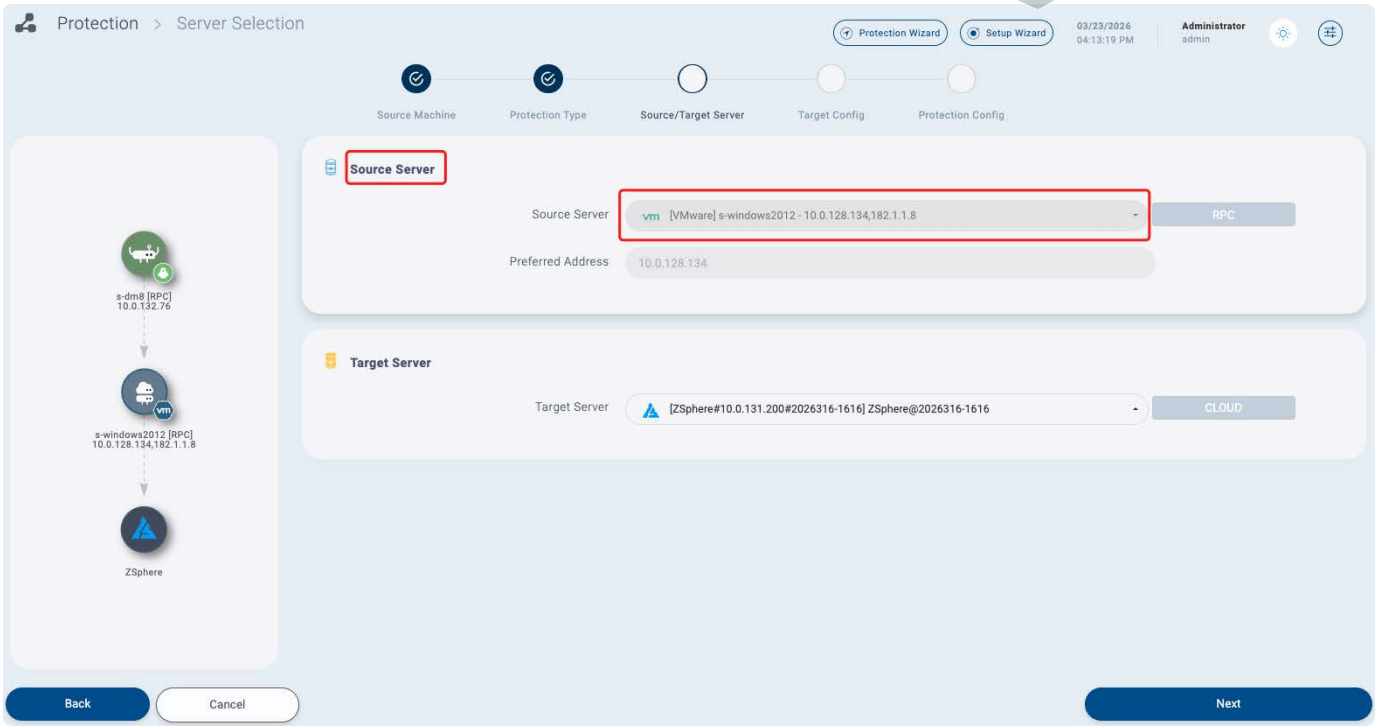
Error message

Error keyword: WebDAV connection failed



Knowledge points

In the synchronization task, the first communication between the transit node (Treker) bound to the source machine and the target node (Treker Lite) is to establish a WebDAV connection.



Troubleshooting ideas

Have you successfully created a TL cloud host?

Key points

- Create an instance.
- Boot normally to the IP configuration interface.

Troubleshooting methods

- Take a screenshot to save the configuration of creating a copy task.
- Use this configuration to manually create a cloud host on the NexaVM platform.

Troubleshooting results

- The TL image is damaged and the instance cannot be created.
- NexaVM has insufficient resources or incorrect resource configuration. You can confirm according to the error message of the NexaVM platform.
- The storage performance connected to the platform is poor, and the TL initialization

and startup is too slow, causing the management console to wait for a timeout.

Is TL's IP address valid?

Key points

- When using API mode, the subnet used by TL needs to enable DHCP.
- The IP address obtained by manual configuration and DHCP cannot conflict with the IP address of other devices.

Troubleshooting methods

- Check whether DHCP is enabled on the subnet used by TL on the NexaVM platform.
- You can try to communicate with the IP by closing TL to confirm whether the IP is in use.

Troubleshooting results

- The subnet used by TL does not have DHCP enabled. It needs to be switched to a subnet with DHCP enabled, or the TL mode must be migrated manually.
- IP address conflict, the IP address needs to be changed.
    - If you are not sure whether the IP conflicts, you can handle it as a conflict.

Is the security group correct?

Key points

- API creation will generally automatically select the correct security group.
- Someone may have modified the security group, or the security group created by the API is incorrect.

Troubleshooting methods

- First confirm the name of the security group bound to TL, and then confirm that the security group port contains at least 20000, 20001, and 20443.

Troubleshooting results

- The security group does not include ports such as 20000, 20001, and 20443, and corresponding port release rules need to be added.

Is the WebDAV connection address configured for the copy task correct?

Key points

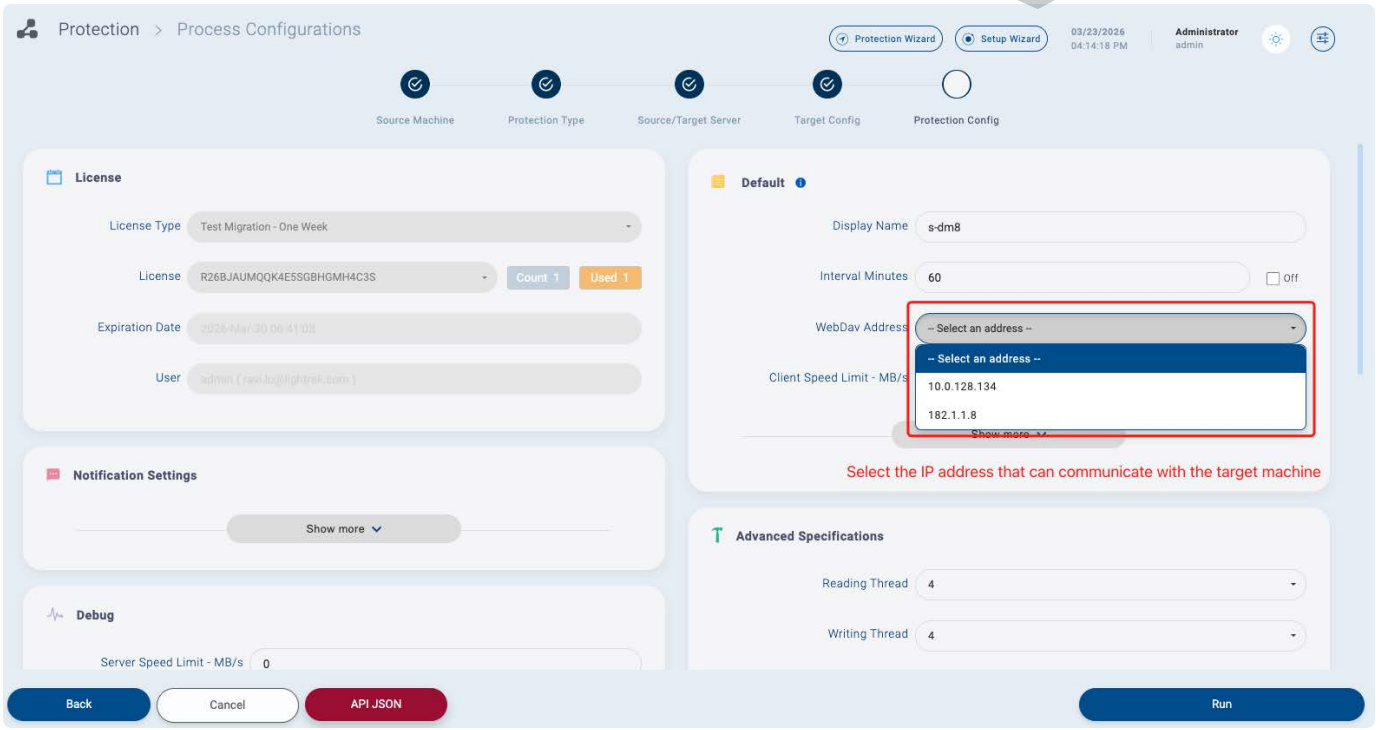
- The WebDAV connection address of the copy task needs to communicate with the TL's IP.
  - Involved ports: 20000, 20001, 20010, 20443.
- There may be multiple IP addresses for the transit data gateway.

Troubleshooting methods

- Release the ICMP of the transit data gateway and TL, ping each other, and confirm whether the ping can succeed.
- Use telnet or tcping to access the other party's 20000, 20001, and 20443 ports.
  - 20010 is only used in https scenarios, so telnet/tcping may not work.
- If the transit data gateway has multiple IP addresses, confirm which IP address can communicate with the TL.

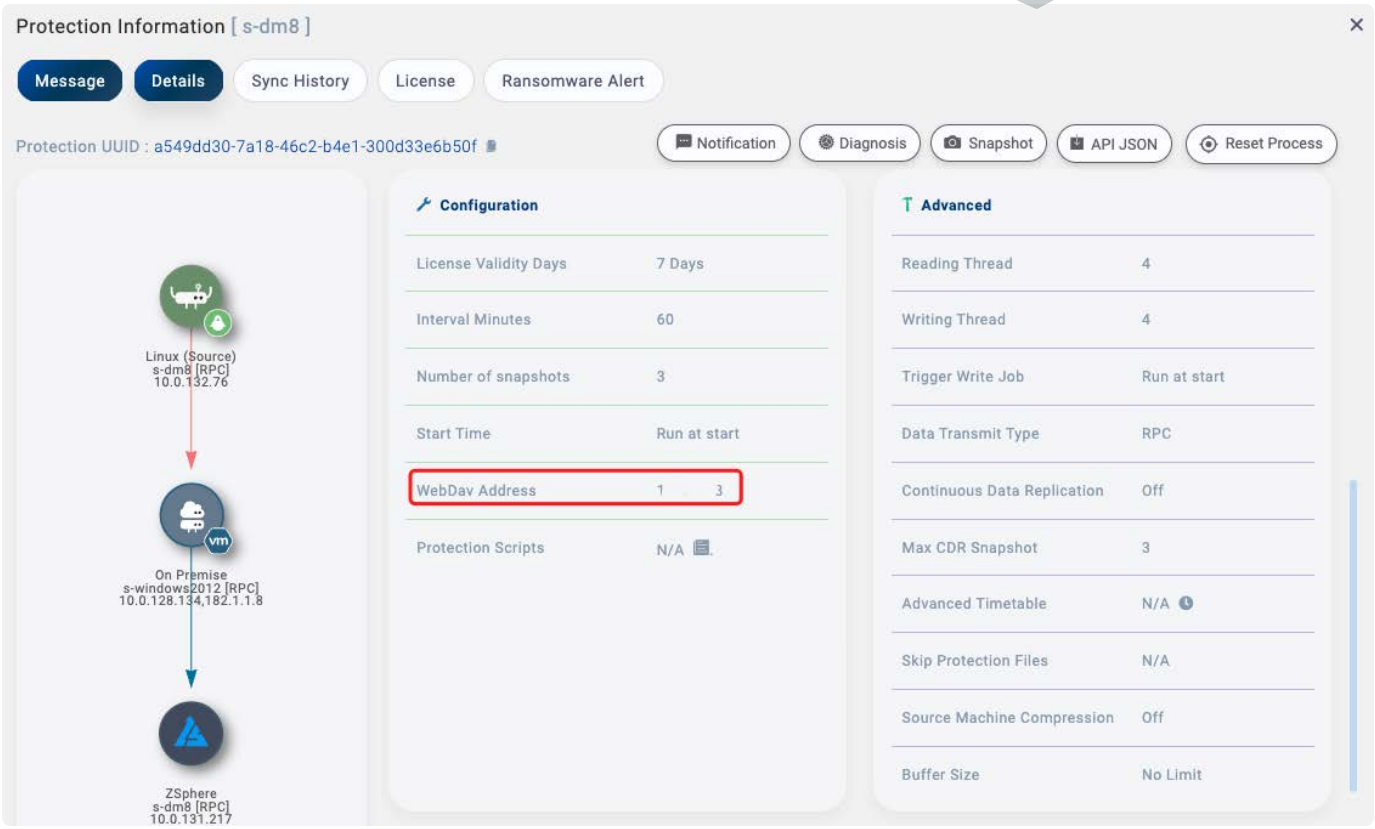
Troubleshooting results

- Under the premise of releasing ICMP, mutual ping fails, which may be due to IP address conflict, incorrect gateway, etc.
- If the port is blocked, it is usually a network problem. You need to contact the user to troubleshoot the network.
- When configuring the replication task, select the IP address that can communicate with the TL.



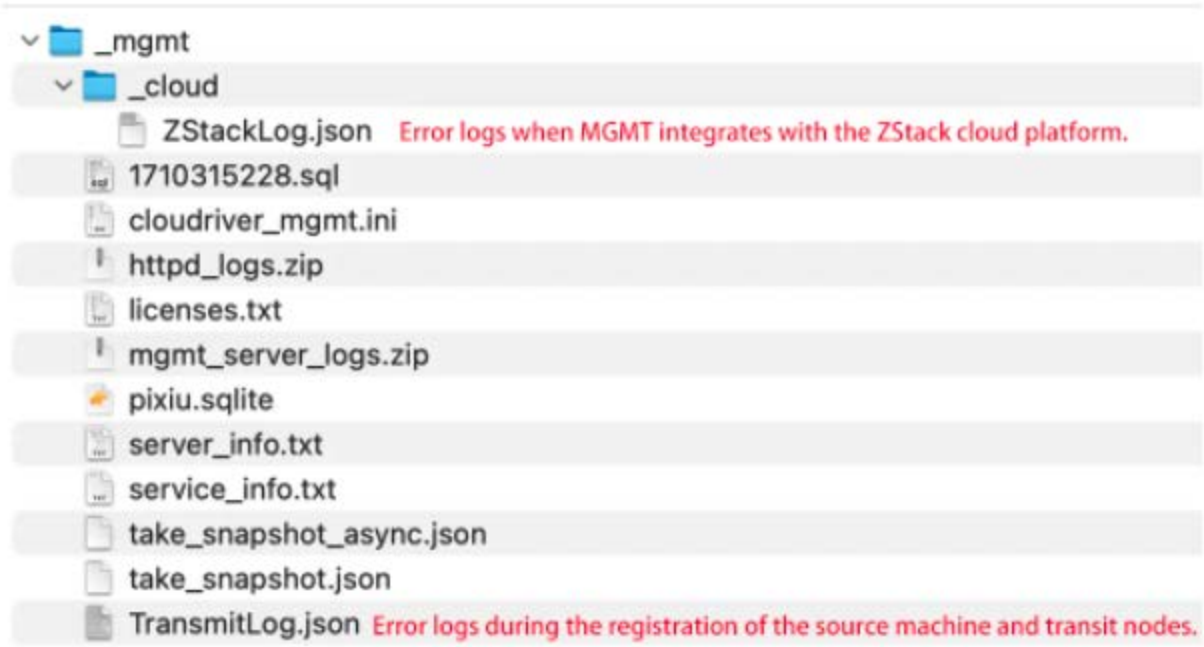
Analyze diagnostic logs

View the WebDAV IP configured for the synchronization task



Create instance phase

1. Download the diagnostic log of the management console and unzip it.



2. View the log content of TransmitLog.json.
3. Confirm the error log based on the error time and Treker Lite's IP address.

NEXAVM

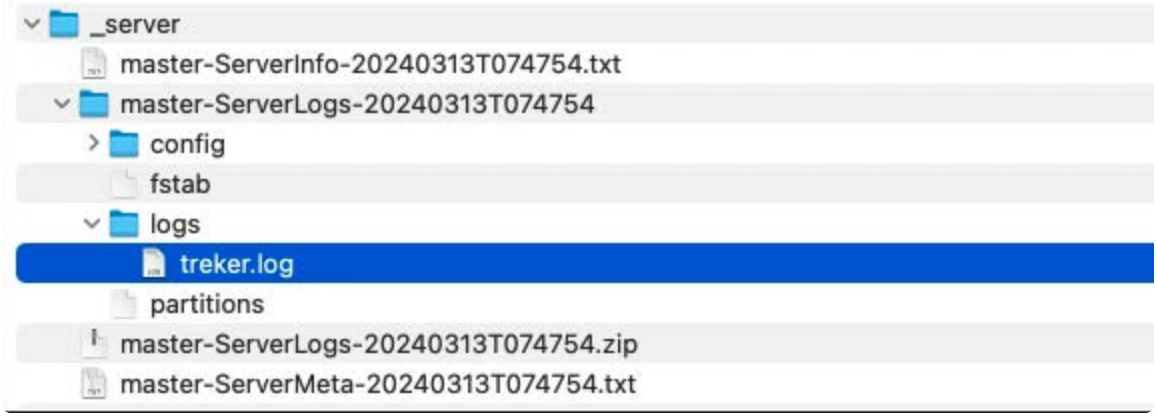
TransmitLog.json*


```
{
  "2024-03-13 15:17:04": {
    "function_name": "get_server_service_info",
    "TException": {
      "why": "Failed to connection to host.",
      "format": "",
      "arguments": [
        "10.0.130.188,"   IP address of TrekerLite
      ],
      "file": "C:\\Program Files\\ZStack\\Treker\\apache24\\htdocs\\_include\\_inc\\_class_transmit.php",
      "line": 164,
      "object": {
      },
      "type": "->",
      "args": [
        "10.0.130.188,"
      ]
    }
  }
},
{
  "2024-03-13 15:17:55": {
    "function_name": "get_server_service_info",
    "TException": {
      "why": "Failed to connection to host.",
      "format": "",
      "arguments": [
        "10.0.130.188,"  IP address of TrekerLite
      ],
      "file": "C:\\Program Files\\ZStack\\Treker\\apache24\\htdocs\\_include\\_inc\\_class_transmit.php",
      "line": 164,
      "object": {
      },
      "type": "->",
      "args": [
        "10.0.130.188,"
```


4. The error message is "Failed to connection to host.", which means that the management console cannot communicate with the Trek Lite's IP.

Analyze TL's diagnostic logs

1. Find treker.log according to the log path.



2. In the treker.log, we can clearly see that we cannot communicate with the IP address of 61...242.

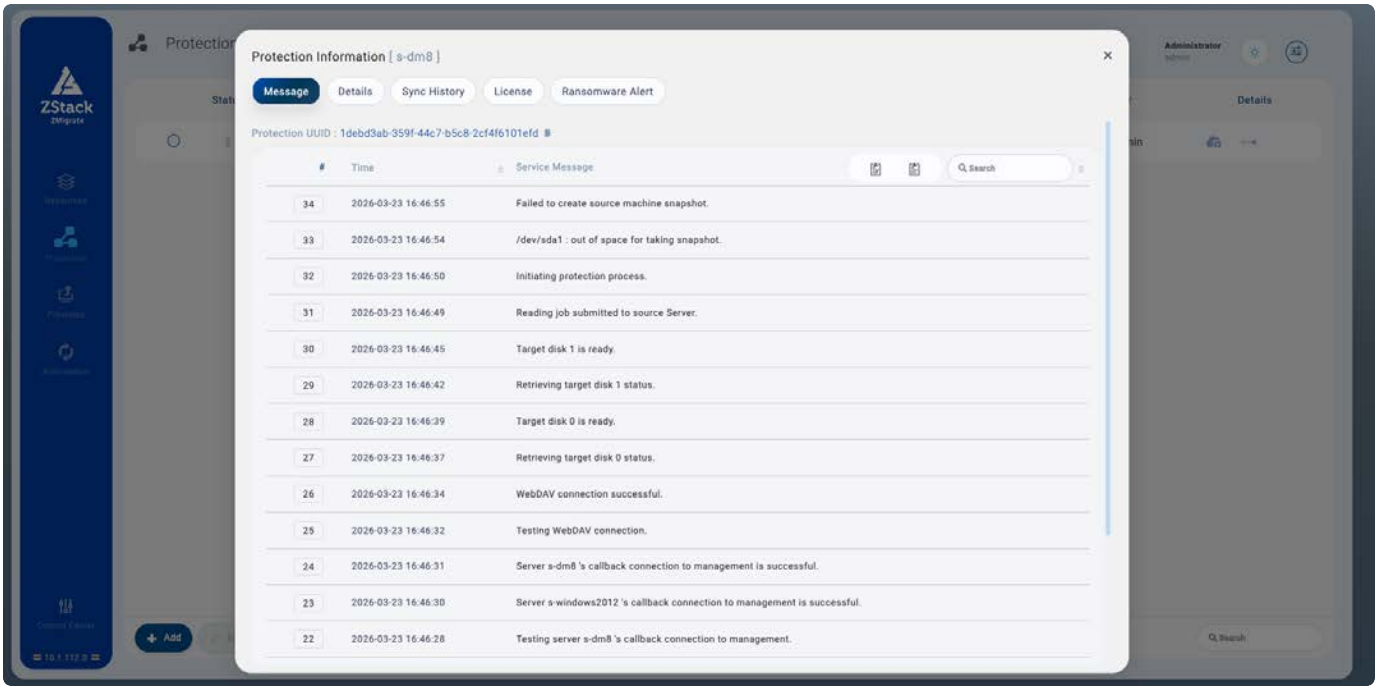
```
2024-Mar-13 07:19:32.997301 (T7fa87980aec0)|R|server_s(214) - boost::thread::hardware_concurrency : 2
2024-Mar-13 07:19:32.999624 (T7fa8725b2700)|R|jobs_sch(422) - scheduler start
2024-Mar-13 07:19:33.023892 (T7fa87980aec0)|W|common_s(109) - Config file does not exit.
2024-Mar-13 07:19:33.038897 (T7fa87980aec0)|R|main(528) - Enabled SSL.
2024-Mar-13 07:19:33.038988 (T7fa87980aec0)|R|main(547) - --- Starting the server ----
2024-Mar-13 07:19:33.039119 (T7fa87980aec0)|R|main(553) - --- Starting ----
2024-Mar-13 07:20:32.160757 (T7fa8705ae700)|E|service_(378) - 61.[illegible]242:20001 - open() timed out
2024-Mar-13 07:20:32.160898 (T7fa8705ae700)|R|webdav(415) - WebDav connect to https://61.[illegible]242/webDav
2024-Mar-13 07:20:33.500928 (T7fa8637fe700)|R|server_s(1525) - Time server(0.cn.pool.ntp.org). UTC time (2024-Mar-13 07:20:33.063000)
2024-Mar-13 07:21:01.927866 (T7fa8705ae700)|E|webdav(421) - Request failed: https://61.[illegible].242/webDav (Timeout was reached)
2024-Mar-13 07:21:01.928011 (T7fa8705ae700)|W|image_op(801) - Image folder https://61.[illegible]242/webDav doesnot exist.
```

3. Rebuild the sync task and select an IP address in WebDAV that can communicate with Treker Lite.

Out of space for taking snapshot

Document Category: Product Related Experience

Error screenshot




```
/dev/sda2 :out of space for taking snapshot.
/dev/vda2 :out of space for taking snapshot.
/dev/mapper/patch-lv_patch :out of space for taking snapshot.
```

Problem analysis

This type of error is reported when the partition or lv corresponding to the mount point has less than 10% space. You need to adjust the ratio or clean up files, move files, etc. to free up 10% of the space.

Solution 1. Clean up or make space

Please ask operation and maintenance personnel to free up 10% or more space at the designated mount point.

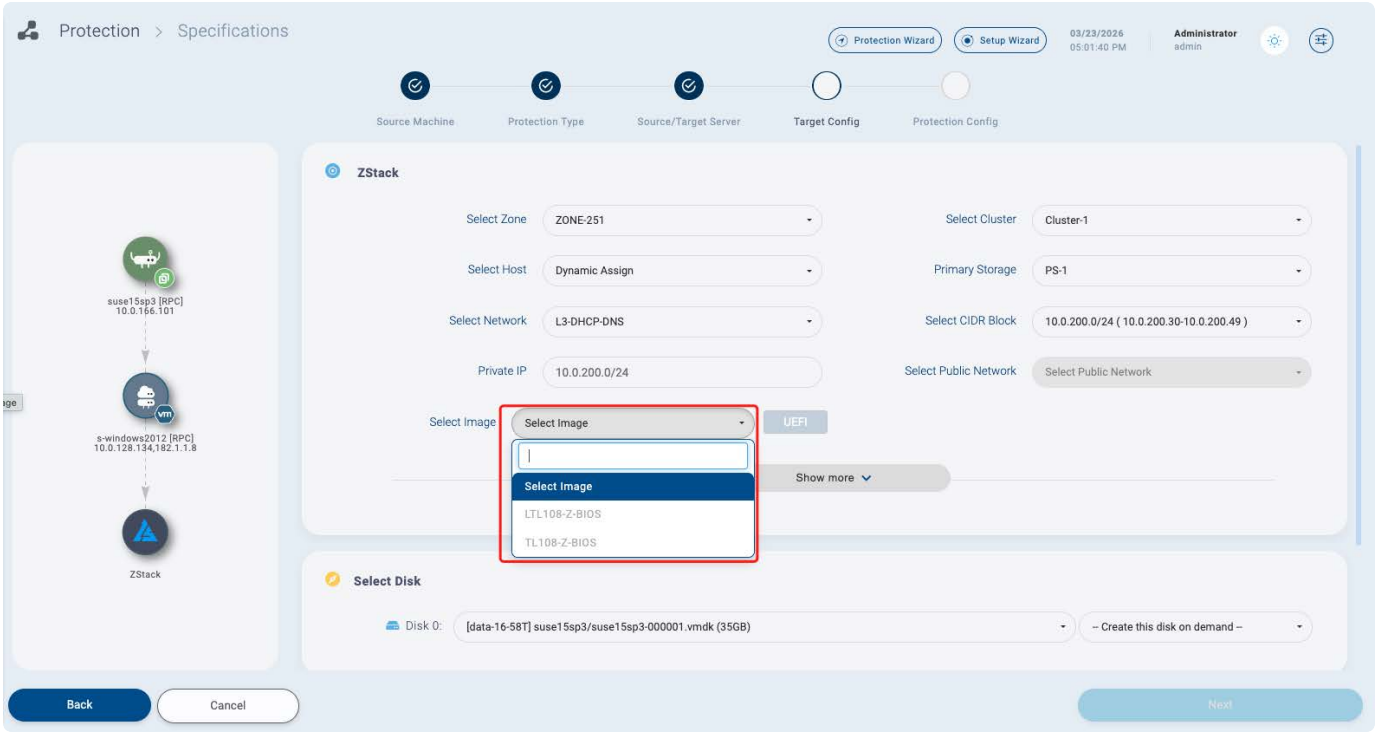
Solution 2. Modify ratio

Refer to the knowledge base "Linux Modification Ratio (Snapshot Size)".

When creating a synchronization task, the uploaded TL image cannot be selected

Document Category: Product Related Experience

Error screenshot



Solution

> For details, please refer to the knowledge base "Uploading Trek Lite Images"

TL mirror does not fill in the introduction

Fill in the introduction: TrekLiteImage

TL image format error

Standard mode can only recognize qcow2 format images and does not support ISO format images.

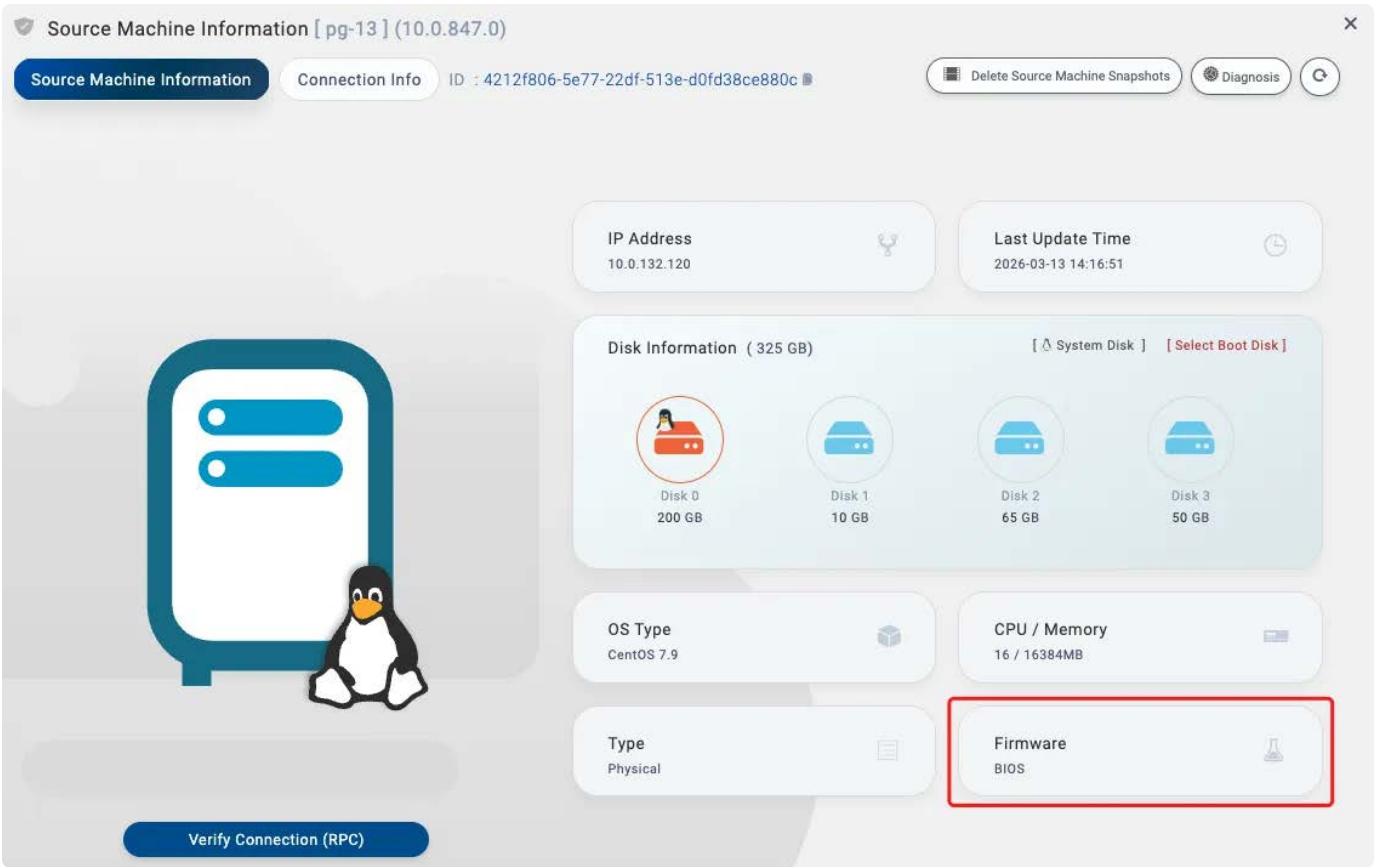
TL's BIOS mode does not match the source machine

When creating a protection task, **filter images with the same BIOS mode based on the BIOS mode of the source host**.

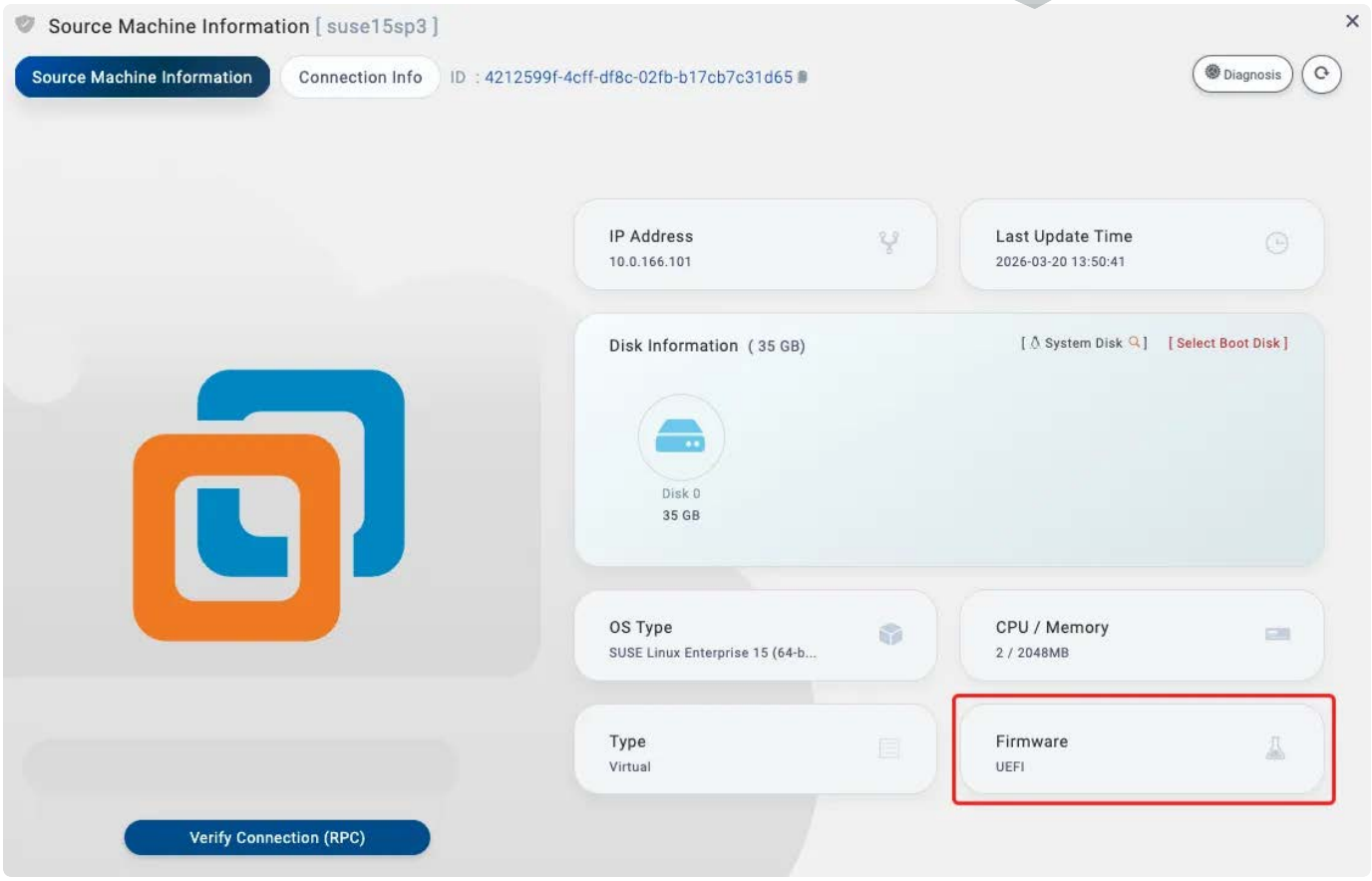
Check the BIOS mode of the source machine

The BIOS mode of the source machine can be viewed in the console --> Resources --> Client --> Details.

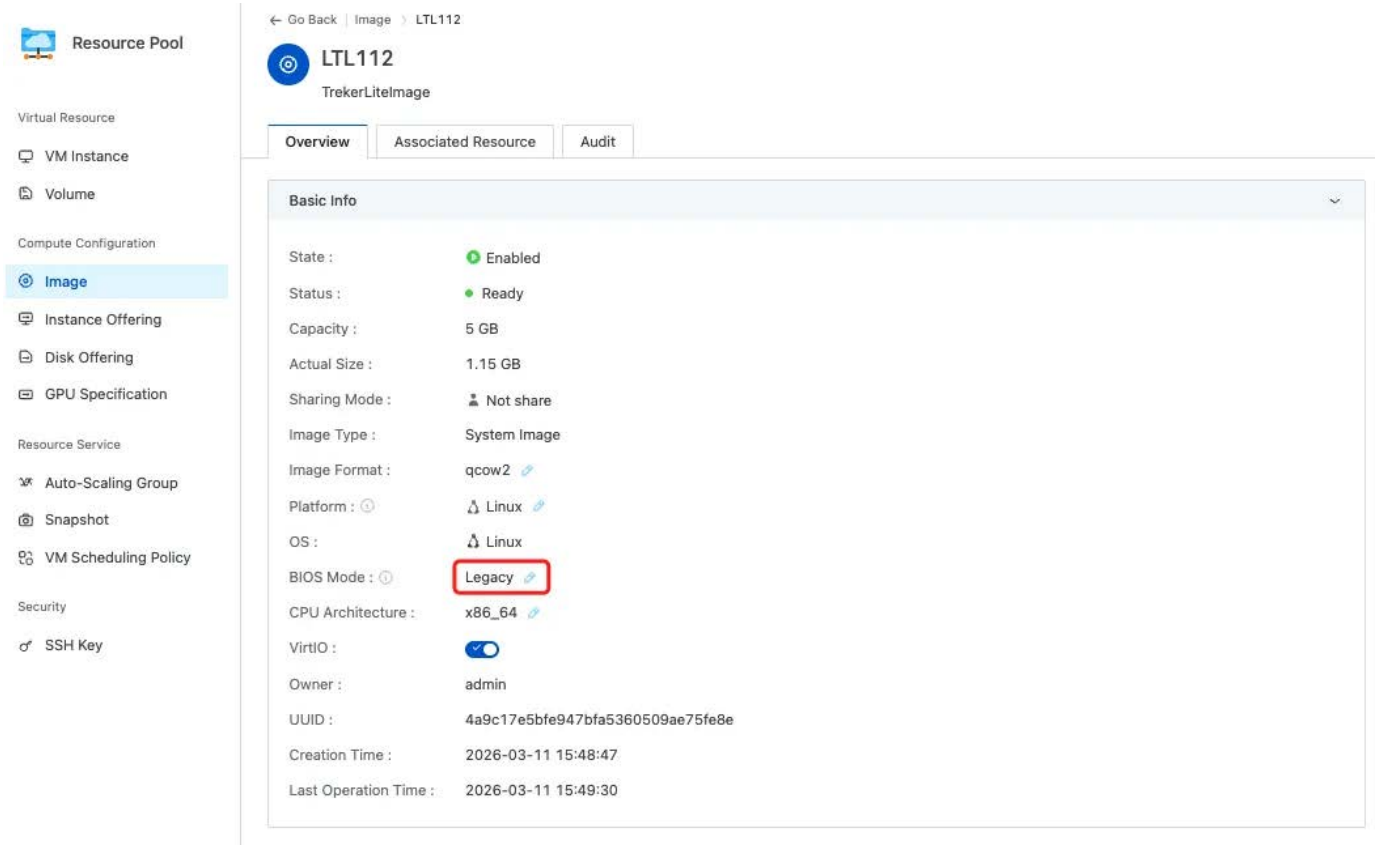
- BIOS=Legacy, requires using legacy mode target image.

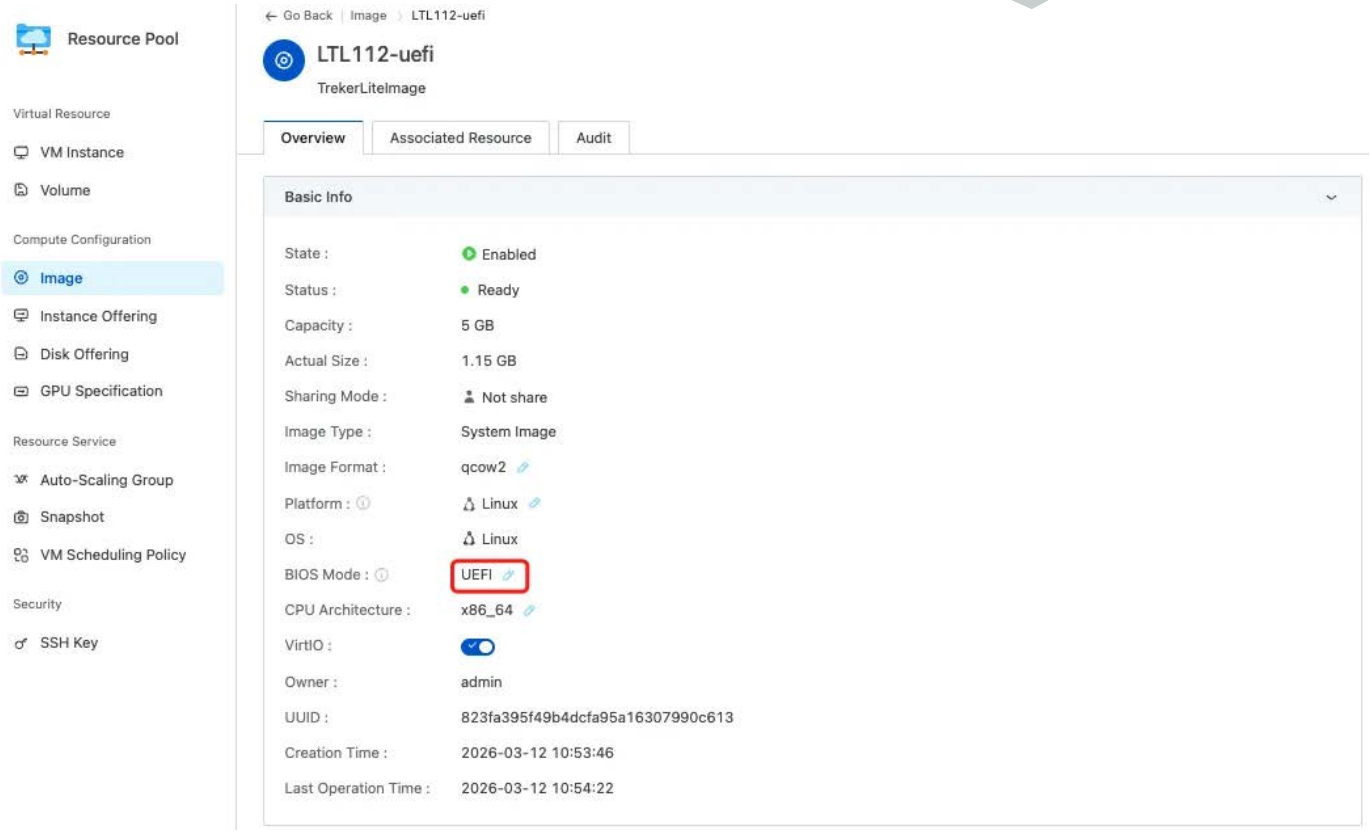


- UEFI=UEFI, you need to use the target image in UEFI mode.



Check the BIOS mode of the target image



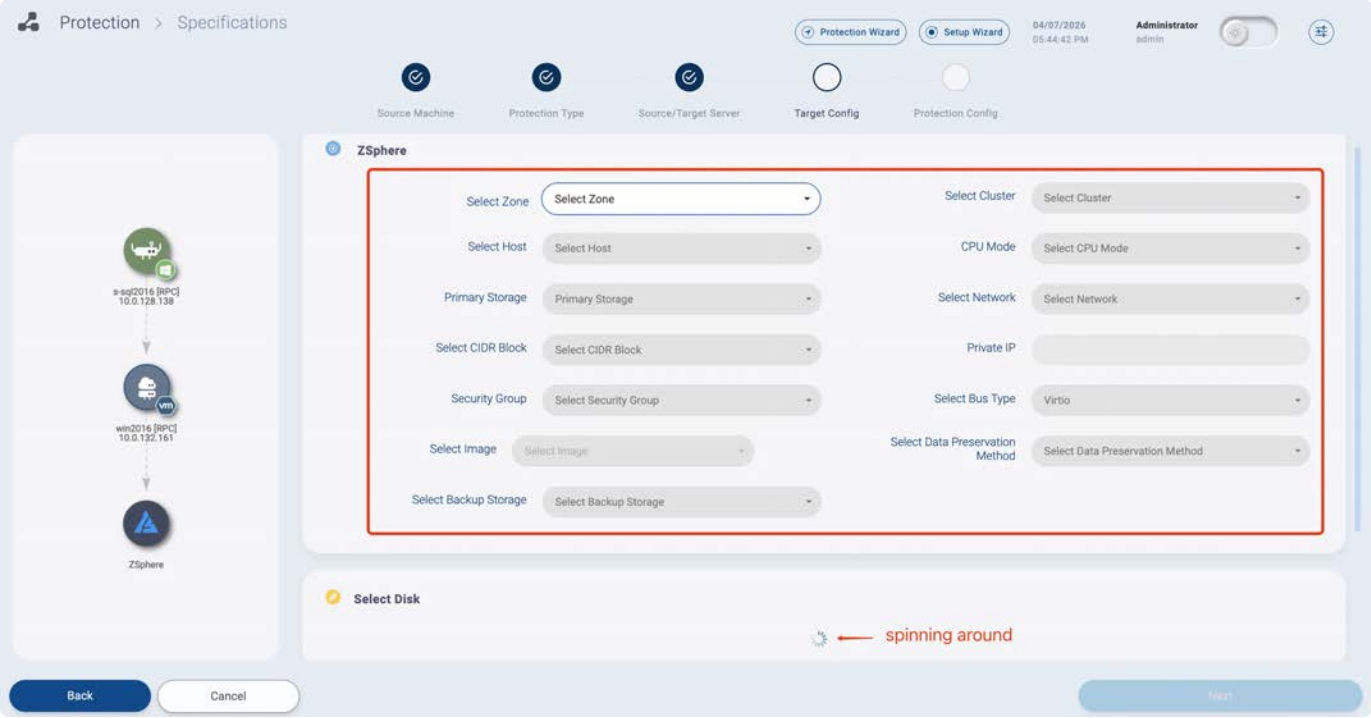

Resource Pool
Virtual Resource
VM Instance
Volume
Compute Configuration
Image
Instance Offering
Disk Offering
GPU Specification
Resource Service
Auto-Scaling Group
Snapshot
VM Scheduling Policy
Security
SSH Key
Go Back | Image | LTL112-uefi
LTL112-uefi
TrekerLiteImage
Overview
Associated Resource
Audit
Basic Info
State : Enabled
Status : Ready
Capacity : 5 GB
Actual Size : 1.15 GB
Sharing Mode : Not share
Image Type : System Image
Image Format : qcow2
Platform : Linux
OS : Linux
BIOS Mode : UEFI
CPU Architecture : x86_64
VirtIO :
Owner : admin
UUID : 823fa395f49b4dcfa95a16307990c613
Creation Time : 2026-03-12 10:53:46
Last Operation Time : 2026-03-12 10:54:22

When creating a protection task, the disk option keeps spinning and waiting

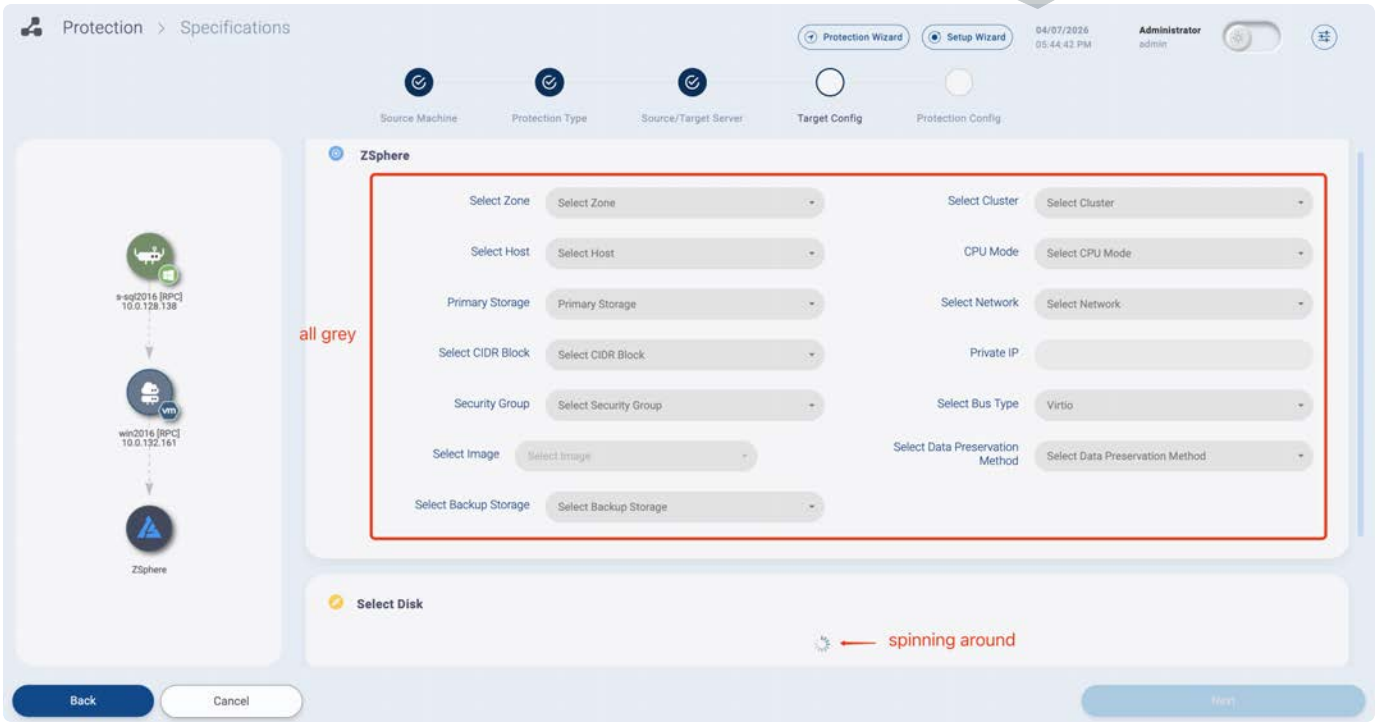
Document Category: Product Related Experience

Error screenshot

Situation 1: Target platform information is optional



Situation 2: The target platform information is all gray and cannot be selected.



Problem analysis

Situation one:

1. When the implementer configured the protection task, the necessary parameters were not configured in the protection task.

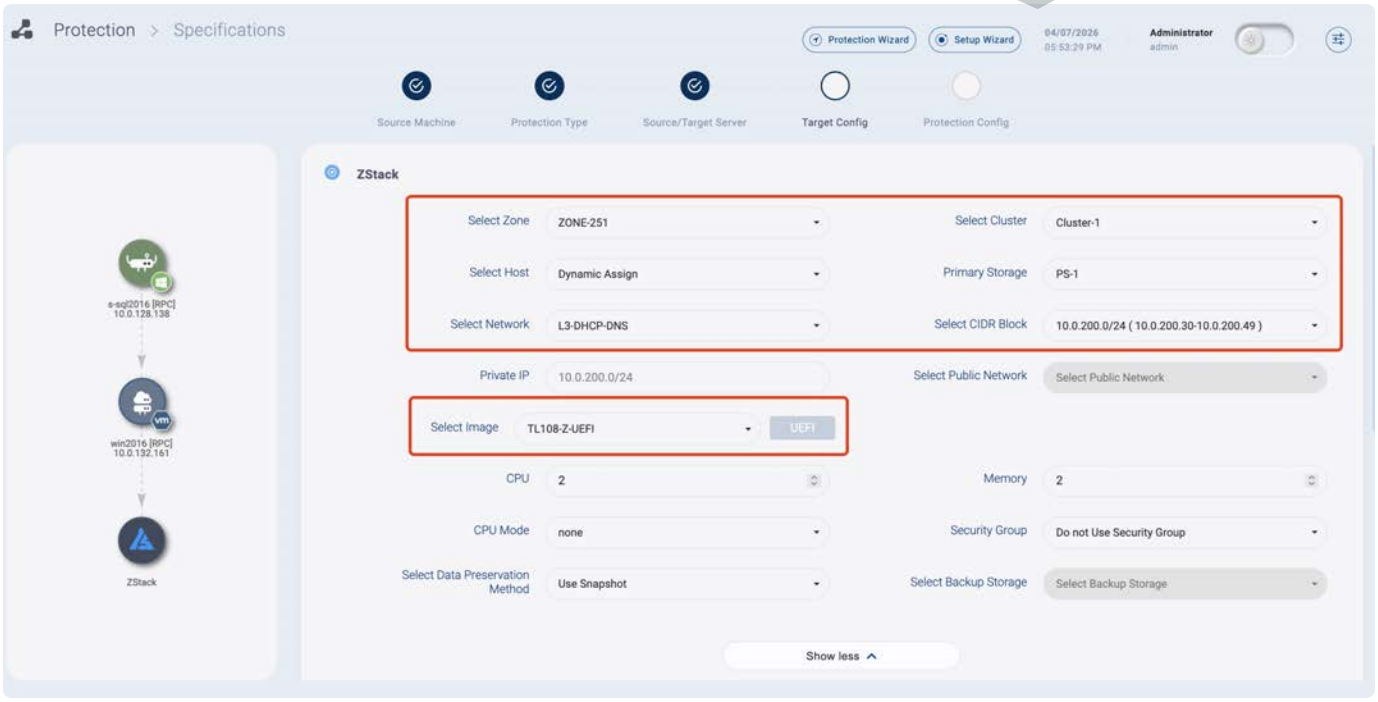
Situation two:

1. The time difference between the migration console and NexaVM exceeds 15 minutes;
2. NexaVM added using the account and password method doesn't communicate with the migration console.

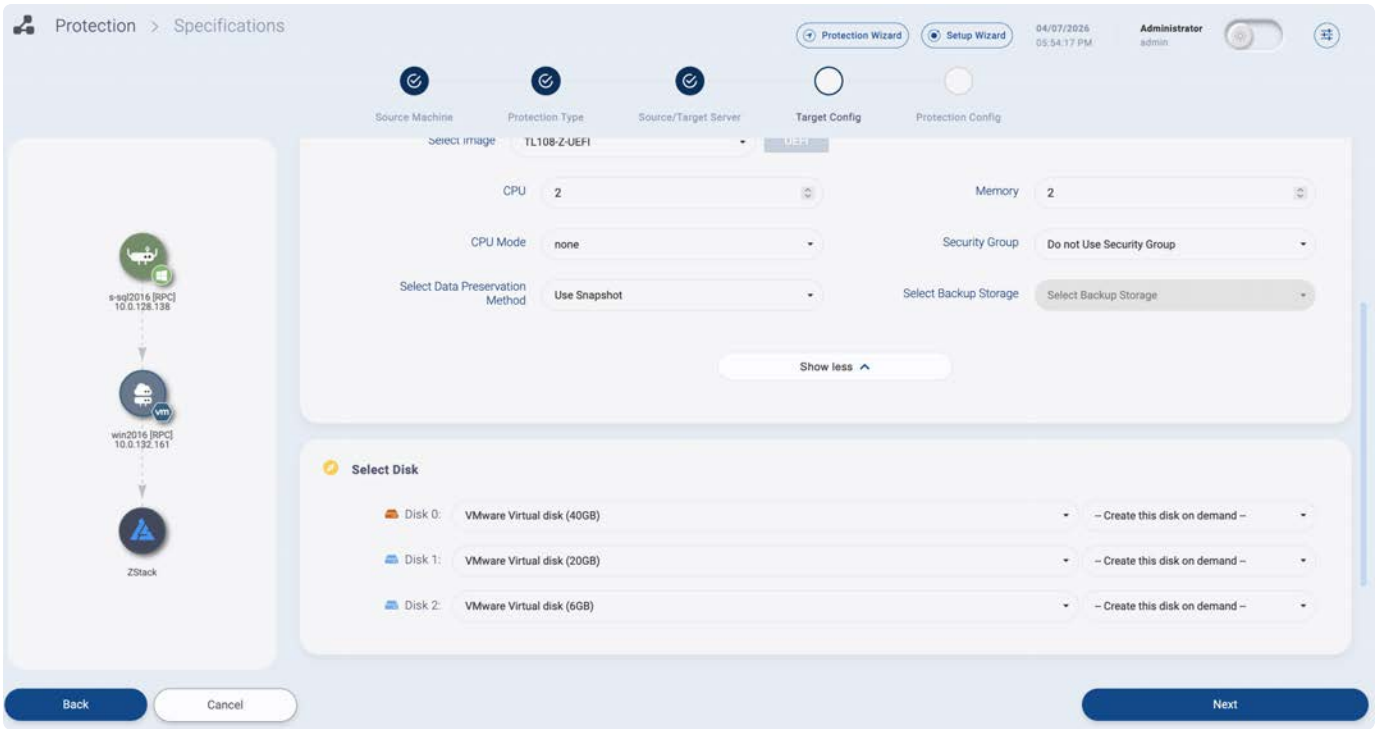
Solution steps

Situation one

1. Swipe up on the page to confirm that the NexaVM platform parameters have been set.
    - At least the following 7 parameters must be set before loading disk information will begin.



2. Pull down again and you can see that the disk can be loaded normally.



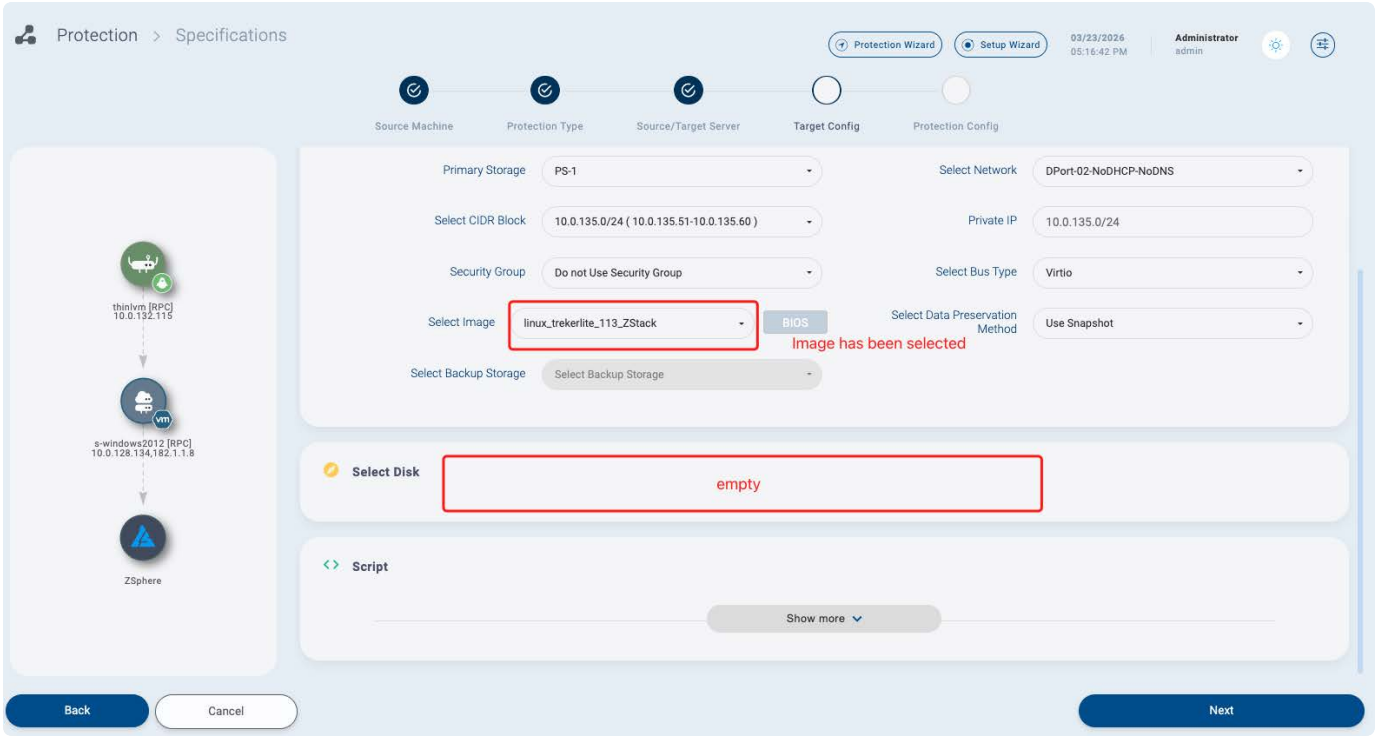
Situation 2

Refer to the knowledge base "Add NexaVM to the cloud platform and report an error" for processing.

The protection task does not display the disk of the source host

Document Category: Product Related Experience

Error screenshot



Problem analysis

1. The source host is Linux and uses Thin LVM.
2. NexaVM or NexaSphere platform verification failed.

Solution 1. The source host is Linux and uses Thin LVM.

1. Log in to the source host and view disk information.

```
1   lsblk
```

2. Check the output of lsblk. If it contains `tmeta` and `tdata`, it is Thin LVM.

```
[root@thinlvm ~]# lsblk
NAME                      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda                         8:0    0  100G  0 disk
├─sda1                      8:1    0    1G  0 part /boot
└─sda2                      8:2    0 47.6G  0 part
  ├─centos-pool00_tmeta   252:0    0   40M  0 lvm
  │ └─centos-pool00-tpool 252:2    0   30G  0 lvm
  │   ├─centos-root       252:3    0   30G  0 lvm  /
  │   └─centos-pool00     252:8    0   30G  0 lvm
  ├─centos-pool00_tdata   252:1    0   30G  0 lvm
  │ └─centos-pool00-tpool 252:2    0   30G  0 lvm
  │   ├─centos-root       252:3    0   30G  0 lvm  /
  │   └─centos-pool00     252:8    0   30G  0 lvm
  ├─centos-swap           252:4    0    4G  0 lvm  [SWAP]
  └─centos-home           252:9    0    4G  0 lvm  /home
```

3. Thin LVM does not support online migration, so you need to use OfflineKit for offline migration.
    - Refer to the knowledge base "OfflineKit Offline Migration".

Solution 2. NexaVM or NexaSphere platform verification failed.

Refer to the knowledge base "Add NexaVM to the cloud platform and report an error" for processing.

A certain disk data in the synchronization task is 0

Document Category: Product Related Experience

Windows

The disk of the user's source host is offline or has no data.

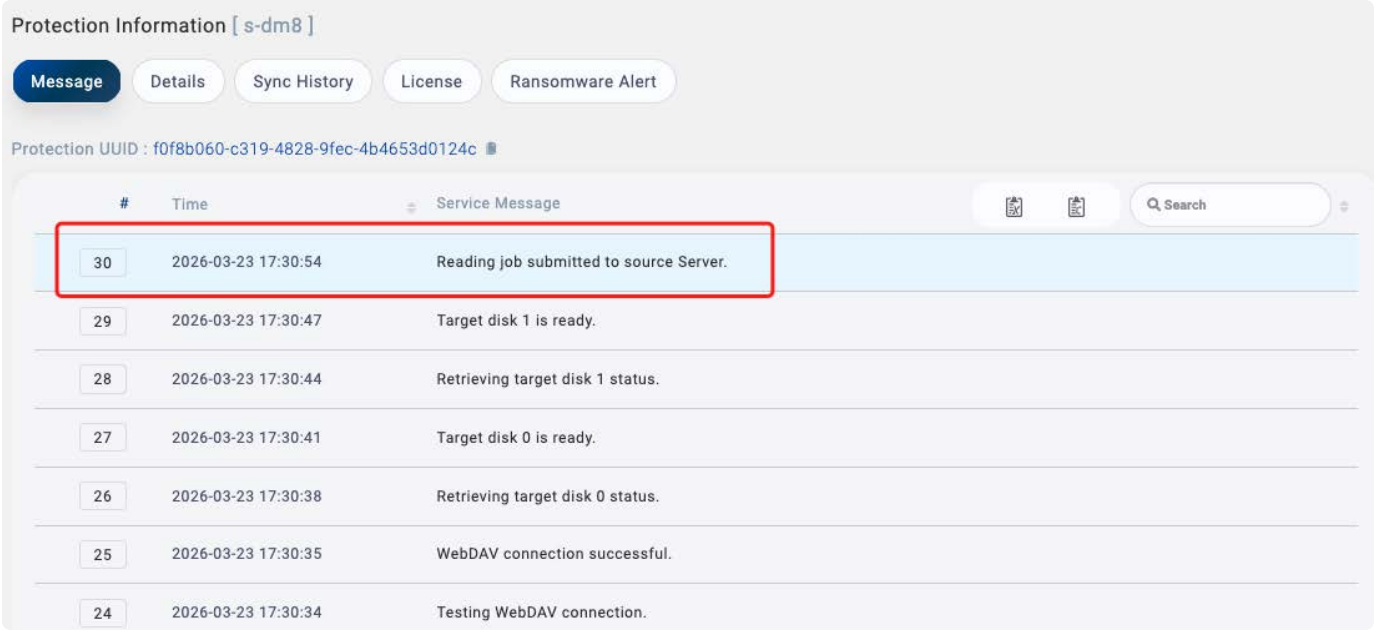
Linux

The disk on the user's source host is not mounted or there is no data.

Protection task stuck at "Read job submitted to origin server"

Document Category: Product Related Experience

Error screenshot



Problem analysis

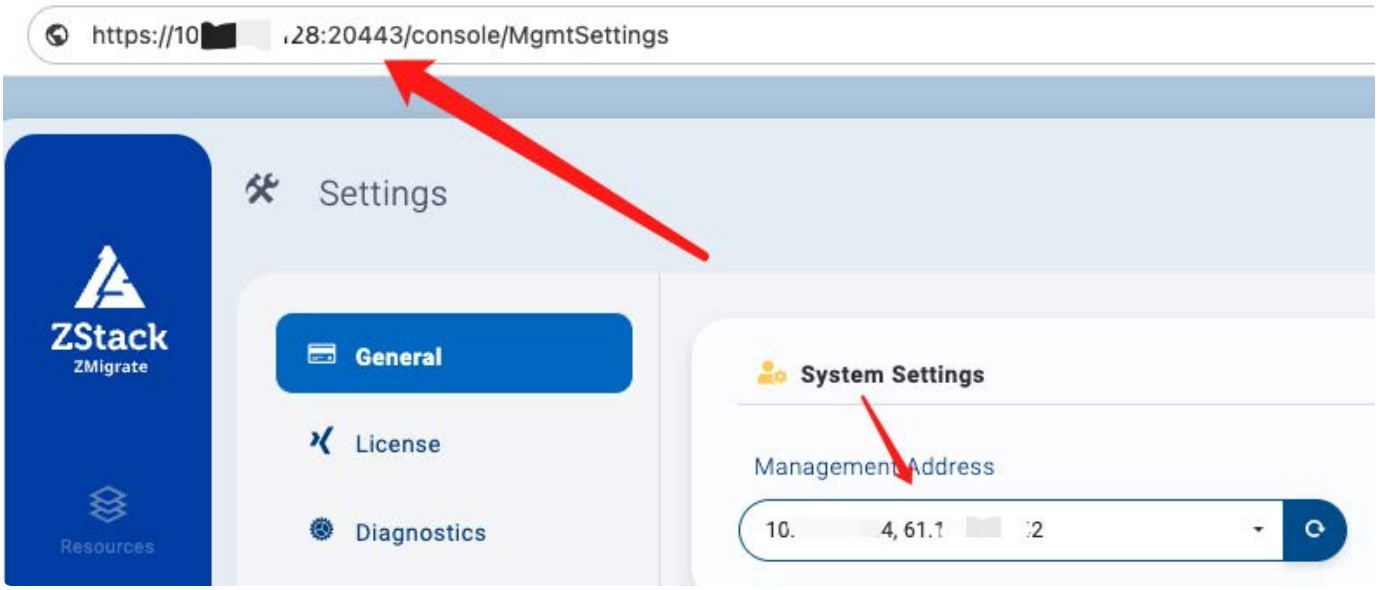
1. The IP address has been modified in the management console, but the central control IP has not been modified.
2. The network between the management console and the target machine is blocked.
3. The system of the management console is abnormal or the management console is installed abnormally.

Solution 1. Management console IP is incorrect

1. Settings in the management console --> Advanced --> `Central Control Address Set`

`tings` .

2. Confirm that the IP address of the management console is consistent with the IP address in the Central Control Address Settings.
    - The screenshot is a negative case: the central control IP address is inconsistent with the management console IP address.



3. If it is inconsistent, please modify it and then recreate the synchronization task.

Solution 2. There is no network connection between the management console and the target machine.

1. Resources in the management console --> Data Gateway --> Add --> pe mode
2. Verify, update.
3. If it can be verified and the update is successful, the network problem is eliminated.

Solution 3. Management console exception

First of all: the management console cannot be copied by cloning, mirroring, etc. The management console can only be installed on a clean system.

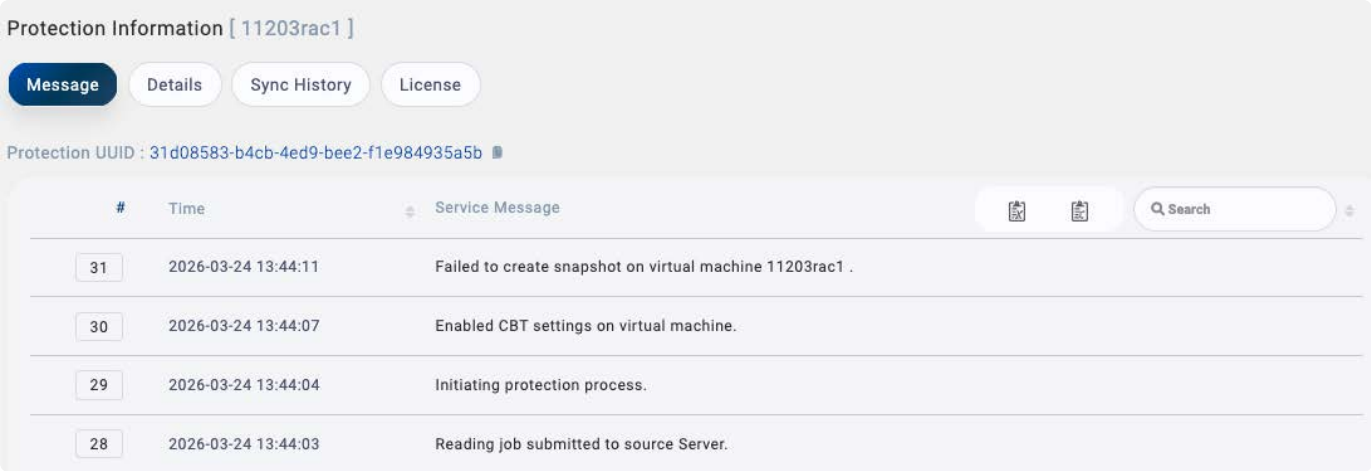
If the management console is copied by cloning, mirroring, etc., please redeploy the Windows system to install the management console!

1. Confirm that the system version is Windows 2016 and above.
2. Check that the IP address of the management console is consistent with the central control address.
3. Troubleshoot the network connection between the management console and the target machine.
4. After reinstalling the management console, try the synchronization task again.
5. If it still doesn't work, reinstall the Windows system or use the Linux version management console.

Failed to create (quiesce) snapshot on virtual machine

Document Category: Product Related Experience

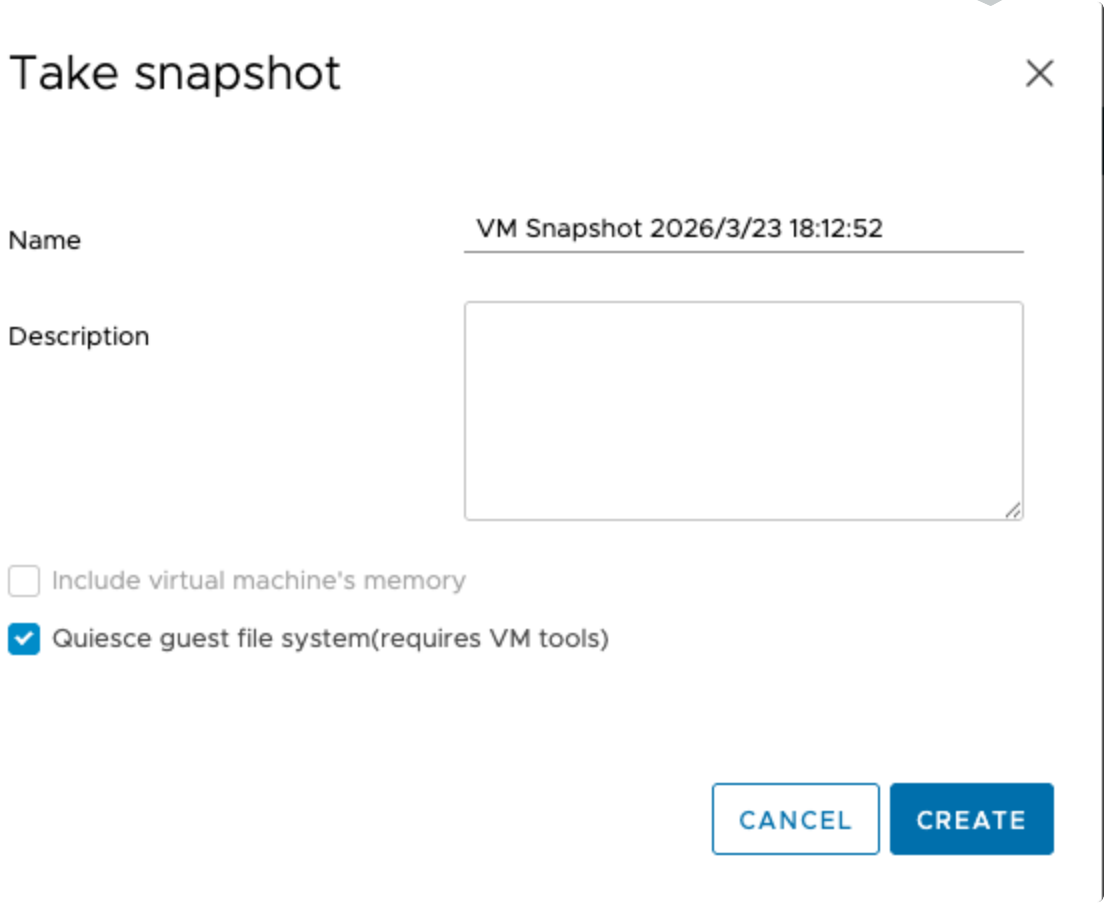
Error screenshot



Troubleshooting method (VMware platform)

1. Find the virtual machine on VMware and manually take a snapshot of the virtual machine.

- Notes:
  a. Uncheck "Include virtual machine's memory"
  b. Be sure to check "Silent guest file system (requires virtual machine tools)"



Solution

Manual snapshot failed

1. Log in to the virtual machine's system.
2. Disable the VMtools service.
    - Note: This is to disable the VMtools service, not to uninstall VMtools.
3. Initiate a synchronization task.
4. If you are stuck in the previous step, you can delete the rebuild synchronization task.

Manual snapshot taken successfully

1. Log in to the virtual machine's system.
2. Check installed software:
    - Windows: Installed software can be viewed in Control Panel.

NEXAVM

- Linux: You can use yum, apt and other commands to list installed software, or use ps –ef to check running software.

3. Check whether there is any software such as disaster recovery and backup that locks I/O.
4. Ask the user whether the service of the relevant software can be suspended.
5. After pausing the services of the relevant software, initiate synchronization of the synchronization task.
6. If you are stuck in the previous step, you can delete the rebuild synchronization task.

final solution

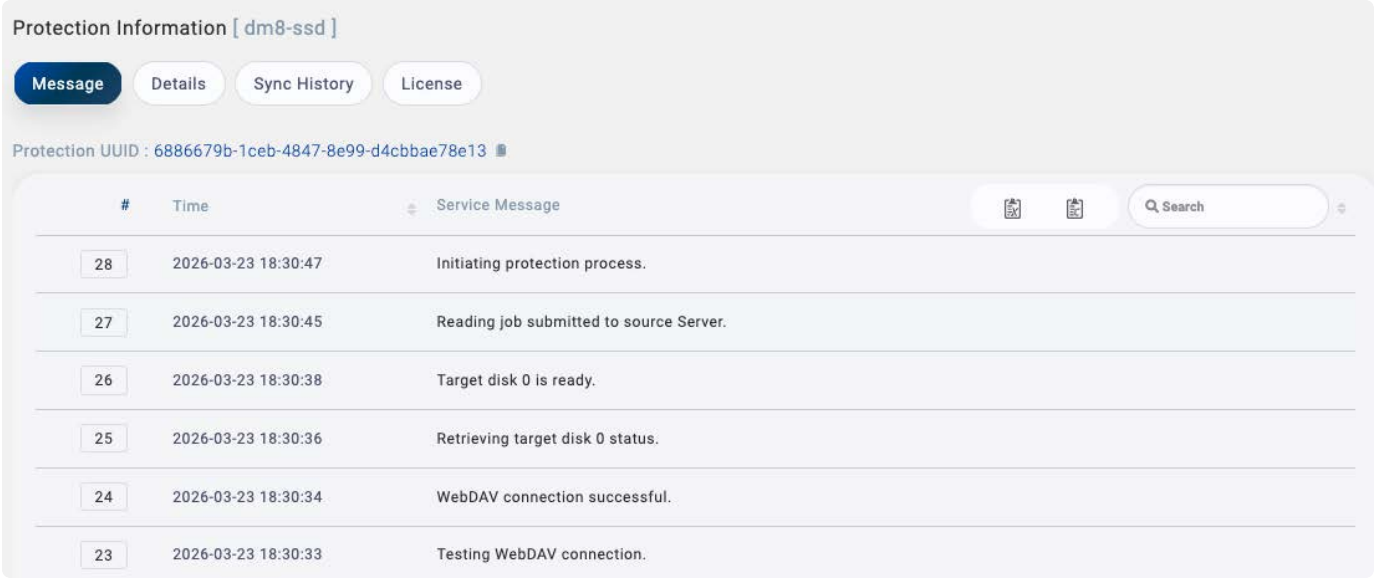
> When none of the above methods are feasible, **you can consider migrating with an agent**;
>
> If the user insists on using proxyless, communicate with the user to use this method.

1. Shut down the virtual machine.
2. Initiate a synchronization task.
3. If the previous step is stuck, you can delete the rebuild synchronization task.
4. After the synchronization task has progressed, start the virtual machine (optional).

Stuck at "Initiating protection process" at agentless senario

Document Category: Product Related Experience

Error screenshot



Problem analysis

1. There are too many ongoing tasks on the VMware platform, or tasks corresponding to the source host are queued.
2. The version of VMware ESXi is incompatible with the version of VMware VDDK on the transit machine.
3. The domain name was configured when deploying VMware, but the local DNS could not resolve the domain name during synchronization.
4. The user's VMware environment has poor performance or is busy.

Solution 1. The VMware platform has many tasks or tasks are queued

1. Prioritize observing the tasks corresponding to the source host and wait for the completion of these tasks.
2. If there is no corresponding task being executed on the source host, check the task of the VMware cloud platform again.

Solution 2.VDDK is not compatible

1. Check the ESXi version of the source machine and the VDDK version of the transit machine.
2. Refer to the knowledge base "Switch VDDK to the specified version" for processing.
    - "Switch VDDK to the specified version" contains the VDDK compatibility list.

Solution 3. VMware domain name cannot be resolved

Error log

NEXAVM

```
2024-11-29 17:32:28.412 (T0856) |W|[NFC ERROR] NfcNewAuthdConnectionEx: Failed to connect: Host address lookup for server <域名> failed: No such host is known
2024-11-29 17:32:28.413 (T0856) |W|[NFC ERROR] NfcNewAuthdConnectionEx: Failed to connect to peer. Error: Host address lookup for server <域名> failed: No such host is known
2024-11-29 17:32:28.413 (T0856) |W|[NFC ERROR] Nfc_BindAndEstablishAuthdCnx2: Failed to create new AuthD connection: The operation completed successfully (NFC_SUCCESS)
2024-11-29 17:32:28.413 (T0856) |W|[NFC ERROR] NfcNewAuthdConnectionEx: Failed to connect: Host address lookup for server <域名> failed: No such host is known
2024-11-29 17:32:28.413 (T0856) |W|[NFC ERROR] NfcNewAuthdConnectionEx: Failed to connect to peer. Error: Host address lookup for server <域名> failed: No such host is known
2024-11-29 17:32:28.414 (T0856) |W|[NFC ERROR] Nfc_BindAndEstablishAuthdCnx2: Failed to create new AuthD connection: The operation completed successfully (NFC_SUCCESS)
2024-11-29 17:32:28.414 (T0856) |E|vmware(7284) - Open image file failure => The server refused connection, error = 14009.
2024-11-29 17:32:28.414 (T0856) |E|virtual_(1117) - Job(8ec1f7e9-703f-4d11-8f15-d2fa0236fb7e.prt) - Cannot open vmdk disk ([VxRail-Virtual-SAN-Datastore-025d9e9d-6abc-4bd0-baab-f4fe07ac1856] 3d242c63-d4d3-0cff-8c6d-b49691f8e4a8/
```

Solution 4. VMware performance is poor and busy

1. Wait 30 minutes.

Unable to create source host snapshot

Document Category: Product Related Experience

Confirm the troubleshooting log files

Synchronization task report: Failed to create source host snapshot.

The snapshot is taken on the source host.

- Then you have to look at the client's antenna.log.

Windows

Too many VSS snapshots

Looking at antenna.log, there are many snapshot ids, and the corresponding created times are distributed at different times.

NEXAVM

```
2024-08-28 09:08:18.928 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{45896f82-6327-11e8-80f4-806e6f6e6963}\), snapshot id(153ba83c-d9ad-49af-907a-2037ea984b42), snapshot set id(7d359328-efa6-473f-92d0-0c9d91377958), created time(2024-Aug-27 19:02:03.856432)
2024-08-28 09:08:18.928 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{45896f82-6327-11e8-80f4-806e6f6e6963}\), snapshot id(008be314-4908-4bec-9310-0949216ae4ab), snapshot set id(f96a0634-084a-47e6-8e1b-91774c74861a), created time(2024-Aug-27 20:01:37.368854)
2024-08-28 09:08:18.928 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{45896f82-6327-11e8-80f4-806e6f6e6963}\), snapshot id(03d6caa9-ec35-446c-b5f1-5b89b95e079c), snapshot set id(a9d9d58e-d3db-465f-8eea-517e0073477a), created time(2024-Aug-27 23:02:23.683820)
2024-08-28 09:08:18.928 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{45896f82-6327-11e8-80f4-806e6f6e6963}\), snapshot id(f338defa-4dea-4d83-be03-436eb3edae4d), snapshot set id(fd1fdc82-126b-479f-bd94-e2b5188bfa33), created time(2024-Aug-28 01:00:54.502567)
2024-08-28 09:08:18.928 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{cc4ae411-49cd-11ec-811e-90d33c7cddf8}\), snapshot id(b6b603b9-b3f5-47de-85d6-f6241aa4bc14), snapshot set id(7d359328-efa6-473f-92d0-0c9d91377958), created time(2024-Aug-27 19:02:03.856432)
2024-08-28 09:08:18.929 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{cc4ae411-49cd-11ec-811e-90d33c7cddf8}\), snapshot id(8a7aceda-b5fc-4179-a8b5-b6a686868574), snapshot set id(f96a0634-084a-47e6-8e1b-91774c74861a), created time(2024-Aug-27 20:01:37.368854)
2024-08-28 09:08:18.929 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{cc4ae411-49cd-11ec-811e-90d33c7cddf8}\), snapshot id(a7a81c87-fc3f-4c48-928e-229e713645b4), snapshot set id(a9d9d58e-d3db-465f-8eea-517e0073477a), created time(2024-Aug-27 23:02:23.683820)
2024-08-28 09:08:18.929 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{cc4ae411-49cd-11ec-811e-90d33c7cddf8}\), snapshot id(7491dc2b-cd0e-41b0-b6e8-2627a9784de8), snapshot set id(fd1fdc82-126b-479f-bd94-e2b5188bfa33), created time(2024-Aug-28 01:00:54.502567)
2024-08-28 09:08:18.929 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{45896f83-6327-11e8-80f4-806e6f6e6963}\), snapshot id(5991f21d-aa95-4838-9200-20e18c47d8d8), snapshot set id(7d359328-efa6-473f-92d0-0c9d91377958), created time(2024-Aug-27 19:02:03.856432)
2024-08-28 09:08:18.929 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{45896f83-6327-11e8-80f4-806e6f6e6963}\), snapshot id(2fbbc827-7ece-482a-b0d0-ee3c4ee99b8b), snapshot set id(f96a0634-084a-47e6-8e1b-91774c74861a), created time(2024-Aug-27 20:01:37.368854)
2024-08-28 09:08:18.929 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{45896f83-6327-11e8-80f4-806e6f6e6963}\), snapshot id(2bc7342c-96cd-42c3-ae2a-a839c30bb020), snapshot set id(a9d9d58e-d3db-465f-8eea-517e0073477a), created time(2024-Aug-27 23:02:23.683820)
2024-08-28 09:08:18.929 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{45896f83-6327-11e8-80f4-806e6f6e6963}\), snapshot id(8f9f2ec3-8203
```

NEXAVM

```
-447f-bfef-7092423c2e8f), snapshot set id(fd1fdc82-126b-479f-bd94-e2b5188b
```

```
2024-08-28 09:06:17.786 (T53736) |R|client_j(355) - Read '\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy310' ...
2024-08-28 09:08:11.406 (T48376) |U|client_j(1790) - (55eb0faa-8cc8-4d09-983a-99fc37688dc2)Disk 1 read completed, data size is 397627392.
2024-08-28 09:08:12.448 (T48376) |R|client_j(1386) - (55eb0faa-8cc8-4d09-983a-99fc37688dc2) : exit
2024-08-28 09:08:18.928 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{45896f82-6327-11e8-80f4-806e6f6e6963}\), snapshot
id(153ba83c-d9ad-49af-907a-2037ea984b42), snapshot set id(7d359328-efa6-473f-92d0-0c9d91377958), created time(2024-Aug-27
19:02:03.856432)
2024-08-28 09:08:18.928 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{45896f82-6327-11e8-80f4-806e6f6e6963}\), snapshot
id(008be314-4908-4bec-9310-0949216ae4ab), snapshot set id(f96a0634-084a-47e6-8e1b-91774c74861a), created time(2024-Aug-27
20:01:37.368854)
2024-08-28 09:08:18.928 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{45896f82-6327-11e8-80f4-806e6f6e6963}\), snapshot
id(03d6caa9-ec35-446c-b5f1-5b89b95e079c), snapshot set id(a9d9d58e-d3db-465f-8eea-517e0073477a), created time(2024-Aug-27
23:02:23.683820)
2024-08-28 09:08:18.928 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{45896f82-6327-11e8-80f4-806e6f6e6963}\), snapshot
id(f338defa-4dea-4d83-be03-436eb3edae4d), snapshot set id(fd1fdc82-126b-479f-bd94-e2b5188bfa33), created time(2024-Aug-28
01:00:54.502567)
2024-08-28 09:08:18.928 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{cc4ae411-49cd-11ec-811e-90d33c7cddf8}\), snapshot
id(b6b603b9-b3f5-47de-85d6-f6241aa4bc14), snapshot set id(7d359328-efa6-473f-92d0-0c9d91377958), created time(2024-Aug-27
19:02:03.856432)
2024-08-28 09:08:18.929 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{cc4ae411-49cd-11ec-811e-90d33c7cddf8}\), snapshot
id(8a7aceda-b5fc-4179-a8b5-b6a686868574), snapshot set id(f96a0634-084a-47e6-8e1b-91774c74861a), created time(2024-Aug-27
20:01:37.368854)
2024-08-28 09:08:18.929 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{cc4ae411-49cd-11ec-811e-90d33c7cddf8}\), snapshot
id(a7a81c87-fc3f-4c48-928e-229e713645b4), snapshot set id(a9d9d58e-d3db-465f-8eea-517e0073477a), created time(2024-Aug-27
23:02:23.683820)
2024-08-28 09:08:18.929 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{cc4ae411-49cd-11ec-811e-90d33c7cddf8}\), snapshot
id(7491dc2b-cd0e-41b0-b6e8-2627a9784de8), snapshot set id(fd1fdc82-126b-479f-bd94-e2b5188bfa33), created time(2024-Aug-28
01:00:54.502567)
2024-08-28 09:08:18.929 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{45896f83-6327-11e8-80f4-806e6f6e6963}\), snapshot
id(5991f21d-aa95-4838-9200-20e18c47d8d8), snapshot set id(7d359328-efa6-473f-92d0-0c9d91377958), created time(2024-Aug-27
19:02:03.856432)
2024-08-28 09:08:18.929 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{45896f83-6327-11e8-80f4-806e6f6e6963}\), snapshot
id(2fbbc827-7ece-482a-b0d0-ee3c4ee99b8b), snapshot set id(f96a0634-084a-47e6-8e1b-91774c74861a), created time(2024-Aug-27
20:01:37.368854)
2024-08-28 09:08:18.929 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{45896f83-6327-11e8-80f4-806e6f6e6963}\), snapshot
id(2bc7342c-96cd-42c3-ae2a-a839c30bb020), snapshot set id(a9d9d58e-d3db-465f-8eea-517e0073477a), created time(2024-Aug-27
23:02:23.683820)
2024-08-28 09:08:18.929 (T46540) |R|client_s(486) - Snapshot : volume(\\?\Volume{45896f83-6327-11e8-80f4-806e6f6e6963}\), snapshot
id(8f9f2ec3-8203-447f-bfef-7092423c2e8f), snapshot set id(fd1fdc82-126b-479f-bd94-e2b5188bfa33), created time(2024-Aug-28
01:00:54.502567)
2024-08-28 09:08:20.835 (T22764) |R|client_j(528) - Job removed.
2024-08-28 10:18:10.701 (T41308) |R|common_s(844) - BIOS Mode : Legacy
2024-08-28 10:18:19.612 (T21768) |R|client(449) - Command : 0xb000300c
```

Use the command in the system of the source host to view the vss snapshot

```
#check vss snapshot
vssadmin list shadows
```

Solution

> Since VSS is a system component, other software may call VSS to take snapshots;
>
> Before clearing the snapshot, you need to confirm with the user whether the operation is allowed.

```
#check snapshot
vssadmin list shadows

#switch to antenna installation directory by using env
cd %srcroot%

#erase snapshot
Antenna.exe --erase

#check snapshot again
vssadmin list shadows
```

```
C:\Users\Administrator>cd %srcroot%

C:\Program Files\[redacted]\Antenna>Antenna.exe --erase
```

```
C:\Users\Administrator>vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Contents of shadow copy set ID: {bcd9e975-5efa-4c97-8841-bb3287551325}
   Contained 1 shadow copies at creation time: 3/23/2026 6:40:04 PM
      Shadow Copy ID: {0c27e5d9-f2ee-42f8-8b85-dc5282647a3f}
         Original Volume: (C:)\\?\Volume{821f374d-953a-456f-b459-a4023b1e8d5c}\
         Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
         Originating Machine: WIN-7QE1SAD752A
         Service Machine: WIN-7QE1SAD752A
         Provider: 'Microsoft Software Shadow Copy provider 1.0'
         Type: ClientAccessible
         Attributes: Persistent, Client-accessible, No auto release, No writers, Differential

                                                snapshot exists
C:\Users\Administrator>
```

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>
C:\Users\Administrator>vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

No items found that satisfy the query.

C:\Users\Administrator>
                                    snapshot not exists
```

Debugging VSS

```
1   #check vss snapshot
2   vssadmin list shadows
```

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>
C:\Users\Administrator>vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

No items found that satisfy the query.

C:\Users\Administrator>
                                    snapshot not exists
```

NEXAVM

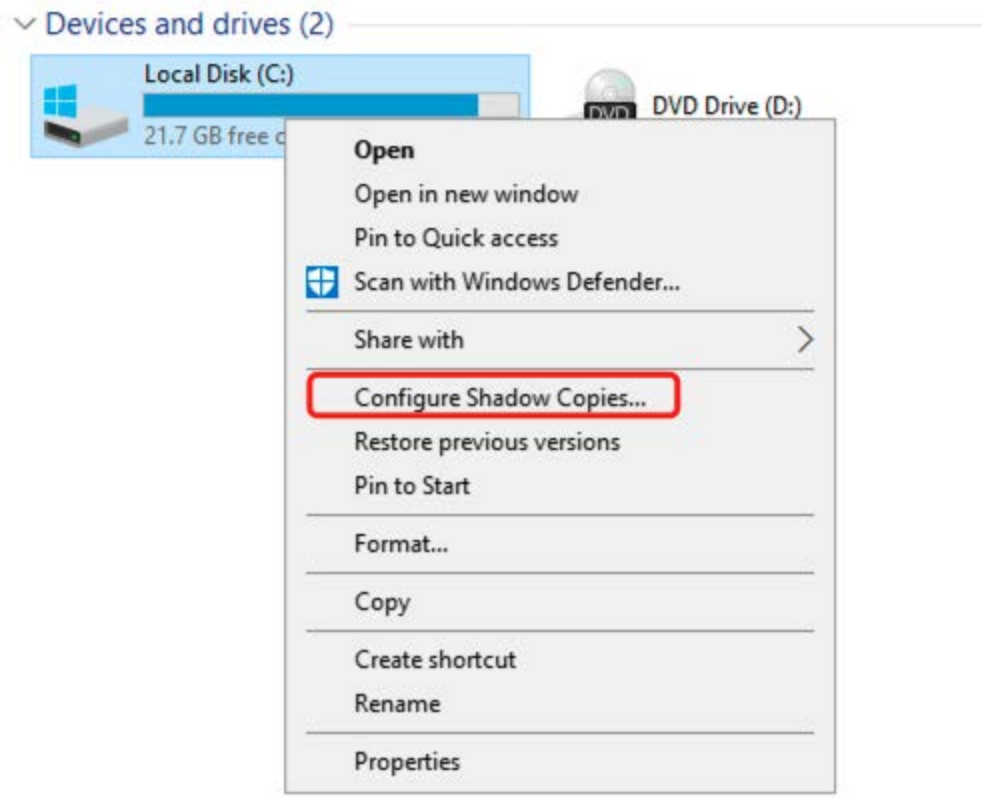
```
C:\Users\Administrator>vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Contents of shadow copy set ID: {bcd9e975-5efa-4c97-8841-bb3287551325}
   Contained 1 shadow copies at creation time: 3/23/2026 6:40:04 PM
      Shadow Copy ID: {0c27e5d9-f2ee-42f8-8b85-dc5282647a3f}
         Original Volume: (C:)\\?\Volume{821f374d-953a-456f-b459-a4023b1e8d5c}\
         Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
         Originating Machine: WIN-7QE1SAD752A
         Service Machine: WIN-7QE1SAD752A
         Provider: 'Microsoft Software Shadow Copy provider 1.0'
         Type: ClientAccessible
         Attributes: Persistent, Client-accessible, No auto release, No writers, Differential

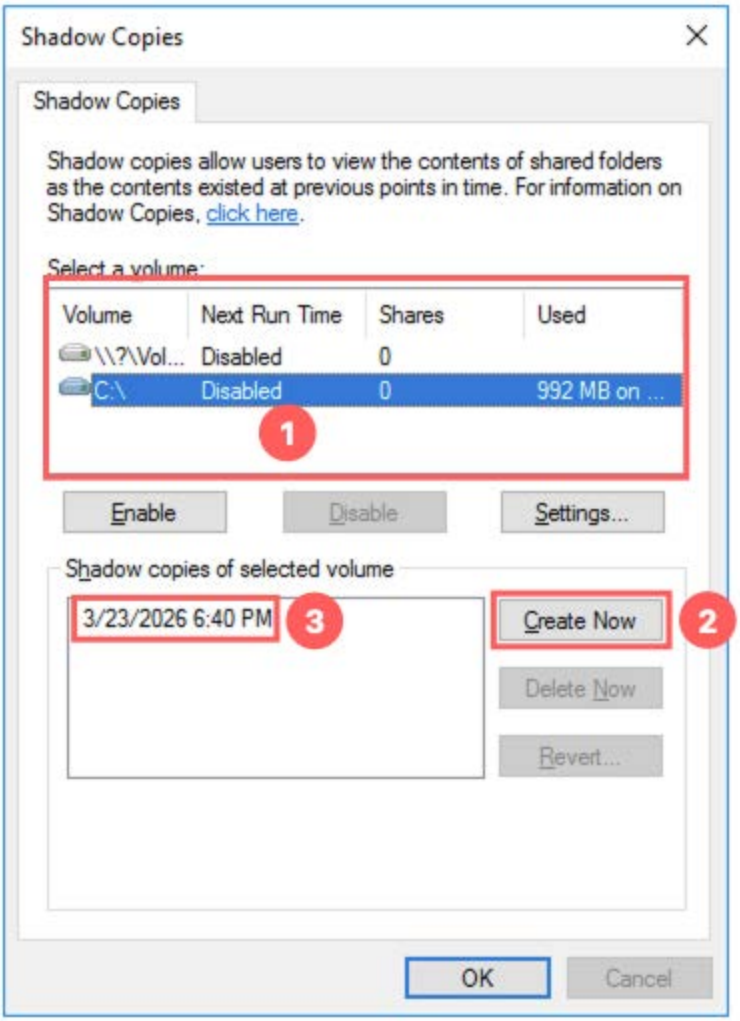
                                                snapshot exists
C:\Users\Administrator>
```

Try taking a snapshot manually

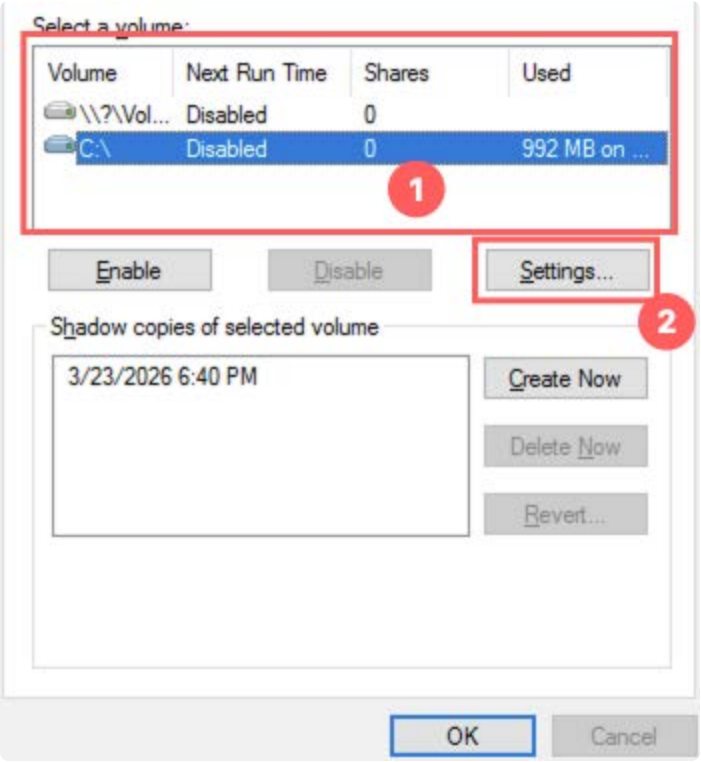
1. Select any drive letter, right-click and select "Configure Shadow Copy".



2. Manually take snapshots of each drive letter in turn, and the snapshot is taken successfully. The screenshot is a snapshot of the C drive that was successfully taken manually. The snapshot is at position 3.

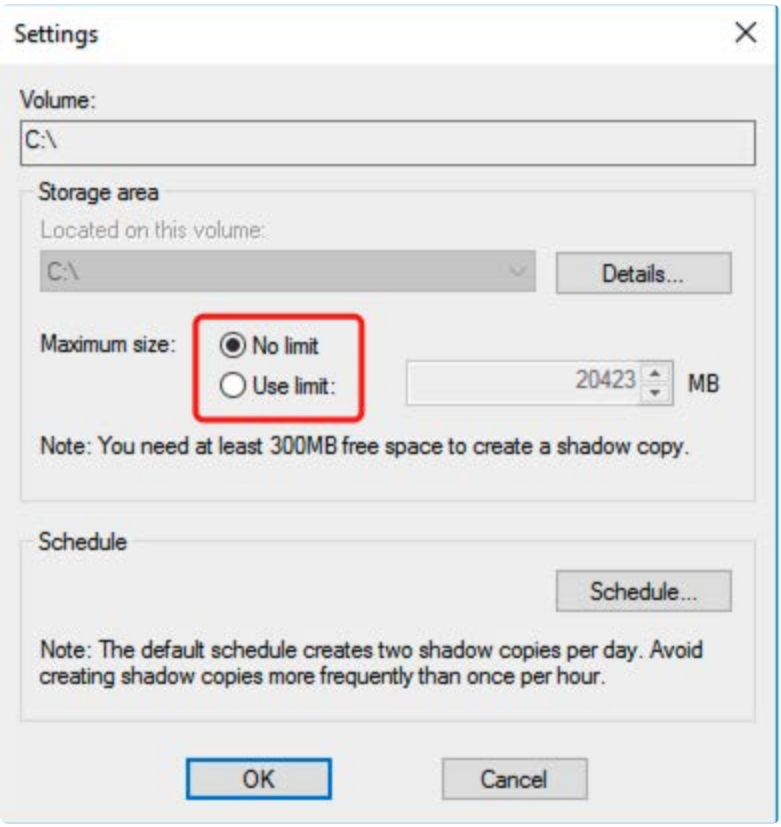


3. If each partition can successfully take a snapshot, synchronization is initiated on the replication task.
    a. If synchronization is initiated and the snapshot still fails to be created, it may be due to poor disk I/O and the snapshot timeout.
4. If one or more partitions fail to take manual snapshots, modify the shadow copy configuration.
5. **Select each drive letter in turn,**modify the settings



6. Toggle between usage restrictions and no restrictions.

- If No restrictions are checked, switch to Usage restrictions, confirm and save.
- If usage restrictions are checked, switch to no restrictions, confirm and save.

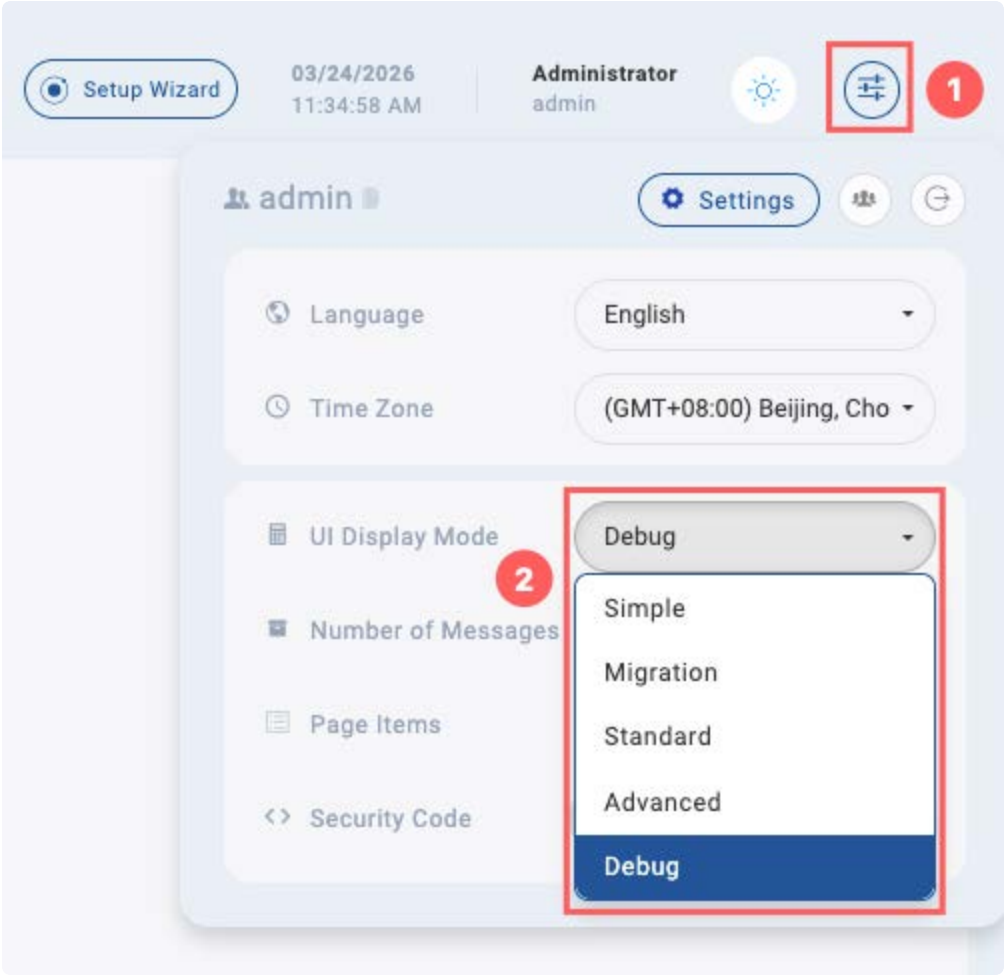


7. Repeat the above steps and try taking a snapshot manually again.

8. If none of the above methods can solve the problem of being unable to take a snapshot, use non-VSS mode instead.

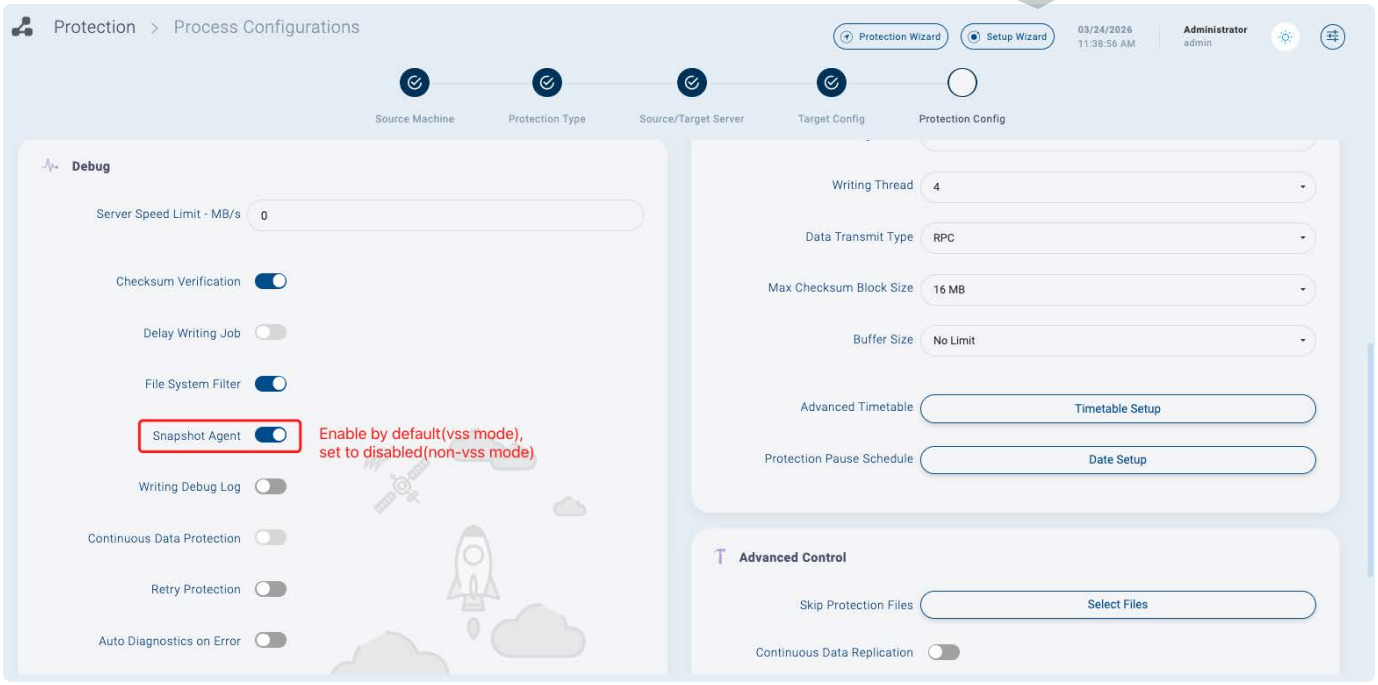
Use non-VSS instead (no snapshot mode)

Prerequisite: Set the configuration status to "" in the settings to troubleshoot.



When creating or editing a synchronization task, turn off the Snapshot Agent.

> Tips:
>
> You can switch between VSS and non-VSS repeatedly in a synchronization task.
>
> The configuration information of the synchronization task will take effect during the next synchronization after modification.



Linux

Not enough space

The default configuration requires 10% free space for each mount point.

```
[root@centos78-2003 ~]# df -hT
文件系统                类型      容量  已用  可用 已用% 挂载点
devtmpfs                devtmpfs  908M     0  908M    0% /dev
tmpfs                   tmpfs     920M     0  920M    0% /dev/shm
tmpfs                   tmpfs     920M  8.9M  911M    1% /run
tmpfs                   tmpfs     920M     0  920M    0% /sys/fs/cgroup
/dev/mapper/centos-root xfs        32G  1.9G   31G    6% /
/dev/sda1               xfs      1014M  154M  861M   16% /boot
tmpfs                   tmpfs     184M     0  184M    0% /run/user/0
/dev/sdb1               ext3       99G  461M   93G    1% /data
[root@centos78-2003 ~]#
```

Clean up space and make 10% free space.

Or refer to the operating experience knowledge base "Linux Modification Ratio (Snapshot Size)" to reduce the ratio.

The mount point corresponding to fstab is abnormal

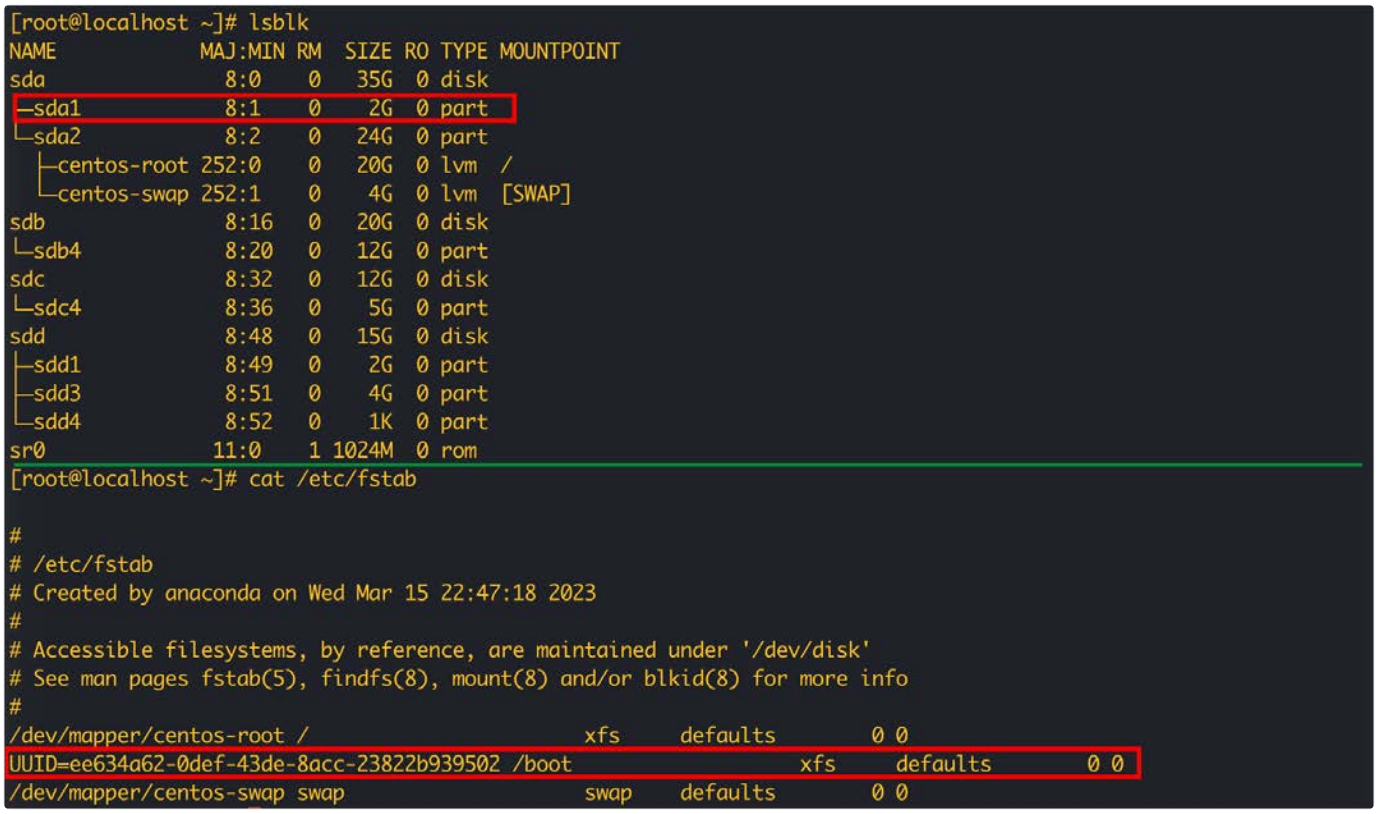
In Antenna.log, there is usually a log indicating that the mount point failed to create a snapshot.

NEXAVM

```
#for example,sda1 (boot) mount point is abnormal
failed to create snapshot of partition : sda1 (/boot,).
```

Check the mount point of fstab and check whether the mount point is mounted normally based on the output of lsblk.

In the screenshot example, the sda1 (boot) partition is not mounted.



After mounting the corresponding partition correctly, you can initiate manual synchronization of the task.

```
# taking sda1 (boot) as an example
mount /dev/sda1 /boot/
```

bite snapshot file

You can see `block device is already being traced` in dmesg.

```
ltbd: block device is already being traced: -22
```

Just clear the snapshot and then initiate synchronization.

```
/usr/local/antenna/antenna --erase
```

ext3 causes timeout

ext3 is an older file type with poorer performance. Taking a snapshot will take a long time.

```
localhost:~ # df -hT
Filesystem     Type      Size  Used Avail Use% Mounted on
/dev/sda2      ext3       33G  3.8G   28G  12% /
devtmpfs       devtmpfs  940M   92K  940M   1% /dev
tmpfs          tmpfs     940M  100K  940M   1% /dev/shm
```

For particularly large disks ext3 needs to modify the ratio.

Refer to the operating experience knowledge base "Linux Modification Ratio (Snapshot Size)" for processing.

Incorrect disk type

```
[root@c79-178-lcc ~]# df -hT
Filesystem              Type      Size  Used Avail Use% Mounted on
devtmpfs                devtmpfs  908M     0  908M   0% /dev
tmpfs                   tmpfs     920M     0  920M   0% /dev/shm
tmpfs                   tmpfs     920M   17M  903M   2% /run
tmpfs                   tmpfs     920M     0  920M   0% /sys/fs/cgroup
/dev/mapper/centos-root xfs        37G  1.8G   36G   5% /
/dev/sda1               xfs      1014M  160M  855M  16% /boot
/dev/sda3               ext4       30G  267M   28G   1% /data
/dev/sdb1               ext4       40G  311M   37G   1% /data2
tmpfs                   tmpfs     184M     0  184M   0% /run/user/0
[root@c79-178-lcc ~]# fdisk /dev/sda -l

Disk /dev/sda: 107.4 GB, 107374182400 bytes, 209715200 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000b8766

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048     2099199     1048576   83  Linux
/dev/sda2         2099200    83886079    40893440   8e  Linux LVM
/dev/sda3        83886080   146800639    31457280   8e  Linux LVM
[root@c79-178-lcc ~]#
```

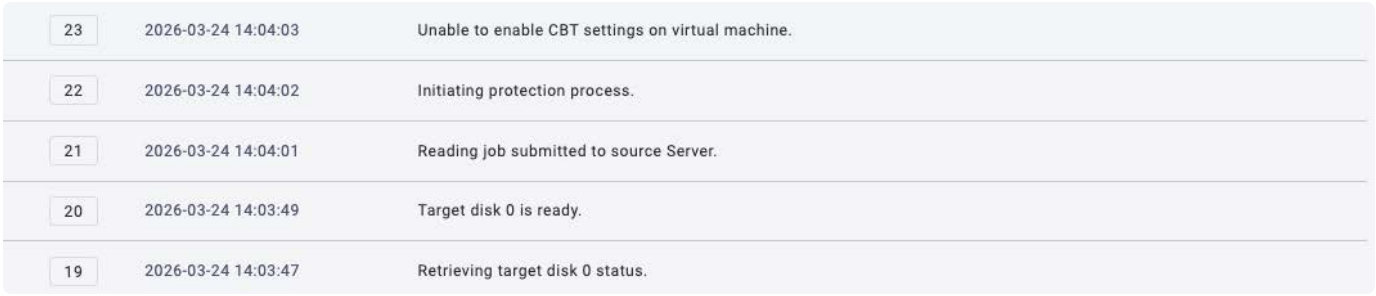
The user's source host environment configuration is incorrect: the disk uses standard partitions, but the type in the disk information is LVM.

Please refer to the operating experience knowledge base "Linux Modification Partition Type" for processing.

Unable to enable CBT settings on VMware virtual machine

Document Category: Third Party Related Experience

Error screenshot



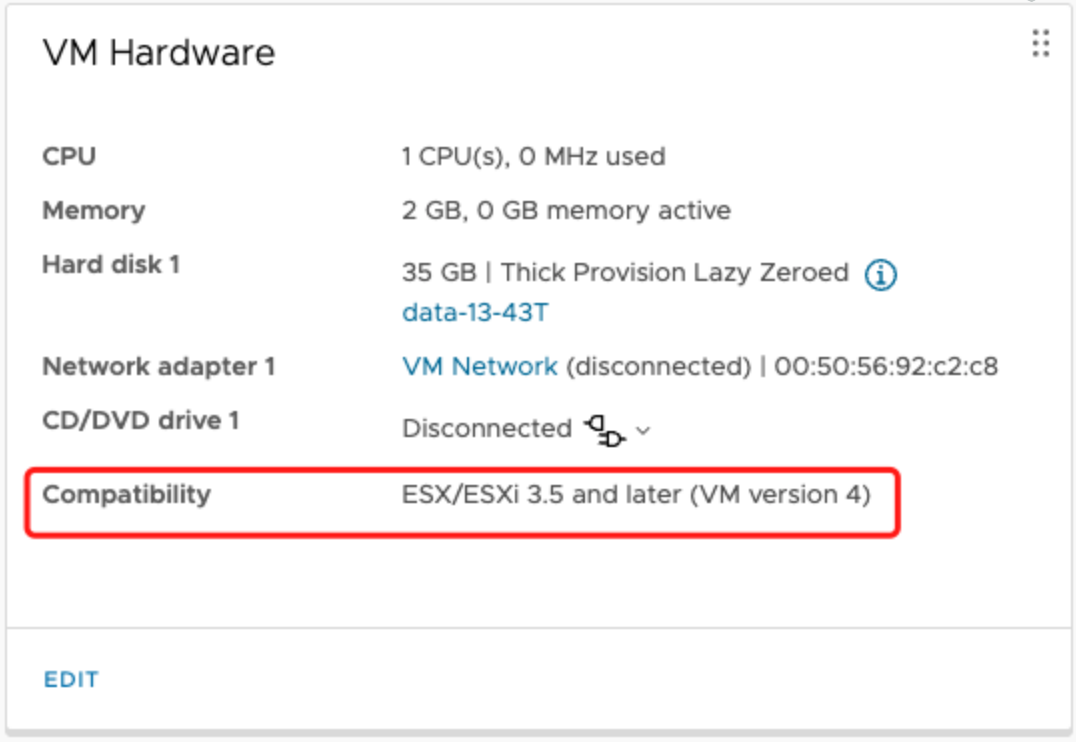
23	2026-03-24 14:04:03	Unable to enable CBT settings on virtual machine.
22	2026-03-24 14:04:02	Initiating protection process.
21	2026-03-24 14:04:01	Reading job submitted to source Server.
20	2026-03-24 14:03:49	Target disk 0 is ready.
19	2026-03-24 14:03:47	Retrieving target disk 0 status.

Problem analysis

1. The compatibility of the virtual machine is too low and does not match the version of ESXi it is running.
2. The disk is of a type not supported by VMware VADP.
3. An exception occurred with VMware Changed Block Tracking (CBT).

solution

The compatibility of the source machine is too low



Refer to the knowledge base "Upgrading VMware Virtual Machine Compatibility".

If the user does not agree to upgrade the virtual machine compatibility, please use antenna installation method to migrate.

The disk of the virtual machine is an independent disk

Agentless transfer is not supported for "RDM, independent–persistent, independent–non–persistent" type disks or disks that are directly iscsi–to–virtual machines.

You can only install antenna to complete the migration.

CBT error on source host

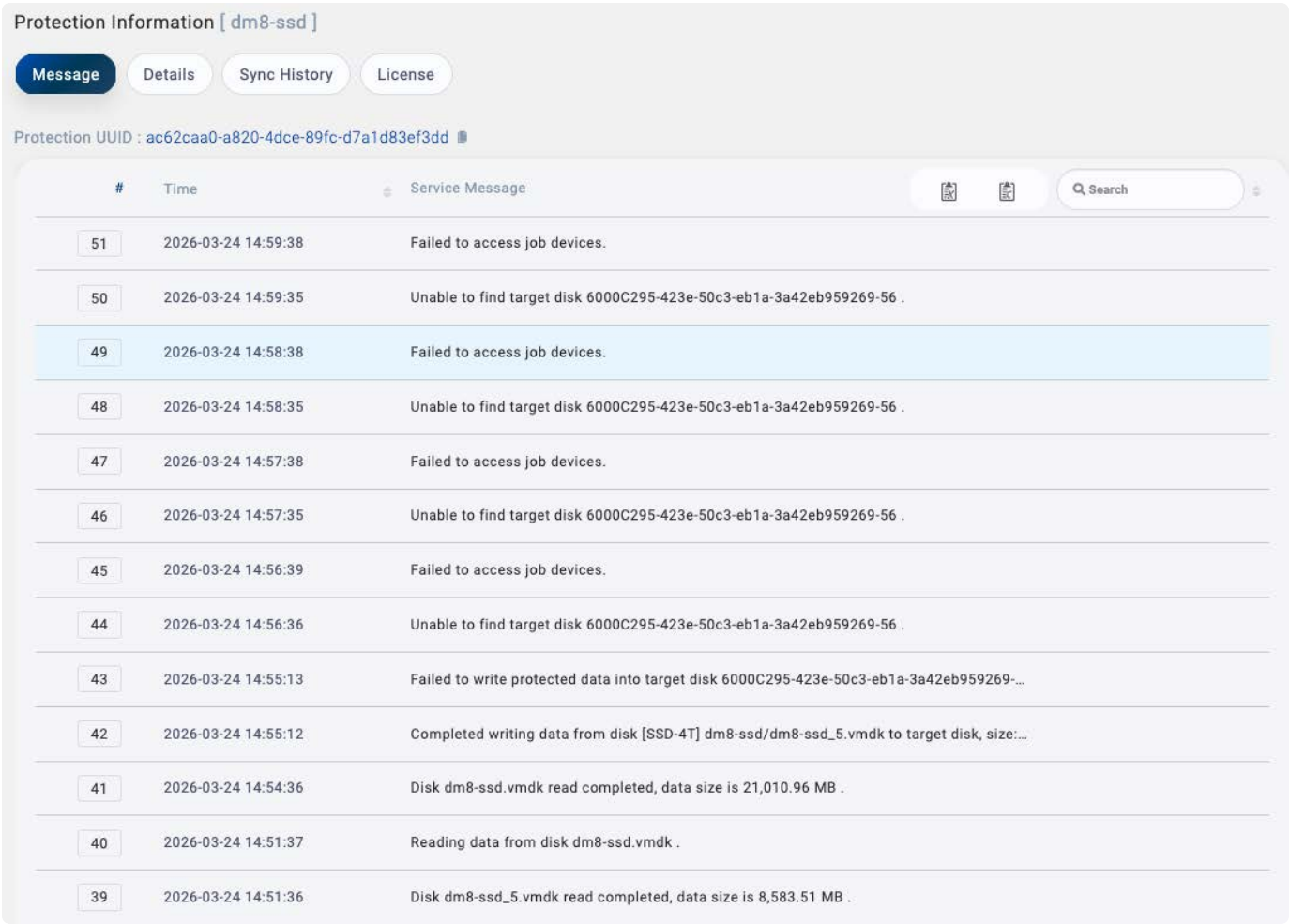
Refer to the knowledge base "VMware Reset CBT".

Failed to access job devices

Document Category: Product Related Experience

Error screenshot

Failed to access job device, unable to find target disk



Cause analysis

1. The target disk was not successfully mounted to the target machine.
2. It has been mounted on the target disk but cannot be recognized by the target machine (common in target mount mode).

Solution 1. Failure to successfully mount the disk

1. Check the number of disks and disk size of the source host on the management console.
2. Find the target machine IP according to the synchronization task, or record the source host name to the target platform to find the corresponding target machine.
3. Check the number and size of disks on the target machine. After confirming that disks are missing or the size is abnormal, check the audit log to confirm the reason for the abnormal number or size of disks (usually insufficient storage space).
    - The target system disk is 5G larger than the source system disk, and the data disk is the same size.
4. After the exception is resolved, the synchronization task can be rebuilt.

Solution 2. Mounted disk not recognized

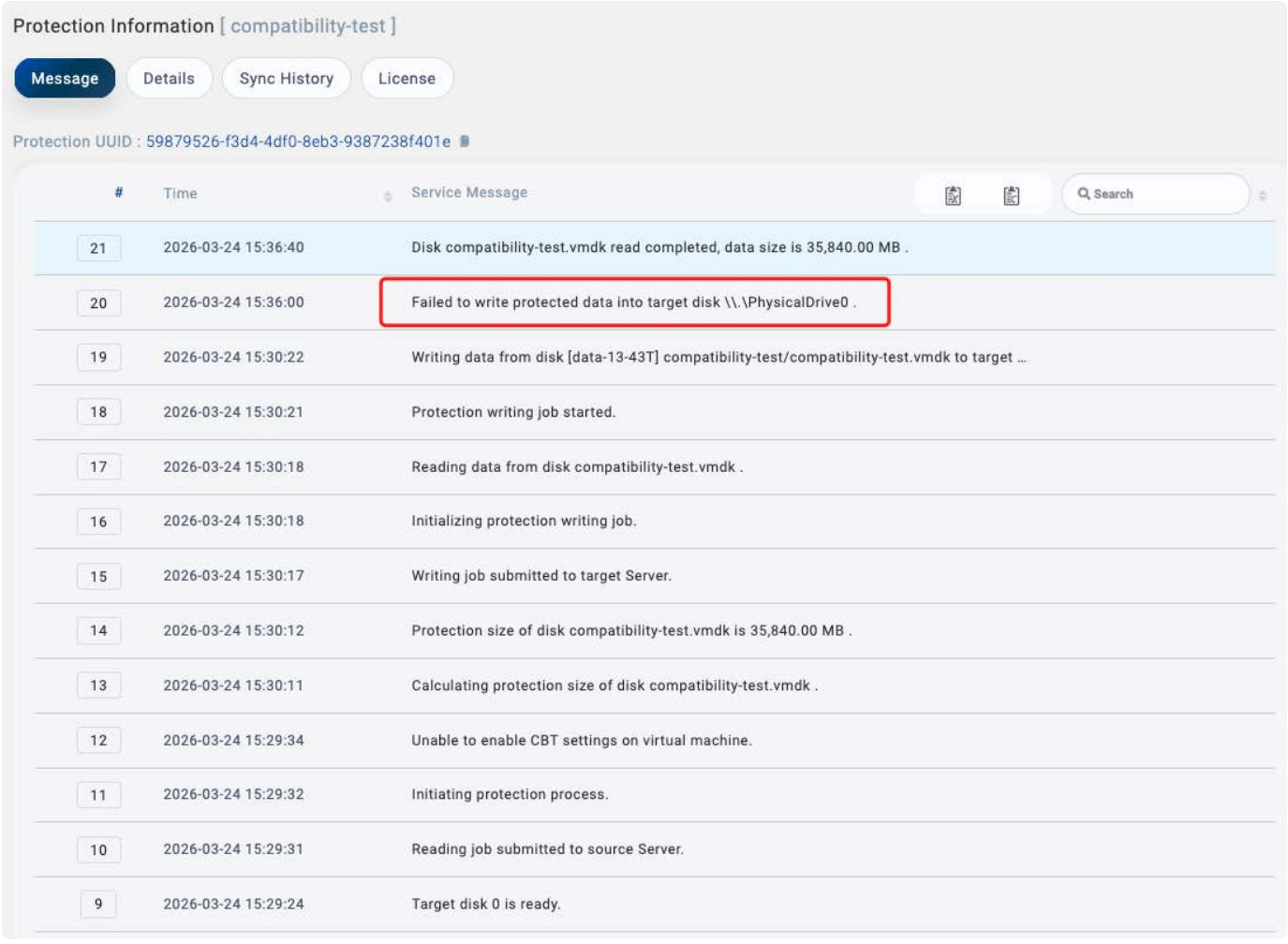
1. Verify that the target machine has the correct size and correct number of disks mounted.
2. Start virtio on the target machine.
3. Rebuild the synchronization task.

Failed to write protected data into target disk \.\PhysicalDriver

Document Category: Product Related Experience

Error screenshot

Situation 1: The task stops after an error is reported



Scenario 2: After the error is reported, the reading and writing speed is good, and the synchronization task is

completed after waiting for a period of time.

Problem analysis

Scenario 1: Usually the target disk is smaller than the disk on the source host.

Situation 2: The storage sector where the target machine is located is busy or wrong, and the task writes successfully after trying to write multiple times.

Knowledge points

The relationship between the disk size of the target machine and the source host:

	Source host	Target machine	Remarks
System disk	50G	55G	Target machine=source host+5G 55=50+5
Data disk 1	100G	100G	Generally, the sizes are the same. However, if the disk of the target machine is larger than the disk of the source host, it is also allowed.
Data disk 2	80G	80G	
Data Disk 3	500G	500G	
.....	N	N	

Troubleshooting process

1. Confirm the IP address of the target machine through the topology diagram of the synchronization task.
2. Find the source host in the management console, click Information, and view the disk size and quantity.
3. Find the target machine based on the IP address on the NexaVM platform and check the disk size and quantity.
4. Compare the size and number of disks on the source host and target machine.
5. When the disk size of the target machine does not meet the requirements in the table, the fault is determined to be caused by the small disk size of the target machine.

solution

Scenario 1: Occasionally

It may be that NexaVM is busy and the response times out. Just delete and rebuild the synchronization task.

Situation 1: This error is reported when creating protection tasks multiple times

It is likely that the default storage pool space is insufficient.
You can manually create a cloud host on the NexaVM platform for verification.

1. Log in to the NexaVM cloud platform.
2. Create a cloud host manually.
    - Notice:
        - Specifications: Customized, recommended ⩾2C2G.
        - Image: Select the image to use when creating the protection task.
        - Cloud disk: The system disk and data disk are created according to the actual size of the migration source host.
        - Network: Keep the same as the network configured when creating the protection task.
        - **Storage allocation strategy: Be sure to choose system allocation! ! !**
        - Other parameters: Keep the defaults.

3. Submit the creation and observe whether the creation is successful.
    a. Created successfully: Eliminate the problem of insufficient storage pool space.
        - Generally, it is enough to rebuild the protection task. **(Problem Solved)**
    b. Creation failed: troubleshoot according to the error message of the platform.
        - There is a high probability that the default storage pool has insufficient resources. Create a cloud host by manually specifying the storage pool.
4. Due to insufficient space in the default storage pool, migration can only be done by manually creating a target machine for the time being. **(Problem Solved)**

Situation 1: This error occurs after running normally for a period of time

It may be that the source host's disk has been expanded, but the target machine's disk will not be automatically expanded. Therefore, the source machine's disk > the target machine's disk will appear, causing this problem.

1. Check the actual disk size and number of the source host and compare it with the disk size and number of the source host in the management console;
2. Check the target machine’s disk size and number;
3. Compare the size of the source machine disk and the target machine disk;
4. Refer to the "Knowledge Points" section of this knowledge base to confirm whether the disk size meets the migration conditions.
5. If the disk size of the source host does not meet the conditions in "Knowledge Points", you need to delete the rebuild synchronization task.

Scenario 2: After the error is reported, the reading and writing speed is good, and the synchronization task is completed after waiting for a period of time.

Usually when writing data to the target machine, a certain sector in the storage is wrong, and then the data is written normally again after retrying.

Go to the target cloud platform to check that the target disk size is not smaller than the source machine disk size and has read and write speeds. Just wait for the task to be completed.

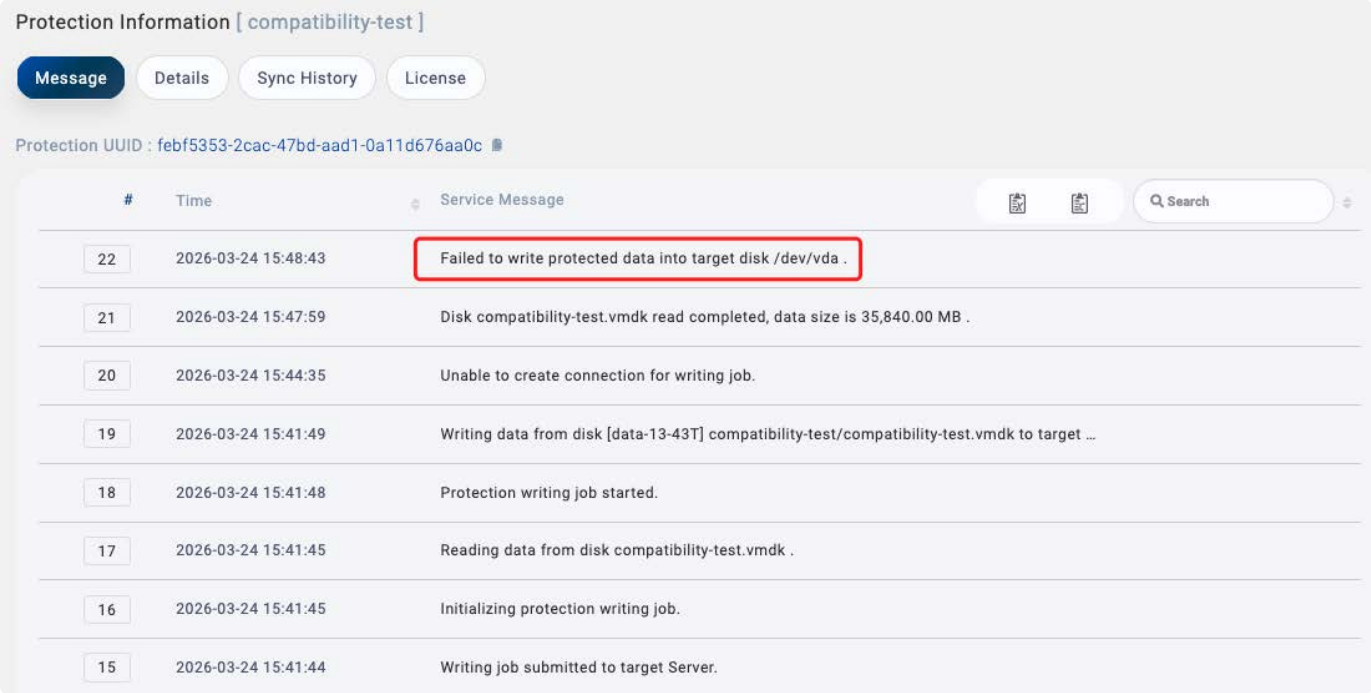
If you are worried about data integrity, you can manually initiate synchronization and select "Complete synchronization".

Failed to write protected data into target disk /dev/vda, etc.

Document Category: Product Related Experience

Error screenshot

Situation 1: The task stops after an error is reported



Scenario 2: After reporting an error, wait for a period of time before the synchronization task is completed.

Problem analysis

Scenario 1: Usually the target disk is smaller than the disk on the source host.

Situation 2: The storage sector where the target machine is located is busy or wrong, and the task writes successfully after trying to write multiple times.

Knowledge points

The relationship between the disk size of the target machine and the source host:

	Source host	Target machine	Remarks
System disk	50G	55G	Target machine=source host+5G 55=50+5
Data disk 1	100G	100G	Generally, the sizes are the same. However, if the disk of the target machine is larger than the disk of the source host, it is also allowed.
Data disk 2	80G	80G	
Data Disk 3	500G	500G	
.....	N	N	

Troubleshooting process

1. Confirm the IP address of the target machine through the topology diagram of the protection task.
2. Find the source host in the management console, click Information, and view the disk size and quantity.
3. Find the target machine based on the IP address on the NexaVM platform and check the disk size and quantity.
4. Compare the size and number of disks on the source host and target machine.

5. When the disk size of the target machine does not meet the requirements in the table, the fault is determined to be caused by the small disk size of the target machine.

solution

Scenario 1: Occasionally

It may be that NexaVM is busy and the response times out. Just delete and rebuild the synchronization task.

Situation 1: This error is reported when creating protection tasks multiple times

It is likely that the default storage pool space is insufficient.
You can manually create a cloud host on the NexaVM platform for verification.

1. Log in to the NexaVM cloud platform.
2. Create a cloud host manually.
    - Notice:
        - Specifications: Customized, recommended ⩾2C2G.
        - Image: Select the image to use when creating the protection task.
        - Cloud disk: The system disk and data disk are created according to the actual size of the migration source host.
        - Network: Keep the same as the network configured when creating the protection task.
        - **Storage allocation strategy: Be sure to choose system allocation! ! !**
        - Other parameters: Keep the defaults.
3. Submit the creation and observe whether the creation is successful.
    a. Created successfully: Eliminate the problem of insufficient storage pool space.
        - Generally, it is enough to rebuild the protection task. **(Problem Solved)**
    b. Creation failed: troubleshoot according to the error message of the platform.
        - There is a high probability that the default storage pool has insufficient resources. Create a cloud host by manually specifying the storage pool.

4. Due to insufficient space in the default storage pool, migration can only be done by manually creating a target machine for the time being. **(Problem Solved)**

Situation 1: This error occurs after running normally for a period of time

It may be that the source host's disk has been expanded, but the target machine's disk will not be automatically expanded. Therefore, the source machine's disk > the target machine's disk will appear, causing this problem.

1. Check the actual disk size and number of the source host and compare it with the disk size and number of the source host in the management console;
2. Check the target machine's disk size and number;
3. Compare the size of the source machine disk and the target machine disk;
4. Refer to the "Knowledge Points" section of this knowledge base to confirm whether the disk size meets the migration conditions.
5. If the disk size of the source host does not meet the conditions in "Knowledge Points", you need to delete the rebuild synchronization task.

Scenario 2: After reporting an error, wait for a period of time before the synchronization task is completed.

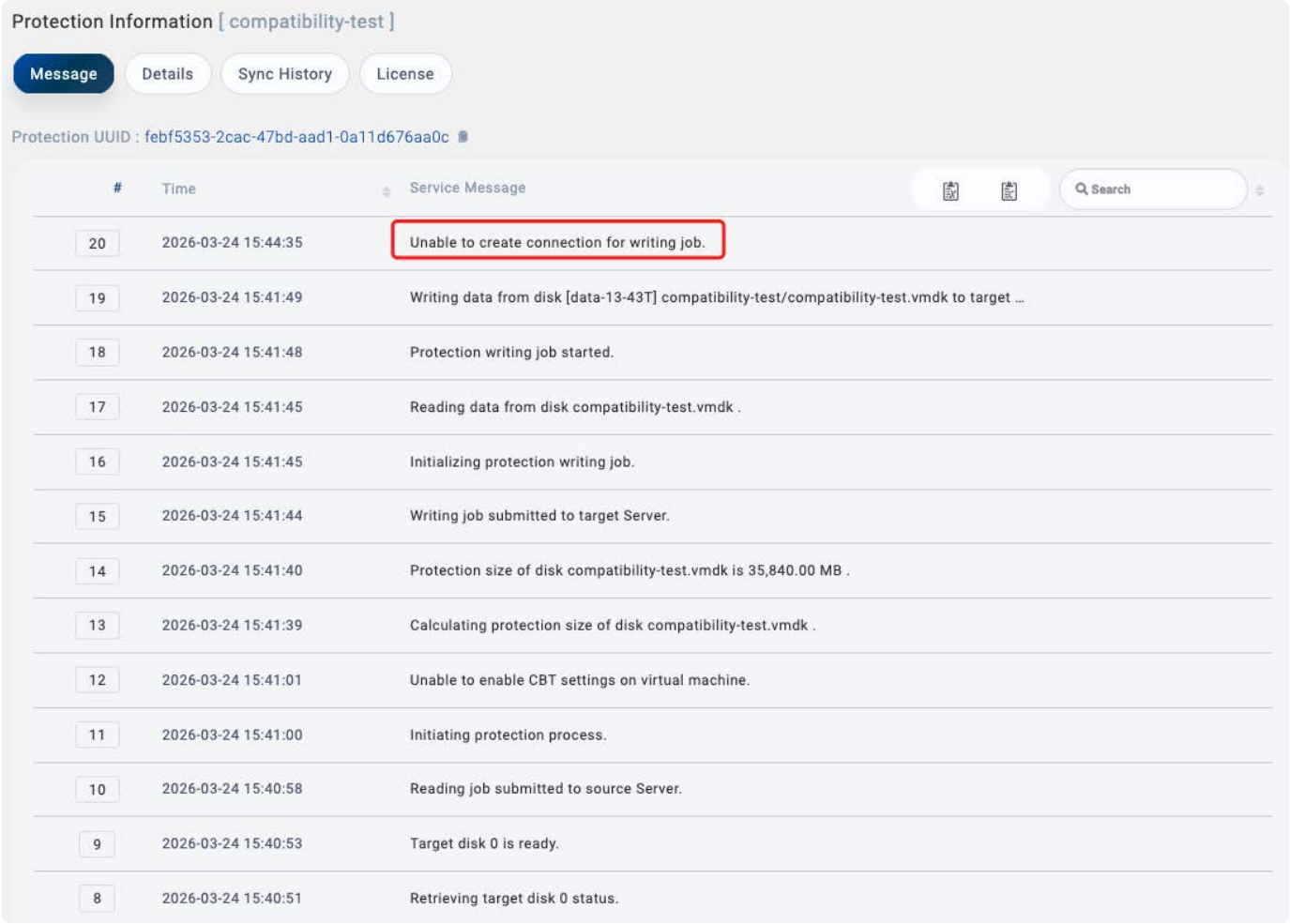
Usually when writing data to the target machine, a certain sector in the storage is wrong, and then the data is written normally again after retrying.

If you are worried about data integrity, you can manually initiate synchronization and select "Complete synchronization".

Unable to create connection for writing job

Document Category: Product Related Experience

Error screenshot



Cause analysis

1. The network from the management console to the target machine is unstable.
2. The management console cannot access the target machine: The target machine has been deleted.
3. The management console cannot access the target machine: The network between the management console and the data gateway to the target machine is abnormal.

Solution.1 The network is unstable

When the network is unstable, usually after this error occurs, the system will retry in the background. After the retry is successful, reading and writing will be normal. Observe the reading and writing speed and percentage changes. You can wait for the synchronization task to be completed.

Solution.2 Unable to access the target machine – the target machine was accidentally deleted

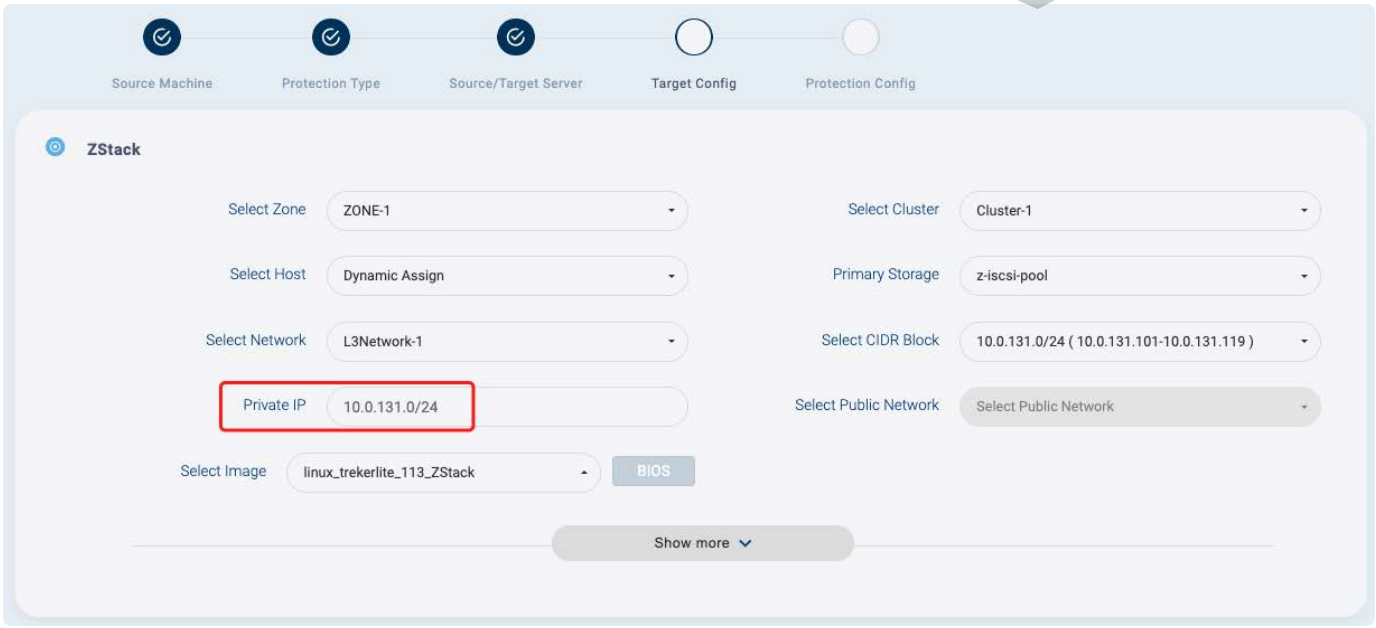
Check whether the target machine exists. It may have been accidentally deleted by other administrators. If it was accidentally deleted, consider restoring it from the Recycle Bin or rebuilding the synchronization task.

Solution.3 Unable to access the target machine – the network of the target machine is abnormal

Check the network from the management console, relay data gateway to the target machine:

1. Ping the IP of the target machine and observe whether it is connected and whether there is any packet loss.
2. Telnet the 20000 and 20001 ports of the target machine and observe whether they are connected.
3. Find the target machine in the data gateway of the management console, select the target machine, and click Modify below to test connectivity.

After troubleshooting, it is confirmed that it is a network problem. You can consider rebuilding the synchronization task. When creating the synchronization task, specify an unused IP in the `Private IP` field.


Source Machine
Protection Type
Source/Target Server
Target Config
Protection Config
ZStack
Select Zone
ZONE-1
Select Cluster
Cluster-1
Select Host
Dynamic Assign
Primary Storage
z-iscsi-pool
Select Network
L3Network-1
Select CIDR Block
10.0.131.0/24 (10.0.131.101-10.0.131.119)
Private IP
10.0.131.0/24
Select Public Network
Select Public Network
Select Image
linux_trekerlite_113_ZStack
BIOS
Show more

Failed to read VMDK disk *.vmdk

Document Category: Product Related Experience

VDDK version is incompatible

VMware's VDDK is version compatible with VMware ESXi.

Collect vCenter or ESXi version information and refer to "Switching VDDK to the Specified Version" to replace the compatible version of VDDK.

Transit data gateway Treker.log

```
2025-03-05 09:50:18.739 (T6504) |E|server_j(410) - (b04f4d63-c082-47c1-9a65-bf97beb824ee.prt)Unable to open disk image 6000C292-82e8-d497-c9d6-bca2dbf19284-215_13bc5234-6872-4c40-a752-7cd7fabd5156.
2025-03-05 09:50:21.719 (T9988) |W|[NFC ERROR] NfcAioRcvErrorMsg: Error from server: NfcAioProcessOpenFileMsg: Failed to open '[nfs20230306] 195.073 20230823web05/195.073 20230823web05_1-000003.vmdk': DiskLib error 16392: Failed to lock the file
2025-03-05 09:50:23.231 (T6504) |R| Last message repeated 1 times
2025-03-05 09:50:23.231 (T6504) |R|vmware(7266) - Open image file failure => Unknown error, error = 1.
2025-03-05 09:50:23.232 (T6504) |E|server_j(410) - (b04f4d63-c082-47c1-9a65-bf97beb824ee.prt)Failed to read VMDK disk 195.073 20230823web05_1-000003.vmdk.
```

VDDK compatibility issues

If you encounter this problem when using vCenter to add VMware to the management console, try changing to ESXi to add VMware to the management console.

If you encounter this problem when using ESXi to add VMware to the management console, try changing to vCenter to add VMware to the management console.

Ports 443 and 902 of vCenter or ESXi are unreachable

NEXAVM

It can be verified by telnet vCenter on the management console or ESXi ports 443 and 902.

Unable to resolve VMware domain name

Modify hosts in the management console and data transfer gateway systems, and add mapping between IP addresses and domain names.

- Some environments require correct intranet DNS configuration.

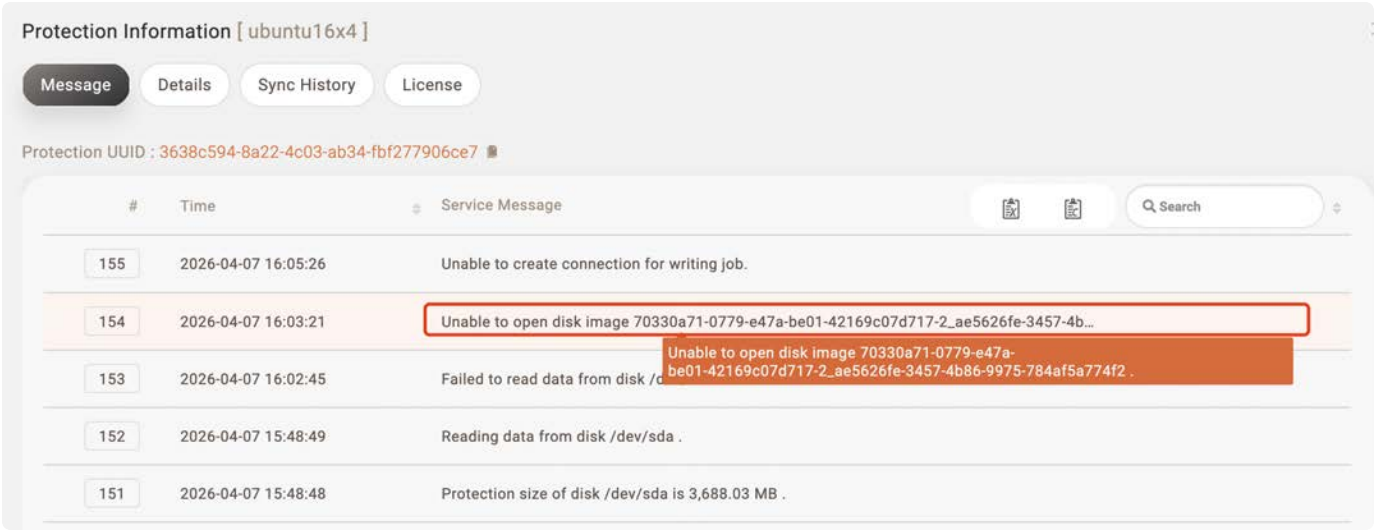
Transit data gateway Treker.log reference

```
2025-03-10 10:28:58.009 (T6732) |W|vmware(7316) - VixDiskLib : Failed to prepare for access (20005).
2025-03-10 10:28:58.009 (T6732) |W|virtual_(1109) - Job(1939812f-ee09-4252-b8df-34b47fbe9680.prt) - doing full disk replication for replication.
2025-03-10 10:28:58.150 (T6732) |W|[NFC WARNING]Plain-text connection is deprecated; use SSL to connect to NFC server
2025-03-10 10:28:58.150 (T6732) |W|[NFC ERROR]NfcNewAuthdConnectionEx: Failed to connect: Host address lookup for server <域名> failed: No such host is known
2025-03-10 10:28:58.150 (T6732) |W|[NFC ERROR]NfcNewAuthdConnectionEx: Failed to connect to peer. Error: Host address lookup for server <域名> failed: No such host is known
2025-03-10 10:28:58.150 (T6732) |W|[NFC ERROR]NfcEstablishAuthCnxToServer: Failed to create new AuthD connection: Host address lookup for server <域名> failed: No such host is known
2025-03-10 10:28:58.150 (T6732) |W|[NFC ERROR]Nfc_BindAndEstablishAuthdCnx3: Failed to create a connection with server <域名>: Host address lookup for server <域名> failed: No such host is known
2025-03-10 10:28:58.166 (T6732) |E|vmware(7266) - Open image file failure => The server refused connection, error = 14009.
2025-03-10 10:28:58.166 (T6732) |E|virtual_(1115) - Job(1939812f-ee09-4252-b8df-34b47fbe9680.prt) - Cannot open vmdk disk ([nfs20230306] 195.073 20230823web05/195.073
```

Unable to open disk image (string)

Document Category: Product Related Experience

Error screenshot



Problem analysis

When copying data, reading may fail due to factors such as the user's network and disk I/O, and this message will appear.

The software will continue to read and retry in the background. If the read is successful, synchronization will continue.

Case 1. There is copy speed

Just wait for the synchronization task to complete.

Case 2. No copy speed

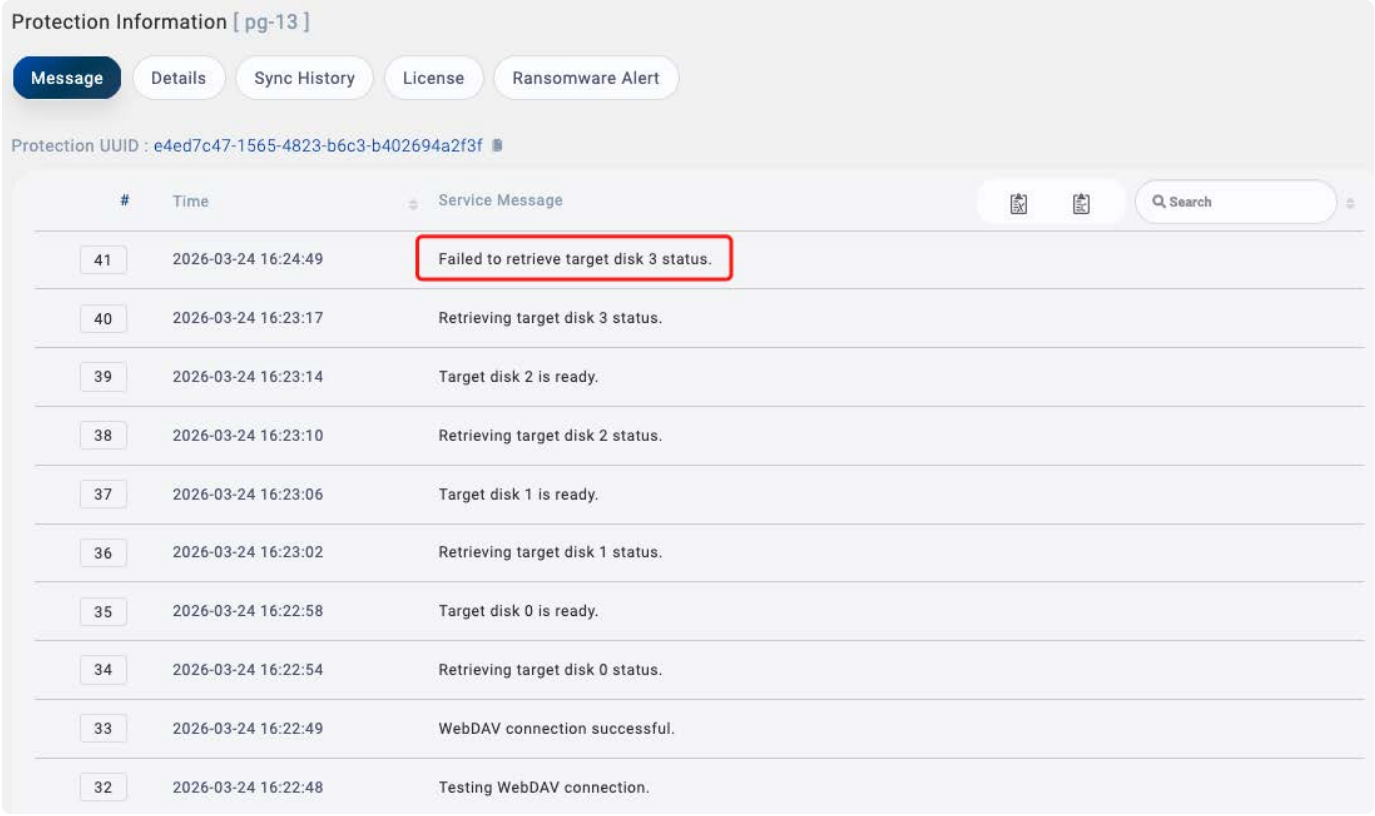
1. Stop the synchronization task.

2. Refer to the operating experience knowledge base "reset Job–Handling synchronization task stuck" Reset Job.
3. Select the protection task and click the "Initiate Now" button to manually initiate synchronization.
4. If the synchronization proceeds normally, the problem is solved.
5. If the synchronization is stuck, or an error is still reported, collect the synchronization task diagnostic report again, and contact Support for technical support.

Failed to retrieve target disk (numeric) status

Document Category: Product Related Experience

Error screenshot



Problem analysis

The user's network policy does not permit the required ports

- Check the trekercontrol.log of the transit machine

```
2024-May-22 02:19:48.448732 (T7fb63f7fe700)|E|service_(370) - 10.0.133.35:20001 - socket open() error: No route to host
2024-May-22 02:19:48.448879 (T7fb63f7fe700)|E|common_s(14) - Cannot connect to host (10.0.133.35).
2024-May-22 02:20:22.528476 (T7fb63effd700)|E|service_(370) - 10.0.133.35:20001 - socket open() error: No route to host
2024-May-22 02:20:22.528590 (T7fb63effd700)|E|common_s(14) - Cannot connect to host (10.0.133.35).
2024-May-22 02:20:56.608396 (T7fb63ffff700)|E|service_(370) - 10.0.133.35:20001 - socket open() error: No route to host
```

NexaVM has insufficient storage resources

1. Check whether the number of disks on the target host is consistent with the number of disks on the source machine.
2. Cloud disk --> Not instantiated, whether the data disk of the target disk exists.
    - If so, please manually mount it to the target instance.
3. Check whether the target storage has sufficient free space.

The system type of the BootImage image is incorrectly selected.

- Check the system type of BootImage, it cannot be other.
- Other can only recognize the IDE's disk.

vhost storage is not compatible with BootImage

- Check whether the storage used by NexaVM is vhost.
- vhost storage needs to use the specified version of BootImage.

Tips

Unable to read target disk 0 status, usually a network problem.

The status of the target disk (non-zero numbers such as 1, 2, 3, etc.) cannot be read, usually because there is insufficient storage space or the wrong system type is selected.

Solution 1. Network strategy

Just release the corresponding port according to the error report.

Solution 2. Insufficient storage resources

Expand storage capacity according to project needs.

Solution 3. Wrong system type selection

1. Modify the system type of the BootImage image to Windows or Linux.
2. Delete the rebuild synchronization task.

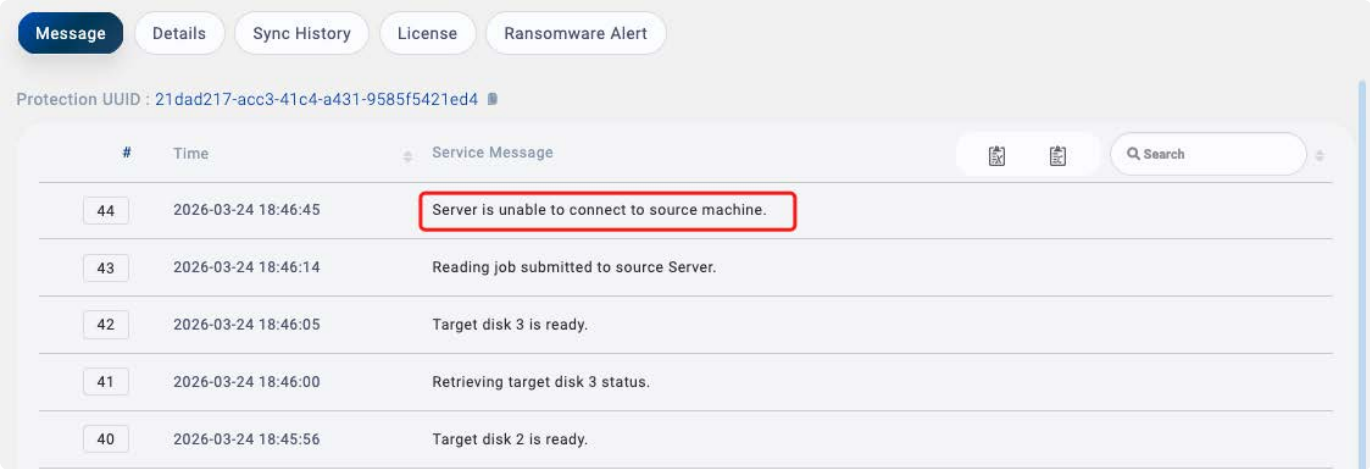
Solution 4.vhost storage is incompatible with BootImage

Use LinuxBootImage ⩾ 676 version.

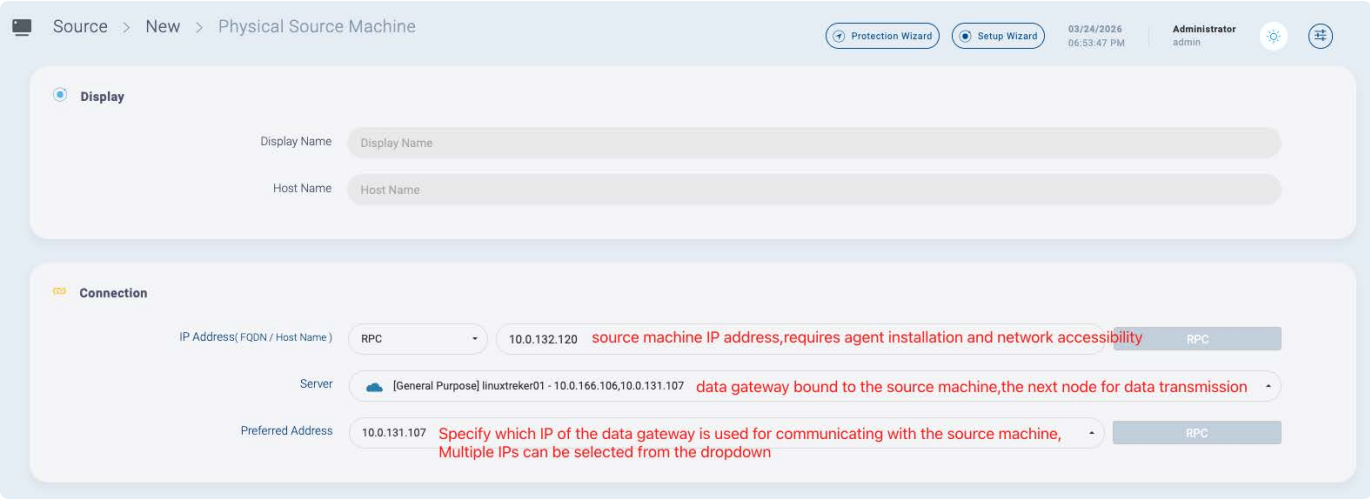
Server is unable to connect to source machine

Document Category: Product Related Experience

Error screenshot



Knowledge points



Connect to the source host, that is, the data gateway bound to the source machine can communicate with the source machine.

The following conditions must be met:

1. The data gateway bound to the source machine can communicate with the source machine.

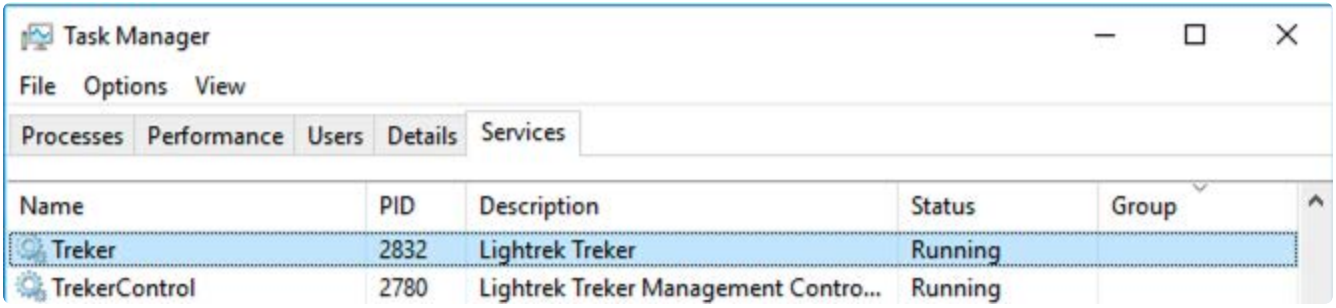
NEXAVM

- The data gateway can telnet to port 20005 of the source host.
  - Take the above picture as an example: 10.0.132.181 telnet 10.0.130.41 port 20005 is open.
- The source host can telnet to ports 20000 and 20001 of the data gateway.
  - Take the above picture as an example: 10.0.130.41 telnet 10.0.132.181 ports 20000 and 20001 are open.

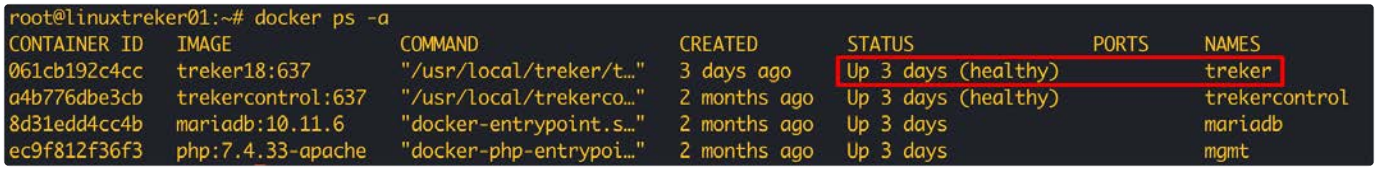
2. The Treker service of the data gateway must be running.

Data gateway service

Windows Data Gateway



Linux data gateway



3. The Antenna service on the source host must be running.

Source hosting service

Windows source machine



Linux source machine

NEXAVM

```
[root@localhost ~]# systemctl status antenna
● antenna.service - Lightrek antenna
   Loaded: loaded (/etc/systemd/system/antenna.service; enabled; vendor preset: disabled)
   Active: active (running) since 四 2024-09-05 02:54:26 EDT; 4 days ago
 Main PID: 7314 (antenna.sh)
    Tasks: 4
   Memory: 226.2M
   CGroup: /system.slice/antenna.service
           ├─7314 /bin/bash /usr/local/antenna/antenna.sh
           └─7371 /usr/local/antenna/antenna

9月 05 02:54:26 leon systemd[1]: Started Lightrek antenna.
9月 05 02:54:26 leon antenna.sh[7314]: Initializing firewall successful
9月 05 02:54:28 leon antenna.sh[7314]: Service starting...
```

Troubleshooting steps

Manual troubleshooting

1. Check the service status of the data gateway and source host.
2. Check whether 20000 and 20001 of the source host's telnet data gateway are accessible.
3. Check whether the 20005 of the source host of the data gateway is telnet accessible.

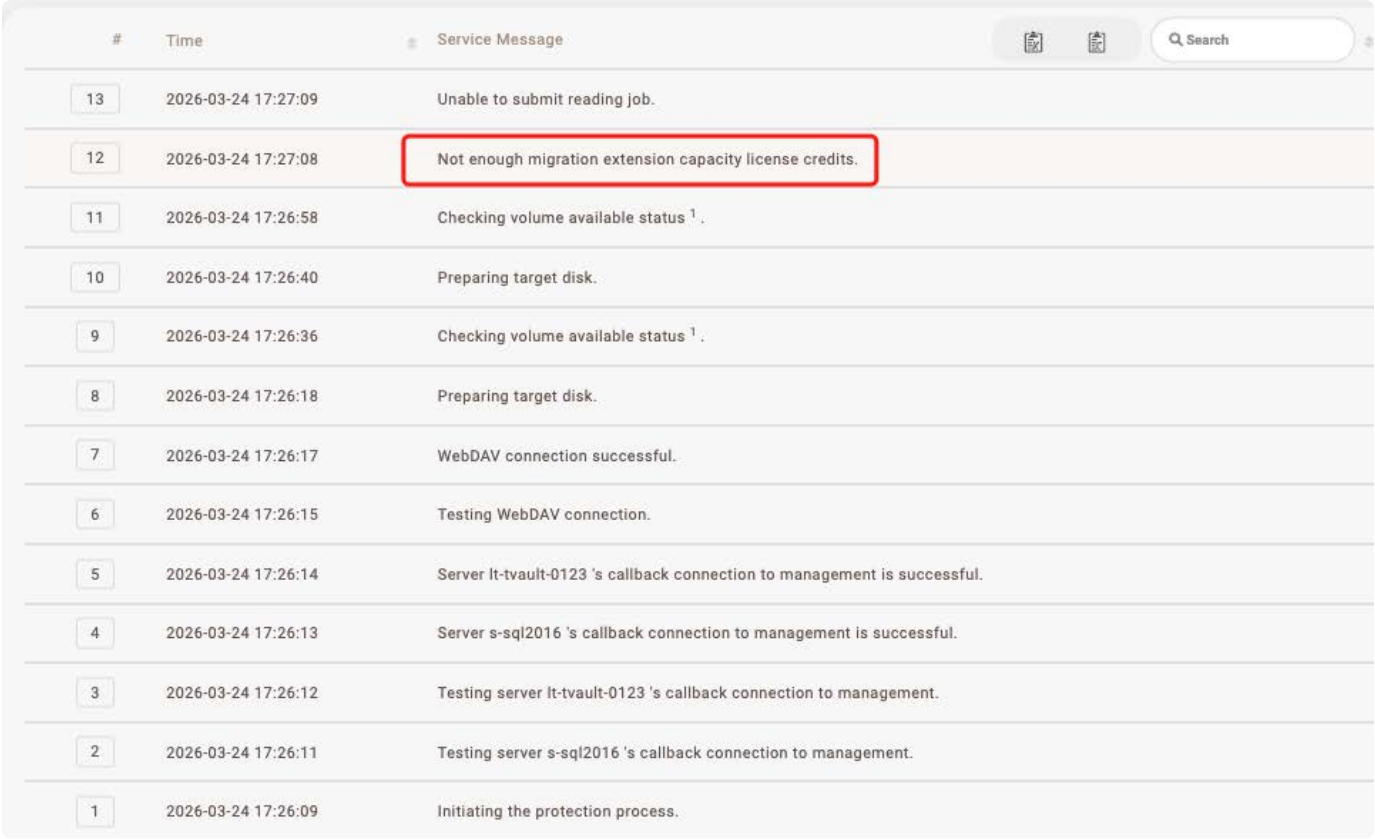
Analyze diagnostic logs

1. Collect the diagnostic log of the synchronization task.
2. Check the treker.log of the target machine.

Not enough migration extension capacity license credits

Document Category: Product Related Experience

Error screenshot



#	Time	Service Message
13	2026-03-24 17:27:09	Unable to submit reading job.
12	2026-03-24 17:27:08	Not enough migration extension capacity license credits.
11	2026-03-24 17:26:58	Checking volume available status [1] .
10	2026-03-24 17:26:40	Preparing target disk.
9	2026-03-24 17:26:36	Checking volume available status [1] .
8	2026-03-24 17:26:18	Preparing target disk.
7	2026-03-24 17:26:17	WebDAV connection successful.
6	2026-03-24 17:26:15	Testing WebDAV connection.
5	2026-03-24 17:26:14	Server lt-tvault-0123 's callback connection to management is successful.
4	2026-03-24 17:26:13	Server s-sql2016 's callback connection to management is successful.
3	2026-03-24 17:26:12	Testing server lt-tvault-0123 's callback connection to management.
2	2026-03-24 17:26:11	Testing server s-sql2016 's callback connection to management.
1	2026-03-24 17:26:09	Initiating the protection process.

Problem analysis

The disk capacity that needs to be synchronized on the source host exceeds 5T.

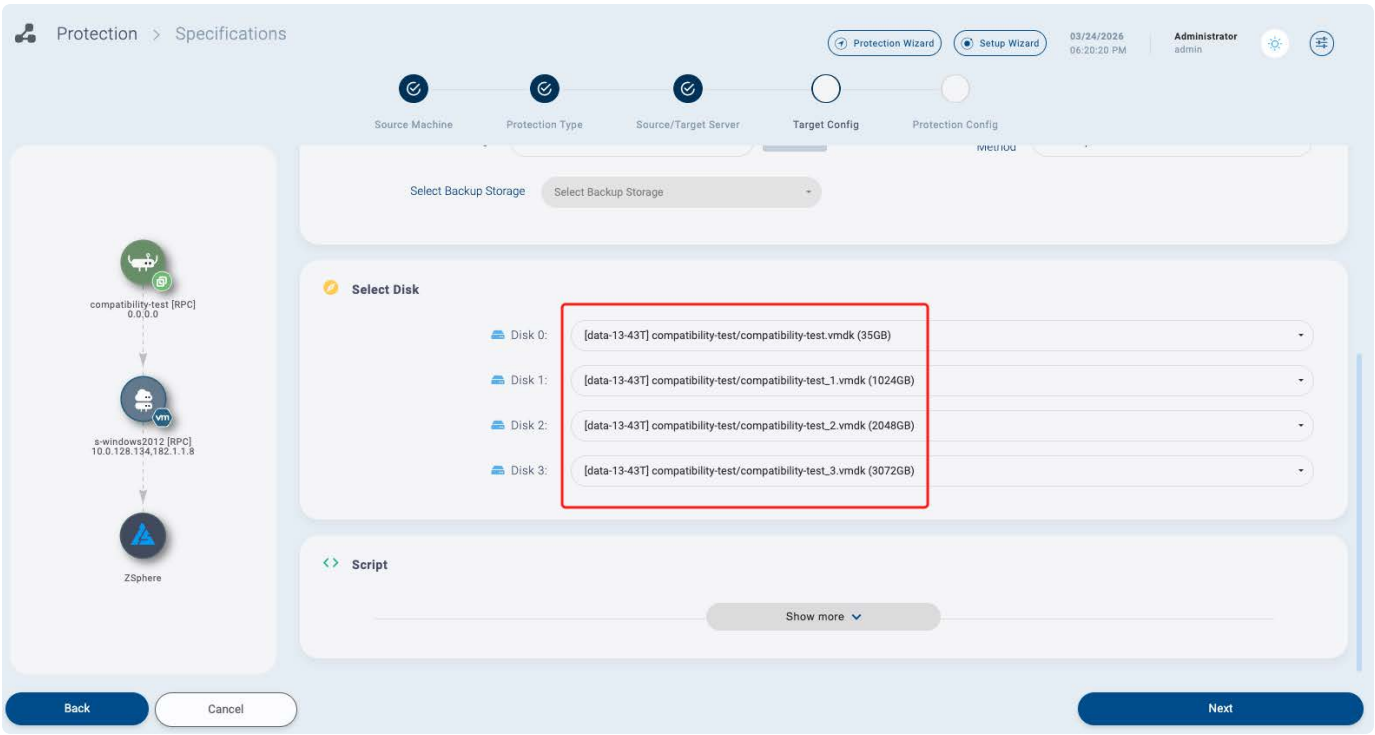
Knowledge point 1

Migration permission: By default, disks within 5T are supported for migration, and the source host synchronizes the total size of the disk.

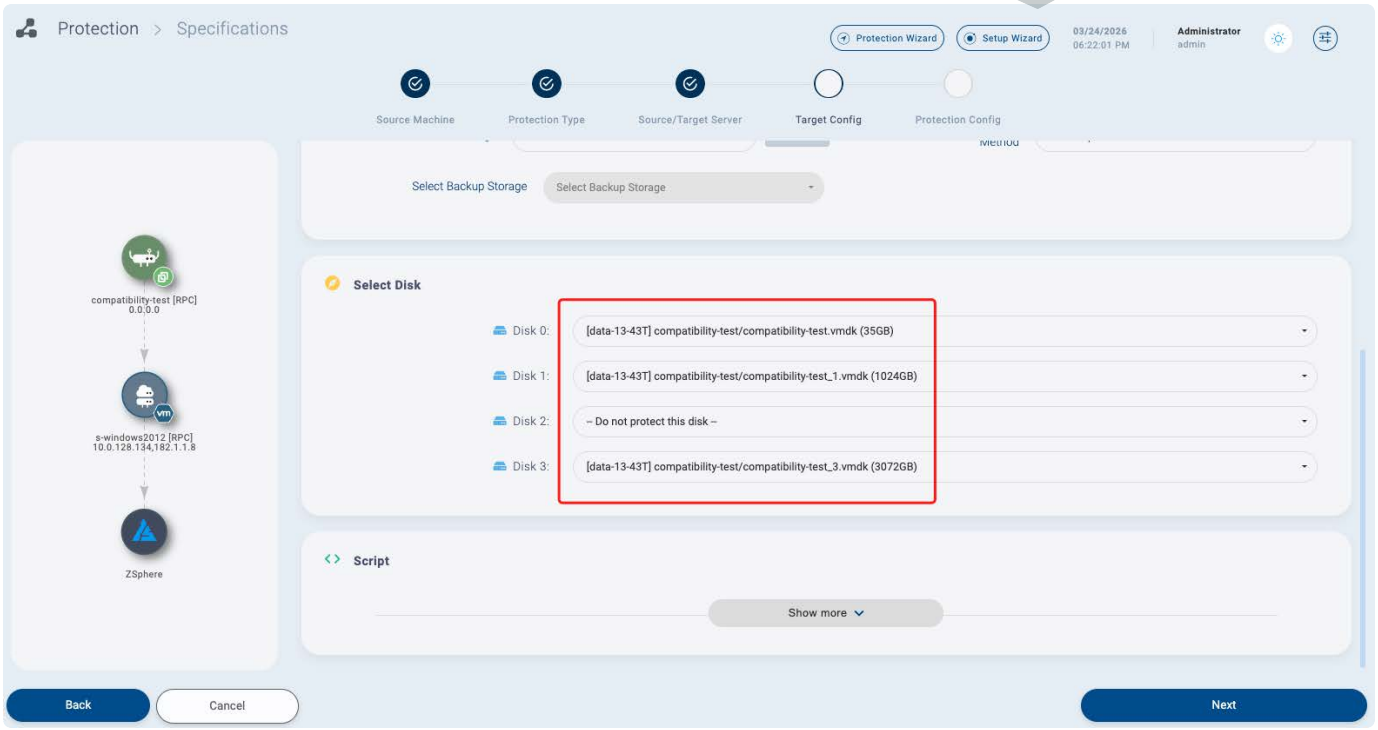
Capacity license: When the disk exceeds 5T, you need to add a capacity license, the minimum unit is 1T.

Knowledge point 2

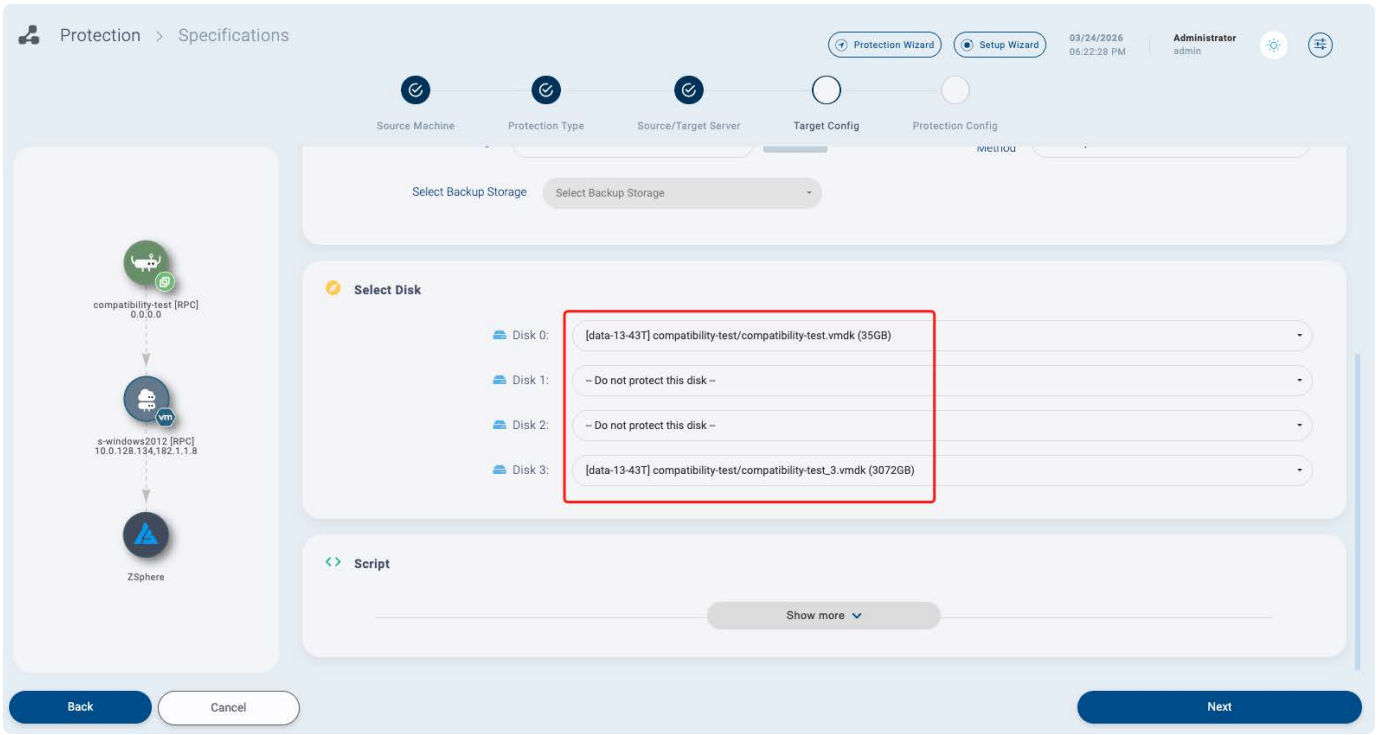
Total disk size: 6179G



Total disk size: 4131G



Total disk size: 3107G



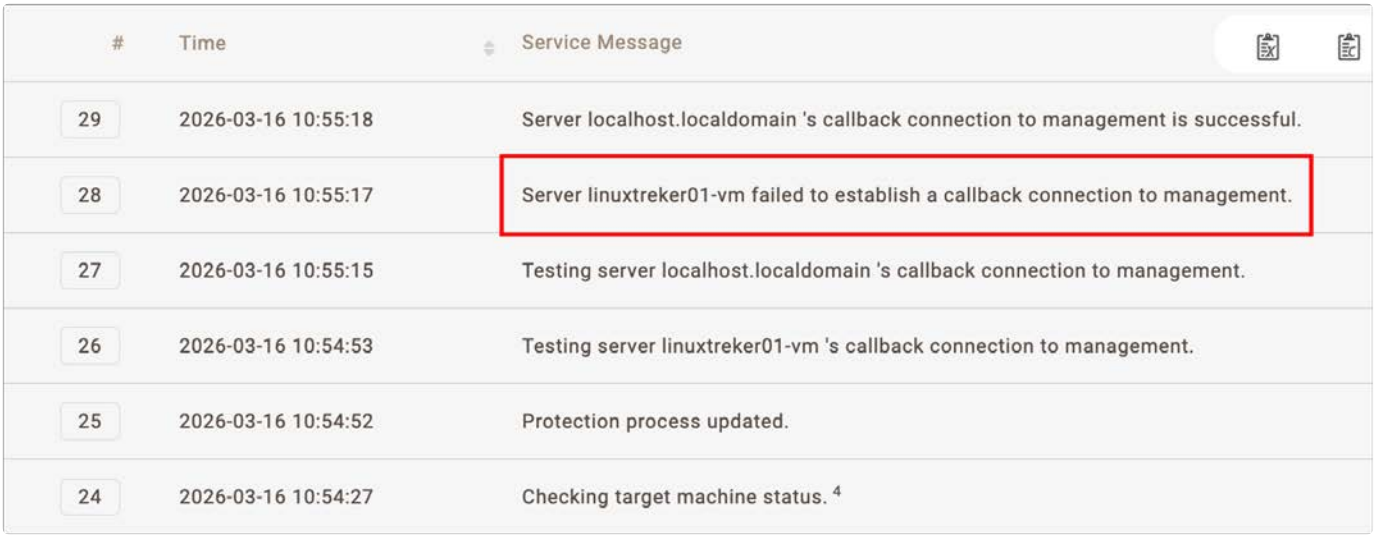
Solution

Apply for the corresponding capacity license as needed, and then re-create the synchronization task after activation.

Server (transit data gateway hostname) failed to establish a callback connection to management

Document Category: Product Related Experience

Error screenshot



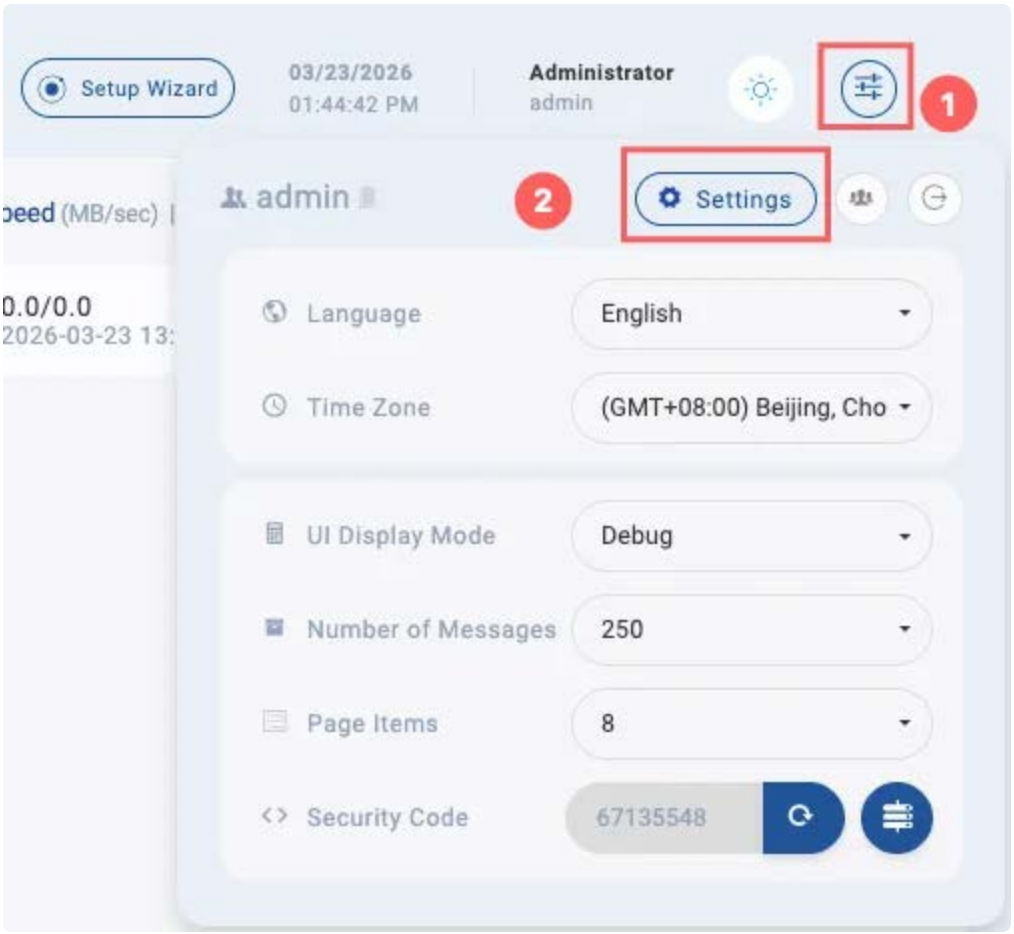
#	Time	Service Message
29	2026-03-16 10:55:18	Server localhost.localdomain 's callback connection to management is successful.
28	2026-03-16 10:55:17	Server linuxtreker01-vm failed to establish a callback connection to management.
27	2026-03-16 10:55:15	Testing server localhost.localdomain 's callback connection to management.
26	2026-03-16 10:54:53	Testing server linuxtreker01-vm 's callback connection to management.
25	2026-03-16 10:54:52	Protection process updated.
24	2026-03-16 10:54:27	Checking target machine status. [4]

Problem analysis

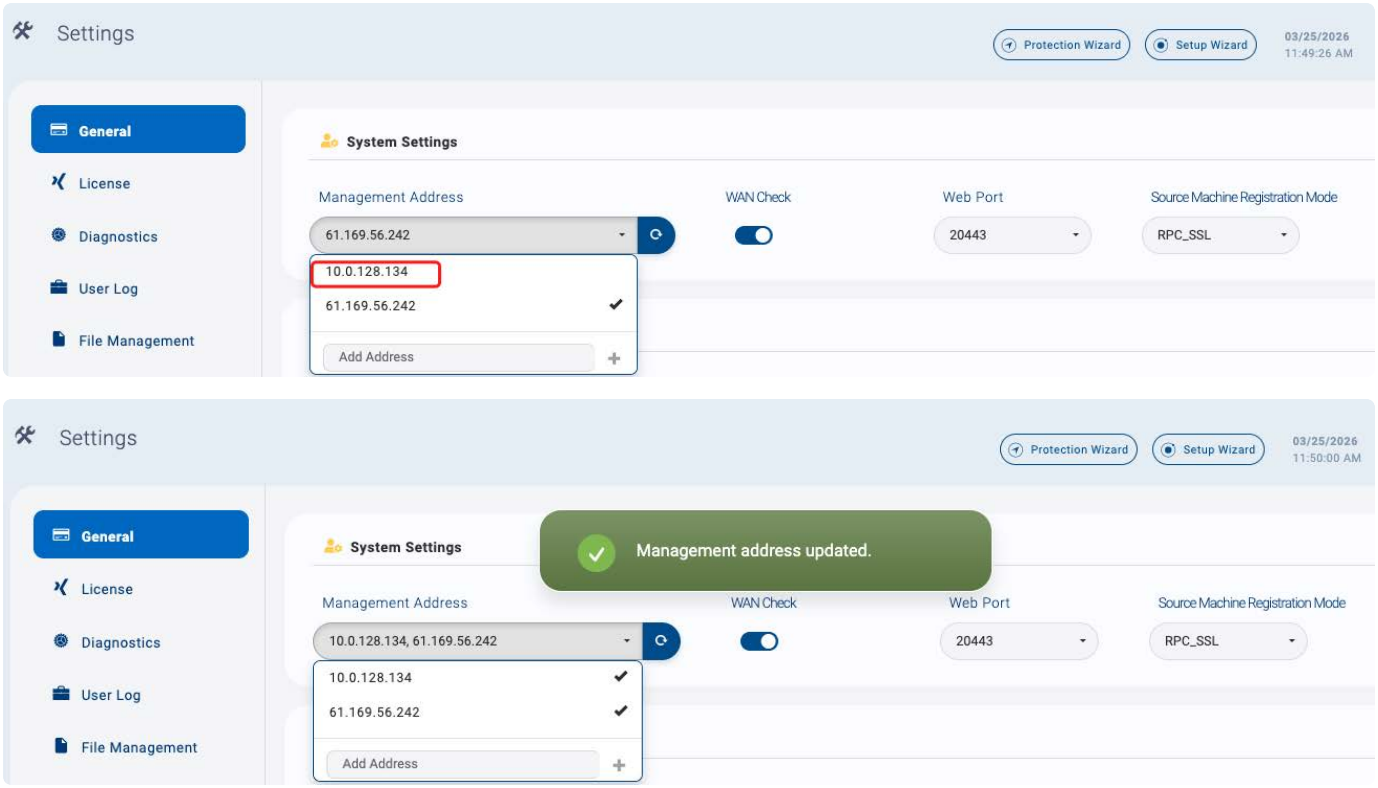
1. The management console has multiple IPs, and the multiple IPs to be used are not set as central control addresses.
2. When the transit server and the management console are the same, the Treker service of the management console may have stopped.

Solution 1. Select less or wrong IP addresses

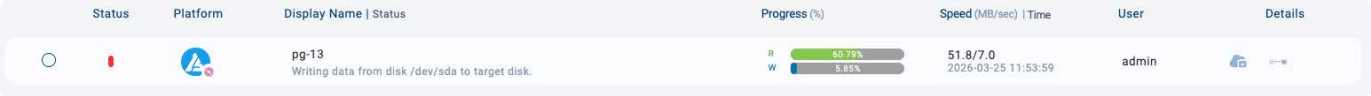
1. Delete the sync task.
2. Settings icon –-> Settings



3. Advanced --> Central control address settings, check the necessary IPs used in migration (click the IP with the mouse to check).

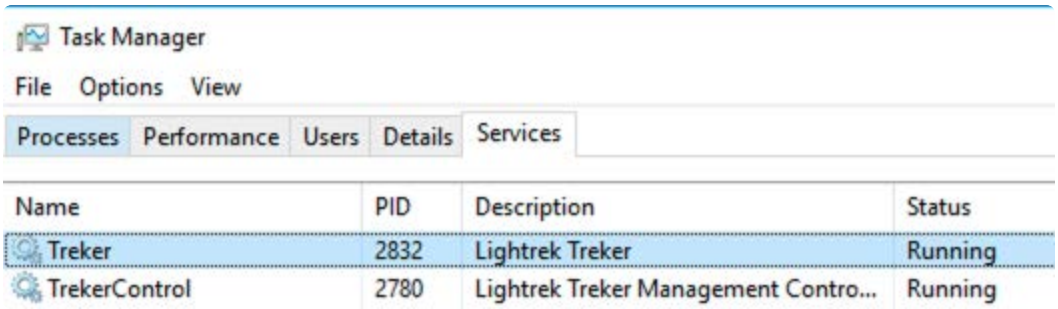


4. Re-create the sync task.



Solution 2.Treker service stopped

1. Log in to the system in the management console and check the Treker service.

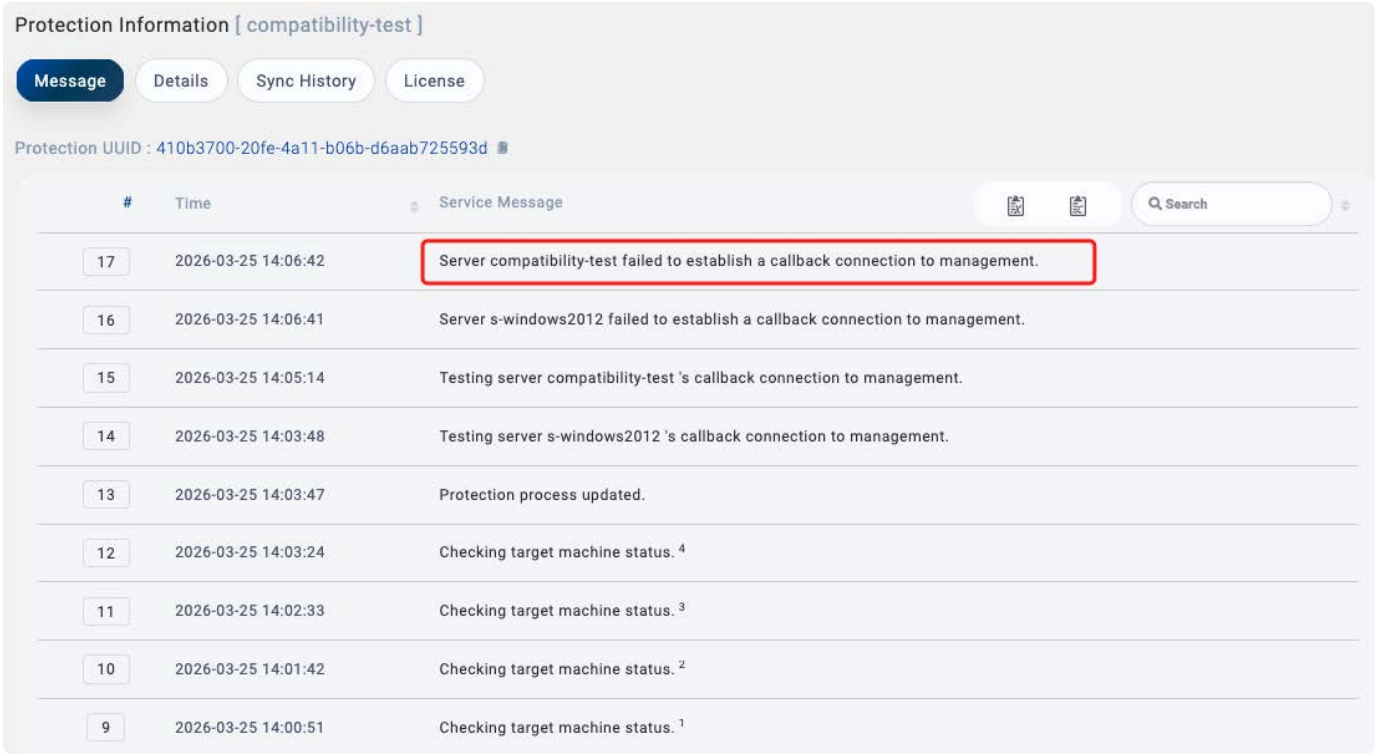


2. Start the Treker service manually.
3. Re-create the sync task.

Server (target hostname) failed to establish a callback connection to management

Document Category: Product Related Experience

Error screenshot

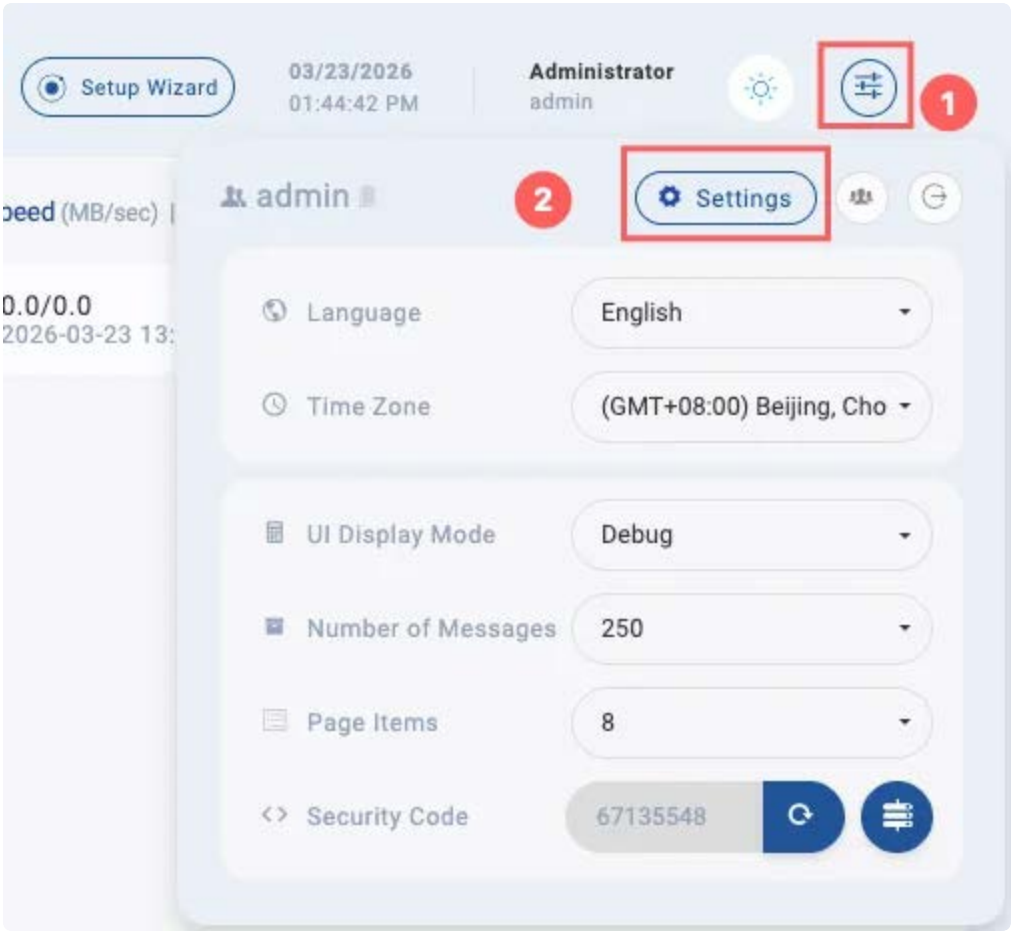


Problem analysis

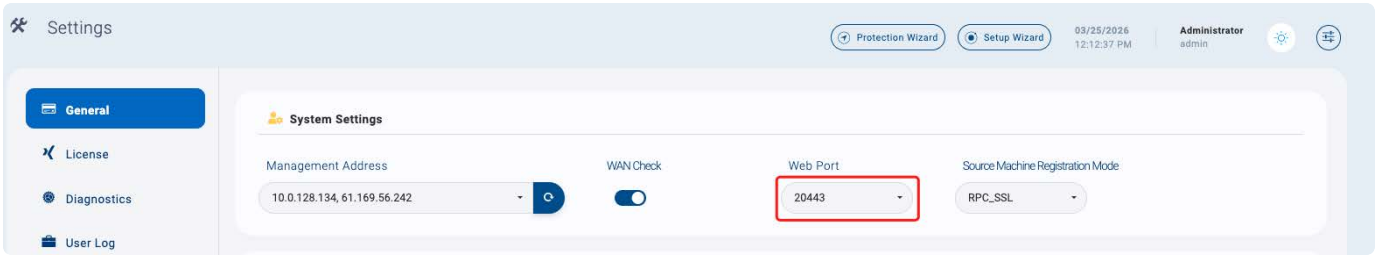
1. The management console has multiple IPs, and the multiple IPs to be used are not set as central control addresses.
2. The management console has multiple IPs, and the **`service listening address`** of the synchronization task is misconfigured**, causing the communication between the target machine and the management console to fail.
3. The target machine has an IP address conflict, or the IP address is unavailable.

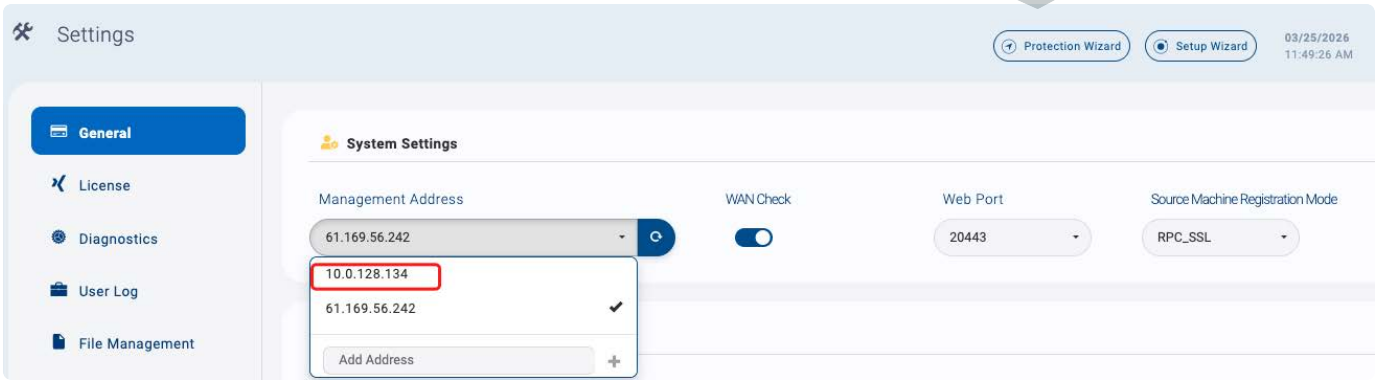
Solution 1. Select less, choose the wrong IP address, or the port is unavailable

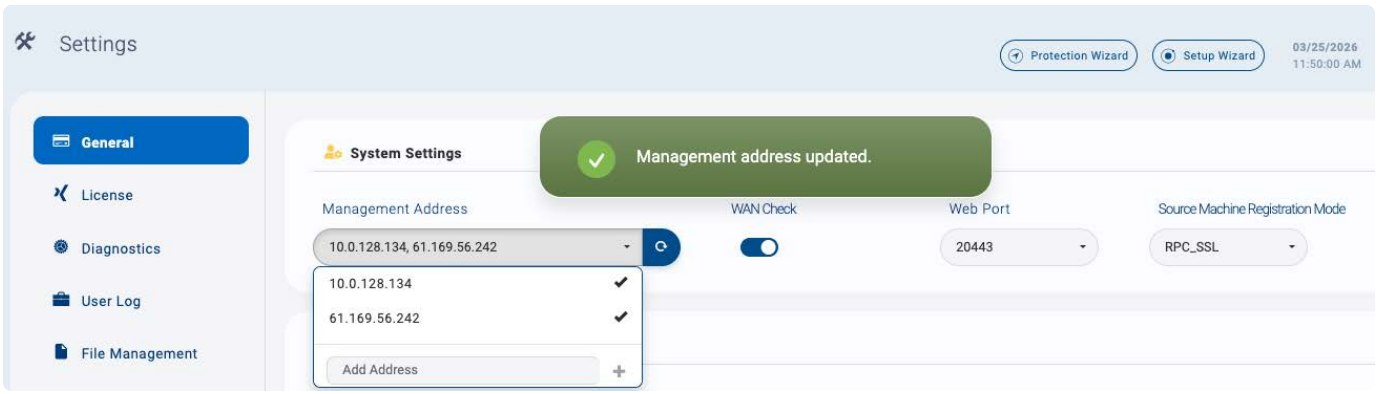
1. Delete the sync task.
2. Settings icon –-> Settings



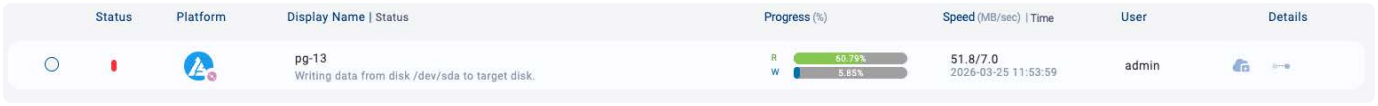
3. Advanced –-> Central control address setting, check Necessary IP used in migration (click the IP with the mouse to check).
    - **If 443 is unavailable, change the central control port to 20443 here. **





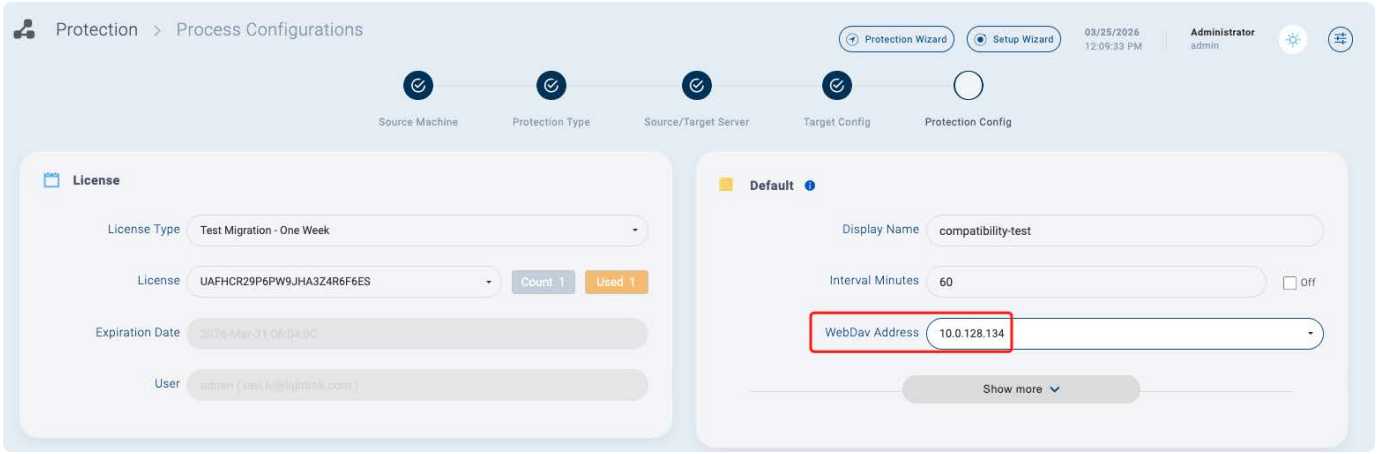


4. Re-create the sync task.



Solution 2. Choose the correct service listening address

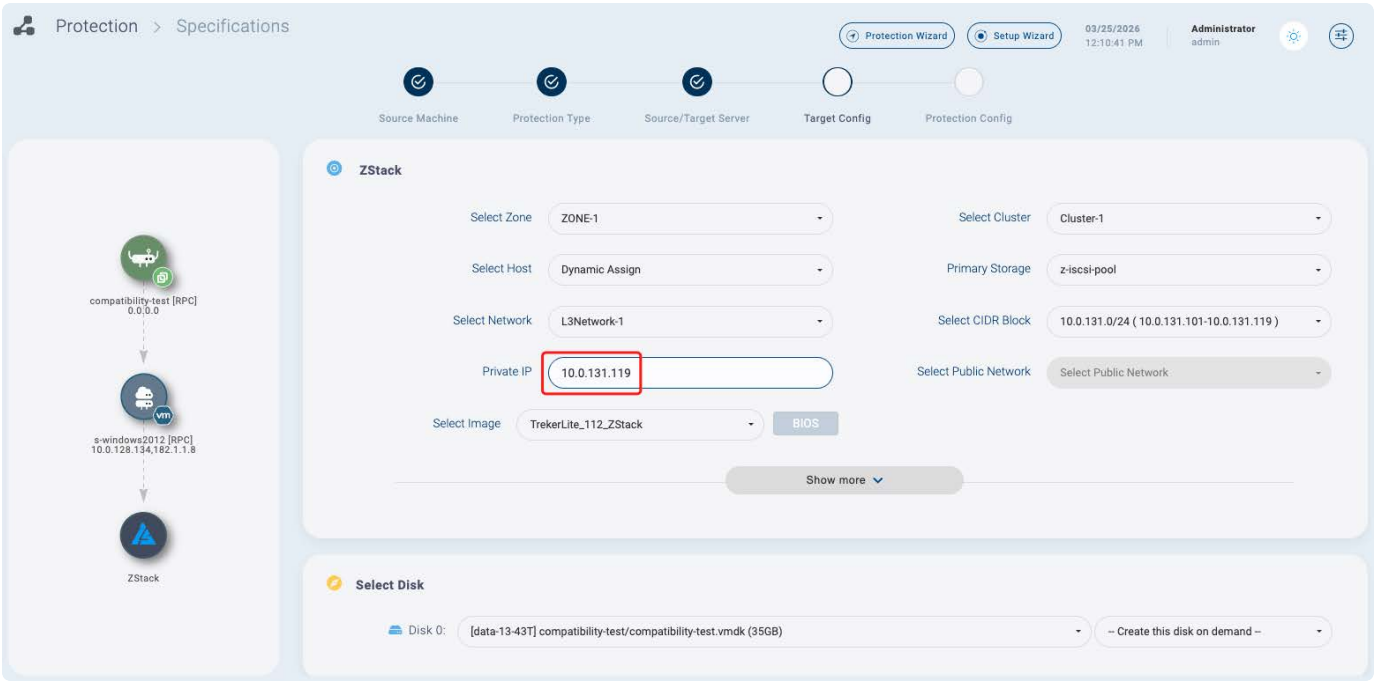
1. Delete the sync task.
2. Re-create the synchronization task and select a `service listening address` that can communicate with the target machine.



Note: Modifying the service listening address of the current task is invalid and must be deleted and rebuilt!

Solution 3. IP address conflict or unavailability

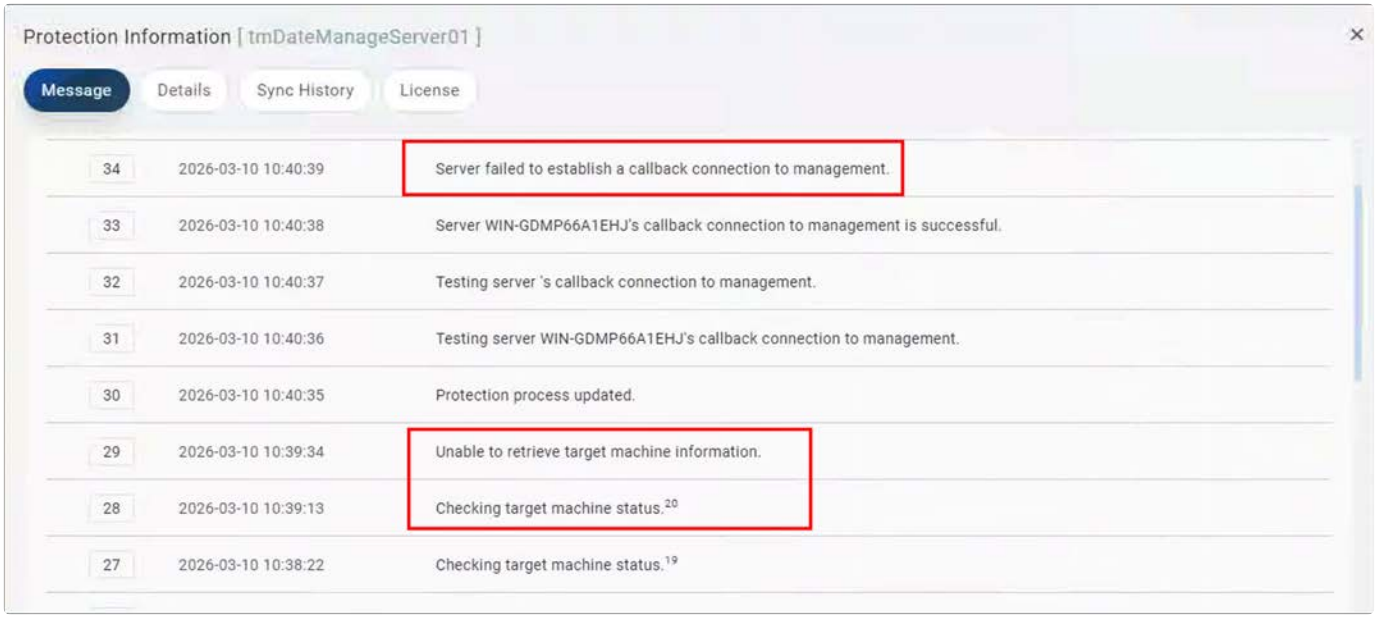
1. Delete the sync task.
2. Re-create the synchronization task and manually specify a different available IP.



Server failed to establish a callback connection to management

Document Category: Product Related Experience

Error screenshot



Problem analysis

1. The IP address has been modified in the management console.
2. The network used by the target machine does not have DHCP enabled, and the target machine does not obtain an IP address.
3. The IP address of the target machine conflicts.
4. The target machine did not boot successfully.
5. The target machine took too long to power on and the wait timed out.

Troubleshooting methods

Go to the target platform to check the startup status of the target machine, and check against the three troubleshooting items in `Problem Analysis`.

solution

Modified the IP address of the management console

Refer to the knowledge base "Modify the IP address of the management console" to configure the IP address of the console correctly.

Target subnet does not have DHCP

- Use a subnet with DHCP enabled for migration.

or

- Refer to the kb "Using NexaVM API for migration when the target network does not have DHCP" to migrate by manually configuring IP.

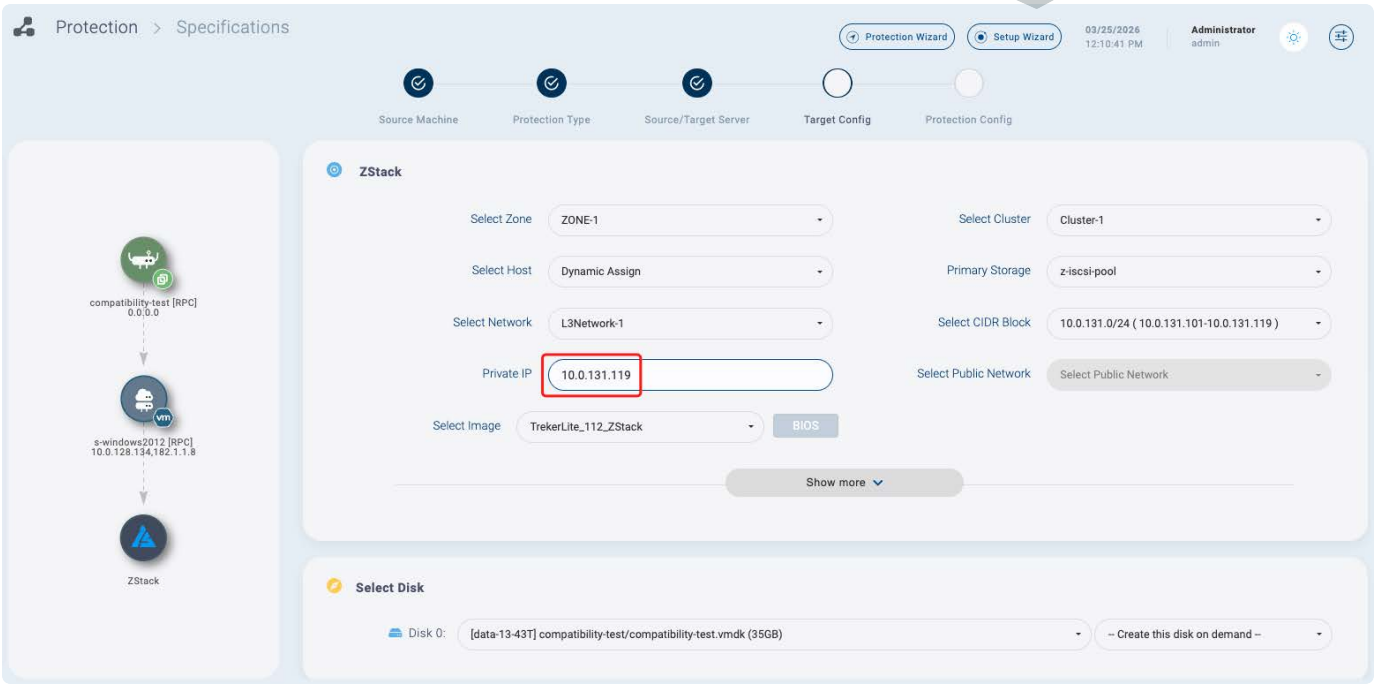
or

- Refer to the knowledge base "Management Console and Data Gateway Dual Network Card Architecture" to migrate using the temporarily created DHCP subnet.

IP address conflict

When creating a synchronization task, specify an unused IP address to create the task.

Specify the IP address in `LAN information`:



Did not boot successfully

Check the startup status of the target machine on the NexaVM platform. If it fails to boot successfully, you can manually boot it on the NexaVM platform to check whether an error is reported.

If an error is reported, proceed to the next step based on the error message.

Boot time is too long

The default wait time is 20 times. If the storage performance of NexaVM is poor, the boot time may be too long, resulting in timeout.

1. If it is a Windows BootImage, turning on virtio for the image will increase the startup speed and may solve this problem.
2. If the image has virtio enabled and problem still exists you can go to the NexaVM platform to observe the startup status of the target machine when creating a synchronization task and waiting for the target machine to start. If it is confirmed that the startup is too slow and causes a timeout, you can modify the waiting times to extend the waiting time.
    - Refer to the knowledge base "Modify the number of times the synchronization task waits for the target disk" for modification.

Standard mode synchronization task cannot create target machine (TrekerLite)

Document Category: Product Related Experience

network problems

Check whether the console can communicate with port 8080 of all NexaVM management nodes (including VIP).

API compatibility issues

Check whether the version of NexaVM is an API compatible version.

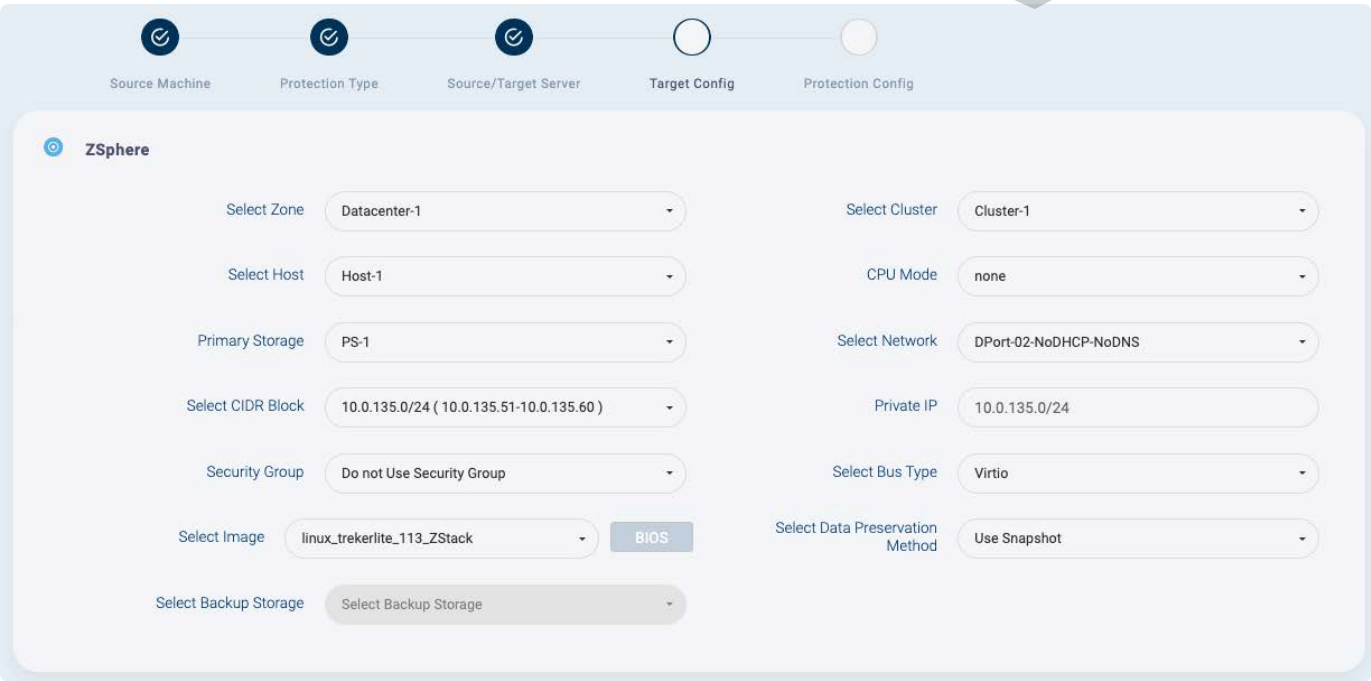
Insufficient NexaVM resources or abnormal resources

Manually create a cloud host according tothe computing specifications, storage, subnet, and IP address used when creating the synchronization task.

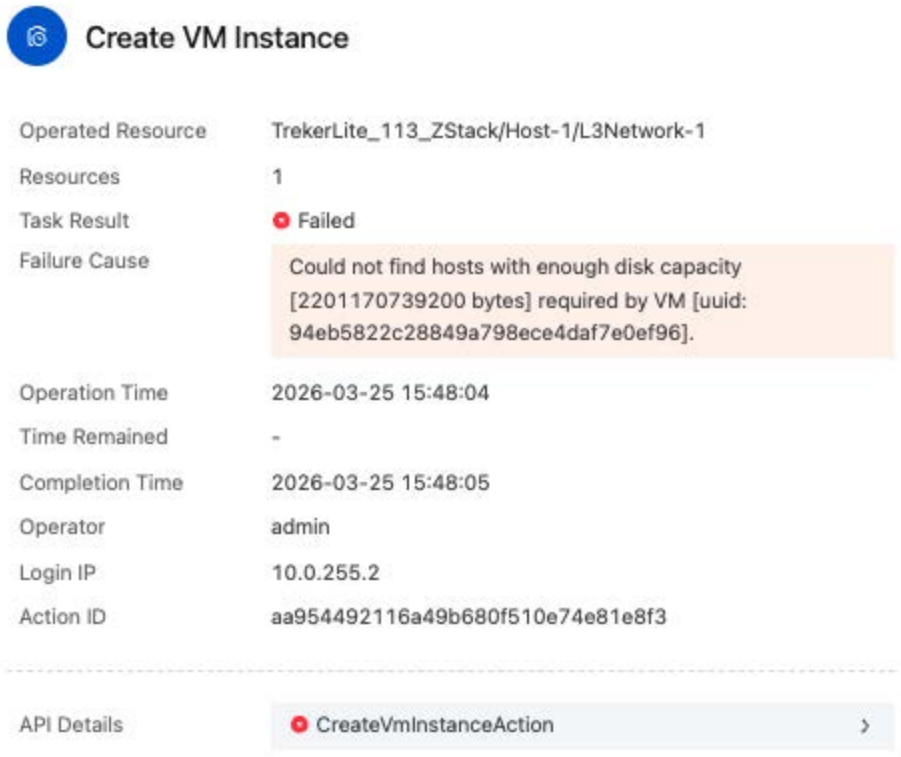
- If the creation is successful, the problems of insufficient resources and abnormal resources can be eliminated.
- If the creation fails, check which resource is insufficient based on the error message of the cloud platform.

Operation steps:

- Configuration of screenshot synchronization task

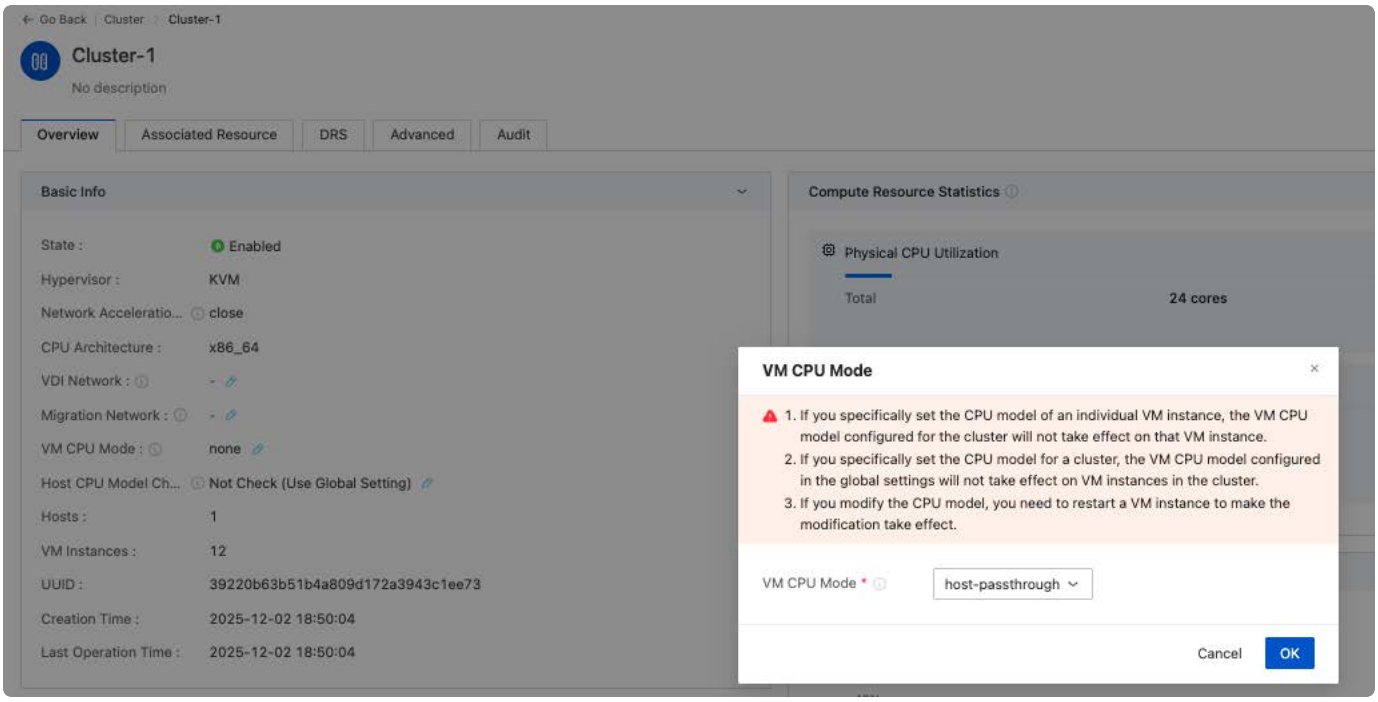


- Manually create a cloud host on NexaVM platform according to the above parameters and observe whether an error is reported.
  - Take storage error reporting as an example: You need to ask NexaVM's second line to troubleshoot the cause of the error, or change other storage to create a synchronization task.

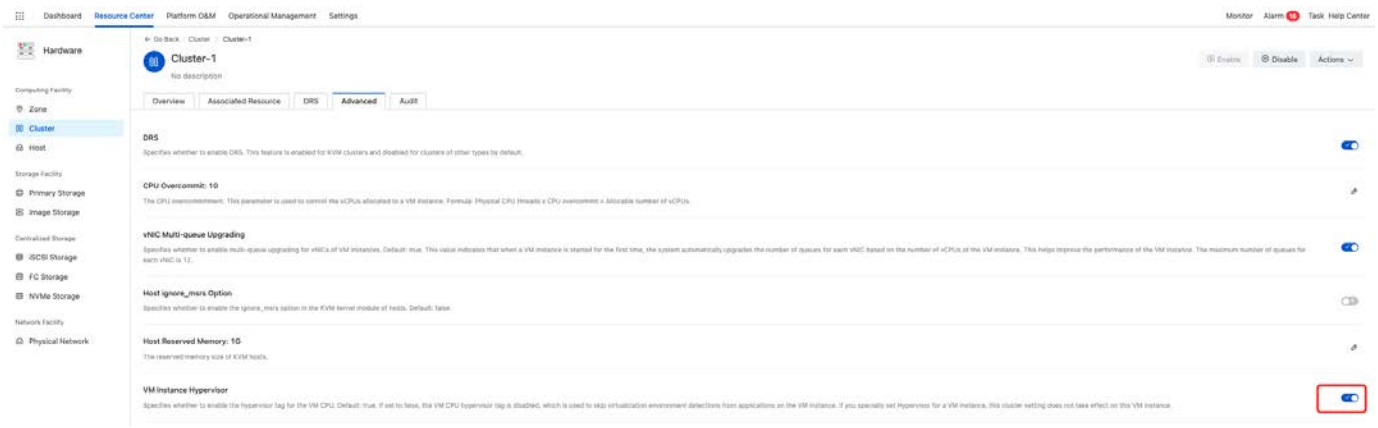


NexaVM setting problem

1. Find `cluster` in NexaVM platform –-> `Used cluster`
2. `Overview` : CPU mode changed to `host-passthrough` .



3. `Advanced Settings` : Turn off `VM Instance Hypervisor` .

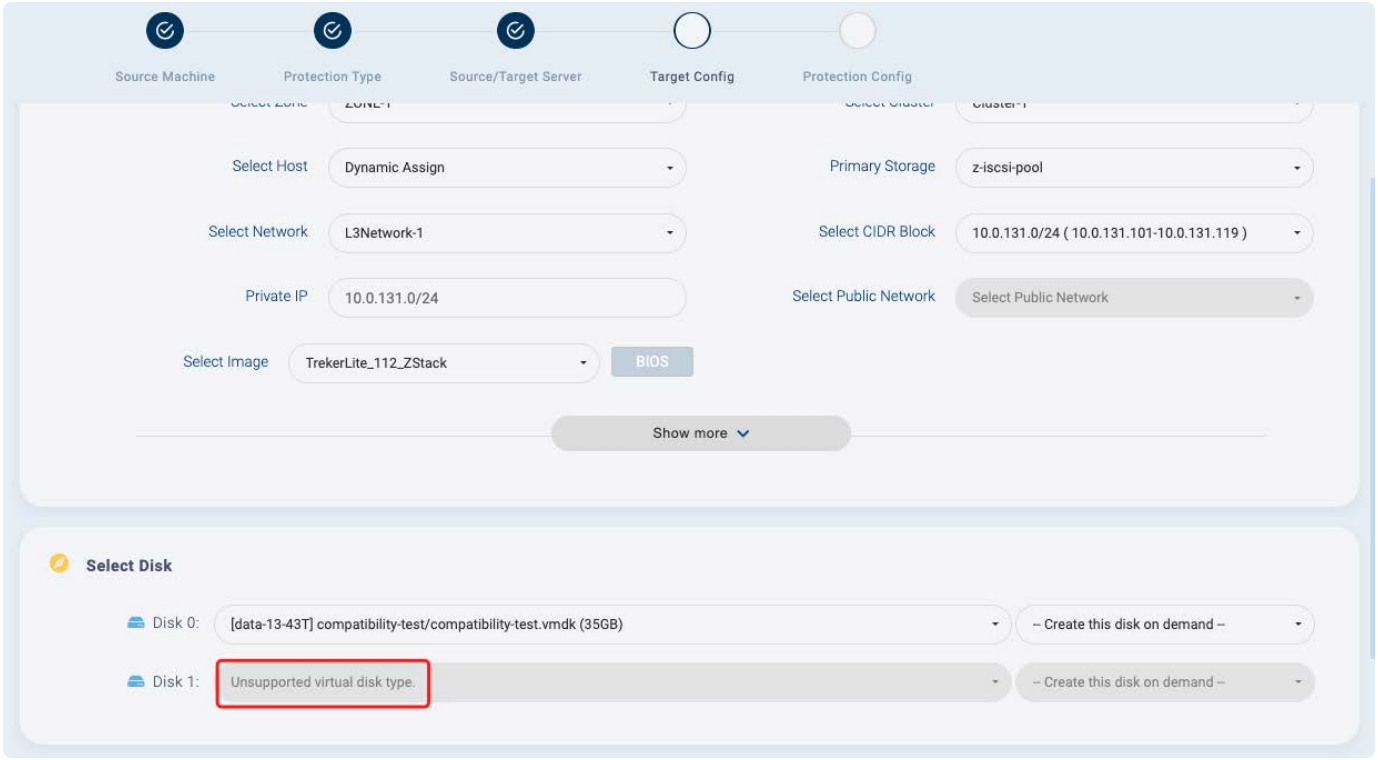


4. Just re-create the synchronization task.

Report "Unsupported virtual disk type" when selecting Disk

Document Category: Product Related Experience

Screenshot display



Reason

This disk is an independent disk, and VMware VADP does not support migrating independent disks.

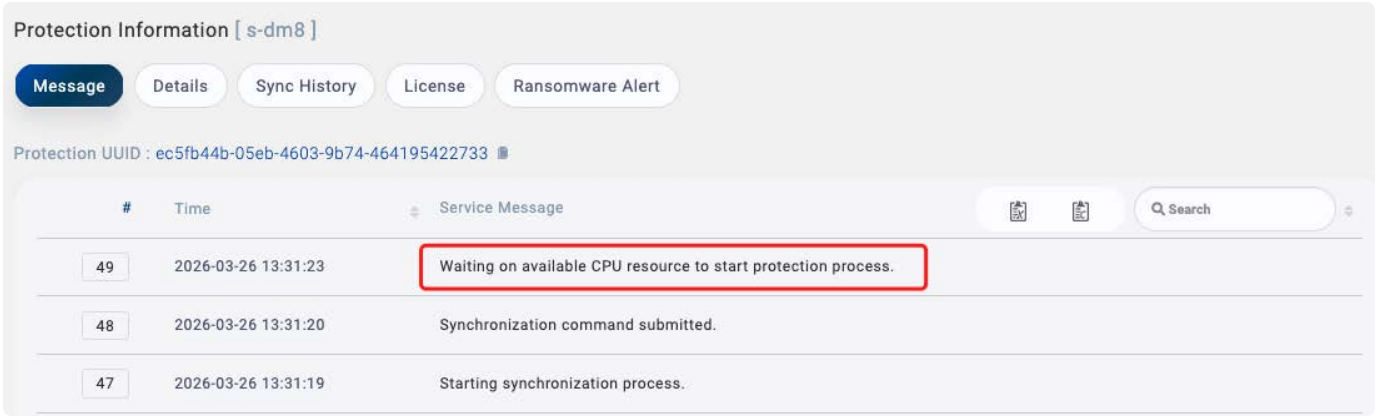
Solution

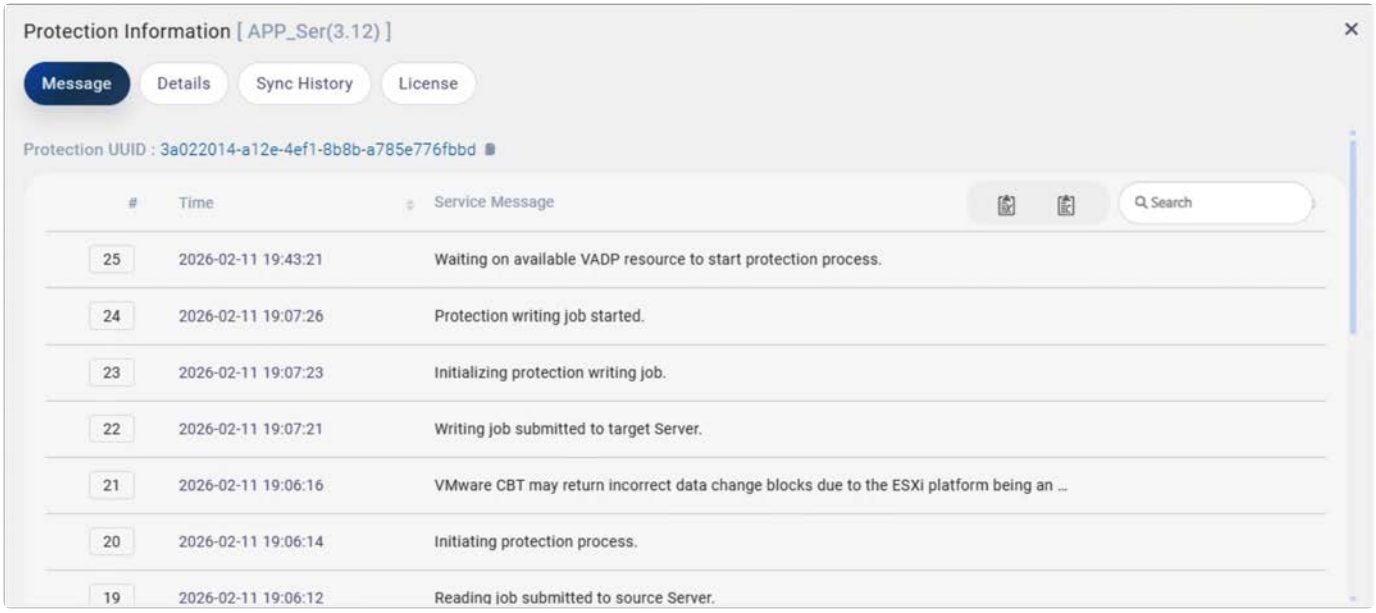
If you need to migrate independent disks, please install the agent and then migrate.

Waiting on available CPU resource to start process

Document Category: Product Related Experience

Error screenshot





Problem analysis

There are too many parallel synchronization tasks initiated, and the computing resources of the transit data gateway (Treker) are insufficient.

Solution 1

Plan task schedules and reduce parallel synchronization tasks;

Or the waiting task will be automatically executed after the previous task is completed.

Solution 2

Expanding the computing specifications of the transit data gateway (Treker).

Specification recommendations

> Note: When computing resources are tight, computing resources can be more compact.

1. It is recommended to reserve for Win/Linux system: 4c4g
2. A synchronization task is reserved at least: 1c256m.

Calculate the specifications required for parallel tasks

The transit data gateway (Treker) requires parallel10 synchronization tasks:

- CPU: 4+1*10=14C
- Memory: 4+256/1024*10=6.5G
- 4c4g in the calculation formula is reserved for system operation.

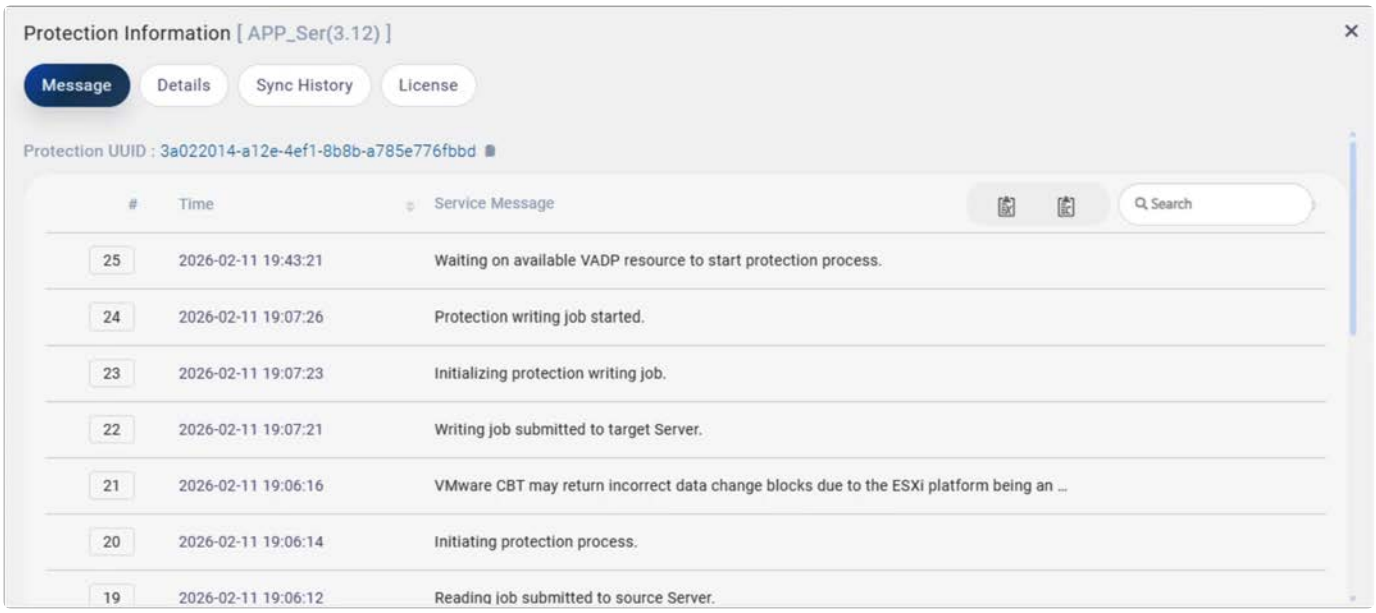
In summary, the calculation specification of the transit data gateway (Treker) is: 14C6.5G, so it is generally set to 16C8G.

Waiting on available VADP resource to start protection process

Document Category: Product Related Experience

Error Screenshot

Waiting on available VADP resource to start protection process.



Problem Analysis

VMware agentless backup defaults to a limit of 1 data gateway per ESXi host, allowing only 1 concurrent task.

Solution 1

Wait for the preceding tasks to complete.

Solution 2

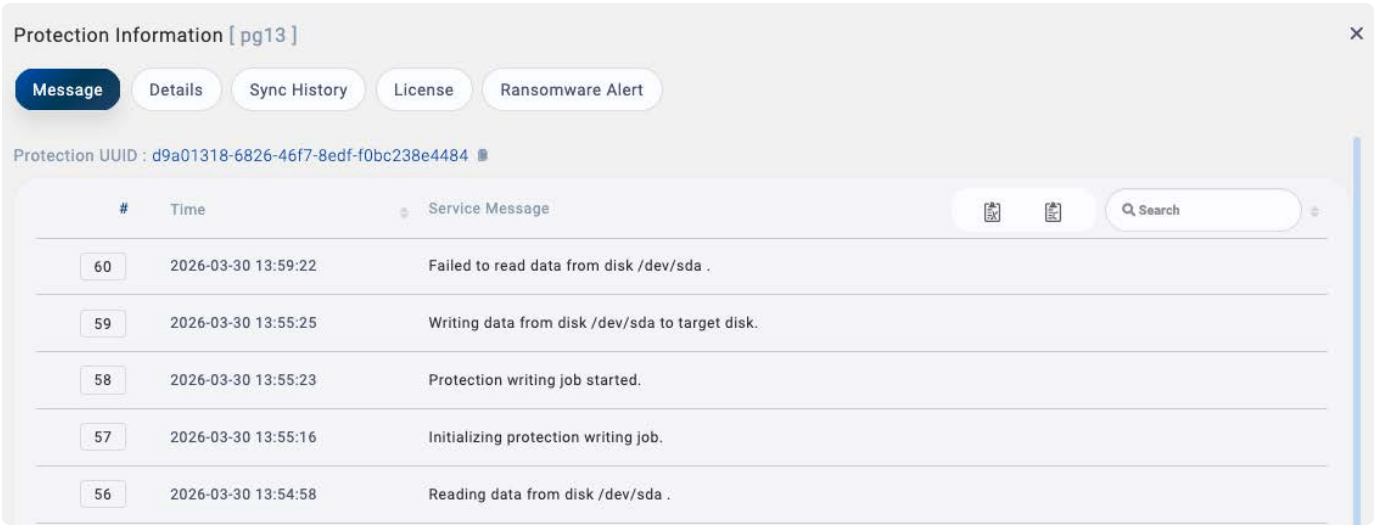
Modify the concurrency limit. Please refer to the knowledge base article "Modifying VMware Agentless Concurrency Limit".

Replication snapshot discarded or disk information cannot be read

Document Category: Product Related Experience

Error screenshot





Windows

Source host disk error

The system log of the source host may not contain relevant information. You need to run the chkdsk command to check.

NEXAVM

```
#Check C drive for bad sectors
c:
chkdsk

#Check D drive for bad sectors
d:
chkdsk

#Check E drive for bad sectors
e:
chkdsk

#And so on
```

**After an error is detected, there are two solutions. **

1. Fix the errors before migrating.

or

2. To modify software parameters to skip errors, refer to the operating experience knowledge base "Ignore Disk Errors During Migration".

Insufficient virtual memory

Check the system log of the source host. Near the time when the snapshot is discarded, an insufficient virtual memory error will be reported.

Solution

Increase the virtual memory of the source host before initiating synchronization.

Linux

Memory usage exceeds 95%

Check the message log. Near the discarded snapshot, there will be an error message physical memory usage has exceeded 95% threshold..

NEXAVM

```
Mar 24 20:43:29 centos7 kernel: ltbd: system total memory : 15974 (MB)
Mar 24 20:43:29 centos7 kernel: ltbd: physical memory usage has exceeded 95% threshold. cow file update is stopped
Mar 24 20:43:34 centos7 kernel: ltbd: system available memory : 795 (MB)
Mar 24 20:43:34 centos7 kernel: ltbd: system total memory : 15974 (MB)
Mar 24 20:43:34 centos7 kernel: ltbd: physical memory usage has exceeded 95% threshold. cow file update is stopped
Mar 24 20:43:37 centos7 kernel: XFS (lt0): Mounting V5 filesystem in no-recovery mode. Filesystem will be inconsistent.
Mar 24 20:43:37 centos7 kernel: XFS (lt0): Unmounting Filesystem
Mar 24 20:43:37 centos7 kernel: XFS (lt1): Mounting V5 filesystem in no-recovery mode. Filesystem will be inconsistent.
```

Solution

1. Refer to the knowledge base "Turn on drop cache in Linux to alleviate the problem of 95% memory usage" for processing.

or

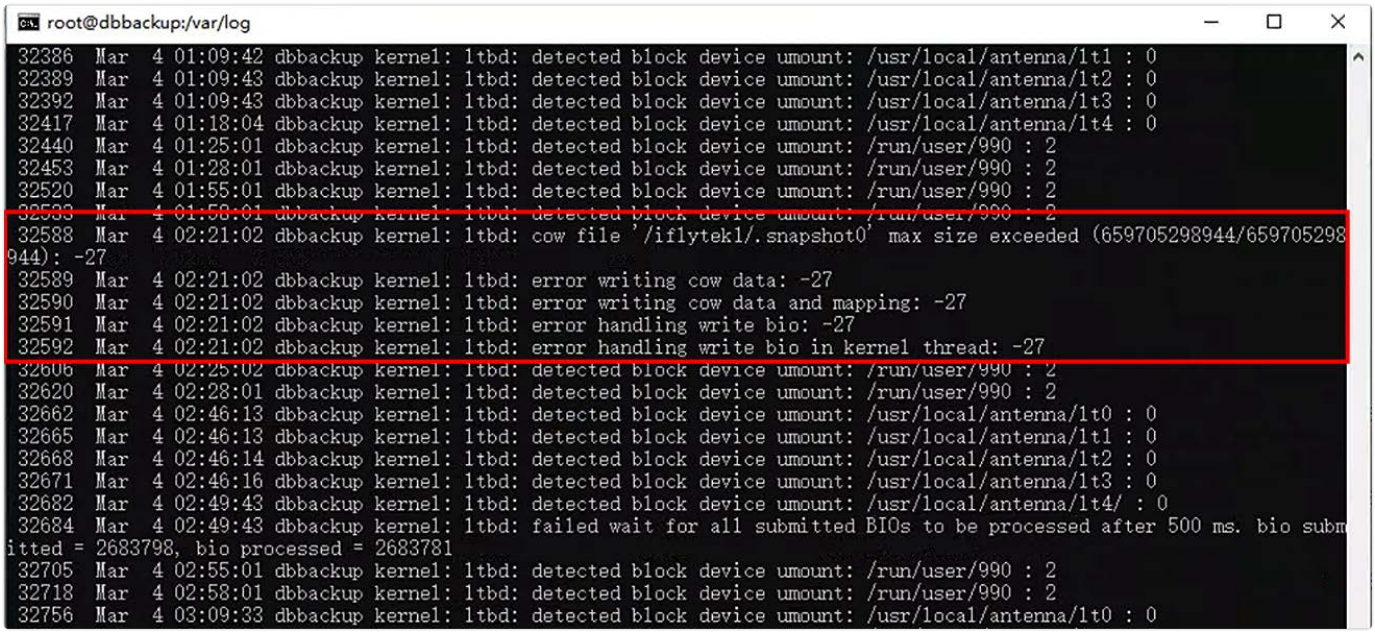
2. Expand the memory of the source host, or initiate synchronization when the business is not busy.

or

3. Or turn off memory detection. Turning off memory detection may cause the source host's memory to occupy 100%, causing downtime.

The amount of data changes is so large that it fills up the snapshot space.

Check the message log. Near the discarded snapshot, there will be an error of max size exceeded (value/value):-27.



Solution

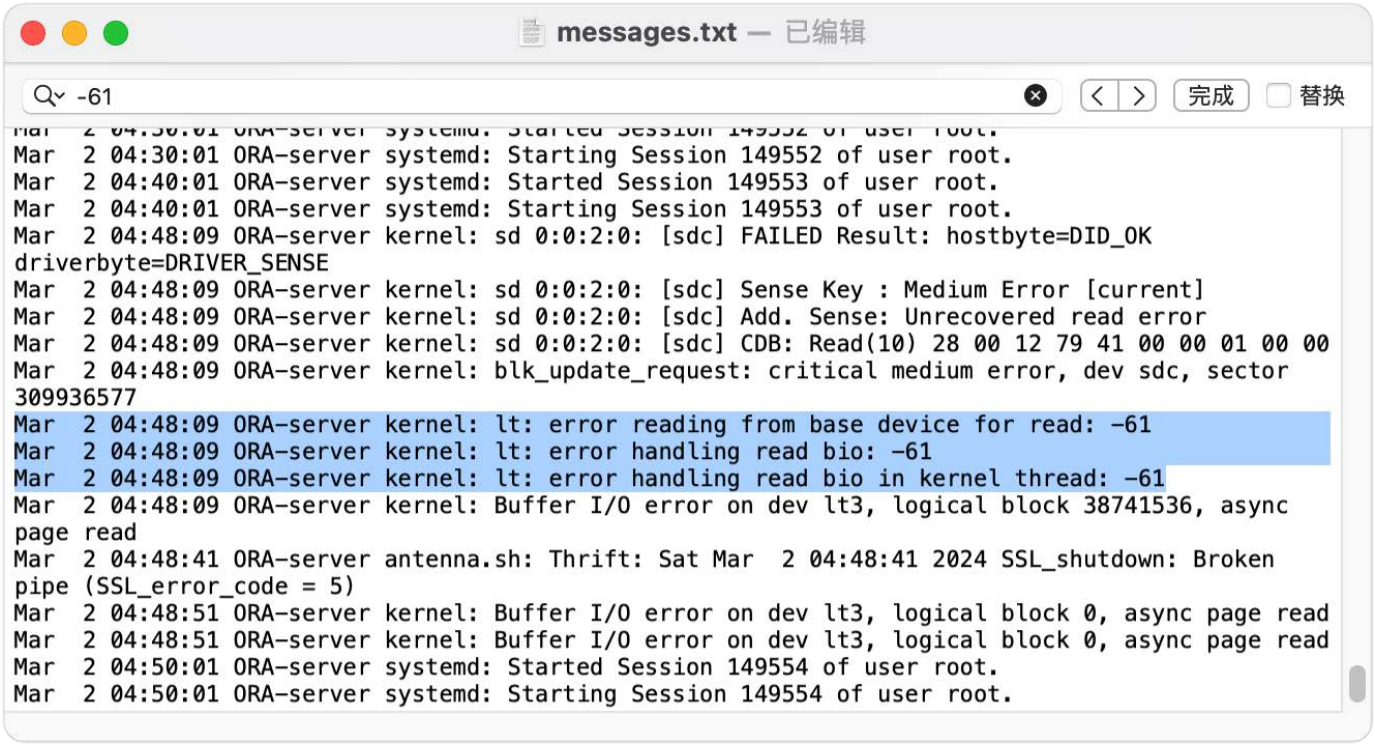
NEXAVM

1. Check the time from the initiation of the synchronization task to the discarding of the snapshot, and evaluate the amount of data changes.
    - If you don't know how to evaluate the amount of change, you can follow step 3 first.
2. Estimate the time it takes to complete a copy based on the copy speed and progress.
3. Refer to the knowledge base "Linux Modification Snapshot Ratio" for processing.

The source host file system has bad blocks (Superblock error)

Check the message log. There will be an error of -61 near the discarded snapshot.

```
Mar  2 04:48:09 ORA-server kernel: lt: error reading from base device for read: -61
Mar  2 04:48:09 ORA-server kernel: lt: error handling read bio: -61
Mar  2 04:48:09 ORA-server kernel: lt: error handling read bio in kernel thread: -61
```



There are two solutions

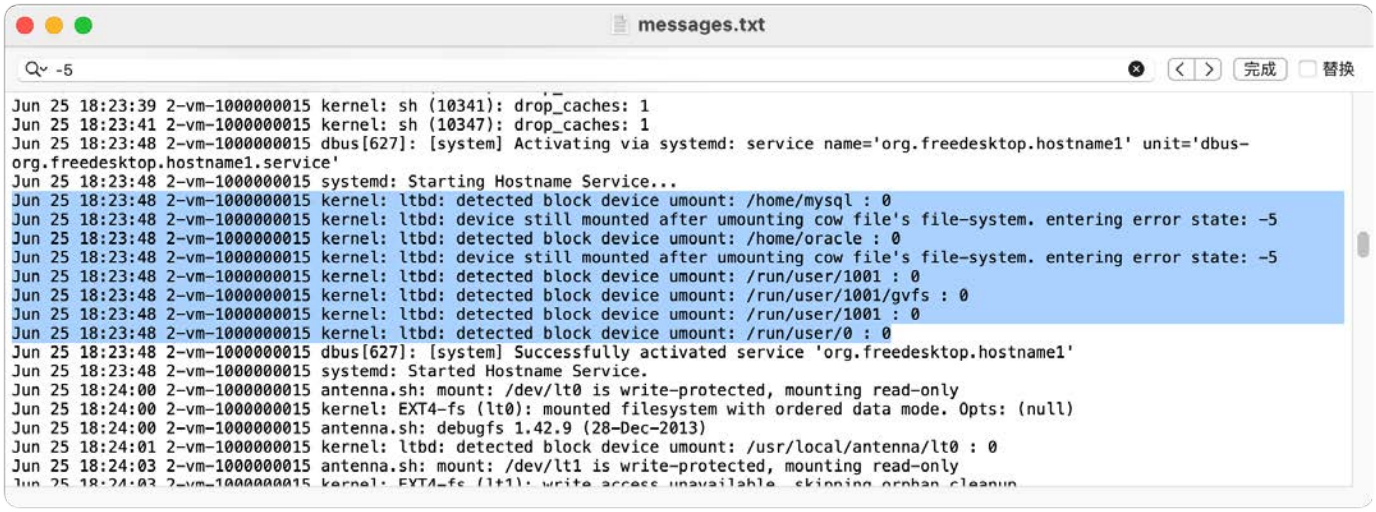
1. Repair bad sectors (Superblock error) before migrating.
2. Modify software parameters to skip bad blocks (Superblock error), refer to the knowledge base "Ignore disk errors during migration"

NEXAVM

Some settings of the file system conflict with the driver

Check the message log. Near the discarded snapshot, there will be an error message umounting cow file's file-system. -5.

```
Jun 25 18:23:48 2-vm-1000000015 kernel: ltbd: detected block device umount: /home/mysql : 0
Jun 25 18:23:48 2-vm-1000000015 kernel: ltbd: device still mounted after umounting cow file's file-system. entering error state: -5
Jun 25 18:23:48 2-vm-1000000015 kernel: ltbd: detected block device umount: /home/oracle : 0
Jun 25 18:23:48 2-vm-1000000015 kernel: ltbd: device still mounted after umounting cow file's file-system. entering error state: -5
Jun 25 18:23:48 2-vm-1000000015 kernel: ltbd: detected block device umount: /run/user/1001 : 0
Jun 25 18:23:48 2-vm-1000000015 kernel: ltbd: detected block device umount: /run/user/1001/gvfs : 0
Jun 25 18:23:48 2-vm-1000000015 kernel: ltbd: detected block device umount: /run/user/1001 : 0
Jun 25 18:23:48 2-vm-1000000015 kernel: ltbd: detected block device umount: /run/user/0 : 0
```



Solution

NEXAVM

```
#Stop the protection task manually

#erase snapshots:
/usr/local/antenna/antenna --erase

#stop antenna:
systemctl stop antenna

#: Write a parameter
echo "options ltbd may_hook_syscalls=0" > /etc/modprobe.d/ltbd.conf

#reload ltbd:
rmmod ltbd
modprobe ltbd

#start antenna
systemctl start antenna

#start the protection again
```

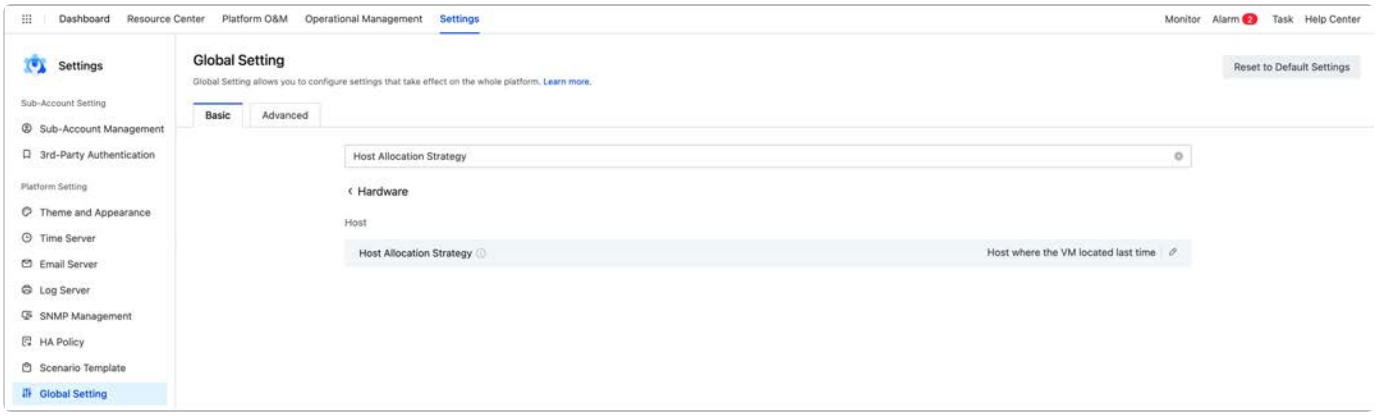
The Protection task specifies a physical machine, but it is still created on another physical machine

Problem Description

When creating a synchronization task, a specific physical machine was designated, but the synchronization task's target machine was still created on a different physical machine.

Solution: Modify Physical Machine Allocation Policy

1. Change the Host Allocation Strategy to "Host where the VM located last time".



2. Recreate the synchronization task.

Linux system conversion failed

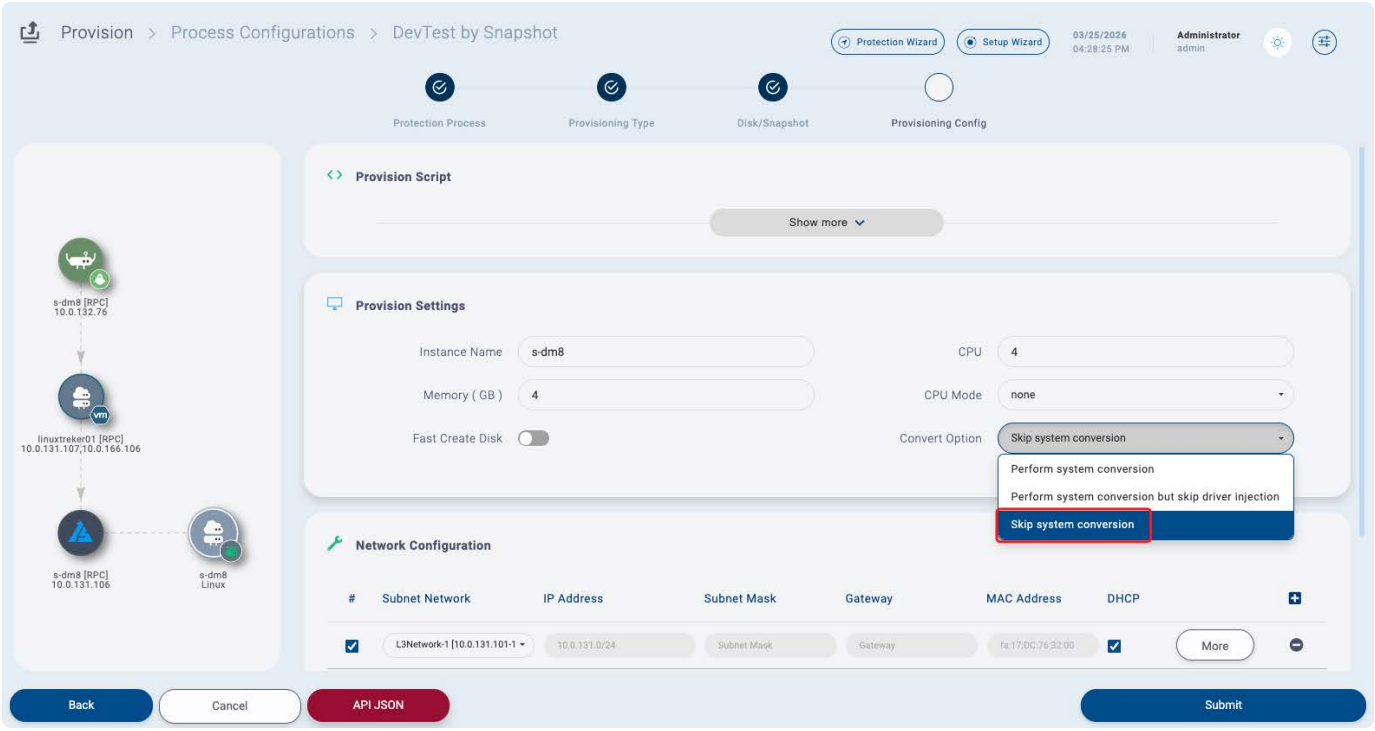
Document Category: Product Related Experience

Cannot find target system info

The source host system is not compatible, or the source host is an OEM release system.

Select "Skip system conversion" when creating the provisioning task, wait for the provisioning task to be completed, stop the target machine, close virtio and then restart it.

- If you need to enable virtio, install the NexaVM performance optimization tool while the computer is powered on, shut down the target machine, enable virtio and then power it on again.



Source VMware's CBT bug causes data block confusion

Refer to the knowledge base "VMware Agentless CBT Related Topics" and use the knowledge base's "Stable Priority Synchronization Task Settings" strategy to rebuild the synchronization task.

There is insufficient disk space in the root directory of the source machine.

- Mainly occurs in VMware and NexaVM agentless mode migration

```
root@trekerlite01:/usr/local/treker# df -hT
Filesystem                    Type      Size  Used Avail Use% Mounted on
udev                          devtmpfs  984M     0  984M   0% /dev
tmpfs                         tmpfs     200M  732K  199M   1% /run
/dev/vda2                     ext4      4.7G  3.3G  1.4G  71% /
tmpfs                         tmpfs     997M     0  997M   0% /dev/shm
tmpfs                         tmpfs     5.0M     0  5.0M   0% /run/lock
tmpfs                         tmpfs     997M     0  997M   0% /sys/fs/cgroup
/dev/vda3                     vfat      105M  9.0M   96M   9% /boot/efi
tmpfs                         tmpfs     200M     0  200M   0% /run/user/0
/dev/mapper/VolGroup-lv_root ext4       45G   45G     0 100% /mnt/m
/dev/mapper/tlbd1             ext4      477M   40M  408M   9% /mnt/m/boot
root@trekerlite01:/usr/local/treker# _
```

Log in to the source host system and check the space usage of each partition.

Fatal glibc error: CPU does not support x86-64-v2

```
fi
r=$(lsinitrd /boot/initramfs-6.6.0-72.0.0.76.oe2403sp1.x86_64.img | egrep -i 'virtio_blk.ko|virtio_scsi.ko|virtio_net.ko' -o | sort -u |
wc -l)
a=$(lsinitrd /boot/initramfs-6.6.0-72.0.0.76.oe2403sp1.x86_64.img | egrep -i 'Arguments: ' -o | sort -u | wc -l)
if [ $r -ge 3 ] || [ $a -eq 0 ]; then
echo 'converted.' >> linux2v/injection.log
else
echo  "r: $r a: $a" >> linux2v/injection.log
fi
fi

umount /sys
umount /dev/pts
umount /dev
umount /run
umount /proc


2025-Jun-13 05:37:57.918077 (T7f8410013740) |D|console(9) - chmod +x /mnt/m/linux2v/chroot_dracut.sh
2025-Jun-13 05:37:57.922645 (T7f8410013740) |D|console(27) - chmod +x /mnt/m/linux2v/chroot_dracut.sh :
2025-Jun-13 05:37:57.922722 (T7f8410013740) |D|console(9) - chroot "/mnt/m" /bin/sh linux2v/chroot_dracut.sh 2>&1
2025-Jun-13 05:37:57.963211 (T7f8410013740) |D|console(27) - chroot "/mnt/m" /bin/sh linux2v/chroot_dracut.sh 2>&1 : Fatal glibc error:
CPU does not support x86-64-v2

2025-Jun-13 05:37:57.964369 (T7f8410013740) |D|console(9) - umount '/mnt/m/boot/efi'
2025-Jun-13 05:37:57.982676 (T7f8410013740) |D|console(27) - umount '/mnt/m/boot/efi' :
2025-Jun-13 05:37:57.982749 (T7f8410013740) |D|console(9) - umount '/mnt/m/boot'
2025-Jun-13 05:37:57.999340 (T7f8410013740) |D|console(27) - umount '/mnt/m/boot' :
2025-Jun-13 05:37:57.999412 (T7f8410013740) |D|console(9) - umount '/mnt/m/'
2025-Jun-13 05:37:58.109702 (T7f8410013740) |D|console(27) - umount '/mnt/m/' :
2025-Jun-13 05:37:58.110240 (T7f8410013740) |D|console(9) - dmsetup remove_all
2025-Jun-13 05:37:58.202370 (T7f8410013740) |D|console(27) - dmsetup remove_all :
```

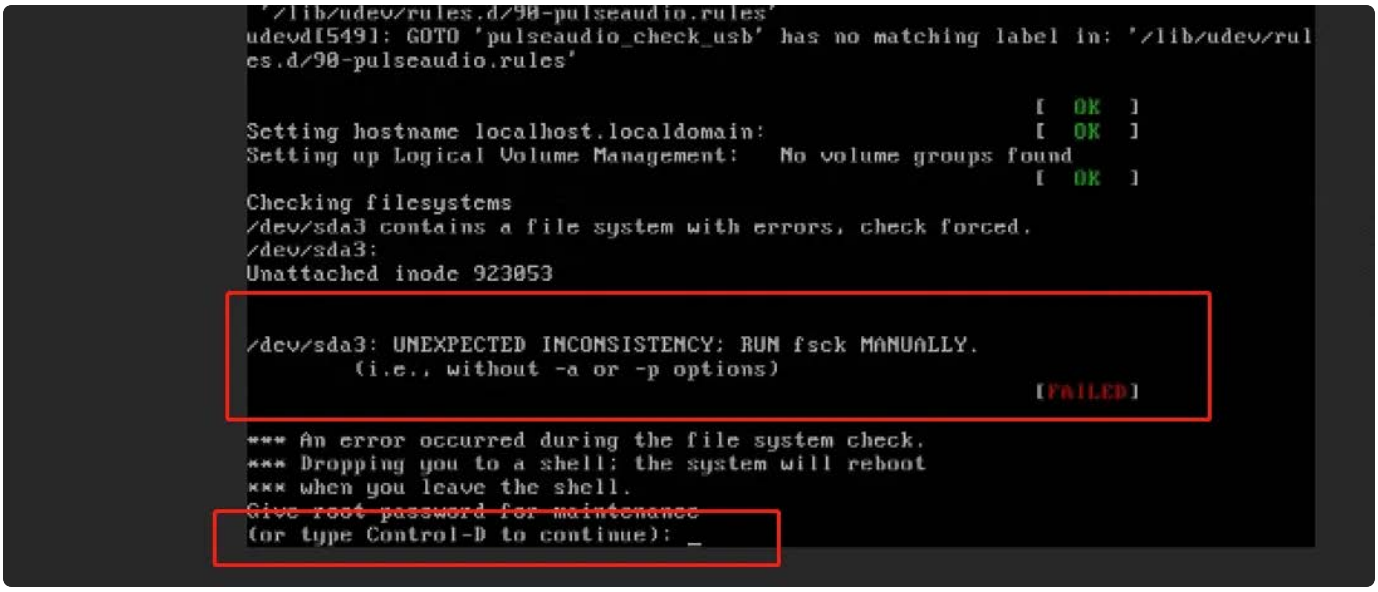
The kernel version of the source host is too high, and the target machine needs to change the CPU mode to **pass-through**.

Linux enters maintenance mode after migration

Document Category: Third Party Related Experience

Scenario 1. Disk needs repair

Error screenshot



Reason for error

There is a problem with the file system of the user's source machine, and fsck needs to be done.

solution

> The operation steps of different Linux distributions may be different, and the repair instructions of different file systems may also be different. This knowledge base only provides a solution for this scenario.

1. Enter the root password in maintenance mode and log in to the system.
2. Use lsblk to confirm which partition /dev/sda3 is.
    - The error-reporting partition in the screenshot is sda3, which should be replaced with

NEXAVM

the actual error-reporting partition during operation.

3. Execute fsck on the error-reported partition.
    - Remember to replace it with the actual error partition! ! !

```
#repair ext3 or ext4 filesystem
fsck -y /dev/sda3
```

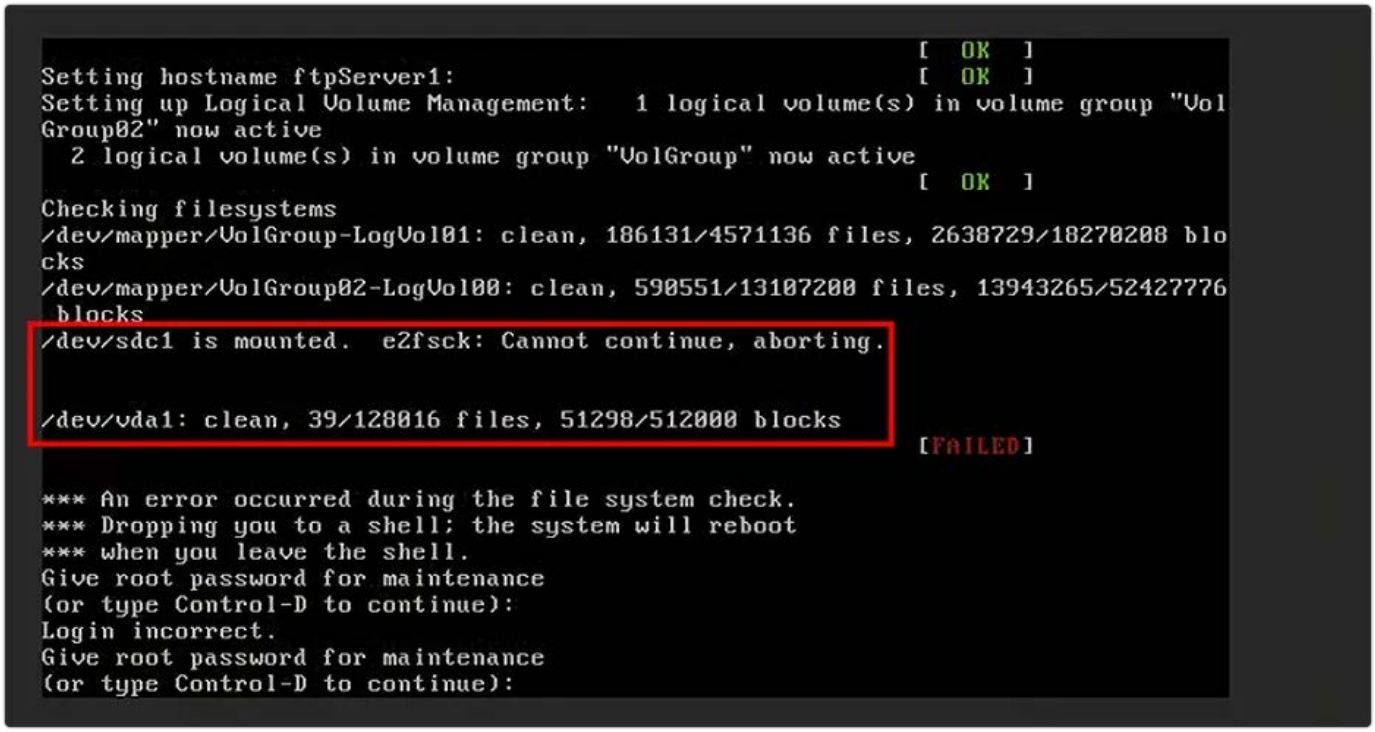
```
#repair xfs filesystem
xfs_repair /dev/sda3
```

4. Just restart after the repair is complete.

```
reboot
```

Case 2. fstab is configured to enable dump and fsck, and UUID is not used.

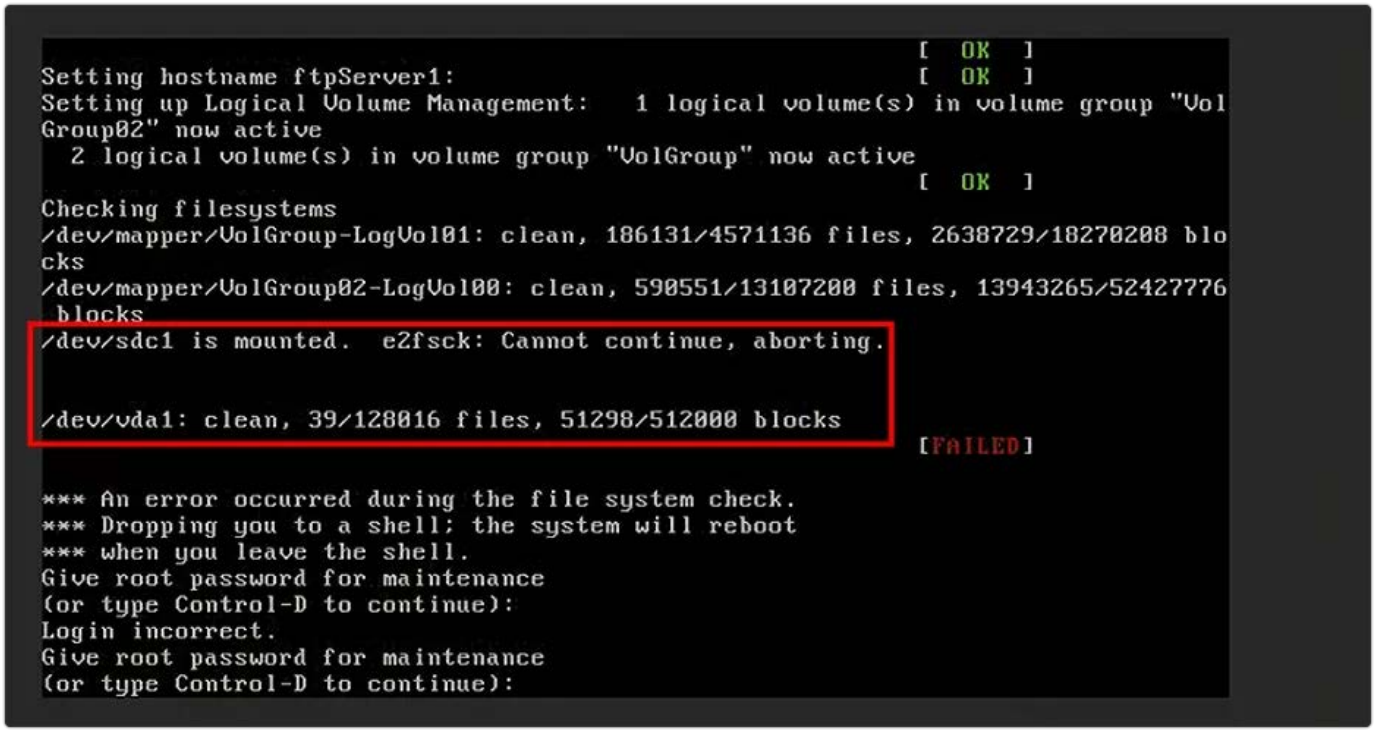
Error screenshot



NEXAVM



There may not be circled information, just a reminder



NEXAVM

Reason for error

The fstab of the user's source machine has dump and fsck enabled. It will fsck the disk every time it is powered on. If fsck does not complete successfully, it will enter maintenance mode.

The disk in the fstab of the user's source machine uses a block device name, such as sda, vda. This name may become vda, sda, xvda, etc. on the target platform. If the system fails to mount according to the block device name in the fstab, it will enter maintenance mode.

solution

> The steps may differ between releases. This knowledge base only provides a solution for this scenario.

1. Enter the root password in maintenance mode and log in to the system.
2. Mount the root directory read-write.

```
mount -o remount,rw /
```

```
root js-file:~ #
root js-file:~ # mount -o remount,rw /
root js-file:~ # _
```

3. View the fstab file.

```
cat /etc/fstab
```

```
root js-file:~ # cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Thu Jan 29 15:20:58 2015
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/VolGroup-lv_root /                       ext4    defaults        1 1
UUID=4f5d52a2-9b4e-44aa-ad12-991ff14c4ede /boot                   ext4    defaul
ts        1 2
/dev/mapper/VolGroup-lv_home /home                   ext4    defaults        1 2
/dev/mapper/VolGroup-lv_swap swap                    swap    defaults        0 0
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
/dev/mapper/vg_store-lv_datum /datum            ext4     defaults        1 2
/dev/sdc1               /YDZB                        ext3    defaults        1 1
```

4. Back up /etc/fstab. The backup file name can be customized. It is recommended to use date

as the suffix for easy identification.

```
1   cp /etc/fstab /etc/fstab.0222
```

```
root js-file:~ # cp /etc/fstab /etc/fstab.0222
root js-file:~ # _
```

5. Set the dump and fsck options in fstab to 0.

```
1   vi /etc/fstab
```

Reference example:

/dev/hda2	/	ext2	default	1	1
/dev/hdb1	/home	ext2	defaults	1	2
/dev/cdrom	/media/cdrom	auto	ro,noauto,user,exec	0	0
/dev/fd0	/media/floppy	auto	rw,noauto,user,sync	0	0
proc	/proc	proc	defaults	0	0
/dev/hda1	swap	swap	pri=42	0	0

Modified output:

```
root js-file:~ # cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Thu Jan 29 15:20:58 2015
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/VolGroup-lv_root /                       ext4    defaults        0 0
UUID=4f5d52a2-9b4e-44aa-ad12-991ff14c4ede /boot                   ext4    defaul
ts        0 0
/dev/mapper/VolGroup-lv_home /home                   ext4    defaults        0 0
/dev/mapper/VolGroup-lv_swap swap                    swap    defaults        0 0
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
/dev/mapper/vg_store-lv_datum /datum            ext4     defaults        0 0
/dev/sdc1               /YDZB                        ext3    defaults        0 0
```

6. If the source is sdx and the target is vdx, the corresponding sdx needs to be changed to vdx.

Before modification:

NEXAVM

```
root js-file:~ # cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Thu Jan 29 15:20:58 2015
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/VolGroup-lv_root /                       ext4    defaults        0 0
UUID=4f5d52a2-9b4e-44aa-ad12-991ff14c4ede /boot                   ext4    defaul
ts        0 0
/dev/mapper/VolGroup-lv_home /home                   ext4    defaults        0 0
/dev/mapper/VolGroup-lv_swap swap                    swap    defaults        0 0
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
/dev/mapper/vg_store-lv_datum /datum            ext4     defaults        0 0
/dev/sdc1               /YDZB                        ext3    defaults        0 0
```

After modification:

```
root js-file:~ # cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Thu Jan 29 15:20:58 2015
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/VolGroup-lv_root /                       ext4    defaults        0 0
UUID=4f5d52a2-9b4e-44aa-ad12-991ff14c4ede /boot                   ext4    defaul
ts        0 0
/dev/mapper/VolGroup-lv_home /home                   ext4    defaults        0 0
/dev/mapper/VolGroup-lv_swap swap                    swap    defaults        0 0
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
/dev/mapper/vg_store-lv_datum /datum            ext4     defaults        0 0
/dev/vdc1               /YDZB                        ext3    defaults        0 0
```

7. Reboot the server

```
1   reboot
```

Disk offline after Windows migration

Disk offline after Windows migration

Document Category: Third Party Related Experience

Applicable scenarios

1. One or more disks are offline after Windows migration.
2. After manually putting the disk online, the drive letter is different from the source machine.

Problem analysis

Disk offline: Windows' disk policy is **OfflineShared (make shared disks offline). **

The drive letter changes after going online: After migration, the CD drive of the cloud host occupies the original drive letter, causing the drive letter to be extended backwards.

solution

1. Manually open Windows Disk Management and bring the offline disk online.
2. Assign drive letters as needed.
    - If the drive letter used by the source machine is already occupied by the CD drive, you can first change the drive letter of the CD drive to another drive letter.

Optimize disk strategy

Open cmd window in Windows after migration

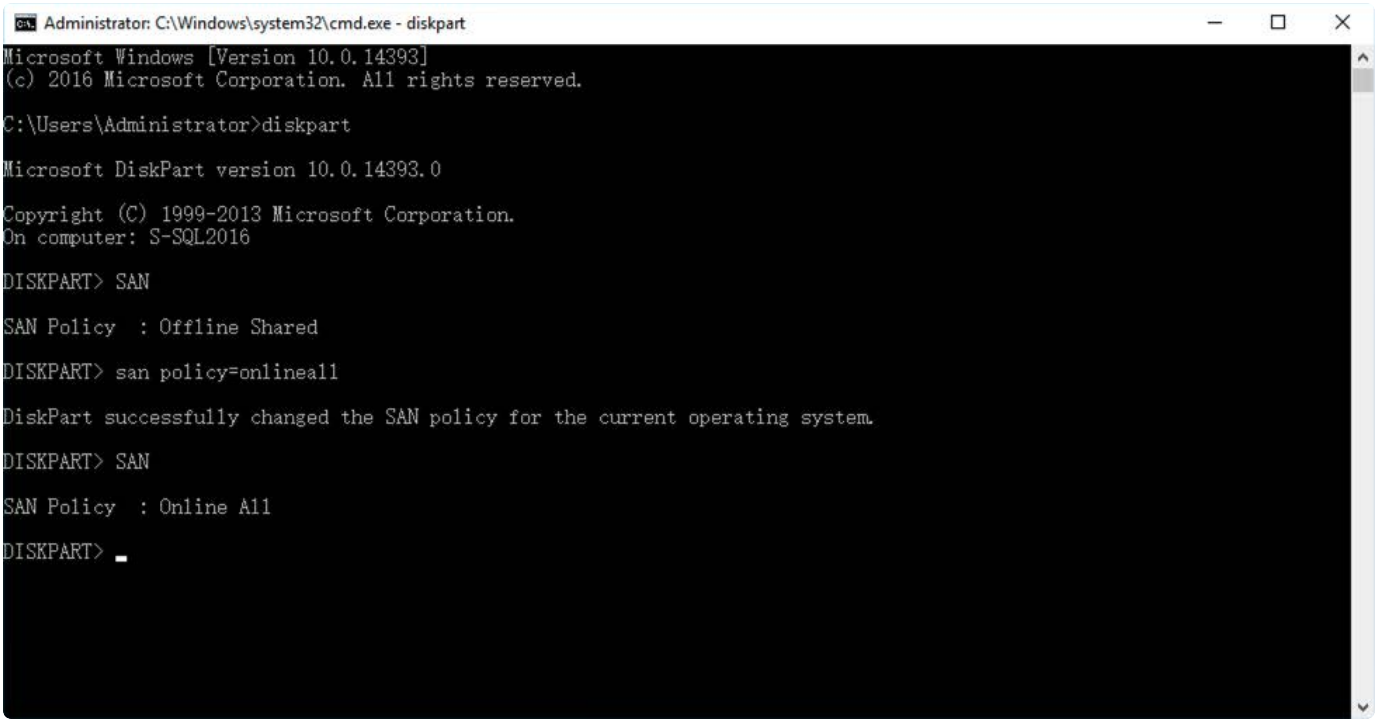
NEXAVM

```
#open diskpart
diskpart

#check disk policy
SAN

#set disk online
san policy=onlineall

#check disk policy again
SAN
```



Attachment: Windows Disk Policy

Reference link：Storage area network (san) policy for Windows operating systems

Windows operating system SAN policies are divided into three types:

1. **OnlineAll**: Indicates that all newly discovered disks are placed in online mode.
2. **OfflineShared (make shared disks offline)**: Indicates that all newly discovered disks on the shared bus (such as FC, ISCSI) are placed in offline mode, and disks on non-shared buses are placed in online mode.
3. **OfflineAll (all offline)**: Indicates that all disks except the system disk are placed in offline mode.

After deleting the provision task, provision cannot be selected again.

Document Category: Product Related Experience

Operation scenario

After deleting the provision task (select the option on the left), no increment is made, and if you create a provision task in the 'Provisioning by Disk' mode again, the current task will not be selected.

Cause of problem

1. After deleting the `Provisioning by Disk` task, the synchronization status of the provision task will be automatically restored.
2. In order to ensure data consistency of provision tasks:
    - When the configuration state is in 'simple mode', it is prohibited to directly create an 'Provisioning by Disk' task. An increment is required before the 'Provisioning by Disk' task can be created.
    - When the configuration state is in 'debug mode', you can directly create an 'Provisioning by Disk' task.

Operation steps

Solution 1. Simple mode: start 'Provisioning by Disk' after increment

1. Initiate an increment on the provision task.
2. Wait for the increment to complete and initiate an 'Provisioning by Disk' task.

NEXAVM

Solution 2. Troubleshooting mode: start 'Provisioning by Disk' again

1. Click the `Settings` icon in the upper right corner and change the configuration status to `Debug`.
2. Create an 'Provisioning by Disk' task in the provision task.

DevTest by snapshot mode, failed to create target machine

Document Category: Product Related Experience

Insufficient NexaVM resources

Manually create a cloud host based on the computing specifications, subnet, and IP address used in the replica disk test.

- If the creation is successful, the problem of insufficient resources can be eliminated.
- If the creation fails, check which resource is insufficient based on the error message of the cloud platform.

The network is blocked

- The subnet selected during provisioning does not have DHCP enabled.
- The wrong security group was selected when provisioning.
- The IP address set during provisioning conflicts.

resource conflict

- The MAC address set during provisioning conflicts, causing the source host to fail to be created.

Storage performance is low and creation is slow

In the information of provisioning tasks: the information of the created instance is always updated.

- Just wait, some storage performance is poor, you may wait 60–120 minutes, or even longer.

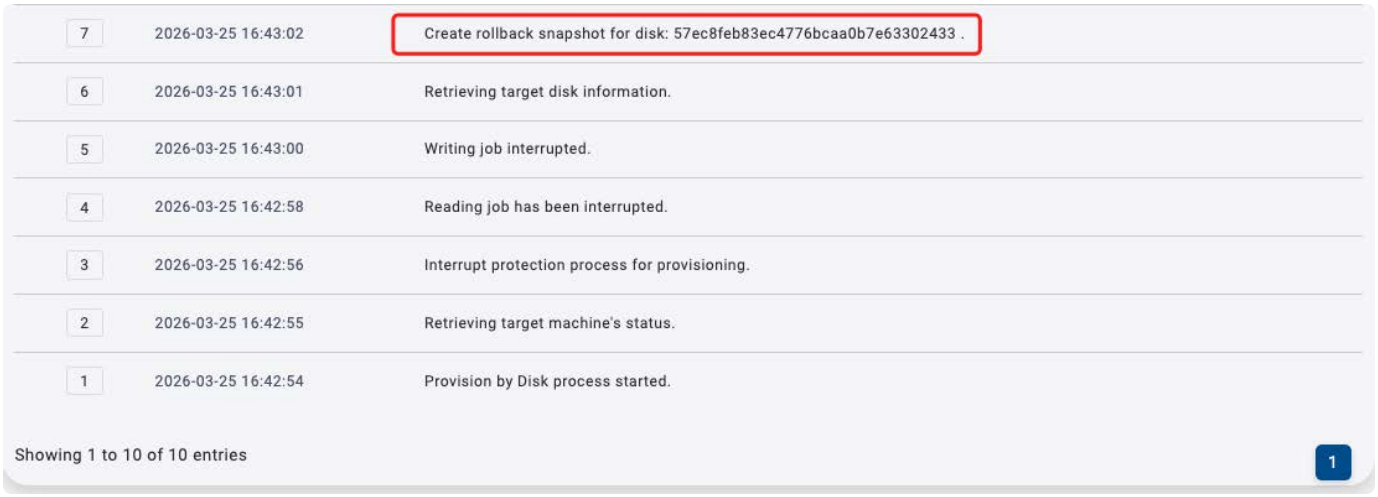
API compatibility

Collect the diagnostic logs and error messages of the management console (expansion and screenshots must include time) and send them to support.

Stuck on creating rollback snapshot

Document Category: Product Related Experience

Error screenshot



7	2026-03-25 16:43:02	Create rollback snapshot for disk: 57ec8feb83ec4776bcaa0b7e63302433 .
6	2026-03-25 16:43:01	Retrieving target disk information.
5	2026-03-25 16:43:00	Writing job interrupted.
4	2026-03-25 16:42:58	Reading job has been interrupted.
3	2026-03-25 16:42:56	Interrupt protection process for provisioning.
2	2026-03-25 16:42:55	Retrieving target machine's status.
1	2026-03-25 16:42:54	Provision by Disk process started.

Showing 1 to 10 of 10 entries

1

Failure analysis

NexaVM snapshot processing timed out.

Solution 1: Delete the rebuild provisioning task

> TrekerLite, also called BootImage, is a migration task target machine created using a target image.

1. Delete the provisioning task and wait for the deletion task to be completed.
    - Options on the left: Delete the provisioning task and execute it again.
2. Restart Treker Lite and restart the corresponding TL from the NexaVM cloud platform.
3. Wait for TrekLite to restart, open the TrekLite console on NexaVM and observe that the IP and other information are displayed.
4. Go to the admin console to verify this Treker Lite.
    - Data gateway –-> Target machine (you can confirm which one based on the IP

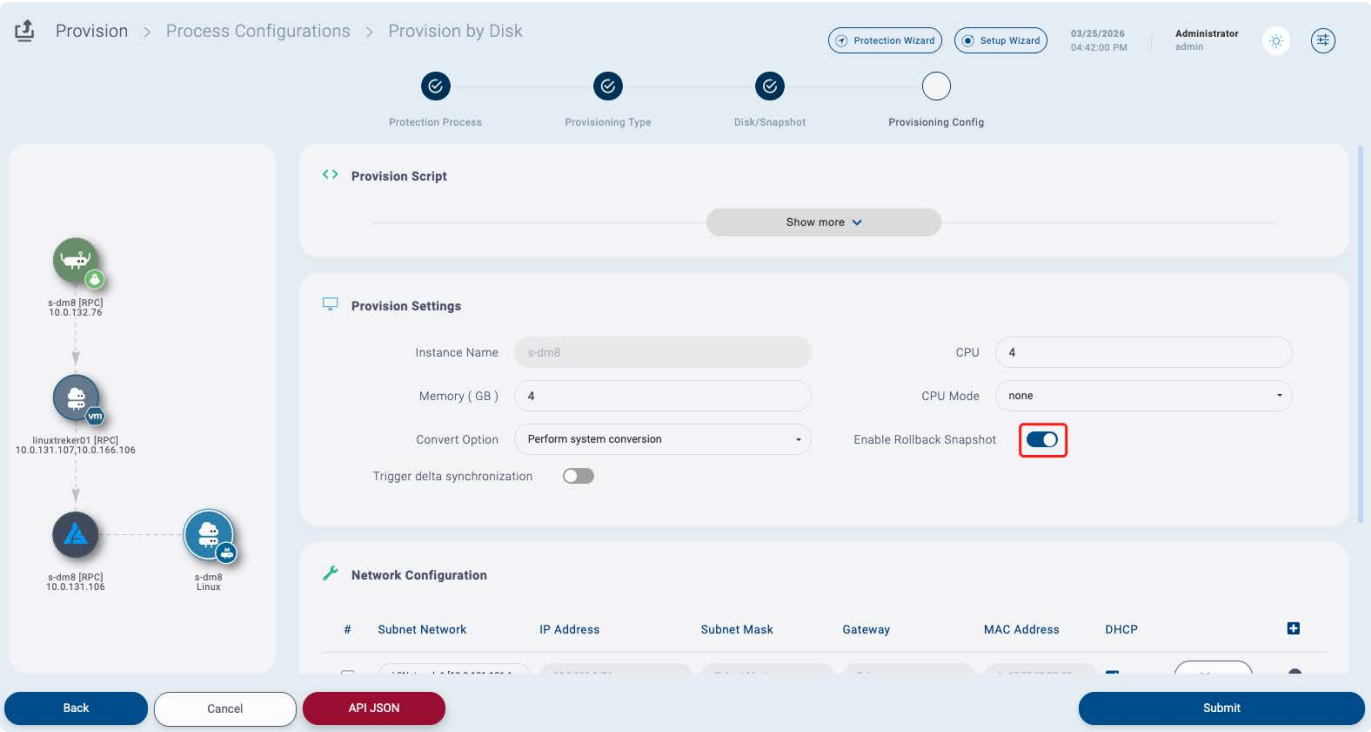
address), select it, click Modify, and verify.

5. Create a provisioning task after the verification is passed.

Solution 2: Disable provisioning tasks to create rollback snapshots

On the provisioning task policy page, turn off the Enable rollback snapshot button.

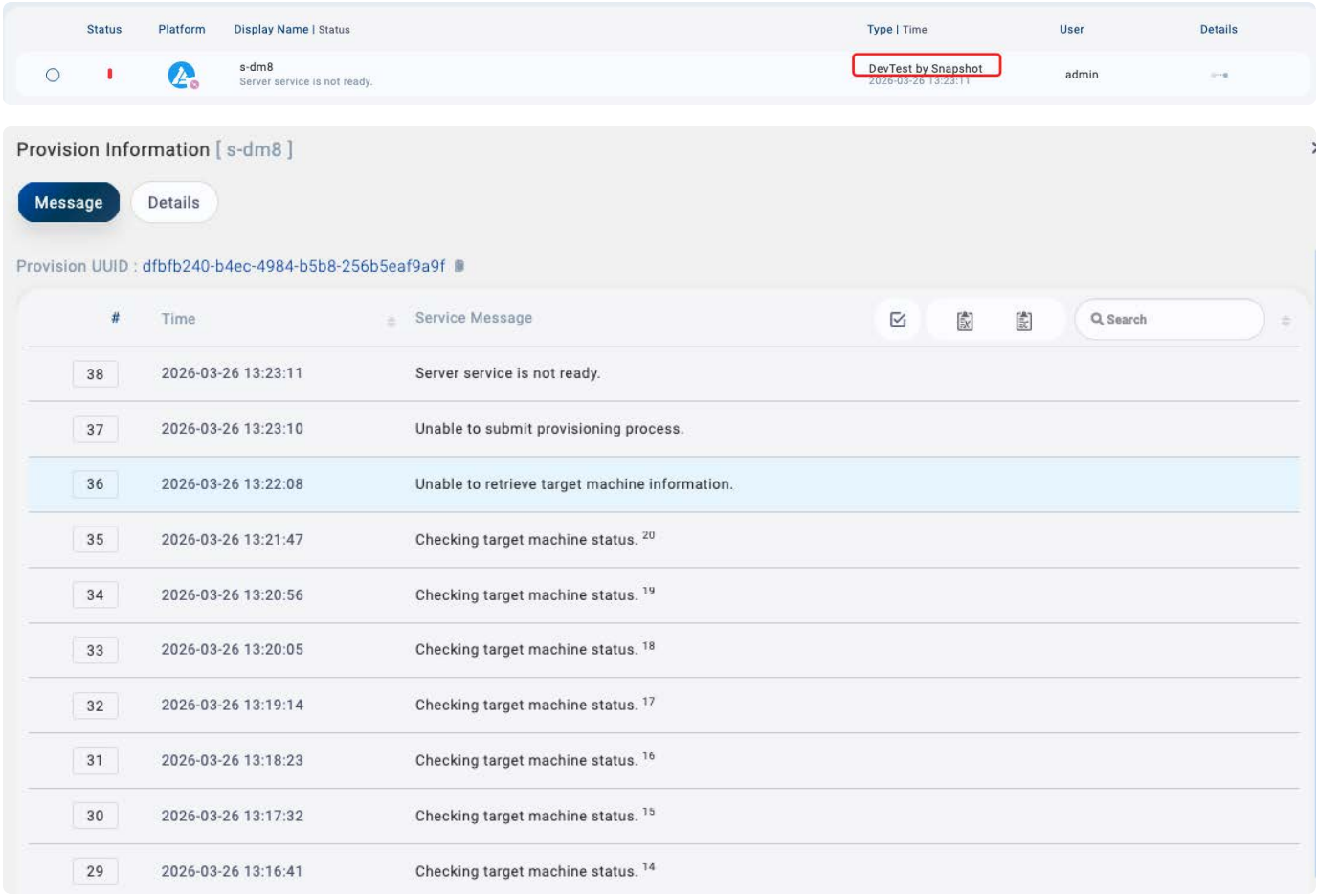
- Disable rollback of snapshots. After the switch is completed, the target machine cannot roll back the snapshot to the state before the switch.
- If you need to roll back, you can manually take a snapshot of the target machine before creating the provisioning task.



Test mode provisioning reports Server service is not ready

Document Category: Product Related Experience

Error screenshot



Problem analysis

The snapshot test mode will clone a target machine. This type of error is caused by the target cloud platform not successfully cloning the target machine, or the target cloud host not successfully obtaining an IP address.

There are many reasons for unsuccessful cloning: insufficient computing resources, insufficient storage resources, insufficient IP address resources, IP address conflicts, mac address conflicts, etc.

solution

Refer to the knowledge base "Copy disk test mode, cloud host cannot be created".

If the issue remains unresolved after referring to the knowledge base, please take a screenshot of the error message and collect console diagnostic logs to seek technical support in the group.

Supplement: special scenes

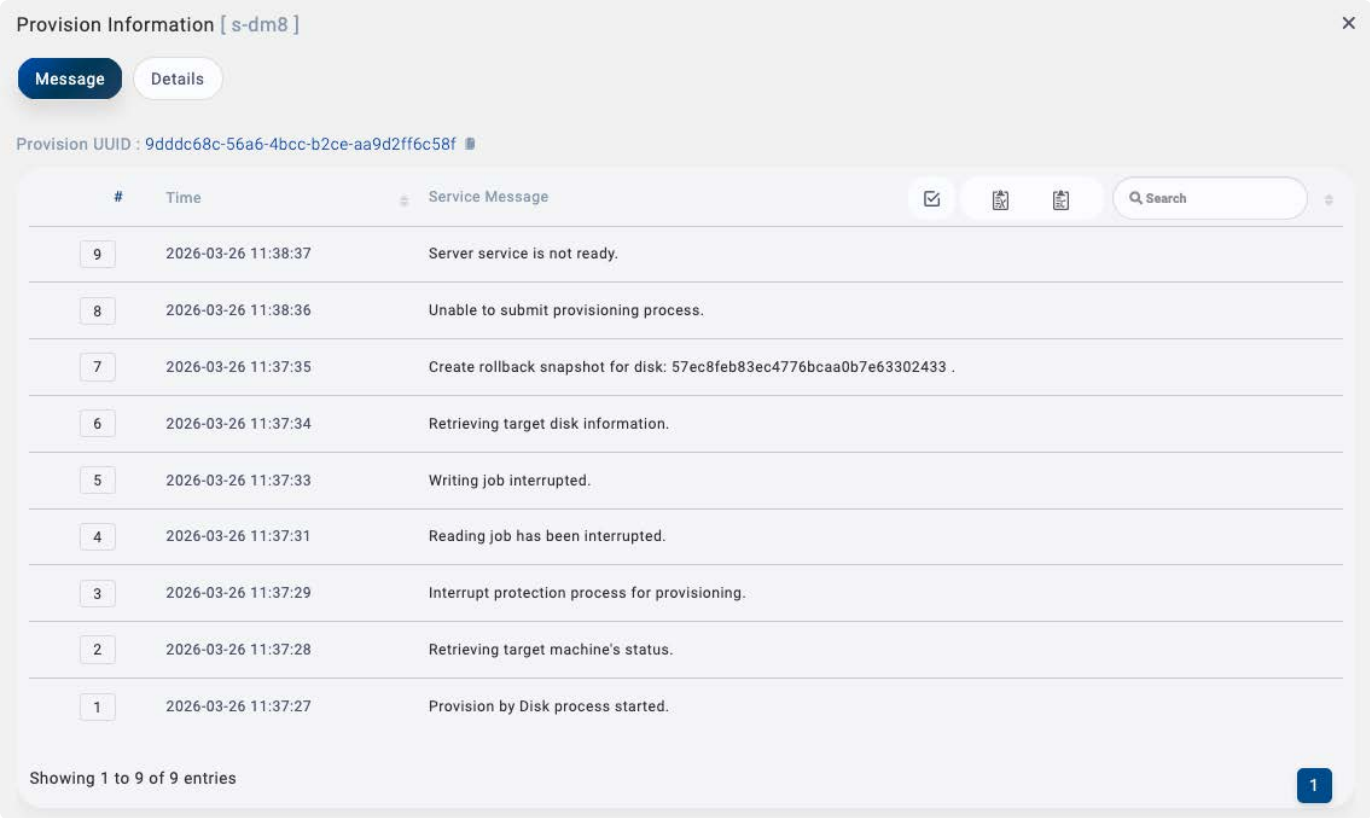
The snapshot selected during test provisioning was overwritten and deleted by the incremental snapshot of the automatically triggered synchronization task.

Solution: Delete the provisioning task and recreate the provisioning task.

Provisioning by Disk and report Server service is not ready

Document Category: Product Related Experience

Error screenshot



Problem analysis

1. Caused by network instability in the user environment.
2. The target machine has a network error, has been shut down, deleted, etc., and is in an abnormal state.

Solution 1. The network is unstable

1. Delete provisioning tasks.
    - Options on the left: Delete the provisioning task and execute it again.
2. Restart Treker Lite (TL for short) and wait for the TL restart to complete.
3. Go to the console to verify this TL
    - Data gateway –-> Target machine (you can confirm which one based on the IP address), select it, click Modify, and verify.
4. Create a provisioning task after the verification is passed.

Solution 2. Target machine is abnormal

1. Go to the target cloud platform to check the running status of the target machine and whether the network is normal.
2. If the target machine's operating status or network is abnormal, please first make the target machine's operating status and network normal, and then refer to the above `Solution 1. Network instability' reconstruction task.
3. After confirming that the operating status of the target machine and the network are normal, refer to the above `Solution 1. Network instability` to rebuild the task.
4. If the target machine has been deleted, please delete the provisioning task and protection task, and then re-create the protection task.

Set the number of multiple copies and only have 1 snapshot when provisioning

Document Category: Product Related Experience

Different NexaVM storage supports different number of snapshots

- If the storage used by NexaVM ceph or nSAN, multiple snapshots can be stored.
- If NexaVM uses non-ceph storage, only one snapshot can be saved.

Concept and comparison of HTTPS and RPC modes

Document Category: Product Related Experience

Write in front

For a better understanding, please first read the operating experience knowledge base "Registering the Source Machine to MGMT Using HTTPS".

RPC and HTTPS concepts

RPC

- Preconditions:
  - Antenna is installed.
  - Requires at least one receiving/transmitting node to be registered on MGMT.
- Registration method:
  - In MGMT --> Resources --> Client --> Add --> Source machine IP, select the transfer node, test --> Confirm.
- Release port: 20005 (inbound direction).

HTTPS

- Preconditions:
  - Antenna is installed.
  - There is no need to register a receiving/transmitting node on MGMT, you can have one.
- Registration method: Execute the command on the source machine to register to MGMT.
  - The Linux version of Antenna only supports command registration.
  - The Windows version of Antenna supports command registration and also has a

graphical registration tool.

  - Refer to the knowledge base "The source machine registers to MGMT using HTTPS".

- Release port: No specification, randomly occupies an idle port (outbound direction).

RPC vs. HTTPS

	RPC	HTTPS
Prerequisites	Antenna has been installed on the source machine At least one receiving/transmitting node needs to be registered on MGMT	Antenna has been installed on the source machine No need to register a receiving/transmitting node on MGMT
Registration method	Enter the IP address of the source machine on MGMT to add	Execute the command on the source machine to register to MGMT
Source machine port	20005 (inbound direction) needs to be released	20005 (inbound direction) does not need to be released

Linux management console configures NTP (time synchronization)

Linux management console configures NTP (time synchronization)

- Operation steps
- Replenish

Document Category: Product Related Experience

Operation steps

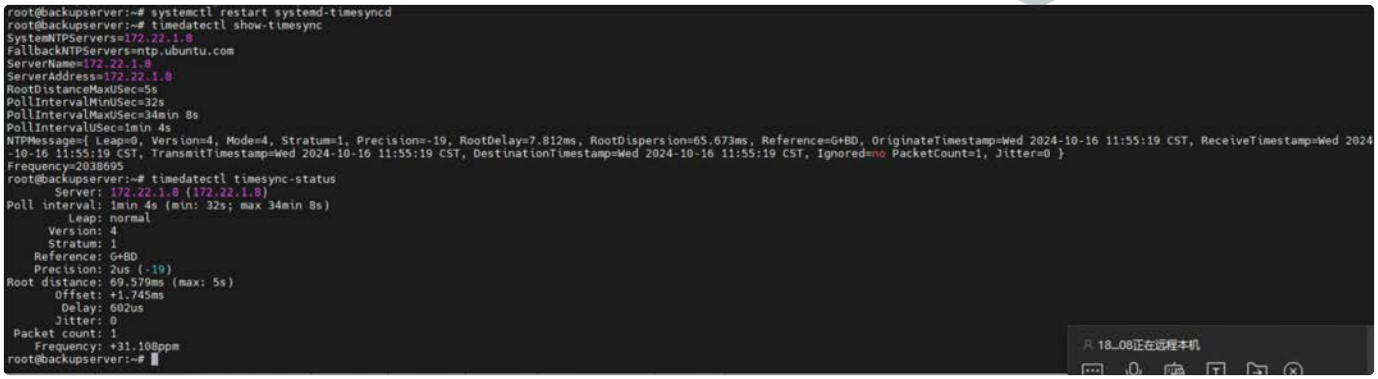
```
#修改Client与Server同步的配置(本机为Client)
vi /etc/systemd/timesyncd.conf

#一般来说timesyncd.conf只需要即可:
[Time]
NTP=x.x.x.x

#重启服务
systemctl restart systemd-timesyncd

#检查系统时间同步状态
timedatectl show-timesync

#显示当前系统的时间同步服务的状态
timedatectl timesync-status
```



Replenish

If the output of `timedatectl timesync-status` does not match the picture above, the service may not be in effect.

You need to check whether there are redundant parameters in the `/etc/systemd/timesyncd.conf` configuration.

Generally speaking, timesyncd.conf only needs:

```
#192.168.1.100为NTP Server的IP地址。
[Time]
NTP=192.168.1.100
```

> Update: 2026-01-05 15:30:56
> Original text: https://lightrek.yuque.com/gsl186/nuigo8/imyopglsa2coy8a2

Necessary conditions for NexaVM mount mode

Document Category: Product Related Experience

Things to note

The prerequisites for this knowledge base are only for NexaVM mount mode.

Necessary conditions for NexaVM mount mode

1. The management console and target data gateway (target end) must communicate with the 8080 port of all management nodes (including VIP) of NexaVM on the target end.
2. **The target data gateway (target side) needs to install performance optimization tools and enable VirtIO (Windows Treker). **
    - **It is recommended to use the Linux version of the data gateway as the target data gateway and enable Virtio. **
3. A data gateway can mount up to 23 cloud disks.
    - The system disk containing the data gateway can mount up to 24 disks.
    - The target data gateway (target end) in the disk mode needs to be properly planned.
4. During switching, the target system disk of the switching task will be cloned. The target cloud platform requires the storage space of `the total disk size of the source machine + 1G` (version 683 and above).

What is the difference whether the NexaVM image has VirtIO enabled or not

Document Category: Third Party Related Experience

Mirroring opens VirtIO

The target cloud host created by the image will start up faster, that is, "the phase of checking the target host will be shorter." The transfer speed will also be faster.

Mirror off VirtIO

The startup and transfer speed of the target cloud host created by the image will be slower.

How to determine whether the image needs to enable virtio

most scenes

It is recommended to enable virtio in the image to optimize transmission performance and the performance of the target machine after switching.

When some systems encounter problems when starting up, they temporarily close VirtIO and restart the system.

special scene

Some systems, such as SuSE10, SuSE11, Kylin v6 and other systems, do not support VirtIO startup due to some reasons, and you need to manually close the virtio of the corresponding target host to enter the system.

In order to reduce manual intervention in this type of system, you can upload a separate image and turn off VirtIO. If you don't mind manual intervention, it is recommended to turn on VirtIO in the image to make the transmission faster, and then turn it off manually when starting up.

4 modes of switching modes

Document Category: Product Related Experience

Switch now

Mode introduction

- will interrupt the synchronization task.
- Switch the target machine to a business system.

Applicable scenarios

- Migration and cutover.

Disk snapshot switching

Mode introduction

- will interrupt the synchronization task.
- Use the snapshot of the target machine to clone a target machine and switch the cloned target machine to a business system.

Applicable scenarios

- Disaster recovery and rescue.

Test based on disk snapshot

Mode introduction

- Will not interrupt sync tasks.
- Use the snapshot of the target machine to clone a target machine and switch the cloned target machine to a business system.

Applicable scenarios

- Migrate verification data and disaster recovery verification data.

File restoration

Mode introduction

- Will not interrupt sync tasks.
- Use a dedicated FileAccess image to create a cloud host and mount the volume created by the specified snapshot to the cloud host.
- After the cloud host is successfully started, the file download service in the corresponding volume will be provided through the web page.

Applicable scenarios

- Disaster recovery projects need to restore a certain file, a certain folder, multiple files, and multiple folders.

Frequently Asked Questions about Upgrading the Management Console

Document Category: Product Related Experience

1. Do I need to back up the management console before upgrading?

Backup required. Backup method: Collect a copy of the diagnostic log of the management console.

2. What checks need to be done before upgrading?

- All synchronization tasks are in `unsynchronized state`.
  - If there is a task in the `synchronization state`, please stop the synchronization task manually. The task information is `stop protection program successfully` and `discard snapshot`.
    - Click Stop during the initial synchronization. The next synchronization will perform a comparison and difference synchronization (checksum).
- All switching tasks are in `switching completed state`.

3. When upgrading the management console, do all agent software need to be reinstalled?

The agent software does not need to be reinstalled. You only need to upgrade the GatewayServer (Treker) of the management console.

4. When upgrading the management console, does BootImage need to be replaced with the same version of the management console?

NEXAVM

It is recommended to upload the same version of the BootImage (target machine image) of the management console, and use the new version of the image when creating a new synchronization task.

Existing tasks can continue to use the old version of BootImage (target machine image).

5. Can the Windows version of the management console be upgraded from a lower version to a higher version?

Generally speaking, you can directly upgrade from a lower version to a higher version. Exceptions are made for particularly major changes in a certain version.

- **Special Note**: As of version 668, it is known that versions below 635 cannot be upgraded to versions above 635, which will cause the Treker service to fail to start.

6. What is the difference between overwriting and installing the upgraded version and uninstalling the old version and then installing the new version?

Overwrite and install the upgraded version:

- All resources (cloud platform, data gateway, source host), tasks (synchronization tasks, switching tasks), etc. will be retained.

Uninstall the old version and install the new version:

- All resources (cloud platform, data gateway, source host) and tasks (synchronization tasks, switching tasks) will disappear (which can be simply understood as clearing the database of the management console).

Configuration items	Overwrite installation and upgrade to new version	Uninstall old version and install new version
Cloud Platform	✅ Reserve	❌ Clear
Data Gateway	✅ Reserve	❌ Clear
Source host	✅ Reserve	❌ Clear

Sync tasks	✅ Keep	❌ Clear
Switch tasks	✅ Keep	❌ Clear
Task Template	✅ Reserve	❌ Clear
Push Configuration	✅ Reserve	❌ Clear
License	✅ Reserved	✅ Reserved

7. Which method is recommended to upgrade the management console?

It is recommended to uninstall the previous version and then install the new version.

8. How to upgrade the management console?

Windows version management console:

- Uninstall and reinstall: Uninstall the old version and install the new version.
- Overlay installation: Directly run the new version installation package, and the installation will be automatically overwritten.

Linux version management console:

- Please contact Support.

> Notes:
>
> Uninstall and reinstall the management console software, the license is retained.
>
> If you reinstall the system on the management console, the license will be lost! ! !

How to use post-scripts

Document Category: Product Related Experience

Introduction to switching task post-scripts

Both immediate switching and copy disk test modes support pre-scripting.

script execution phase

The post-script is executed after the target machine switches from the TL system to the user's production OS and is powered on.

Applicable scenarios

Reset passwords, install software, modify configurations, etc.

Script

Windows

Just use the normal cmd command. **The script name must be run.cmd**, and then compress it into a zip package. The compression password cannot be set, and the compressed package does not support Chinese names and special characters.

Take resetting password as an example:

```
#reset password of administrator to 'ABCabc@123'
#Do not include comments when writing post-scripts
net user administrator ABCabc@123
```

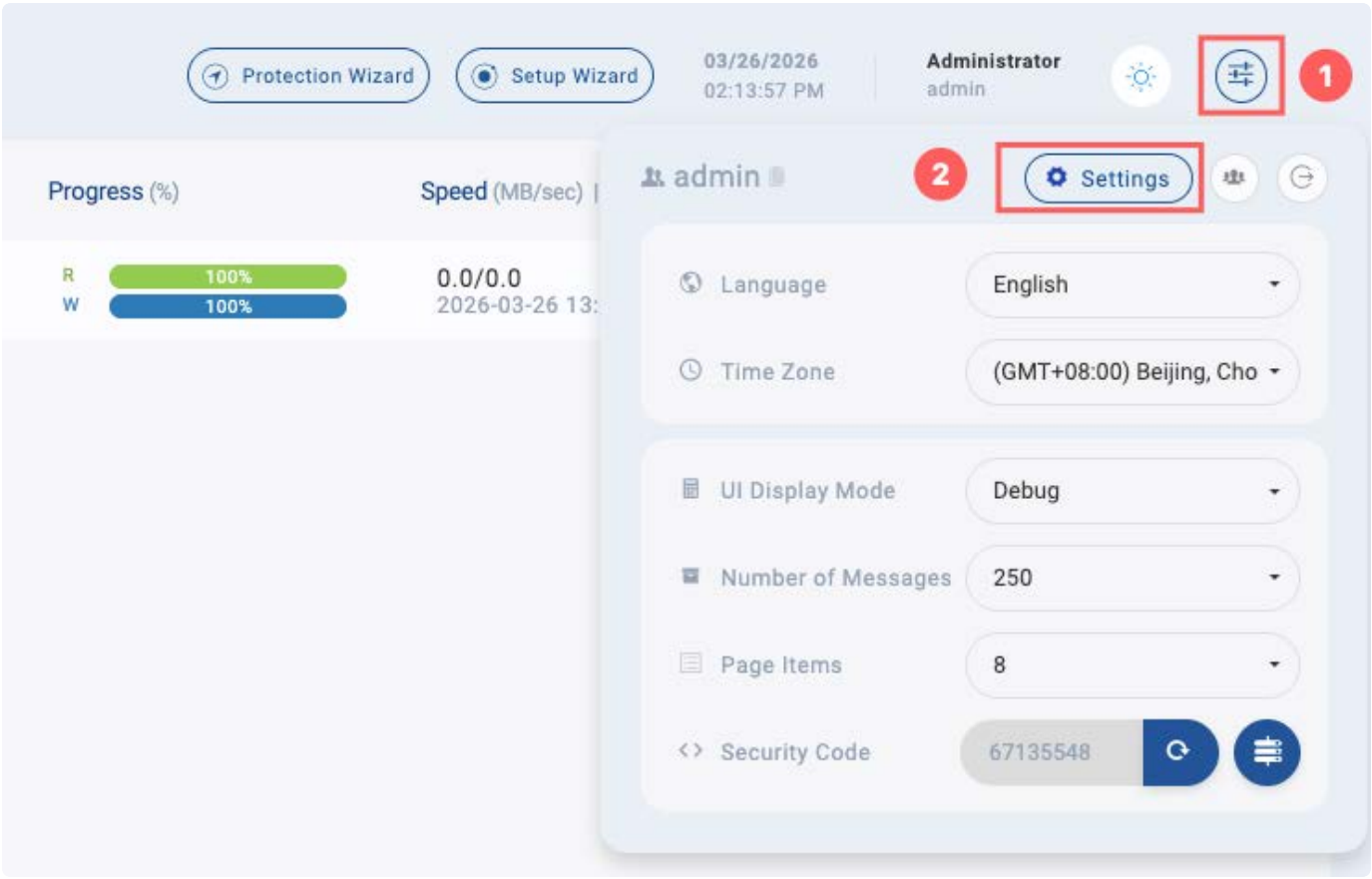
Linux

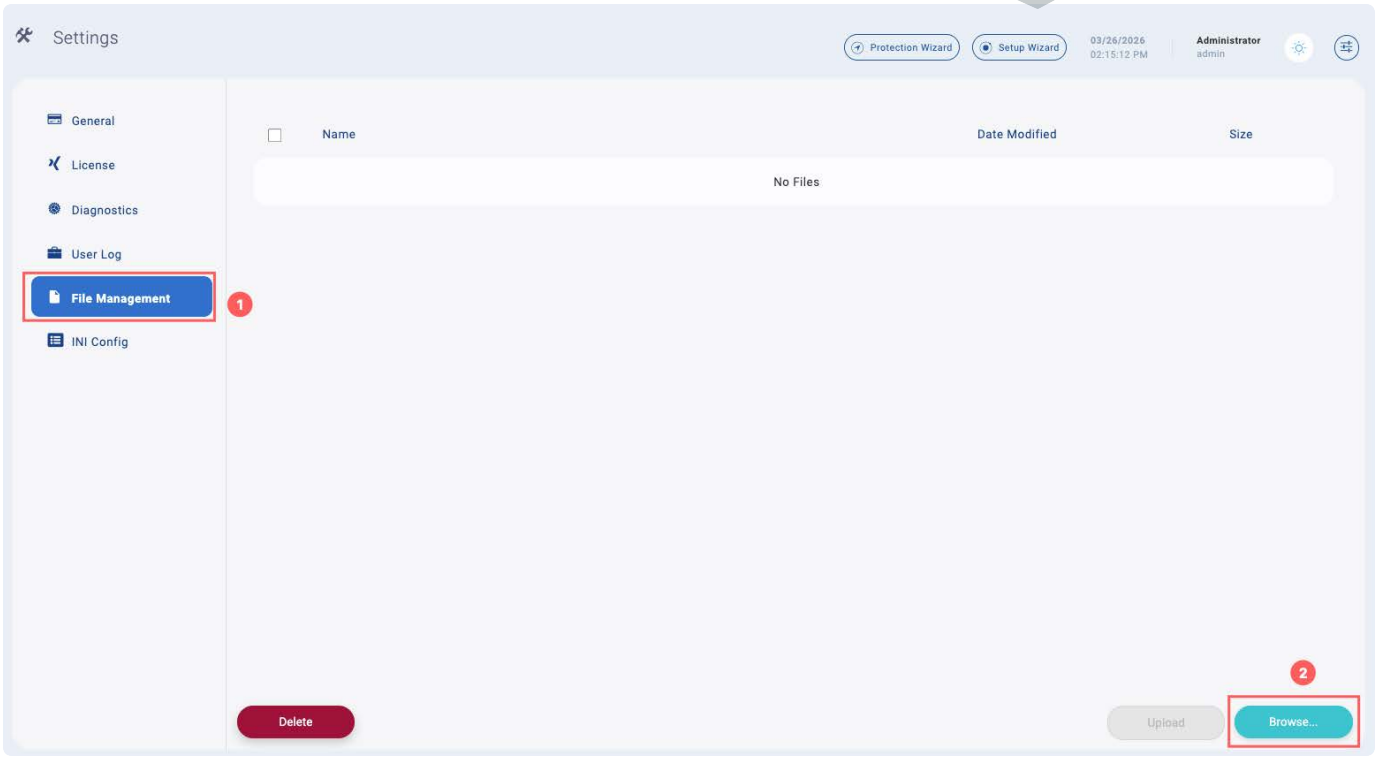
Just write a normal shell script. **The script name must be run.sh**, and then compress it into a zip package. You cannot set a compression password. The compressed package does not support Chinese names and special characters.

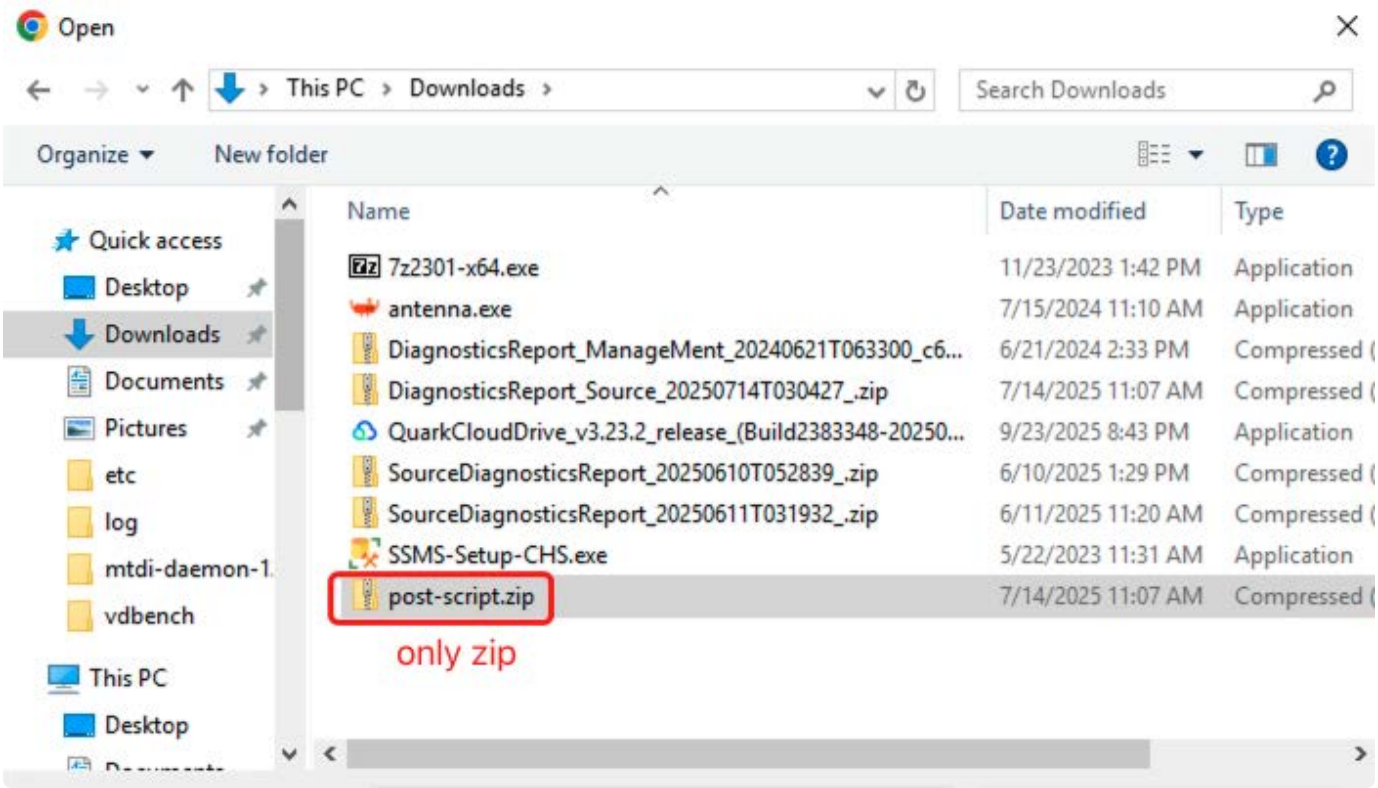
Take resetting password as an example:

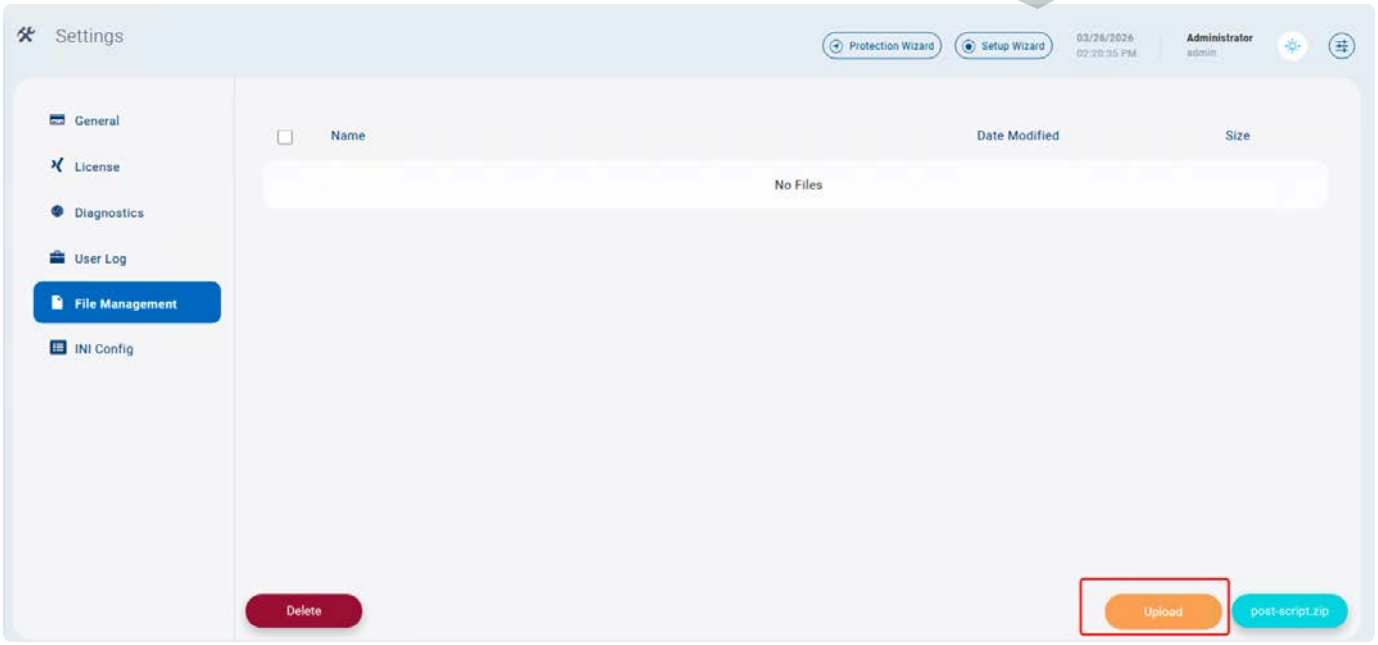
```
#!/bin/sh
#backup shadow
cp -p /etc/shadow /etc/shadow.bak.navi
#Change password using plaintext, in the format: 'username:password'.
echo 'root:root'|chpasswd
```

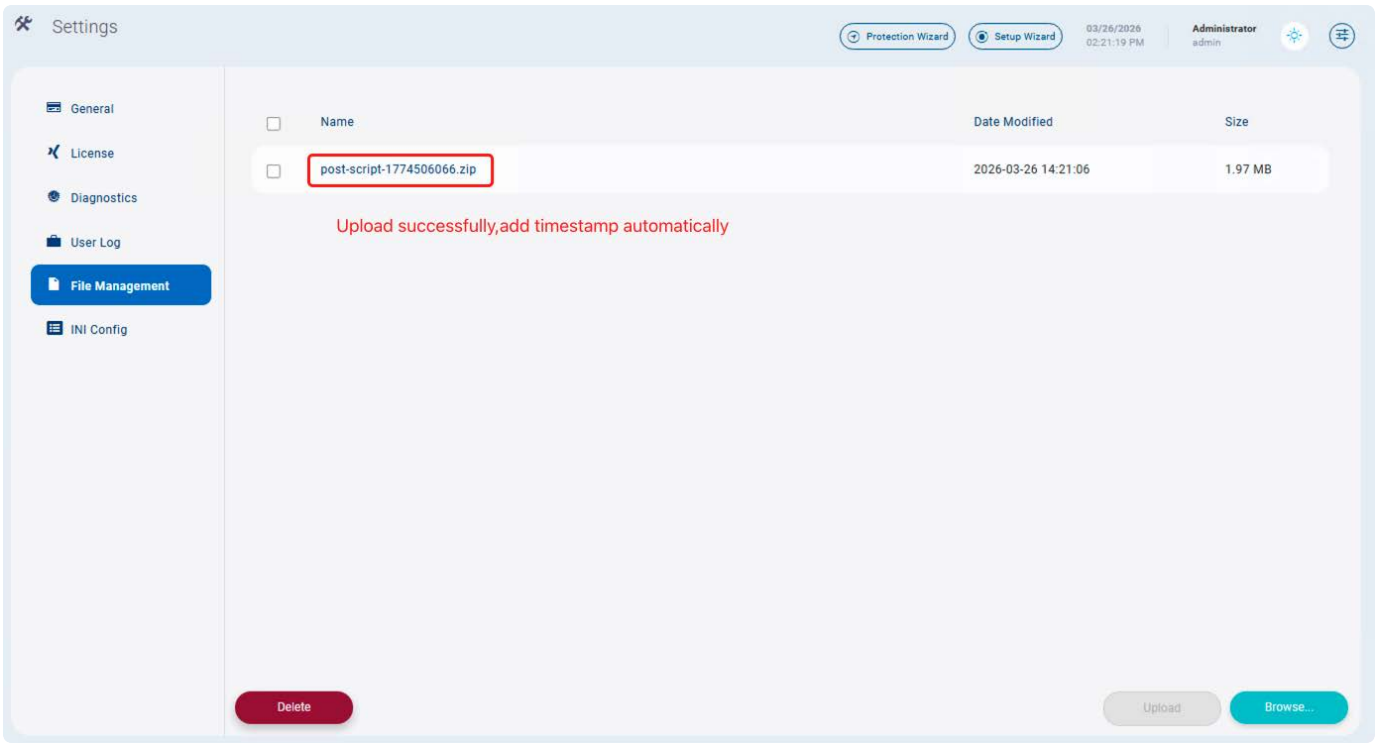
Upload script




Settings
Protection Wizard
Setup Wizard
03/26/2026
02:15:12 PM
Administrator
admin
General
License
Diagnostics
User Log
File Management
INI Config
1
Name
Date Modified
Size
No Files
2
Delete
Upload
Browse...

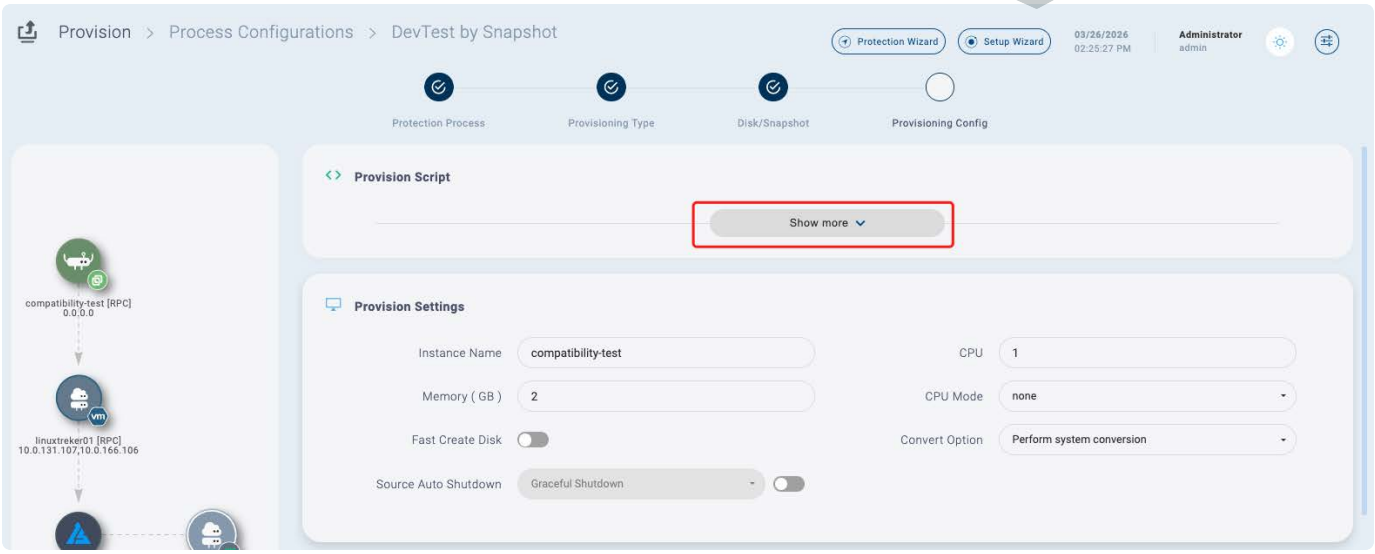

Open
This PC
Downloads
Search Downloads
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
etc
log
mtdi-daemon-1.
vdbench
This PC
Desktop
Name
Date modified
Type
7z2301-x64.exe
11/23/2023 1:42 PM
Application
antenna.exe
7/15/2024 11:10 AM
Application
DiagnosticsReport_ManageMent_20240621T063300_c6...
6/21/2024 2:33 PM
Compressed
DiagnosticsReport_Source_20250714T030427_.zip
7/14/2025 11:07 AM
Compressed
QuarkCloudDrive_v3.23.2_release_(Build2383348-20250...
9/23/2025 8:43 PM
Application
SourceDiagnosticsReport_20250610T052839_.zip
6/10/2025 1:29 PM
Compressed
SourceDiagnosticsReport_20250611T031932_.zip
6/11/2025 11:20 AM
Compressed
SSMS-Setup-CHS.exe
5/22/2023 11:31 AM
Application
post-script.zip
7/14/2025 11:07 AM
Compressed
only zip





Switch tasks to call uploaded scripts

1. On the enable configuration page, expand the enable command.



2. Scroll down "Enable command set (after running)"



3. Select uploaded script



4. Configure other parameters normally and click Confirm.

Installation and uninstallation of Linux Antenna in one picture

Installation and uninstallation of Linux Antenna in one picture

Document Category: Product Related Experience

write in front

Above the green line are the installation steps, and below the green line are the uninstall steps.

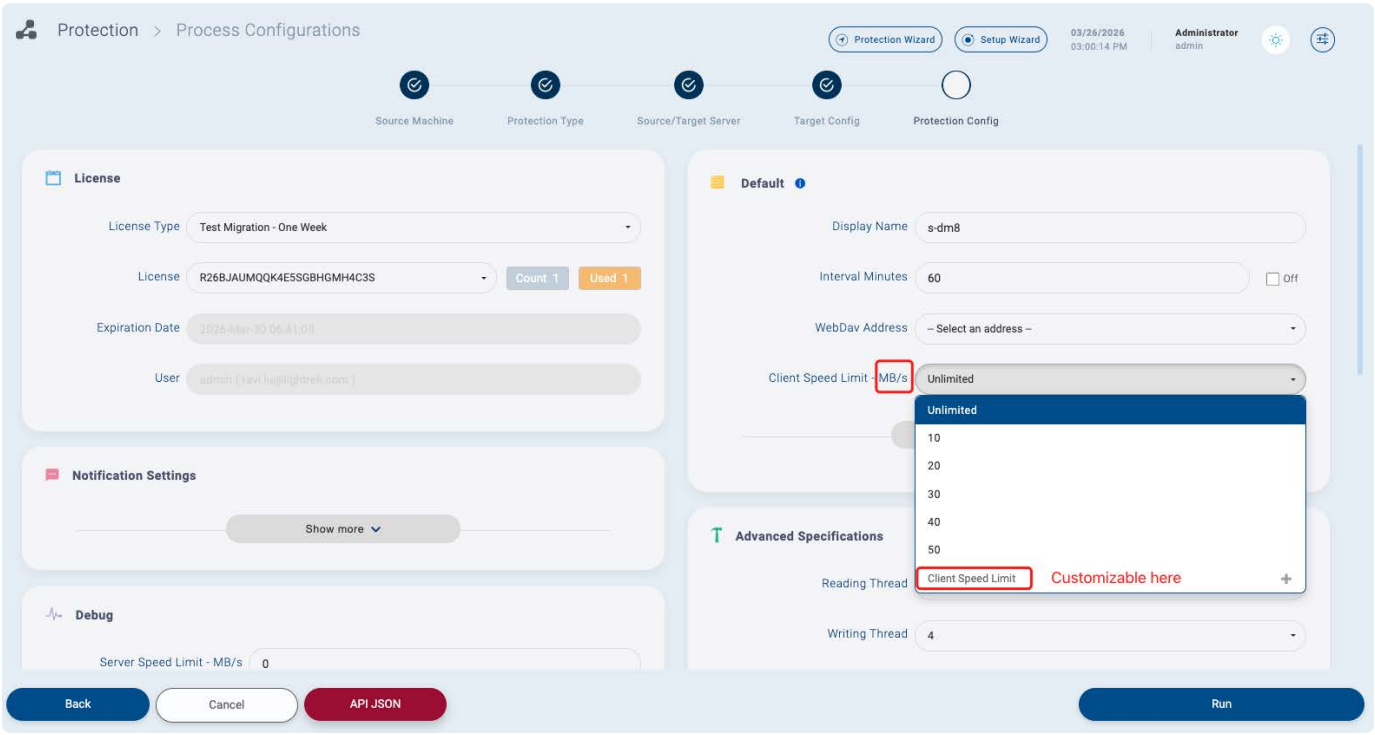
Frequently Asked Questions and Answers

Document Category: Product Related Experience

Does it support speed limit?

Support speed limit.

When creating a task, you can directly set the speed limit value.



If you forget to set the speed limit when creating a task, you can edit the task and set the speed limit, but the speed limit filled in when editing the task will take effect during the next synchronization.

If needs to take effect immediately:

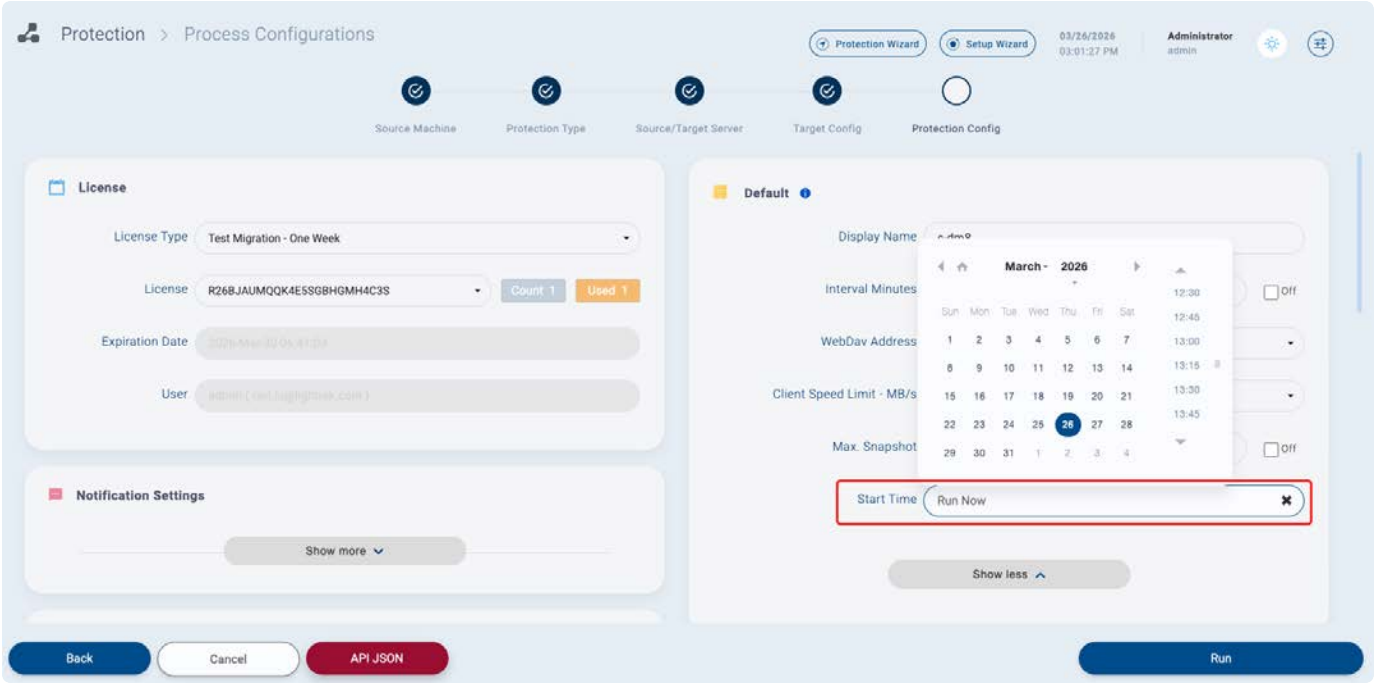
- There is a proxy mode, please refer to the knowledge base "Speed Limiting Synchronization Tasks – Source Host Level".
- For both agentless and agent-based methods, please refer to the knowledge base "Speed Limiting Synchronization Tasks – Cloud Platform Level".

Does it support scheduled synchronization?

When creating a synchronization task, you can set the initiation time of the synchronization task.

Specify the time you want to initiate synchronization in the `Startup window` .

> For more detailed information on `Startup Window` , please refer to the knowledge base "Task Strategy Parameters".



Does it support pausing synchronization tasks?

Supports pausing synchronization tasks.

Stop the Antenna service by logging in to the source host to pause the synchronization task.

For details, please refer to the knowledge base "Pause Synchronization Task".

Does it support resumed downloading?

Supports resumed downloading.

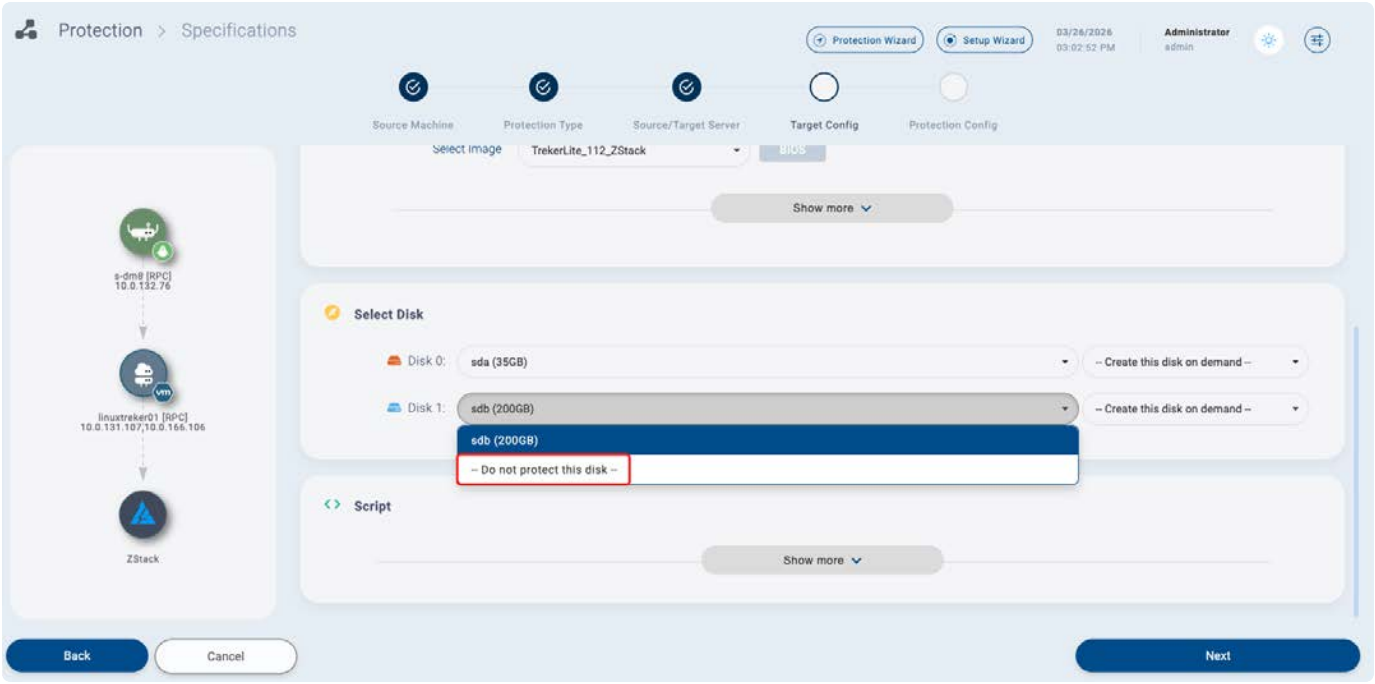
After the network is disconnected abnormally and the network is restored, the synchronization task can be resumed at the break point. However, if the disconnection time is long and the data change exceeds the journal record range, the synchronization task will enter the checksum (compare differential transmission).

Is skipping disk supported?

Supports skipping disks.

When creating a synchronization task, click on the disk that you want to skip and select 'Skip this disk'.

Note: By default, skipping the system disk is not allowed. If you need to skip the system disk, you need to change the `Configuration State' of the management console to Troubleshooting'`.

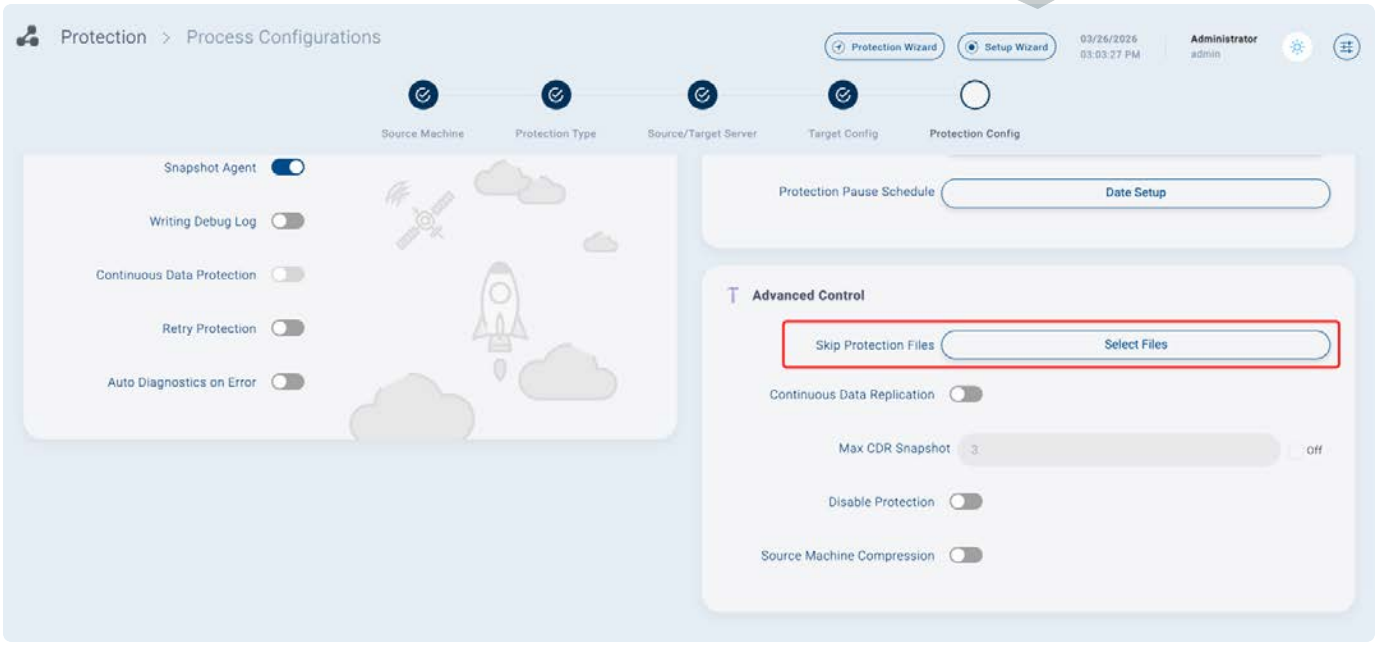


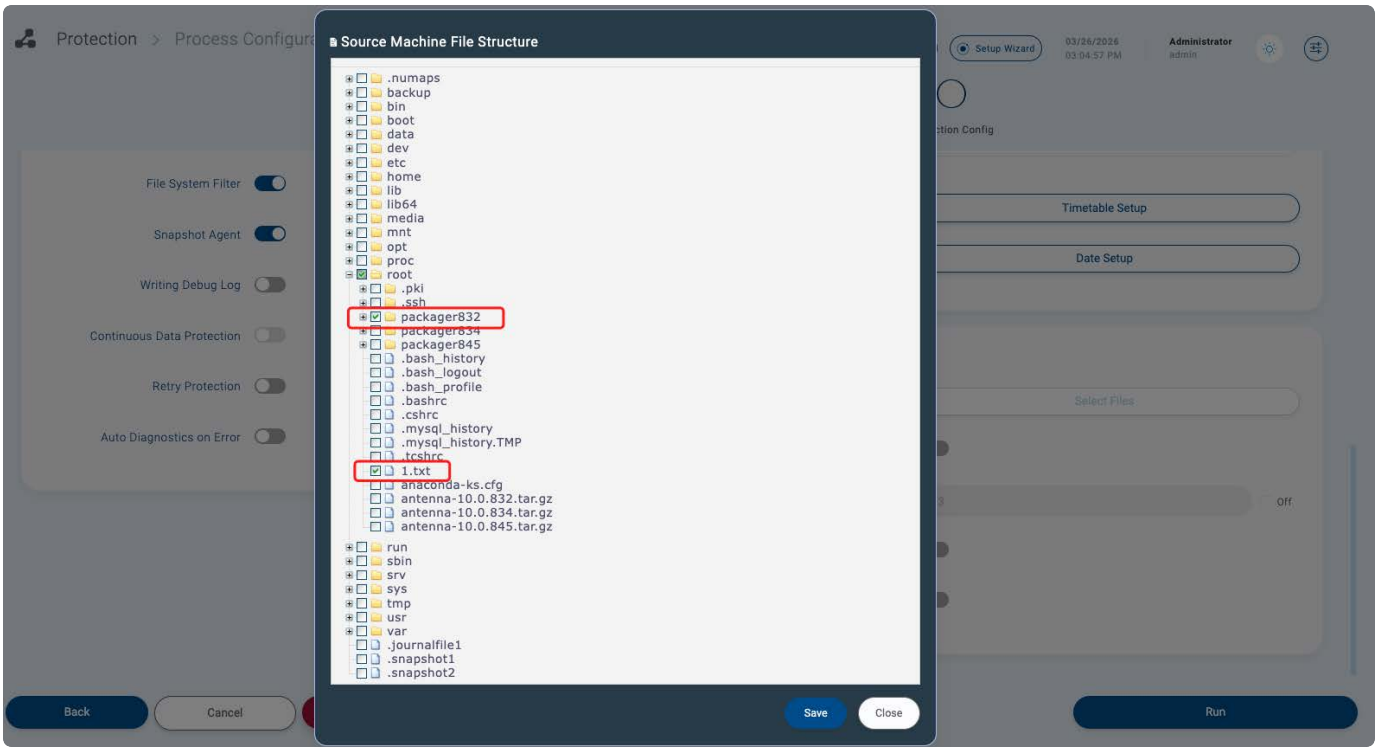
Does it support skipping certain files or folders?

Agentless mode does not support skipping certain files or folders.

There is a proxy mode that supports skipping certain files or folders.

Change `Configuration Status` to `Advanced` or `Troubleshooting`. When creating a task, select the files or folders that need to be excluded in `Advanced Control`.





Differences between Windows Data Gateway and Linux Data Gateway

	Windows Data Gateway	Linux Data Gateway
VDDK	Good stability👍	Average stability

NEXAVM

Size	exe installation, the installation package is small	qcow2 image, the entire image is larger
Management	Windows system graphical	Linux system command line or SSH
System authorization	Windows license activation required (customers activate the system by themselves)	Linux open source does not require a system license

Recommended scenarios for Windows Data Gateway

- Serves as an agentless data gateway for VMware.

Recommended scenarios for Linux data gateway

- Serves as NexaVM Cloud's agentless data gateway.
- Serves as the target data gateway in disk mode for NexaVM Cloud or NexaSphere.

Differences between Windows Management Console and Linux Management Console

	Windows Management Console	Linux Management Console
Apache	Average stability	Good stability👍
Browser	A browser can be installed in the system	The system defaults to no graphics and no browser
Size	exe installation, the installation package is small	qcow2 image, the entire image is larger
Management	Windows system graphical	Linux system command line or SSH
System authorization	Windows license activation required (customers activate the system by themselves)	Linux open source does not require a system license

Recommended scenarios for Windows Management Console

NEXAVM

- The number of migrations or disaster recovery is small, and the management console needs to be accessed through a browser on the local machine.

Recommended scenarios for Linux management console

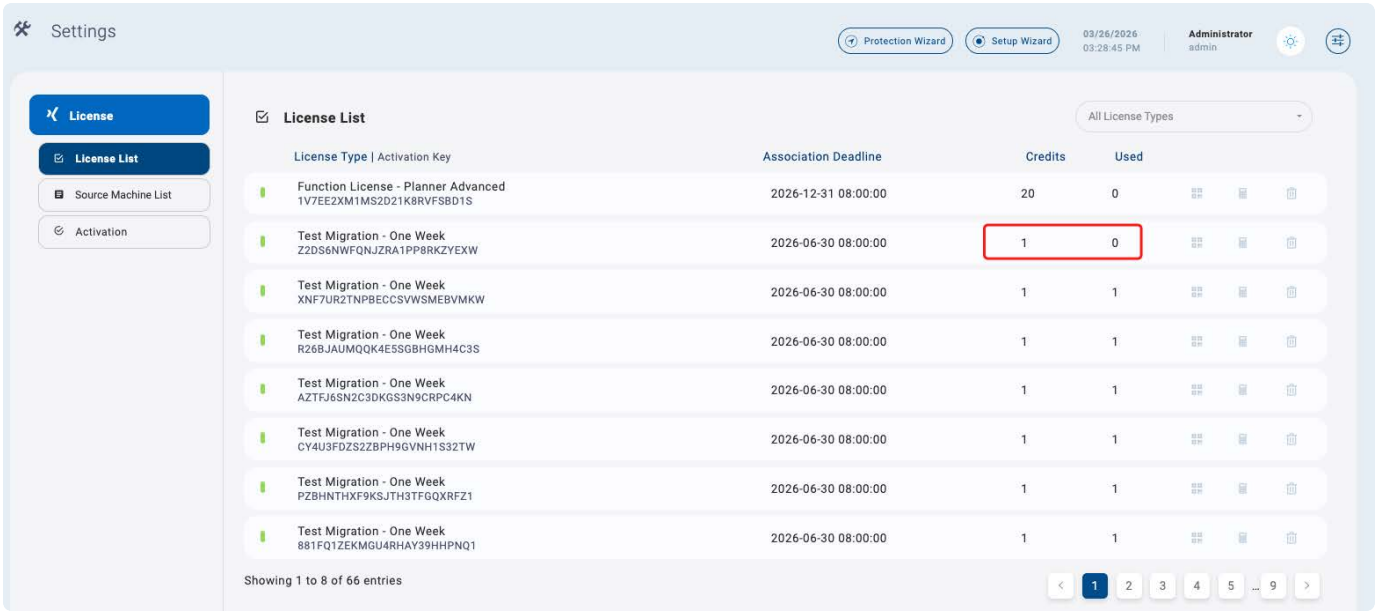
- The Linux management console can be used in environments that do not require local browser access to the management console and do not serve as a VMware agentless data gateway.

Extend the license validity period of a synchronization task

Document Category: Product Related Experience

Activate license

Activate at least one license for extension.

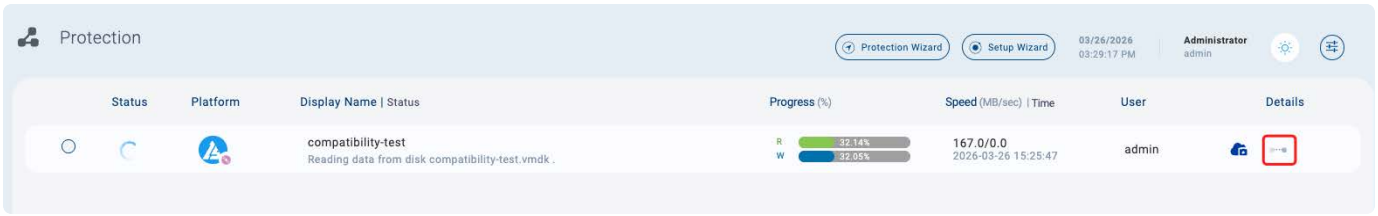


Extend mission clearance

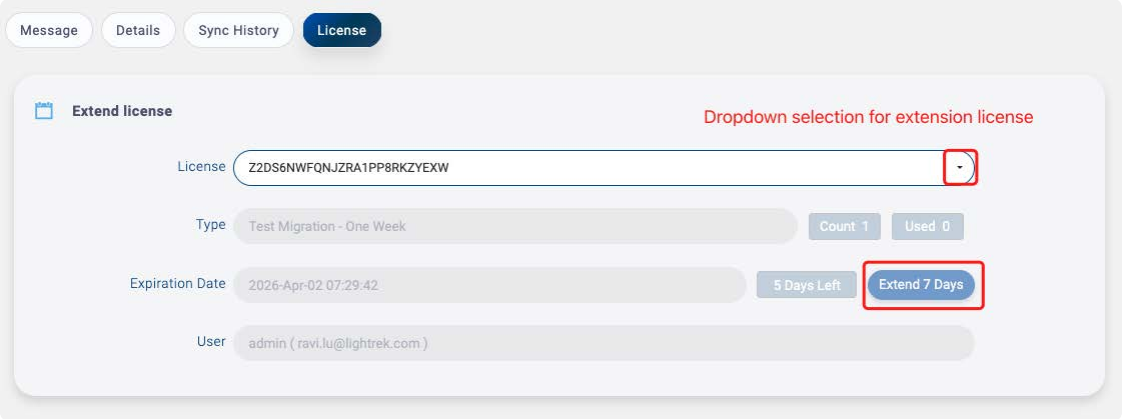
Method one

> Method 1 requires the management console version ⩾ (greater than or equal to) version 666.

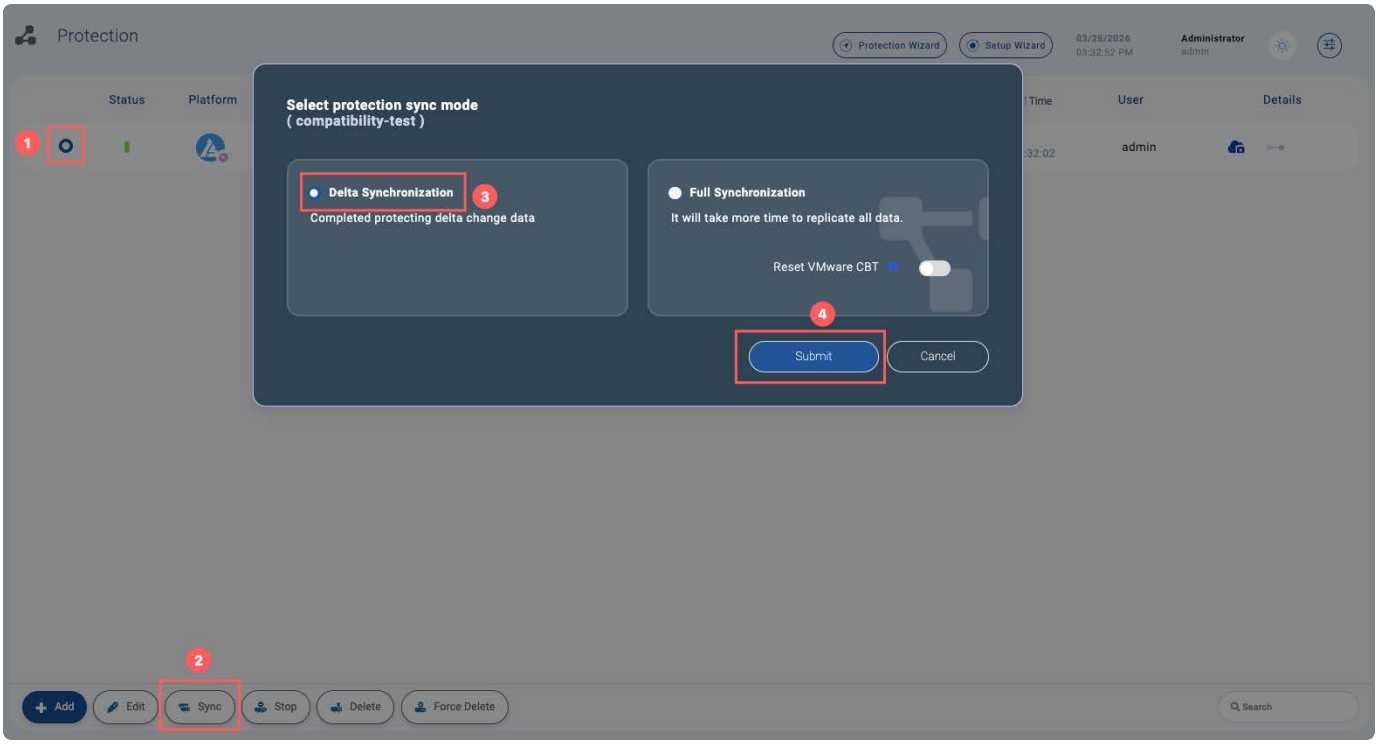
1. Find the synchronization task that requires extended permission and click `Information`.



2. In `Authorization Management`, select `License for Extension` from the drop-down menu and click `Extend`.

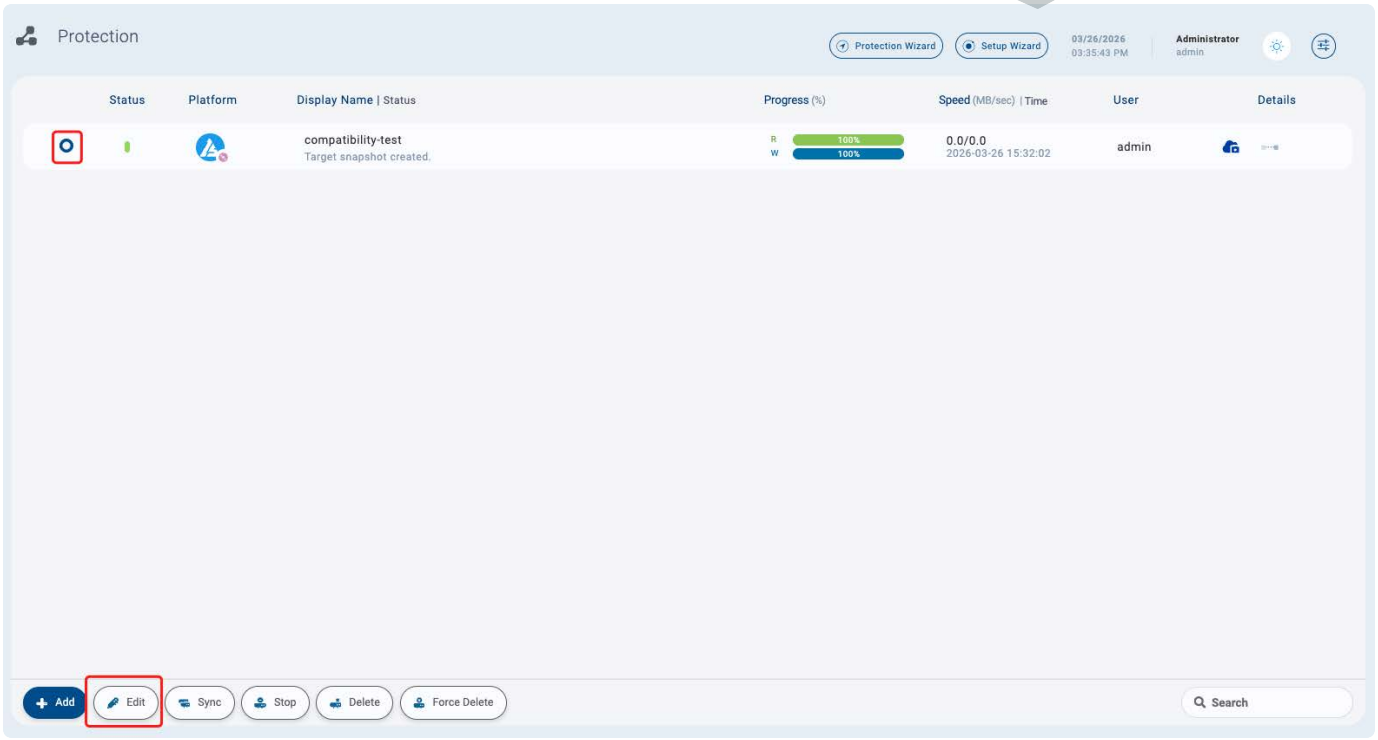


3. Manually initiate an `incremental synchronization`.

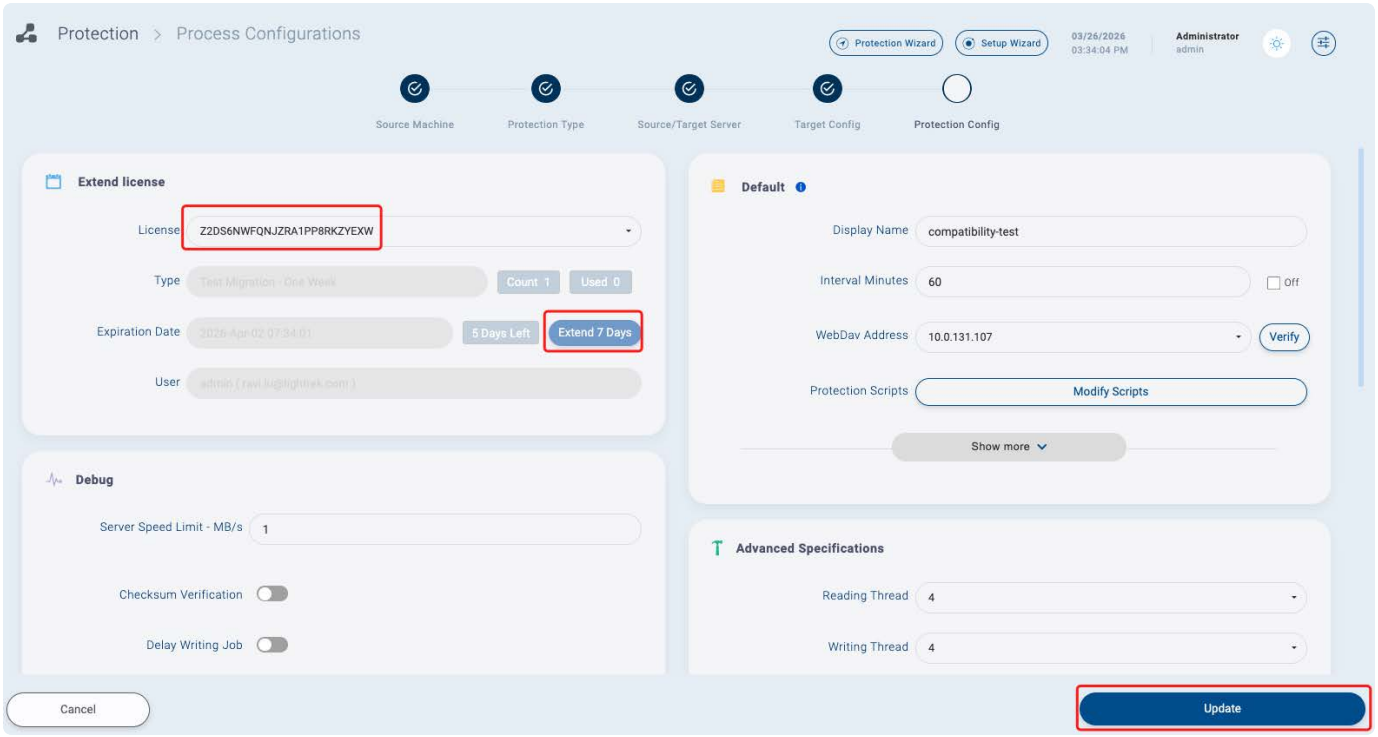


Method two

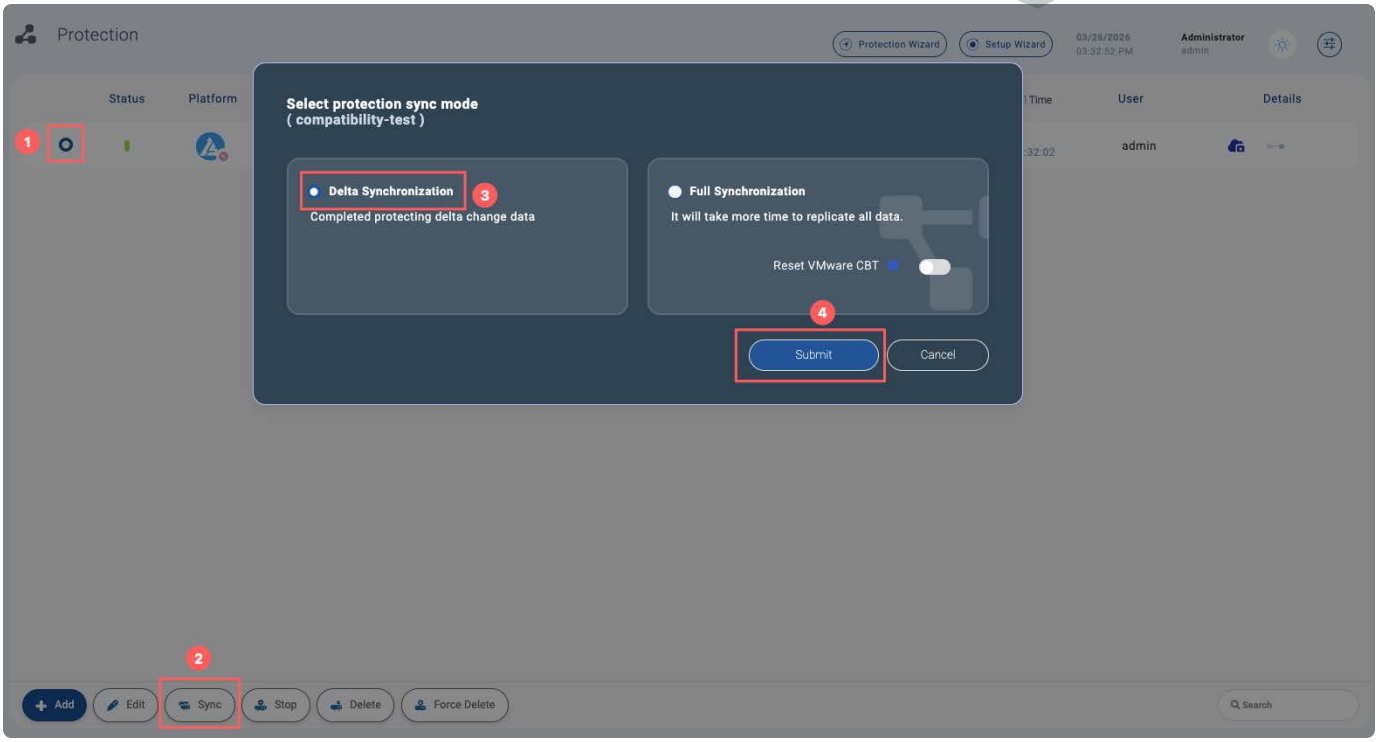
1. Select the synchronization task that requires extended permission and click `Modify`.



2. Pull down to select `License for extension`, click `Extend`, and click `Update` to close the page.



3. Manually initiate an `incremental synchronization`.


Protection
Protection Wizard
Setup Wizard
03/26/2026
03:32:52 PM
Administrator
admin
Status
Platform
Time
User
Details
admin
Select protection sync mode
(compatibility-test)
Delta Synchronization
Completed protecting delta change data
Full Synchronization
It will take more time to replicate all data.
Reset VMware CBT
Submit
Cancel
1
2
3
4
Add
Edit
Sync
Stop
Delete
Force Delete
Search

Manually created Trek Lite spaces are not recognized correctly

Document Category: Product Related Experience

Knowledge points

Treker Lite (TL) and Linux Treker Lite (LTL) will recognize the system disk space when booting for the first time, and will not be recognized again if the system disk is expanded later;

The data disk can be expanded after booting.

Possible reasons

If the system disk is expanded after TL is turned on, the expansion space cannot be identified.

solution

Please delete the TL and create it again.

Agentless mode migration FAQ

Document Category: Product Related Experience

1. Can the agentless mode be shut down and migrated?
    - You can shut down and migrate.
2. When synchronizing in agentless mode, will restarting or shutting down the VM virtual machine affect the synchronization?
    - No impact.

Pause synchronization task

Document Category: Product Related Experience

write in front

Currently, there is no function to pause the synchronization task, but the task can be paused by stopping the service of the source host.

operational risk

If the pause time is long and the data change amount of the source host exceeds the record range of the journal, the snapshot will be discarded, causing this synchronization to fail, and the next synchronization will become a checksum (compare differential transmission).

Operation steps

Stop the Antenna service on the source host to suspend the transmission of synchronization tasks.

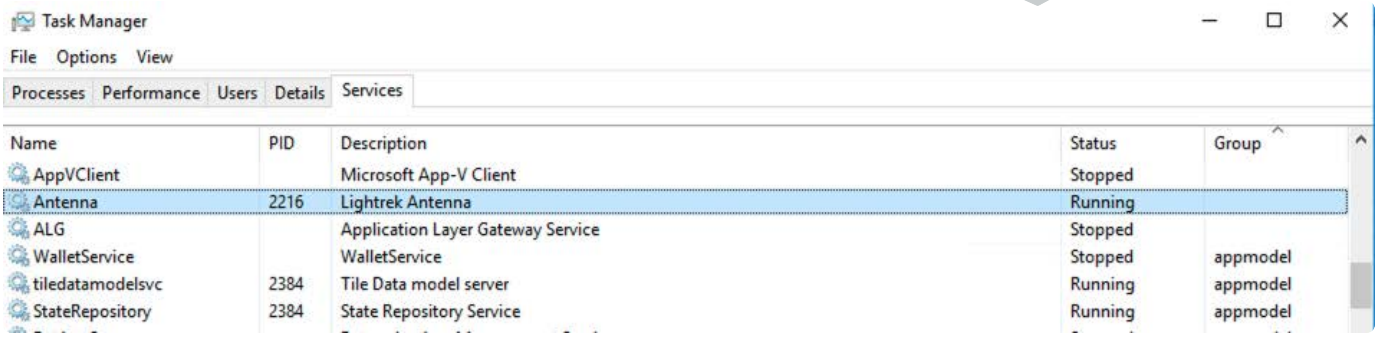
**Note: After stopping the Antenna service, the synchronization task will report "unable to connect to the source host", which is normal! It will automatically resume after the service is started. **

Stop and start services

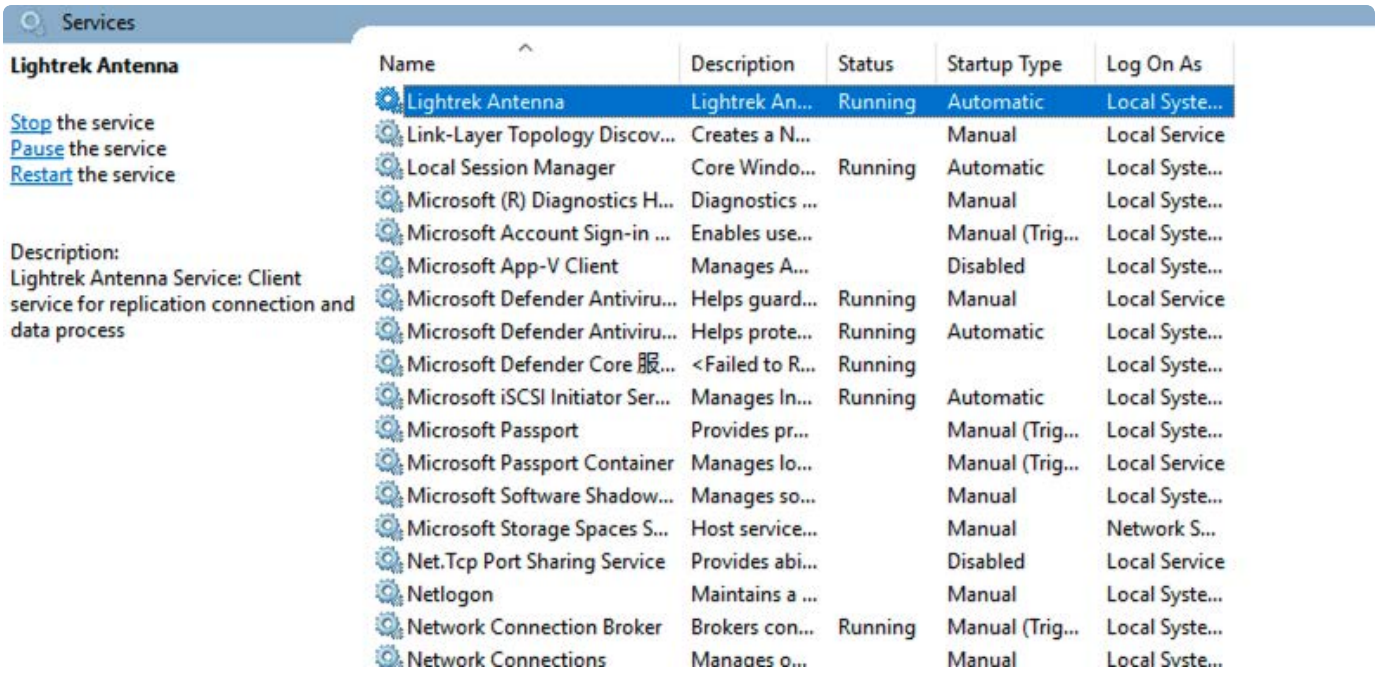
Source host–Windows version

Method 1. Check in the service of the task manager: `Right-click to stop, start, restart`

NEXAVM



Method 2. Check in system services: `Right-click to stop, start, restart`



Source host-Linux version

Method 1. Use `systemctl` to manage services:

```
#Start antenna service
systemctl start antenna

#Restart antenna service
systemctl restart antenna

#Stop antenna service
systemctl stop antenna

#Check antenna service status
systemctl status antenna
```

Method 2. Use `Antenna's parameters` to manage the service in the installation directory:

NEXAVM

```
#Start antenna service
/usr/local/antenna/init_service.sh

#Stop antenna service
/usr/local/antenna/stop_service.sh

#Restart antenna service,it's recommended to use 'ps -ef | grep antenna' to check if the PID has changed.
/usr/local/antenna/antenna --restart
```

Necessary conditions for source-end NexaVM Cloud and NexaSphere agentless

Document Category: Product Related Experience

Things to note

The necessary conditions for this knowledge base are only for **source-side NexaVM Cloud and NexaSphere**

Management console ≥ 689 can support NexaSphere agentless.

Management console ≥ 633 can support NexaVM Cloud agentless.

NexaVM < 1.3.28; NexaSphere < NexaSphere 1.10.18

Implementation logic of source-side agentless (disk mounting)

1. The management console takes a snapshot of the source host's disk, then creates a disk from the source host's snapshot and mounts it to the transit data gateway (source).
2. The transit data gateway (source) synchronizes the disk data created by the snapshot of the source host to the target.
    - **When the disk is large, it may take longer to take a snapshot of the cloud disk and create the disk from the snapshot. **
3. When executing the increment, repeat the above steps, and the management console will perform a checksum (compare differential transmission) on the data.
    - When the amount of data is large, checksum (comparison differential transmission) will be slower than the increment of installed Agent.
    - **If you pursue incremental efficiency, please use the method of installing Agent to migrate. **

Necessary conditions for the source

1. The management console and the transfer data gateway (source end) must communicate with the 8080 port of all management nodes (including VIP) of the source end NexaVM.
2. The transit data gateway (source) needs to be in the same cluster as the source host.
3. The transit data gateway (source) needs to be able to access the storage where the source host disk is located.
4. Enable VirtIO on the transit data gateway (source side).
    - It is recommended to use the Linux version of the data gateway as the target data gateway and enable Virtio.
5. A data gateway can mount up to 23 source host disks.
    - The system disk containing the data gateway can mount up to 24 disks.
    - The transfer data gateway (source) in NexaVM agentless source end needs to be properly planned.

NexaVM ≥ 1.3.28; NexaSphere ≥ 1.10.18

The management console ⩾ 689 only supports source-side agentless CBT (NBD) mode.

Implementation logic of source-side agentless (Cloud CBT/ZSphere CBT)

1. create cbt task: Create a recorded task, the consumption is almost negligible (internal db level)
2. enable cbt task:

- Equivalent to a snapshot (block job), create a disk, top point the current backend file.
- During backup, new data is written. If the old block is overwritten, the data in the old block will be read and written to the temporary snapshot space; similar to COW;
- **When backing up, the temporary snapshot area will occupy twice the space;**
    - Processing should be done during initialization, so when reading CBT, you need to evaluate the storage pool capacity, or appropriately adjust the storage pool over-resolution rate to avoid backup task failure due to capacity calculation problems.
- At this stage**virtual machines cannot create snapshots, backups and other tasks on the**

cloud platform at the same time. If snapshots and backup tasks are created, they will be intercepted by NexaVM.

3. disable cbt task: stop block job; delete temporary space and recycle nbd;
4. delete cbt task: Clear all records.

Necessary conditions for the source

1. **The source host must be powered on. **
2. Enable VirtIO on the transit data gateway (source side).
    - Only the Linux version of the data gateway can be used as the source data gateway.
3. The management console and the transfer data gateway (source end) must communicate with the 8080 port of all management nodes (including VIP) of the source end NexaVM.
4. The management console and the transfer data gateway (source end) must communicate with the NBD port 10501 of all management nodes (including VIP) of the source end NexaVM.
5. The transit data gateway (source) needs to be in the same cluster as the source host.
6. The transit data gateway (source) needs to be able to access the storage where the source host disk is located.
7. On the same computing node of NexaVM, 5 tasks are parallelized by default.
    - If you need to modify the parallel number, please contact NexaVM second line or R&D.

The user does not allow the source to release port 20005

Document Category: Product Related Experience

Solution

You can register using HTTPS.

Operation steps

Refer to the operating experience knowledge base "Registering the source host to the management console using HTTPS".

Some pages on the management console cannot be saved or submitted

Document Category: Product Related Experience

Problem description

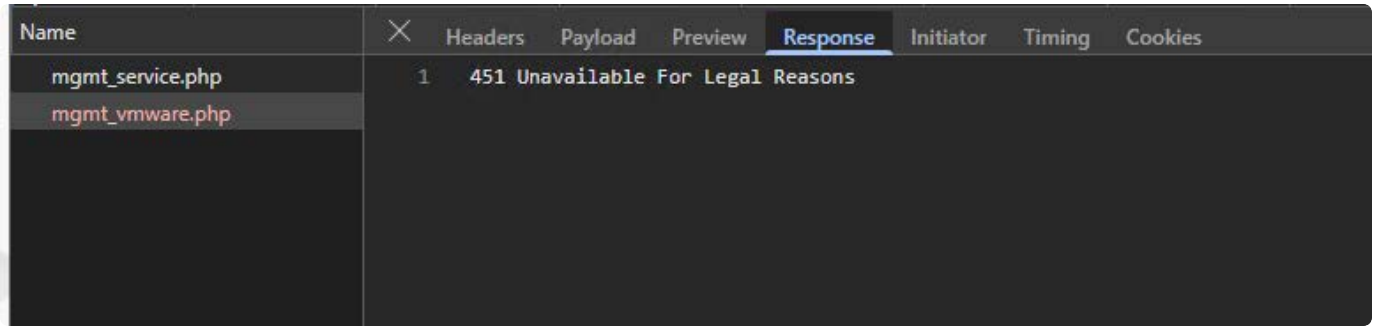
Some pages in the management console cannot be saved or submitted. It may be that there is no response when clicking the button, or it may be stuck after clicking the button.

Problem analysis

It may be that the input box and password box on the current page contain `< `>` '' characters.

Security protection is implemented at the software level. In order to avoid the risk of injection, these injection-related high-risk characters will be intercepted, so it cannot be saved or submitted.

When the management console is ⩾ version 677, you can see a 451 error using the browser's developer tools.



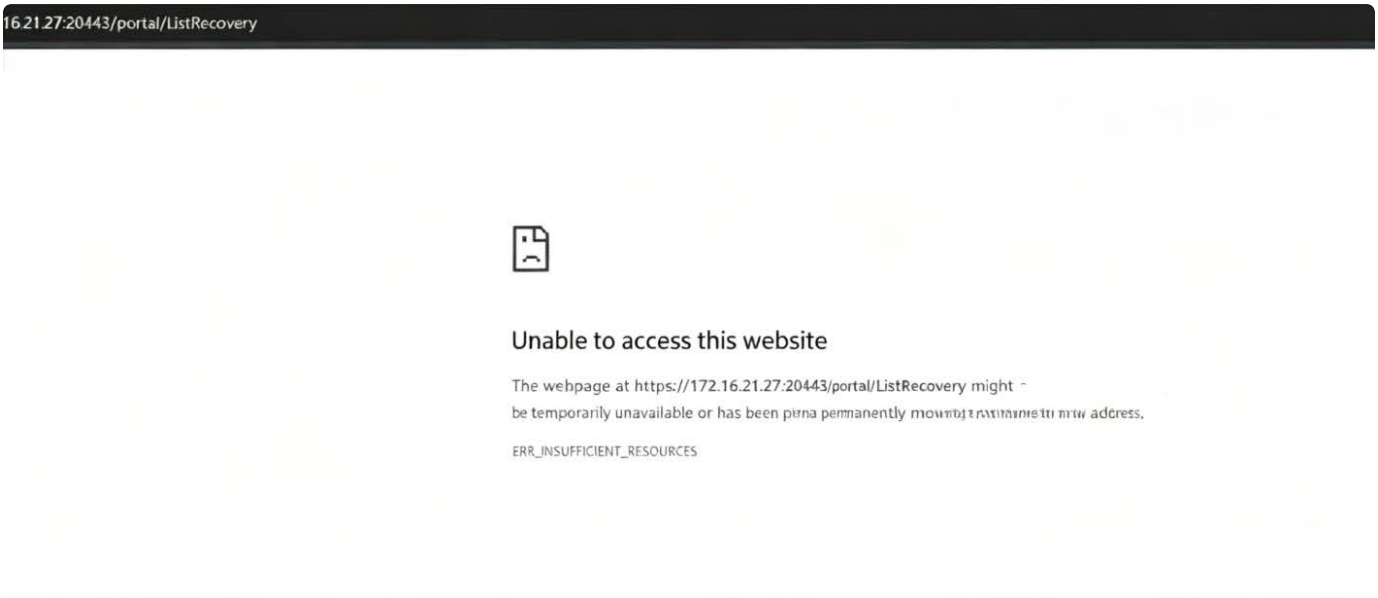
solution

Please avoid text boxes and passwords containing <``>``'' characters.

Cannot Access The Management Console

Document Category: Product Related Experience

Error screenshot



Problem analysis

Google Chrome bug problem.

Solution

Replace with Firefox or Microsoft Edge browser.

Brief description of license validity and expiration dates

Document Category: Product Related Experience

> For more information on licensing, especially licensing for disaster recovery environments, please view the training PPT.

License Overview

License Structure: Key + Credits + Time

- Key: A unique license string (e.g., 8SFZEZP11X9M32H74QXGBEKJN).
- Credits :

Migration License	Each credit allows migration of 1 host.
Capacity License	1. Required if a single host's migrated disk size exceeds 5TB. 2. Each count refers to the available capacity; minimum 1TB to activate, 1GB per use. 3. Can only be paired with an official license (test licenses cannot increase capacity).

- Time:

Association Deadline	The license must be activated and used before this date.
Validity Period (Expiration Date)	1. Starts counting when a Protection process is created 2. Test License: Valid for 1 week. 3. Official License Valid for 2 Months. 4. If the Expiration Date is reached, an additional license is required to extend usage. 5. Multiple migrations of the same host do not consume additional licenses within the validity period.

License Type	Capacity Included	Validity Period
Test Migration	1 TB	1 Week
Migration	5 TB	2 Month
Capacity License	Based on license	According to the paired Migration Key

Migration and cutover process and suggestions

Document Category: Product Related Experience

Cutover process

In order to keep the migrated data as consistent as possible with the source host, please stop the business before the last increment.

1. Create an initial synchronization task.
2. Keep deltas in sync.
    - When creating a synchronization task, the default increment interval is 60 minutes, just keep automatic increment.
3. Confirm the cutover time.
4. Stop the business and stop the database if there is one.
5. Edit the synchronization task and turn off the replication interval.
    - Avoid automatically initiating increments and affecting the cutover plan.
6. Manually initiate an increment (the last increment in the plan).
7. Create a switching task.
8. Verify the business running status of the target host after the switch (must be done).

Related suggestions

1. After the cutover has just been completed, it is recommended not to shut down the source host first.
    - **Use disabling the network card instead of shutting down the source host**, confirm that everything is normal on the target, and then process the source host as needed.
2. After verifying that the business is normal, it is recommended to take a snapshot of the target machine after the cutover and keep it for a period of time.
3. If there is agent mode migration, it is recommended to uninstall the agent software in the target machine after the cutover is completed to avoid being the subject of suspicion when the system runs abnormally in the future.

Windows activation status after migration

Document Category: Third Party Related Experience

Key activated source machine

Generally, the source machine where the key is activated will still be activated after migration.

If it is not activated, you generally need to contact the cloud platform for processing.

KMS activated source machine

The source machine for KMS activation needs to be reactivated using KMS after migration.

Which ports need to be released?

Document Category: Product Related Experience

Source host (Antenna)

20005

Data Gateway (Treker)

20000, 20001, 20010, 20443

BootImage (Treker Lite)

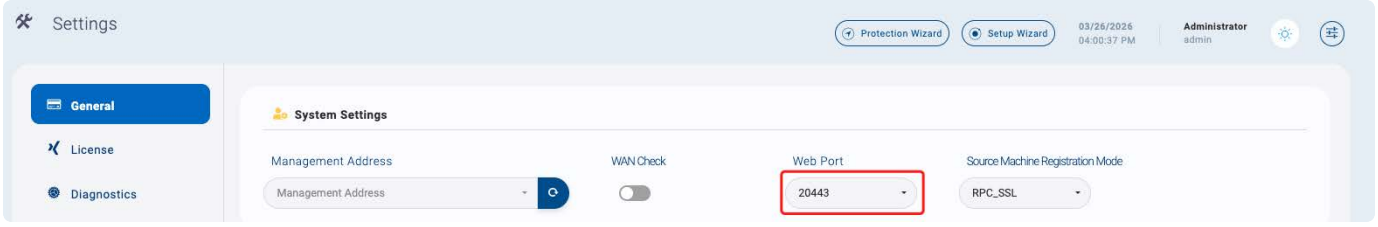
20000, 20001, 20010, 20443

Data Gateway (Management Console)

> When installing Treker, check Management to use this data gateway as the management console.
>
> Among them, 50022 and 3389 are the operating systems used to remotely log in to the management console.

20000, 20001, 20010, 20443, 50022, 3389

Needs to change the central control port of the management console from 443 to 20443.



VMware

> When adding vCenter to Management, 443 and 902 of vCenter and ESXi must be allowed.

443,902

NexaVM

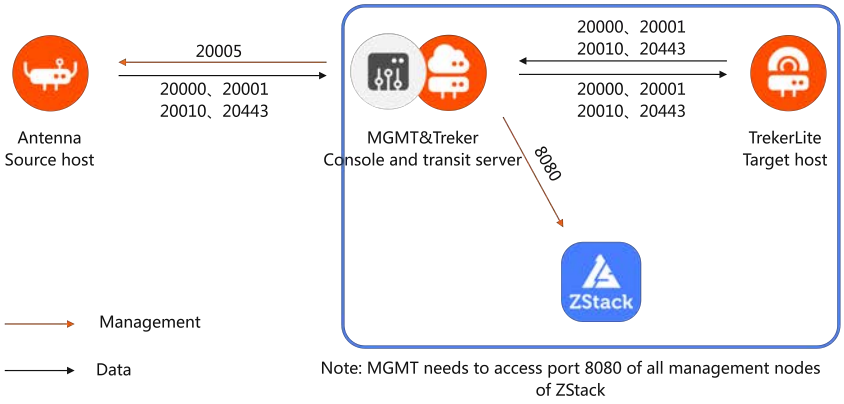
>

8080

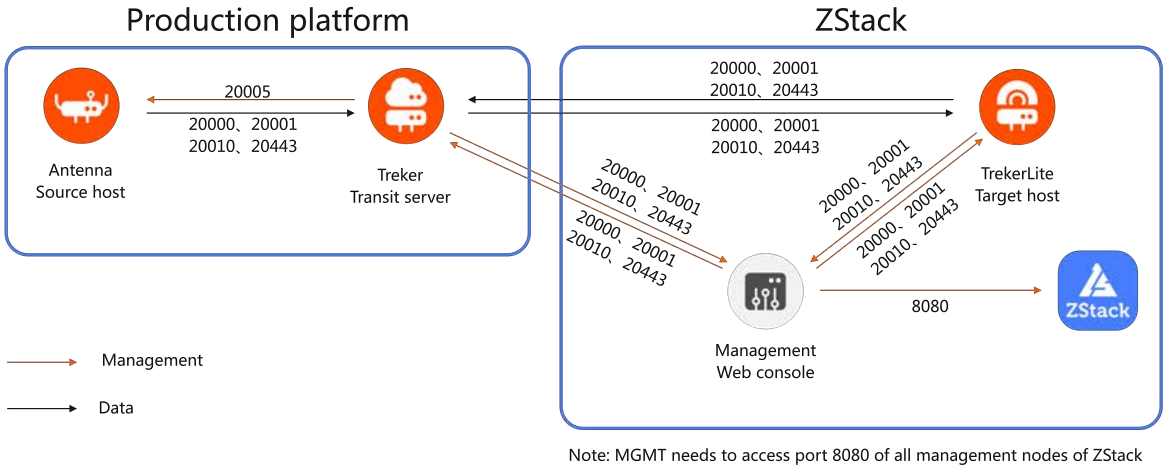
Port release diagram

Agent to NexaVM (reuse management console, not recommended)

> When there are many concurrent migration tasks, the management console and the transit Treker should be separated as much as possible.
>
> The release ports of the transit Treker and the management console are consistent.



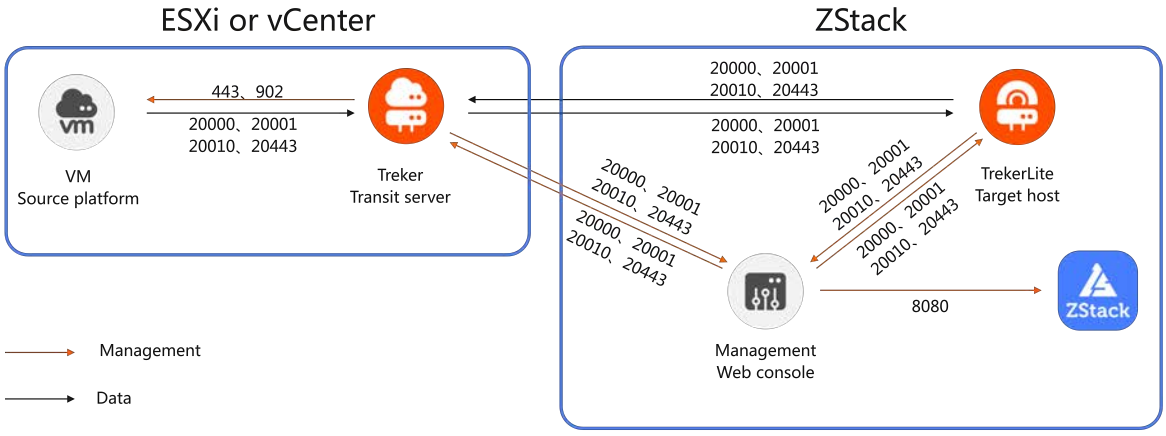
Agent to NexaVM (independent management console, recommended)



Note: MGMT needs to access port 8080 of all management nodes of ZStack

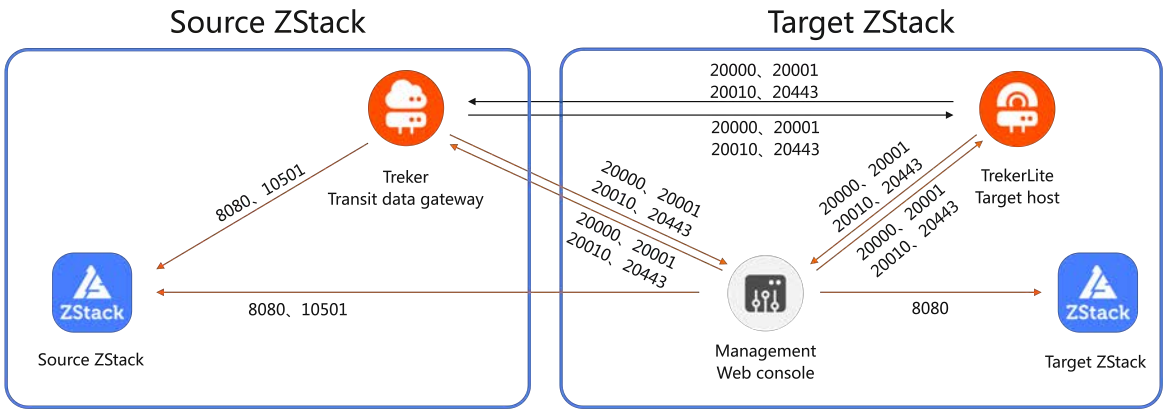
VMware agentless to NexaVM

> The agentless mode is more sensitive to the network, so the transit Treker should be deployed in ESXi as much as possible.



Note: MGMT needs to access port 8080 of all management nodes of ZStack

NexaVM proxyless to NexaVM



Note:
The management console needs to access port 8080 (including VIP) of all management nodes of all ZStacks;
The transit data gateway needs to access port 8080 (including VIP) of all management nodes of the source ZStack.

Source agentless CBT needs to use 10501, and 10501 can be ignored if CBT is not used.

Linux uses none-snapshot synchronization

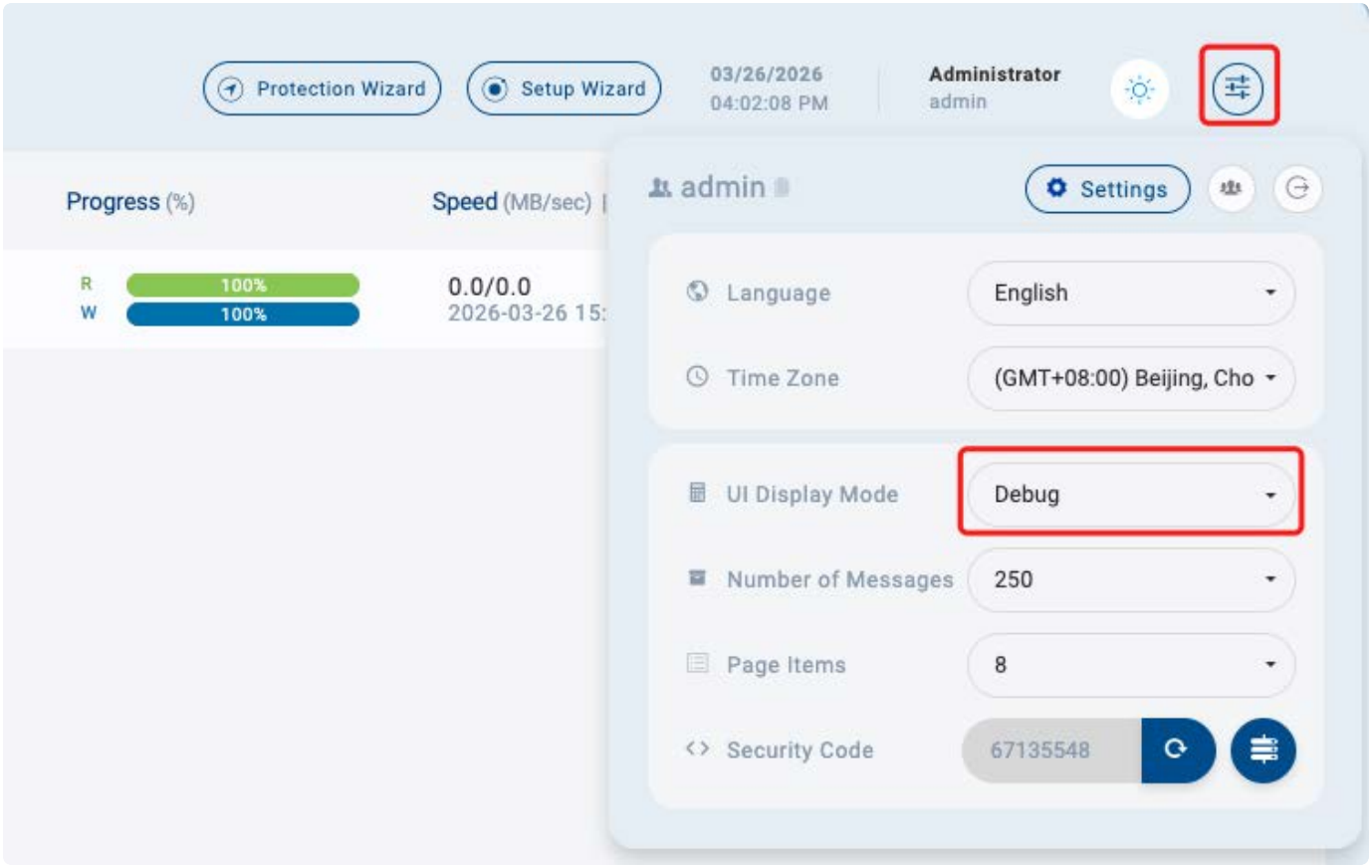
Document Category: Product Related Experience

Preconditions

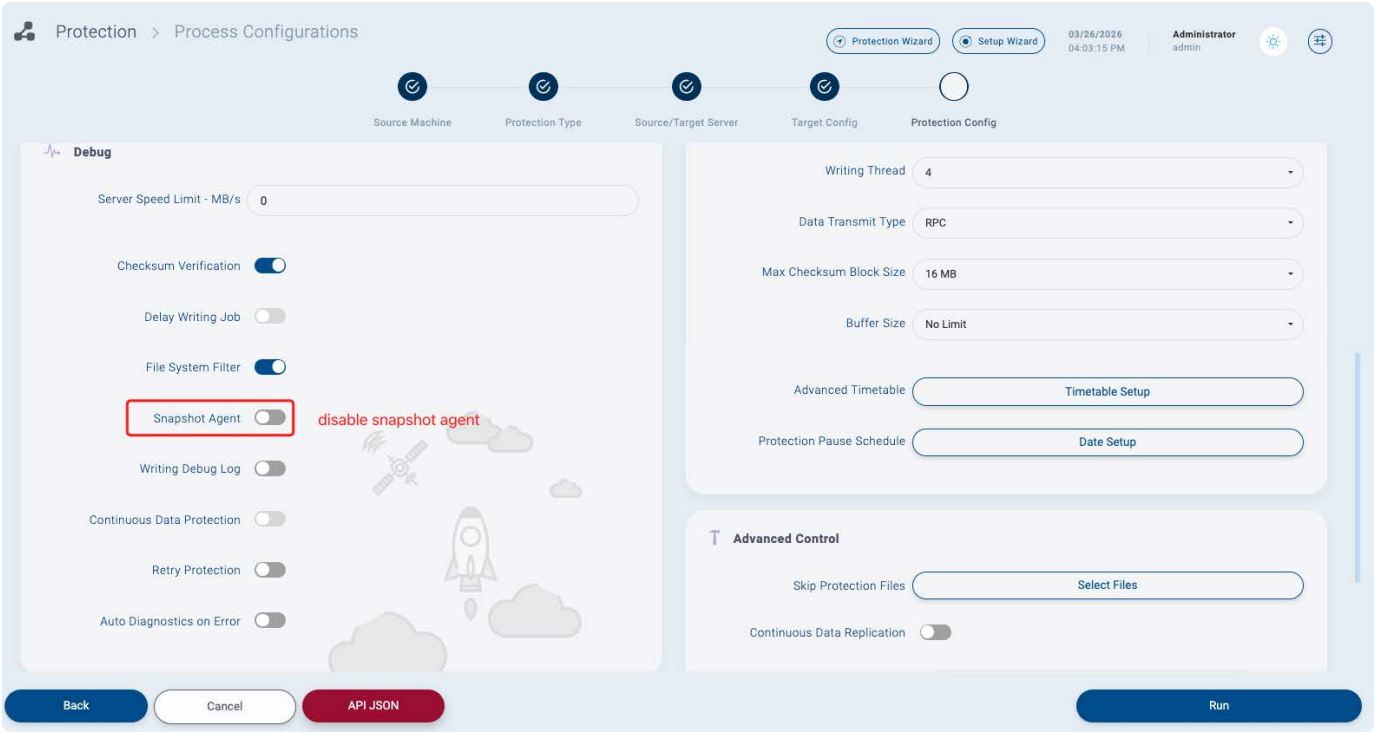
Use the Agent of **Antenna800 series**.

Operation steps

1. If the Antenna600 series has been installed, you need to uninstall the Antenna600 series and then install the Antenna800 series.
    - Uninstall and reinstall without restarting the system.
2. Register to the management console normally.
3. Change the configuration status of the management console to `Troubleshooting`.



4. Create a protection task and turn off `Snapshot Agent` in the task policy interface.

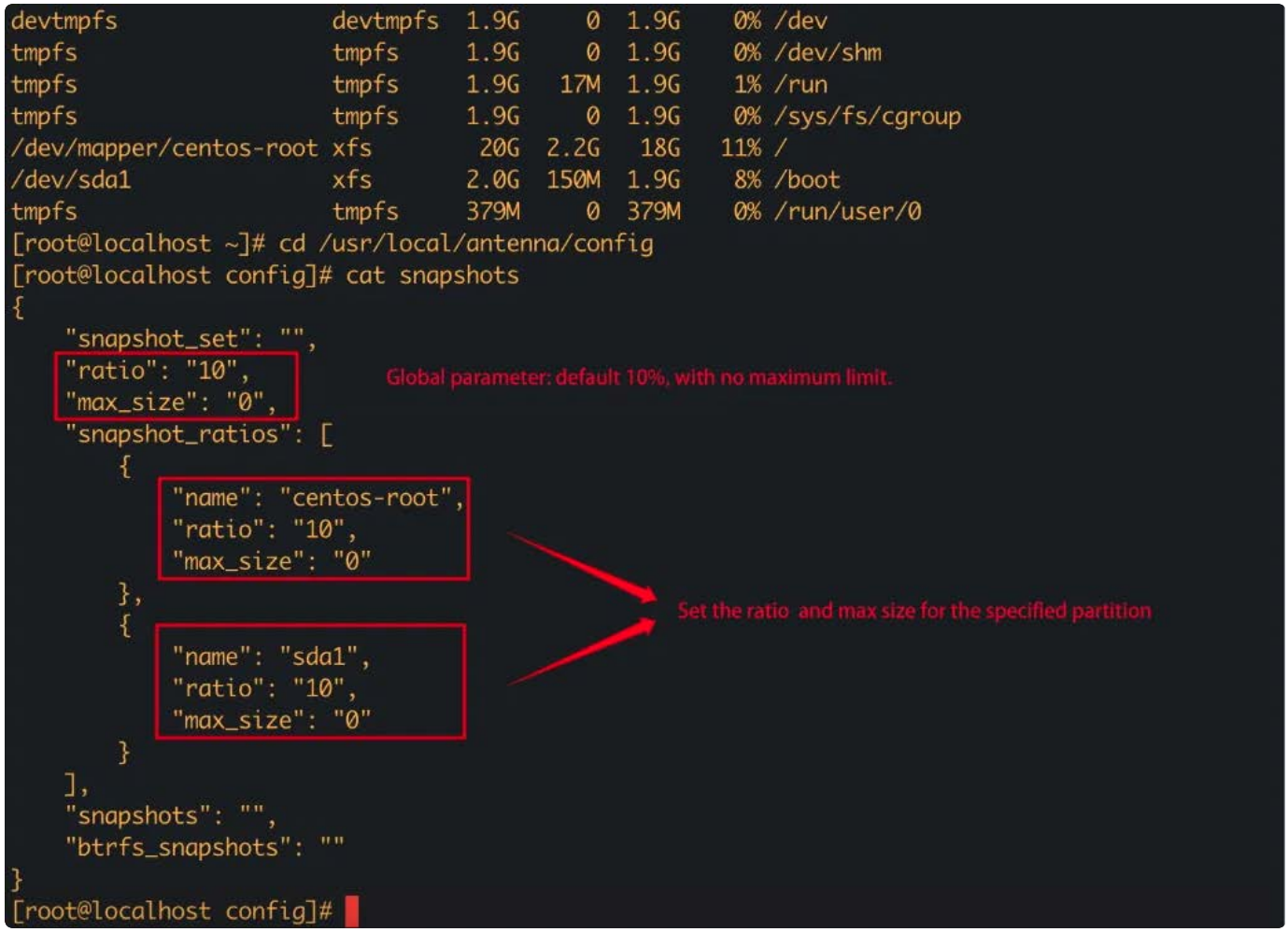


5. Just submit the task.

Linux modify ratio (snapshot size)

Document Category: Product Related Experience

Understanding snapshots files



- The value of ratio is a percentage, 10 means 10%.
- **Ratio modification principle:**
  - **Maximum ratio = mount point free space –1. **
    - **Example: The user's root directory is 92% used and 8% free. **
    - **Then the ratio of the root directory can be set to a maximum of 7 (8–1=7). **
- The unit of max_size is M, 0 means no limit, 500 means the maximum value of snapshot is 500M.
  - If the created snapshot is ⩾500M, limit snapshot=500M.

NEXAVM

- If the created snapshot is less than 500M, limit the snapshot to the actual value.

Calculate the maximum value of the ratio that can be set

Maximum ratio=mount point free space−1.

The root directory is 92% used and 8% of the space is used

The ratio of the root directory can be set to a maximum of 7, that is, 8−1=7.

97% of the home directory is used and 3% of the space is used

The maximum ratio of the home directory can be set to 2, that is, 3−1=2.

The data directory is 95% used and 5% of the space is occupied

The maximum ratio of the data directory can be set to 4, that is, 5−1=4.

The opt directory is 99% used and 1% free

99% of the opt directory is used. It is generally not recommended to use snapshot mode. It is recommended to use none−snapshot mode for synchronization.

Reference knowledge base "Linux uses none−snapshot synchronization"

Operation steps

> **Generally, you only need to modify the ratio of the corresponding partition, and there is no need to modify the max_size of the partition. **

NEXAVM

> **When max_size needs to be modified under special circumstances, Support will propose to modify max_size. **

```
#Check existing snapshots.
cat /proc/ltbd-info

#Clear existing snapshots.
cd /usr/local/antenna/
./antenna --erase

#Check existing snapshots again.
cat /proc/ltbd-info

#Modify the ratio configuration as needed; typically, it is sufficient to modify the ratio for the specified partition.
vi /usr/local/antenna/config/snapshots

#restart antenna
./antenna --restart

#Ratio modification confirmed successfully.
cat /usr/local/antenna/config/snapshots
```

NEXAVM

```
[root@localhost ~]# cat /proc/ltbd-info
{
        "version": "0.10.23",
        "devices": [
                {
                        "minor": 0,
                        "cow_file": "/.snapshot35",
                        "block_device": "/dev/sda1",
                        "max_cache": 314572800,
                        "fallocate": 213909504,
                        "seq_id": 36,
                        "uuid": "ac7cd80630e8427c8026378412481469",
                        "version": 1,
                        "nr_changed_blocks": 52,
                        "state": 2,
                        "ignore_errors": 0,
                        "cow_on_bdev": true
                },
                {
                        "minor": 1,
                        "cow_file": "/.snapshot35",
                        "block_device": "/dev/dm-0",
                        "max_cache": 314572800,
                        "fallocate": 2147483648,
                        "seq_id": 36,
                        "uuid": "a805eed801e84fe1a1999c1669791002",
                        "version": 1,
                        "nr_changed_blocks": 3227,
                        "state": 2,
                        "ignore_errors": 0,
                        "cow_on_bdev": true
                }
        ]
}
```

Output when snapshots exist.

```
[root@localhost ~]# cd /usr/local/antenna/
[root@localhost antenna]# ./antenna --erase
umount: /usr/local/antenna/lt1/: 未挂载
umount: /usr/local/antenna/lt0/: 未挂载
```

Output when clearing snapshots, there may be multiple 'lt' entries.

```
[root@localhost antenna]# cat /proc/ltbd-info
{
        "version": "0.10.23",
        "devices": [

        ]
}
```

Output when snapshot not exist.

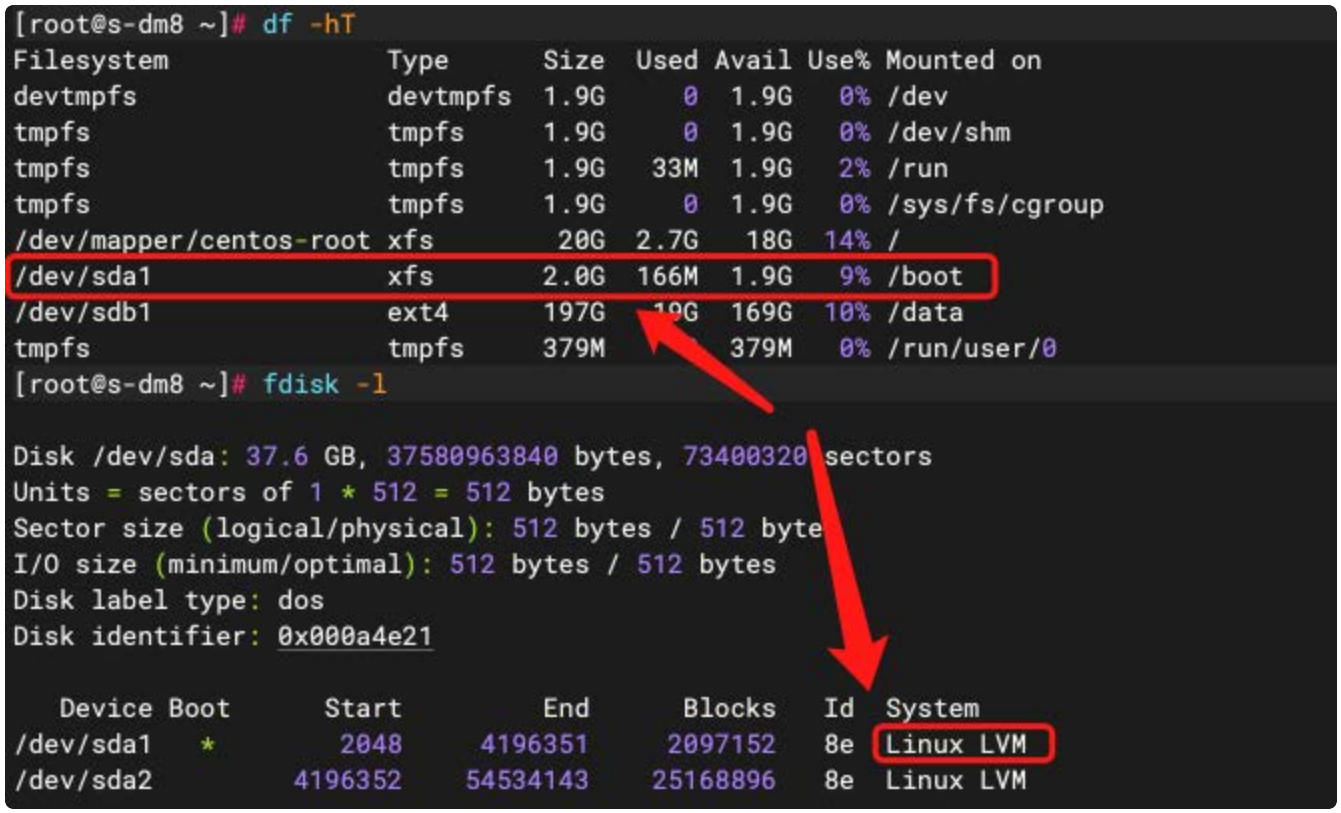
Modify partition type in Linux

Document Category: Third Party Related Experience

Applicable scenarios

When the disk configuration of the user's source machine is incorrect and the standard partition of the disk is recognized as LVM, this method can be used to modify it.

Screenshot example



Operation steps

> Taking sda1 as an example, change Linux LVM to Linux.

NEXAVM

```
fdisk /dev/sda

#print the partition table
Command (m for help): p

#View command help
Command (m for help):m

#change a partition's system id
Command (m for help):t

#select partition number
Partition number (1,2, default 2): 1

#list all hex codes
Hex code (type L to list all codes): L

#input hex code
Hex code (type L to list all codes): 83

#print the partition table
Command (m for help): p

#save
Command (m for help): w
```

NEXAVM

```
[root@s-dm8 ~]# fdisk /dev/sda
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.


Command (m for help): p

Disk /dev/sda: 37.6 GB, 37580963840 bytes, 73400320 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000a4e21

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048     4196351     2097152   8e  Linux LVM
/dev/sda2         4196352    54534143    25168896   8e  Linux LVM

Command (m for help): t
Partition number (1,2, default 2): 1
Hex code (type L to list all codes): L
```

NEXAVM

```
 0  Empty           24  NEC DOS         81  Minix / old Lin bf  Solaris
 1  FAT12           27  Hidden NTFS Win 82  Linux swap / So c1  DRDOS/sec (FAT-
 2  XENIX root      39  Plan 9          83  Linux           c4  DRDOS/sec (FAT-
 3  XENIX usr       3c  PartitionMagic  84  OS/2 hidden C:  c6  DRDOS/sec (FAT-
 4  FAT16 <32M      40  Venix 80286     85  Linux extended  c7  Syrinx
 5  Extended        41  PPC PReP Boot   86  NTFS volume set da  Non-FS data
 6  FAT16           42  SFS             87  NTFS volume set db  CP/M / CTOS / .
 7  HPFS/NTFS/exFAT 4d  QNX4.x          88  Linux plaintext de  Dell Utility
 8  AIX             4e  QNX4.x 2nd part 8e  Linux LVM       df  BootIt
 9  AIX bootable    4f  QNX4.x 3rd part 93  Amoeba          e1  DOS access
 a  OS/2 Boot Manag 50  OnTrack DM      94  Amoeba BBT      e3  DOS R/O
 b  W95 FAT32       51  OnTrack DM6 Aux 9f  BSD/OS          e4  SpeedStor
 c  W95 FAT32 (LBA) 52  CP/M            a0  IBM Thinkpad hi eb  BeOS fs
 e  W95 FAT16 (LBA) 53  OnTrack DM6 Aux a5  FreeBSD         ee  GPT
 f  W95 Ext'd (LBA) 54  OnTrackDM6      a6  OpenBSD         ef  EFI (FAT-12/16/
10  OPUS            55  EZ-Drive        a7  NeXTSTEP        f0  Linux/PA-RISC b
11  Hidden FAT12    56  Golden Bow      a8  Darwin UFS      f1  SpeedStor
12  Compaq diagnost 5c  Priam Edisk     a9  NetBSD          f4  SpeedStor
14  Hidden FAT16 <3 61  SpeedStor       ab  Darwin boot     f2  DOS secondary
16  Hidden FAT16    63  GNU HURD or Sys af  HFS / HFS+      fb  VMware VMFS
17  Hidden HPFS/NTF 64  Novell Netware  b7  BSDI fs         fc  VMware VMKCORE
18  AST SmartSleep  65  Novell Netware  b8  BSDI swap       fd  Linux raid auto
1b  Hidden W95 FAT3 70  DiskSecure Mult bb  Boot Wizard hid fe  LANstep
1c  Hidden W95 FAT3 75  PC/IX           be  Solaris boot    ff  BBT
1e  Hidden W95 FAT1 80  Old Minix
Hex code (type L to list all codes): 83
Changed type of partition 'Linux LVM' to 'Linux'

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
```

```
Command (m for help): p

Disk /dev/sda: 37.6 GB, 37580963840 bytes, 73400320 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000a4e21

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048     4196351     2097152   83  Linux
/dev/sda2         4196352    54534143    25168896   8e  Linux LVM

Command (m for help):
```

Turn on drop cache in Linux to alleviate 95% memory usage problem

Document Category: Product Related Experience

Applicable version

Only supports Antenna600 series.

Impact of turning on Drop cache

Positive Impact

- **RELEASE MEMORY**: Cleaning the page cache frees the memory occupied by the cache, making it available for other processes or system needs. This may help relieve memory pressure in situations where memory resources are tight.

Negative Impact

- **Performance degradation**:
  - **File reading speed slows down**: Because the page cache is cleared, the system needs to re-read file data from the disk, resulting in a significant decrease in file access speed, especially when the same file is accessed frequently.
  - **Increase disk I/O**: More file reading operations require direct access to the disk, which increases the load on the disk and may cause the disk response time to become longer, especially in high-load environments.

Operation steps

1. Select the task and click Abort.
2. Execute the following 2 commands on the source host

NEXAVM

```
#turn on drop cache
touch /usr/local/antenna/drop_cache

#restart antenna
/usr/local/antenna/antenna --restart
```

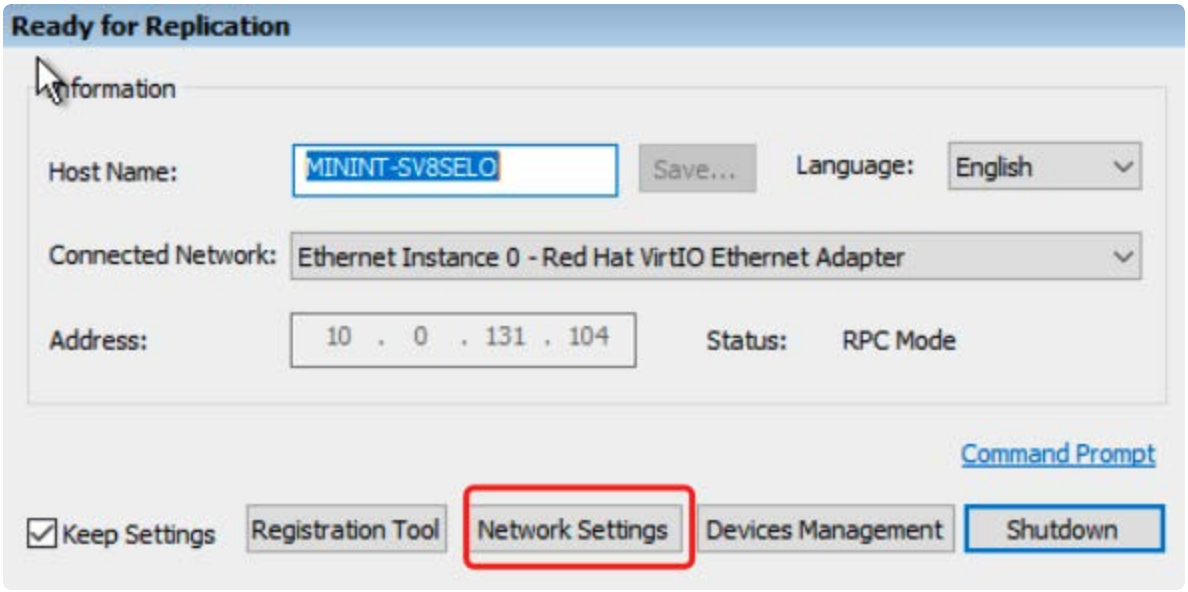
3. Initiate synchronization.

OfflineKit offline migration

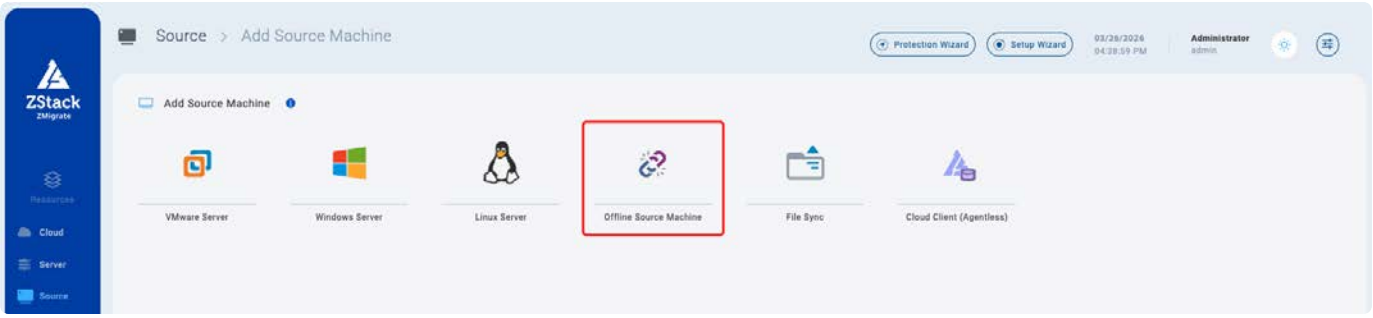
Document Category: Product Related Experience

Operation steps

1. Download OfflineKit.iso
2. Shut down the source host and use OfflineKit.iso to boot.
3. Configure the IP address (it can be the same as the IP address before shutdown, or it can be another available IP).



4. Add it to the source host in the management console and select "Offline Client" when adding.



5. Follow the same steps as using Antenna, just create synchronization tasks and switch tasks normally.

Notes

offlineKit offline migrationgenerally does not require increments. Cutover can be done after the initial copy is completed. Therefore, when creating a synchronization task, you can set the incremental copy interval to off.

SuSE10 agentless migration to NexaVM

Document Category: Product Related Experience

Execute Preload

1. The target machine turns on virtio.
2. Execute the Preload script.
   - Purpose: Modify fstab to UUID mounting, modify the device name of grub and other configurations, and add virtio driver.
3. Create protection tasks in agentless mode.
4. Create a provision task to skip system conversion.
5. Log into the system (no graphics at this time).
6. Fix graphics.
   - Refer to the knowledge base "Fixing the problem that graphics are not displayed after SuSE10 migration"
7. Configure IP address.
   - Try to configure on the graphical interface, command line configuration is a little troublesome.

Preload is not executed

1. The target machine Close virtio.
2. If possible, modify fstab to mount by UUID.
3. Create protection tasks in agentless mode.
4. Create a provision task to skip system conversion.
5. At this point it may be necessary to repair the target machine's configuration.
   - Change the source platform device name (such as sd*) to the target platform device name (such as vd*).
     - /etc/fstab (can be skipped if mounted with uuid)
     - /boot/grub/device.map

NEXAVM

        - /boot/grub/menu.list
    - Refer to the knowledge base "Repair SuSE10sp4 that cannot enter the system after migration"
6. Log into the system (no graphics at this time).
7. Fix graphics.
    - Refer to the knowledge base "Fixing the problem that graphics are not displayed after SuSE10 migration"
8. Configure IP address.
    - Try to configure on the graphical interface, command line configuration is a little troublesome.

VMware agentless does not use VMware CBT to synchronize data

Document Category: Product Related Experience

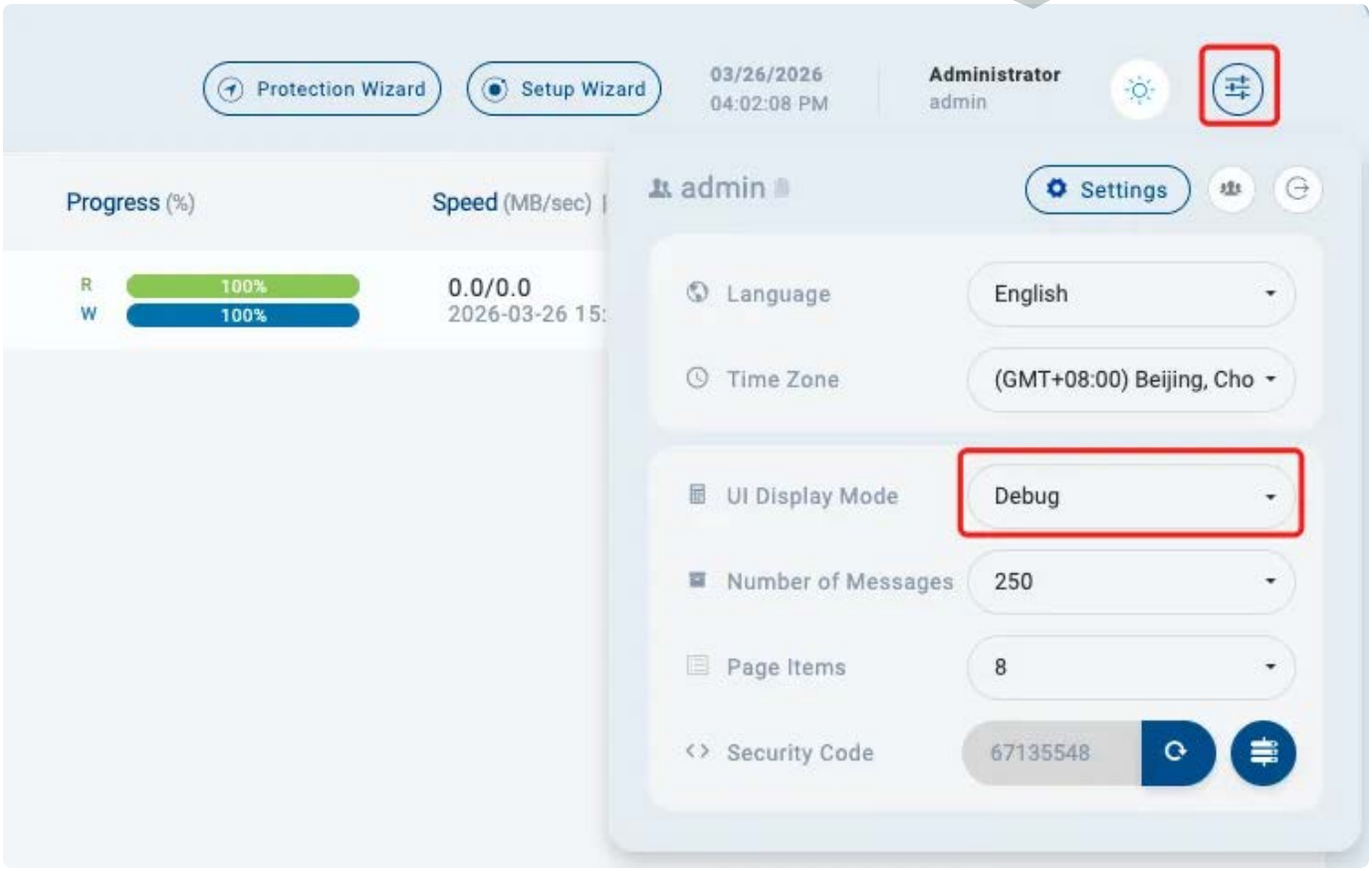
Applicable scenarios

CBT error/exception in VMware environment, user environment does not allow CBT to be reset.

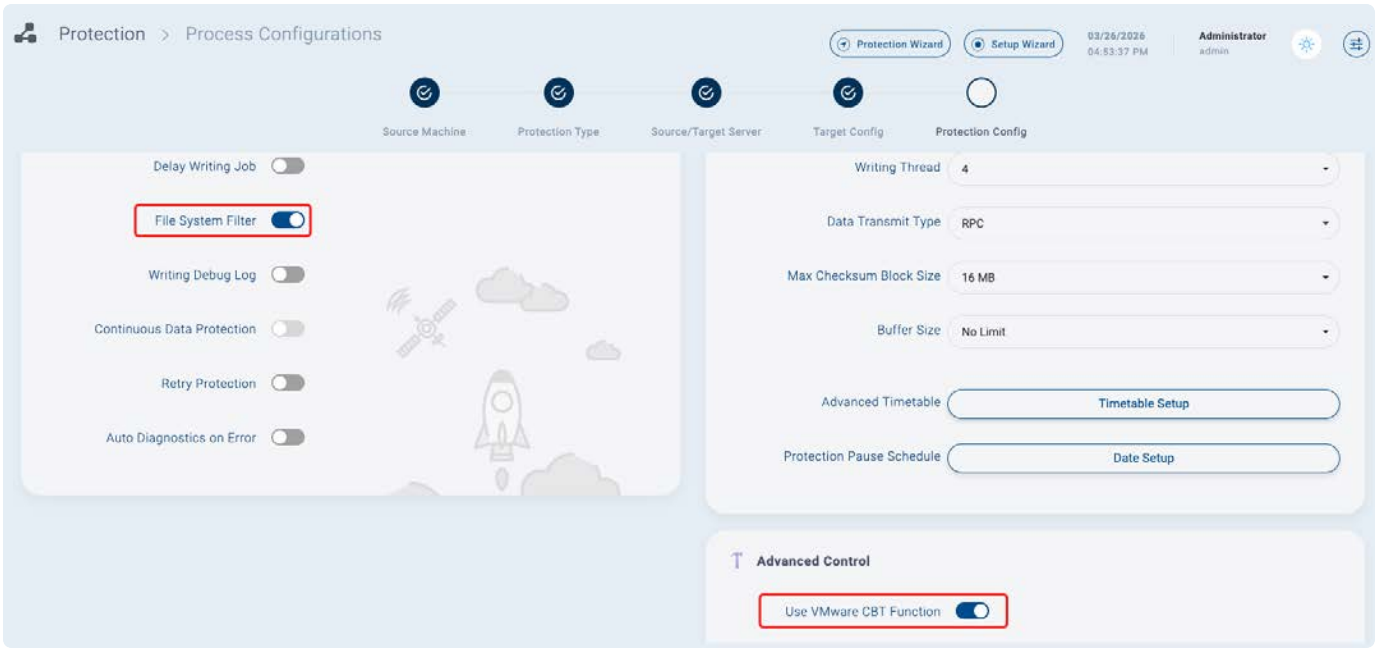
Specific manifestations include: failure to convert the switching task system, failure to boot normally after the switching task is completed, lv or partition loss after booting, etc.

Solution

1. Delete the switching task that has been created. If the switching task is deleted or there is no switching task, proceed to the next step.
2. Delete the synchronization task that has been created. If the synchronization task is deleted or there is no synchronization task, proceed to the next step.
3. Change the `configuration state` of the management console to `Troubleshooting`.



4. Create a synchronization task. On the licensing selection page, scroll down to find `Use VMware CBT function` and turn off this option.
    - [Optional] Turn off `File System Filter`. After turning it off, deleted files, virtual memory, etc. will not be filtered, and the synchronization time will be longer.



5. Submit the synchronization task and wait for the synchronization task to complete.

VMware agentless CBT related topics

Document Category: Product Related Experience

Version requirements

Management Console ⩾ (greater than or equal to) 637

Applicable scenarios

The source VMware has no agent and VMware CBT is wrong.

Introduction to CBT

Reference Links：Changed Block Tracking (CBT) on virtual machines

Changed Block Tracking (CBT) is a VMkernel feature that tracks changes to a virtual machine's storage blocks over time. The VMkernel tracks data block changes on virtual machines, thereby enhancing the backup process for applications developed to leverage VMware's vStorage API.

The backup appliance uses VMware API calls to request snapshot creation. VMware then takes the snapshot and renders it back for backup.

Changed Block Tracking (CBT) is a feature that identifies blocks of data that have been changed or are in use. It supports incremental backups to identify changes from the last backup, writing only the data blocks that have changed or are in use.

Problems caused by CBT errors

The changed block tracking configuration of one or more VM disks is incorrect, causing the switch task system conversion to fail, or the data disk to fail to mount properly.

VMware reset CBT

Refer to the knowledge base "VMware Reset CBT" and you need to shut down the source machine.

Don't want to shut down the source machine:

1. **When creating a new synchronization task, please refer to the Stability-prioritized synchronization task settings** chapter of this article. **

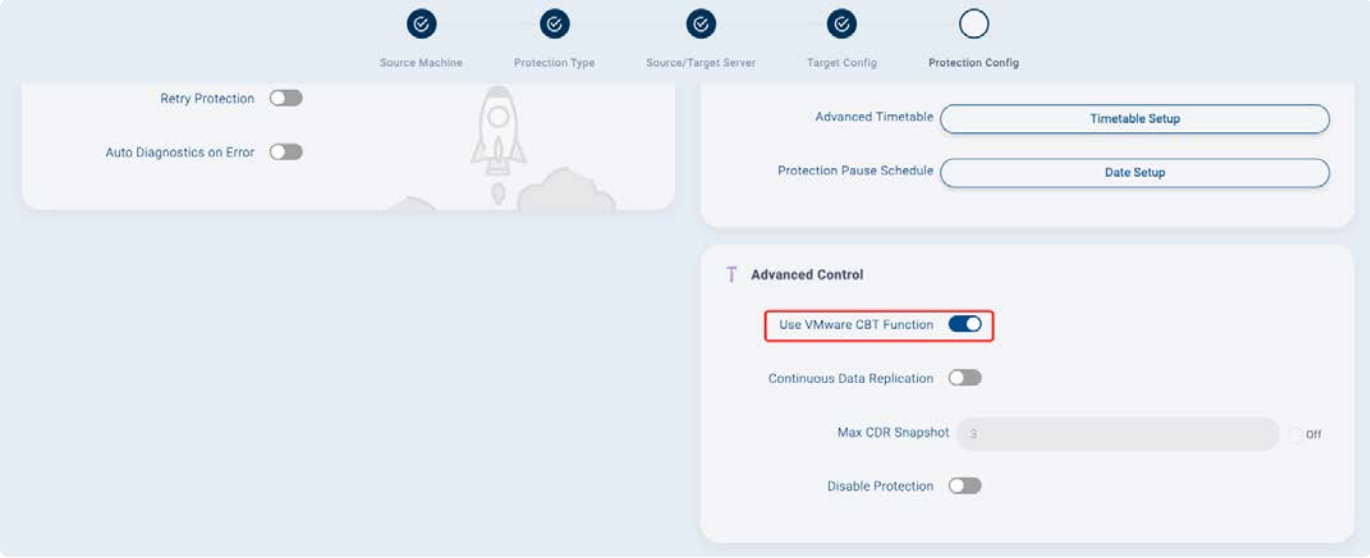
Introduction to CBT related functions

Due to the poor reliability of VMware CBT, during migration, you can choose whether to use CBT and whether to reset CBT.

Using the VMware CBT feature

Enabled by default.

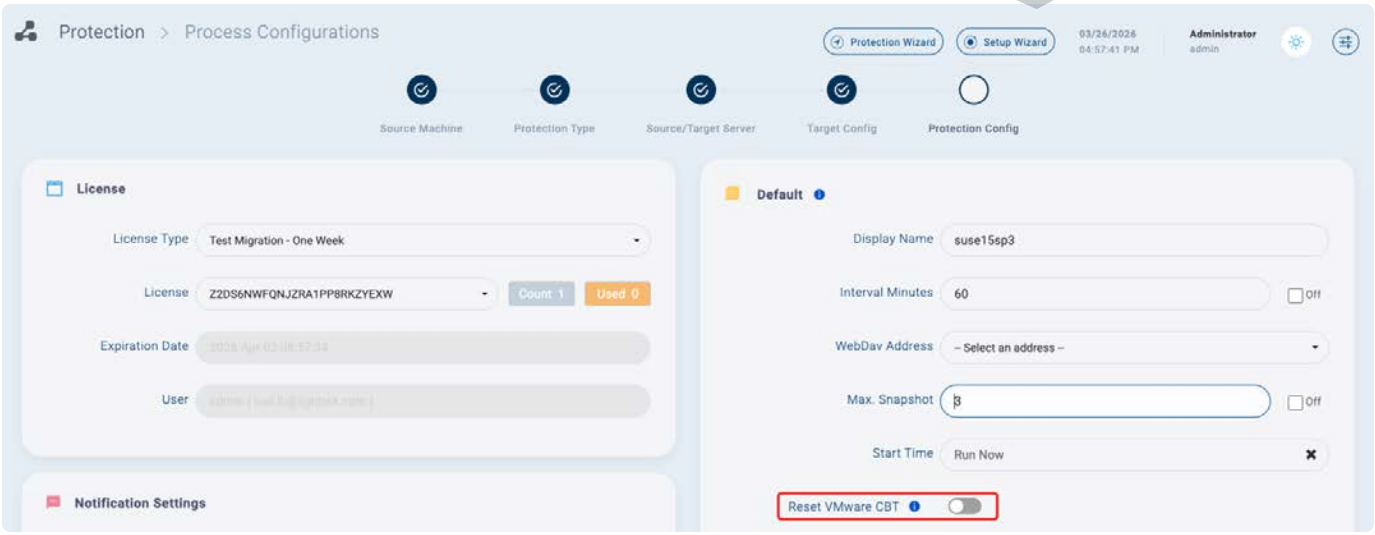
You need to change the configuration state to `Advanced` or `Troubleshooting` before you can see this parameter in `Advanced Control`.



Reset VMware CBT settings

Off by default.

In `Standard`, you need to expand more to see it.



Sync task settings

Synchronization task settings that prioritize efficiency (default)

Use VMware CBT feature: On.

- You need to change the configuration state to `Advanced` or `Troubleshooting` before you can see this parameter in the task policy `Advanced Control`.

Reset VMware CBT Settings: Close.

- In the mission strategy `Standard`, you need to expand more to see it.

Stable priority synchronization task settings

Use VMware CBT feature: Off.

- You need to change the configuration state to `Advanced` or `Troubleshooting` before you can see this parameter in the task policy `Advanced Control`.

Reset VMware CBT Settings: Close.

- In the mission strategy `Standard`, you need to expand more to see it.

NEXAVM

Efficiency priority setting solutions after CBT errors are discovered

Delete and recreate the synchronization task. The synchronization task uses the parameters of `synchronization task setting with stable priority'.

VMware reset CBT

Document Category: Third Party Related Experience

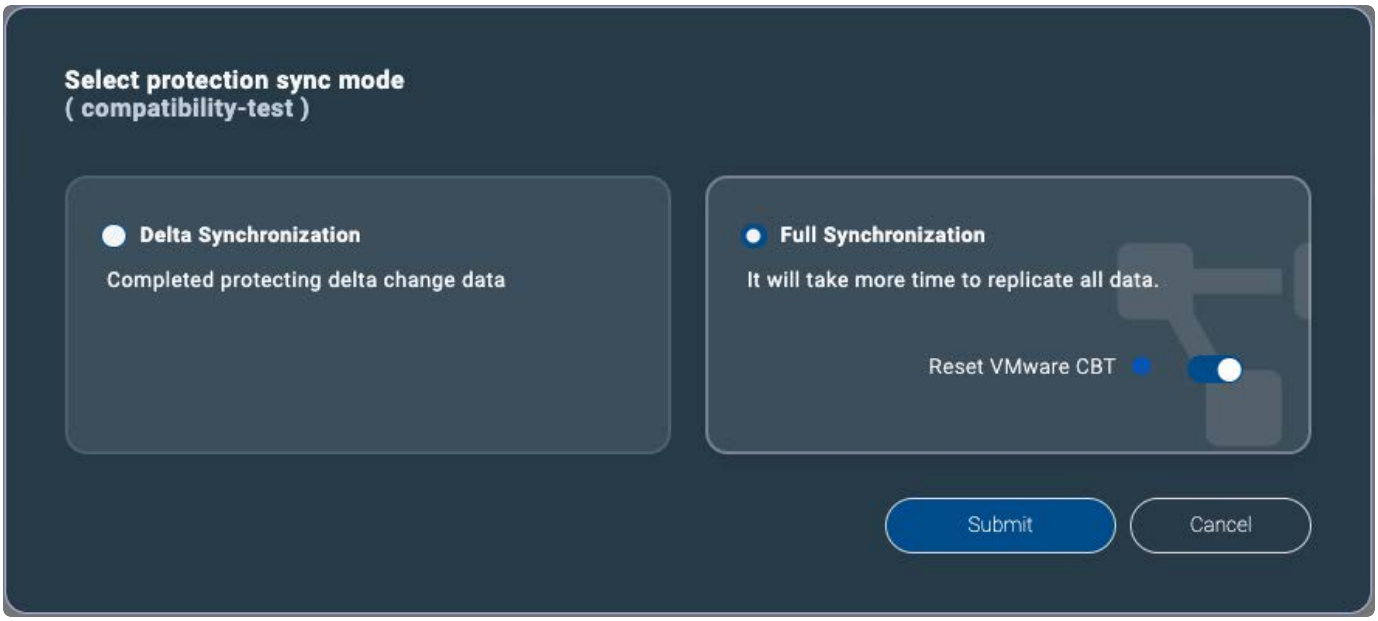
Applicable scenarios

VMware CBT is abnormal, CBT needs to be reset, and the source host does not have a VMware snapshot.

Management console reset CBT operation steps

> If it is detected that the source host has a snapshot on the VMware platform, this operation will skip the step of resetting CBT.

1. Select the synchronization task corresponding to "CBT error".
2. Click `Manual Sync`, select `Full Sync` and check `Reset VMware CBT Settings`.

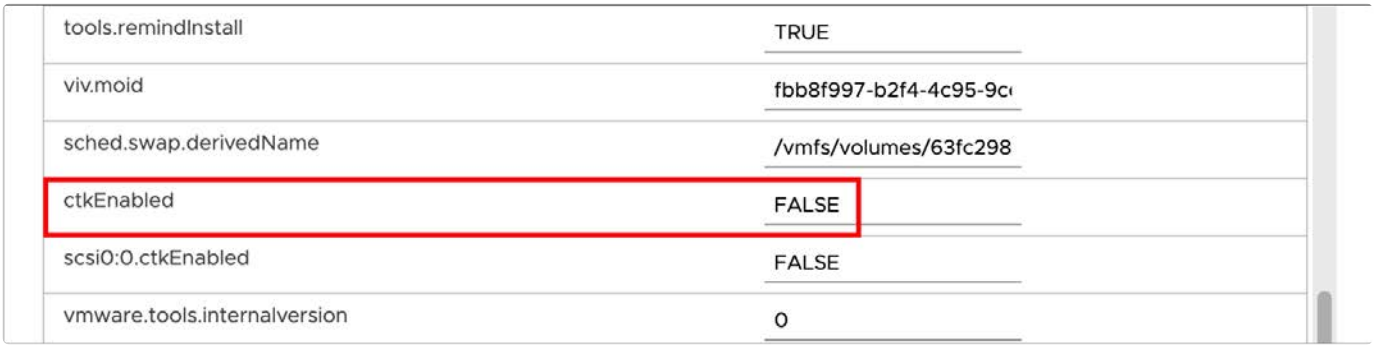


Manually reset CBT operation steps

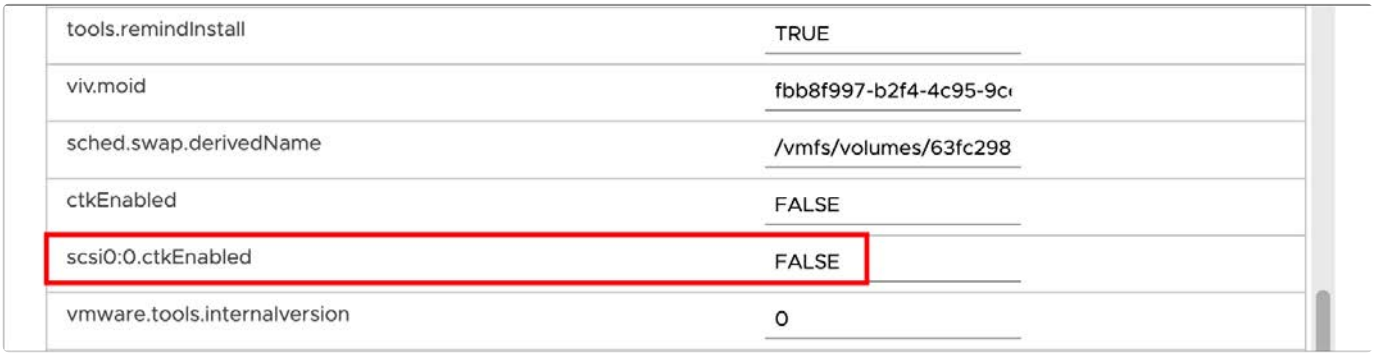
> VMware official document states that the prerequisite for resetting CBT is that the source host has not created a snapshot on VMware. Therefore, resetting CBT is not 100% successful when

> the source host has a snapshot.
>
> Based on project experience, the success rate of resetting CBT is about 90% when the source host has a snapshot.

1. Power off the virtual machine.
2. Right-click the virtual machine and click Edit Settings.
3. Click the Options tab.
4. Click General below the Advanced area, and then click Configuration Parameters. The Configuration Parameters dialog box opens.
5. Set the ctkEnabled parameter of the desired SCSI disk to false.



6. The scsi0:0.ctkEnabled parameter is set to false. **If there are multiple scsi:*.ctkEnabled, all need to be changed to false. **



7. Power on the virtual machine (shutdown migration can skip the power on step).
8. Click Synchronize in MGMT (**Select the second complete data copy**).

Reference link

https://cloudbase.it/vmware-vm-cbt-reset-guide/

https://knowledge.broadcom.com/external/article?legacyId=2139574

https://knowledge.broadcom.com/external/article/338480/changed-block-tracking-cbt.html

Windows partition (separate C drive) migration

Document Category: Product Related Experience

Notes

Windows currently only supports splitting the disk where C drive is located into C drive and other drives.

This solution is not suitable for source host agentless mode migration.

Example

before split

- disk0: C, D, E
- disk1: F, G
  +disk2:H

After split

> When copied, it will become 4 disks.

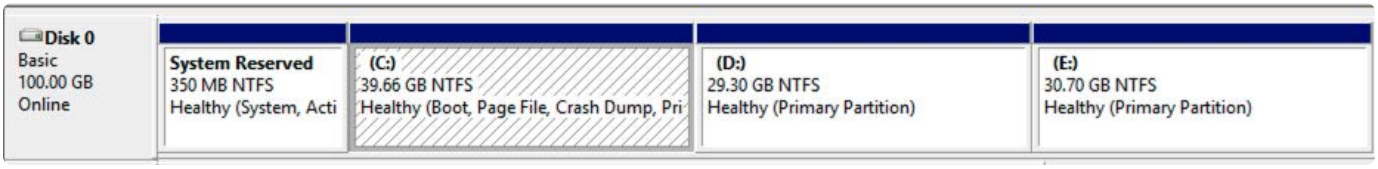
> It is only displayed as 4 disks on the management console, and system disk management is not affected.

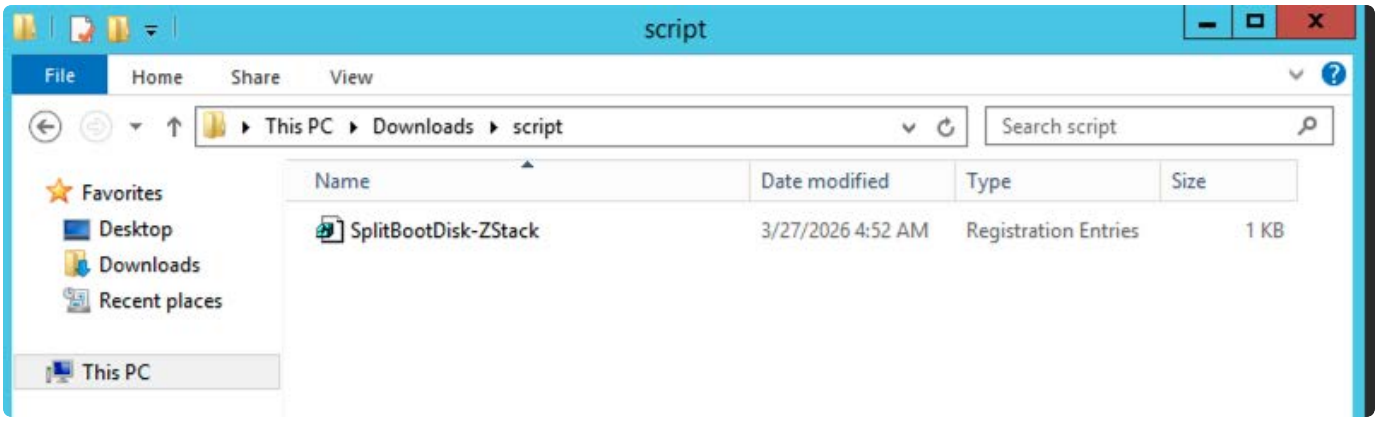
+disk0:C

- disk1: D, E
- disk2: F, G
  +disk3:H

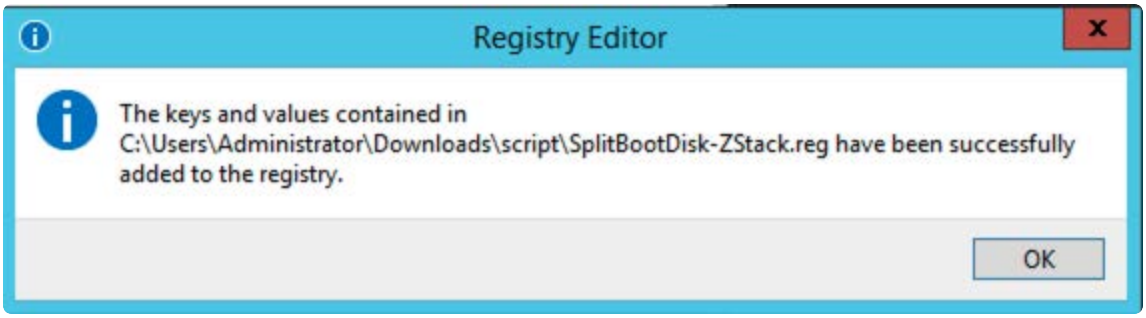
Operation

1. The source host installs Agent (Antenna) normally.
2. Execute the partition script (SplitBootDisk-ZStack.reg) on the source host.
    - It only makes the migration software recognize that the C drive is independent and does not modify the disk information of the source host.









3. Register to the management console and check the disk information of the source host on the management console.
    - If the source host has been added to the management console before, please delete it and add it again.
    - You can clearly see that the original disk 0 has been recognized as disk 0 (part1) and

disk 1 (part2).



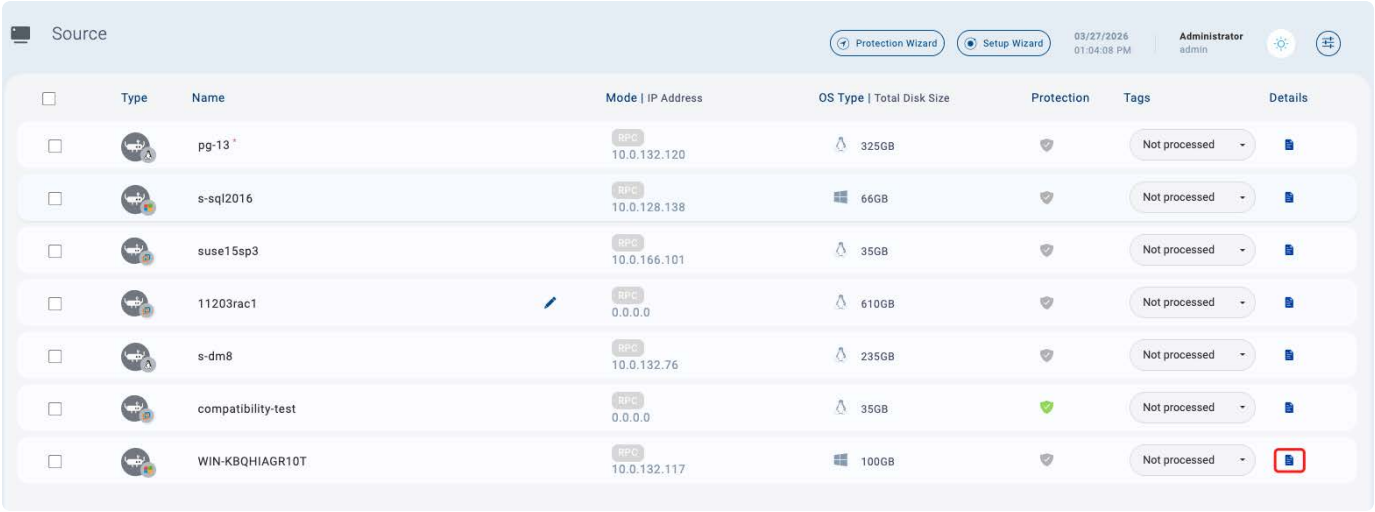
Disk size requirements

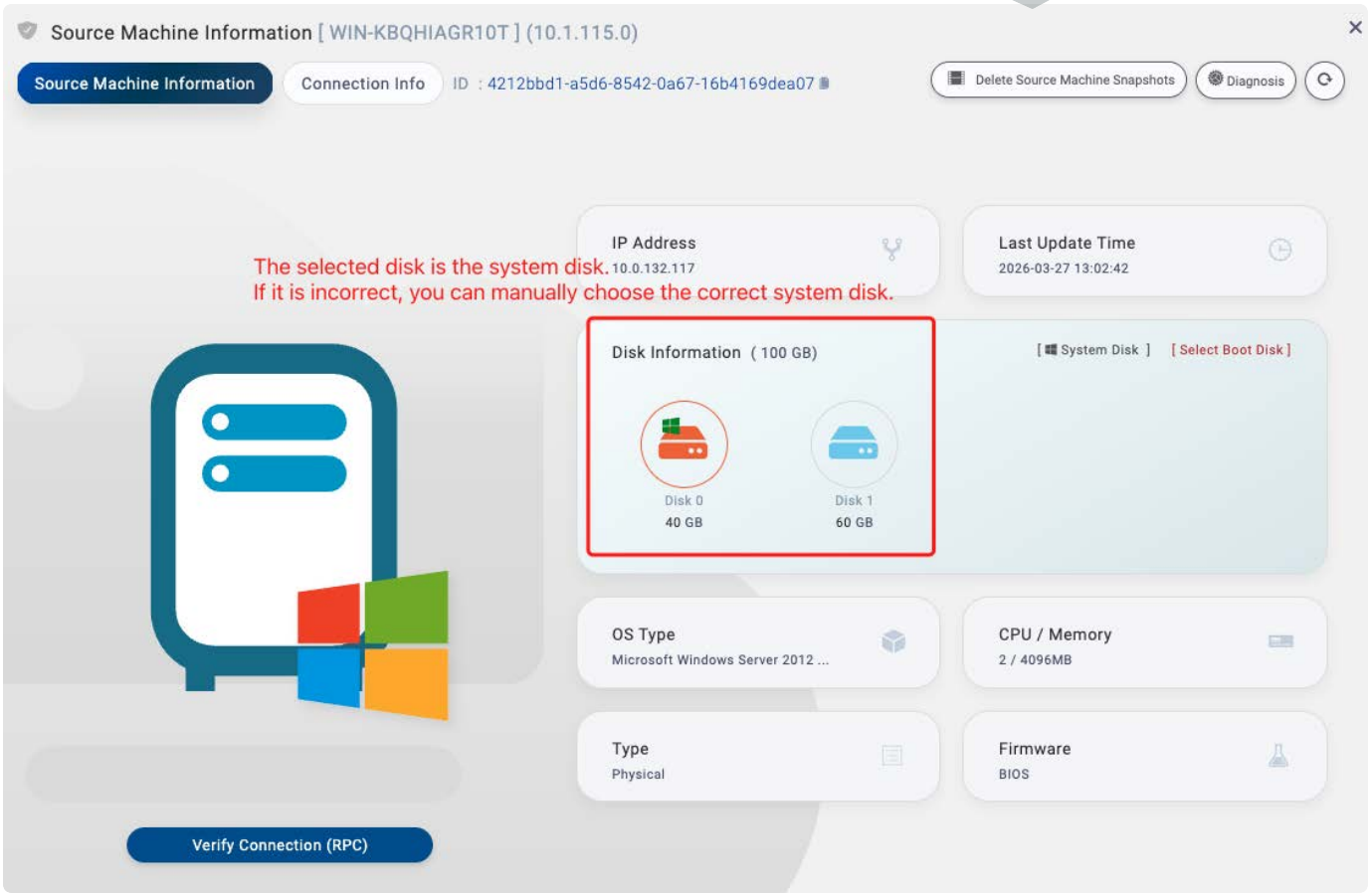
The API automatically creates the target machine, so there is no need to pay extra attention to the disk size.

In manual target mode, you need to pay attention to the disk size when creating the target machine.

- **The source machinesystem disk** is 100G, and the target machine size=100G+1G+5G=106G. **
- **The source machinedata disk** is 200G, and the target machine size=200G+1G=201G. **

The source machine disk size is subject to identification by the management console.

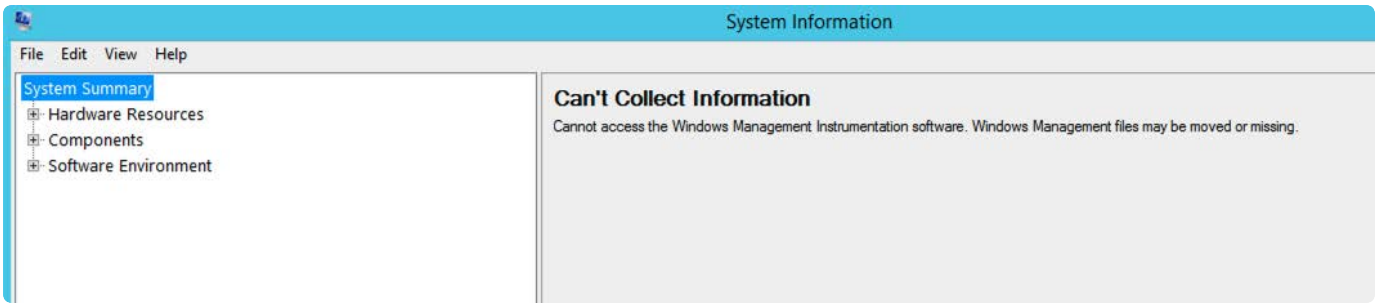



Source Machine Information [WIN-KBQHIAGR10T] (10.1.115.0)
Source Machine Information
Connection Info
ID : 4212bbd1-a5d6-8542-0a67-16b4169dea07
Delete Source Machine Snapshots
Diagnosis
IP Address
10.0.132.117
Last Update Time
2026-03-27 13:02:42
The selected disk is the system disk.
If it is incorrect, you can manually choose the correct system disk.
Disk Information (100 GB)
[System Disk]
[Select Boot Disk]
Disk 0
40 GB
Disk 1
60 GB
OS Type
Microsoft Windows Server 2012 ...
CPU / Memory
2 / 4096MB
Type
Physical
Firmware
BIOS
Verify Connection (RPC)

Windows source machine reports error when executing msinfo32

Document Category: Third Party Related Experience

Error screenshot



Problem analysis

WMI database corruption causes `msinfo32` error.

Operation steps

> Note: For reference only, please carefully evaluate whether to follow this method.

To resolve this issue, delete these files and then re-create them in the %SystemRoot%System32\Wbem\Repository folder. To do this, follow these steps:

1. Click Start, then right-click My Computer.
2. On the shortcut menu, click Manage.
3. In the left pane of the Computer Management console, double-click Services and Applications.
4. Under Services and Applications, click Services.
5. In the right pane of the Computer Management console, locate and right-click Windows Management Instrumentation.

NEXAVM

6. On the shortcut menu, click Stop.
7. Start Windows Explorer and locate the %SystemRoot%System32\Wbem\Repository folder.
8. Delete all files in the %SystemRoot%System32\Wbem\Repository folder.
9. Restart the computer.

When the computer restarts, the deleted files are recreated.

Note: The Windows Management Instrumentation service starts automatically when the computer is restarted.

Windows source machine uses partition script to migrate

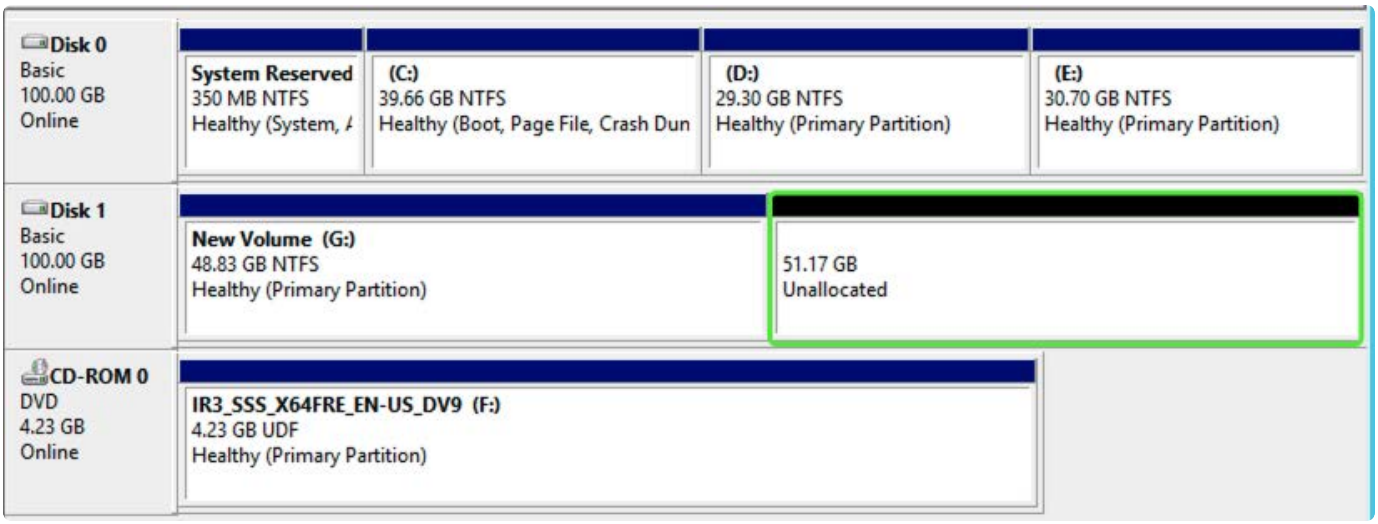
Document Category: Product Related Experience

Applicable scenarios

This solution is not suitable for source host agentless mode migration.

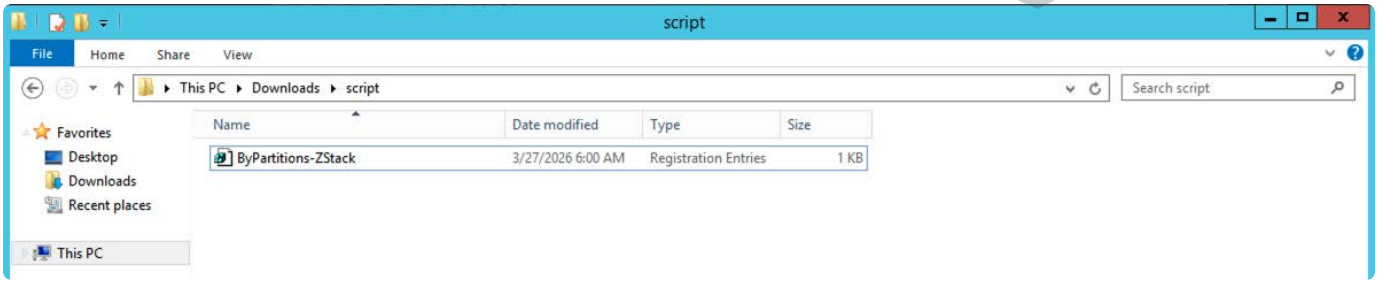
After the Windows source machine compresses the disk, there is **black unallocated space at the end.** Use this solution to migrate, **will not migrate the trailing black space to the target**.

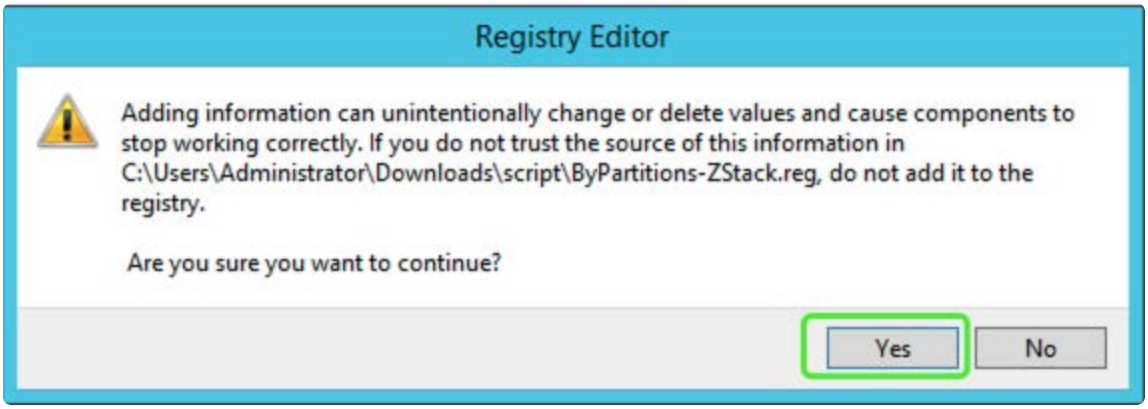
- Those selected by the green box will occupy the target disk space.

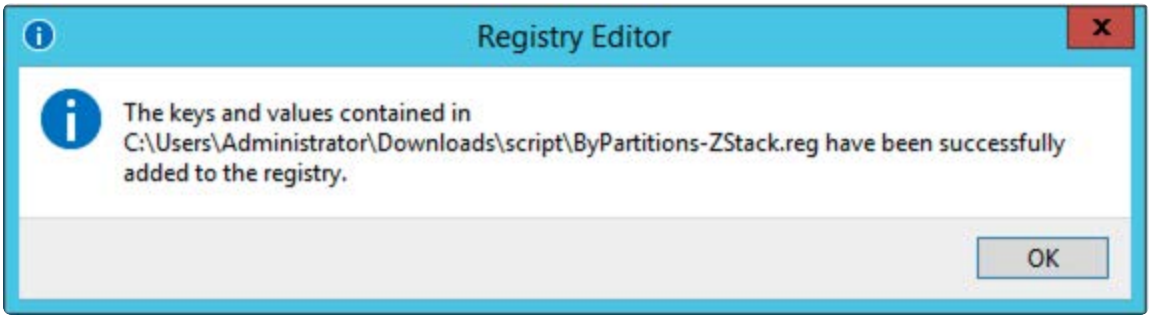


Operation steps

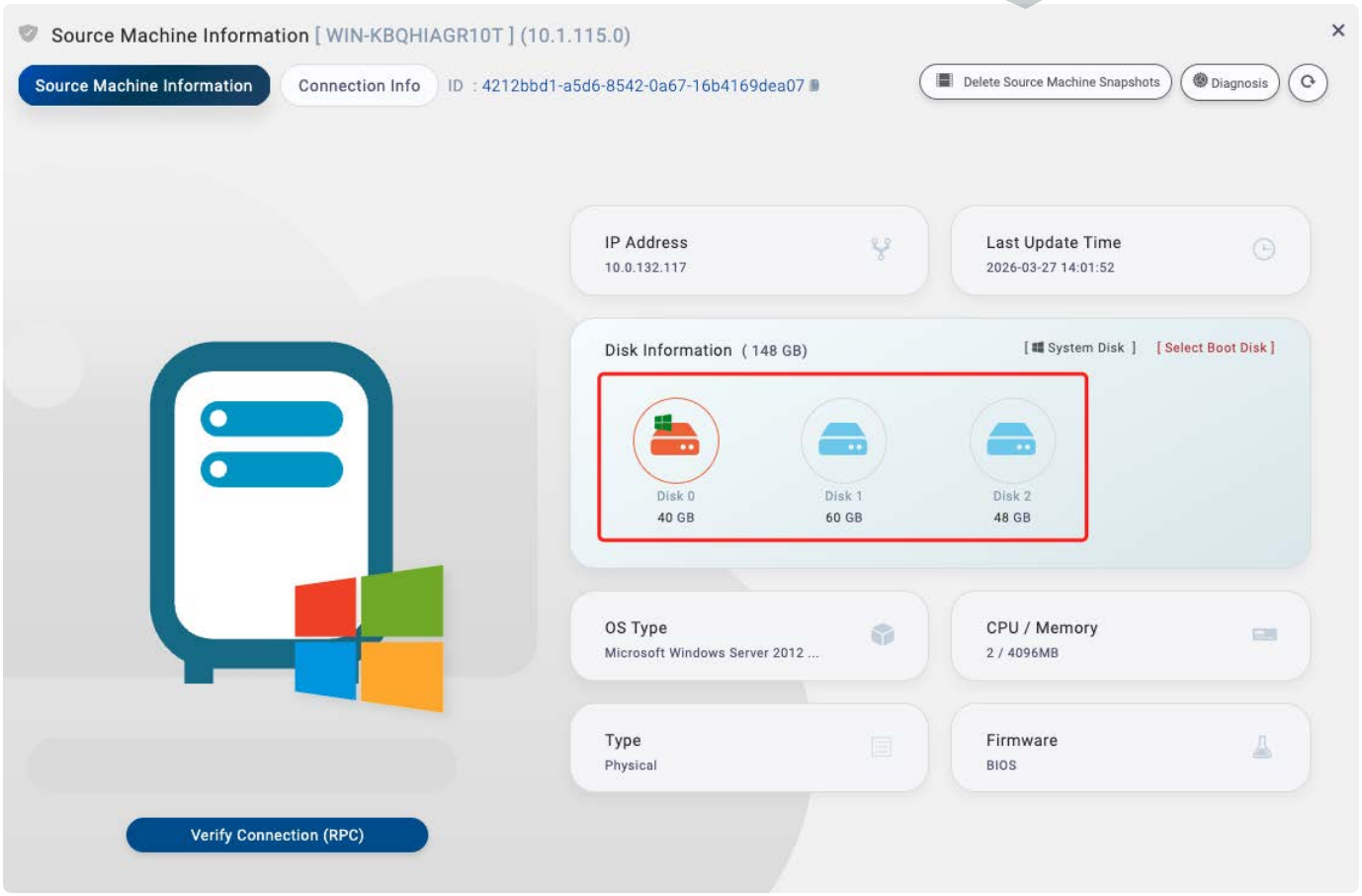
1. The source machine installs Agent (Antenna) normally.
2. Execute the partition script (ByPartitions–ZStack.reg) on the source host.



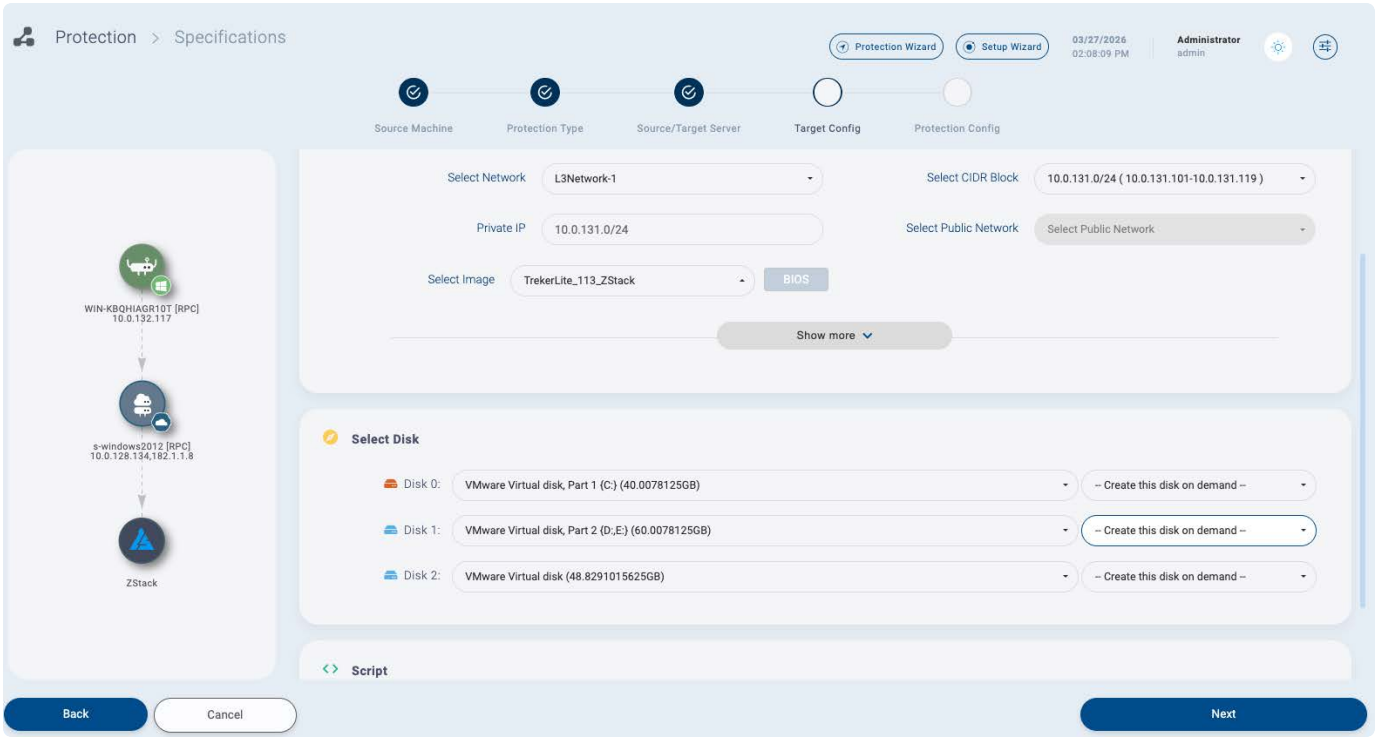




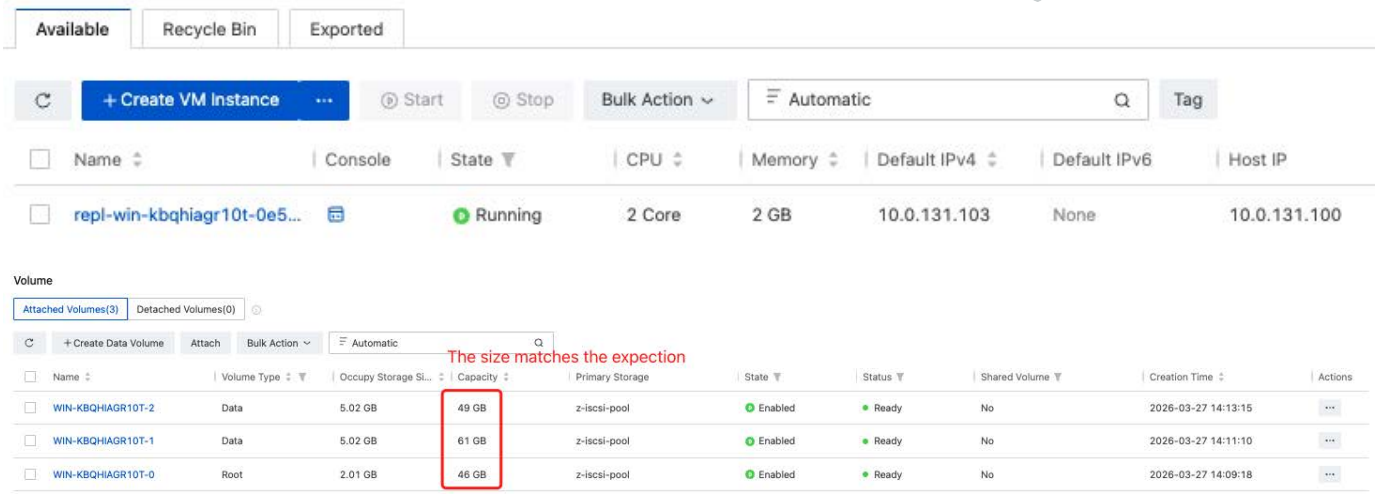
3. Register to the management console and check the disk information of the source host on the management console.
    - You can see that the disk is recognized to be the size minus the black part at the end.



4. Create the synchronization task normally and keep the "Create new cloud disk" option.



5. (Optional)After the target machine**is successfully booted**, you can check whether the disk size of the target machine is as expected.



6. Wait for the synchronization task to complete.
7. Just do the switch normally.

Disable target snapshots in NexaVM standard mode

Document Category: Product Related Experience

Applicable scenarios

1. The storage space of NexaVM is limited, and you do not want to take a snapshot of the target machine during the synchronization process.
2. The storage performance of NexaVM is poor, and taking snapshots takes too long. I don't want to take snapshots of the target machine.

Impact of disabling target snapshots

1. Disk snapshot testing cannot be used directly in the management console.
    - If you need to test and verify, you can refer to the knowledge base "Manual BootImage (TL) Mode for Verification Testing"
2. After the switch is completed, the target machine cannot roll back the snapshot to the state before the switch.
    - If you need to roll back, you can manually take a snapshot of the target machine before creating the switching task.

Knowledge points

**The snapshot strategy of the synchronization task and the snapshot strategy of the switching task are independent. **

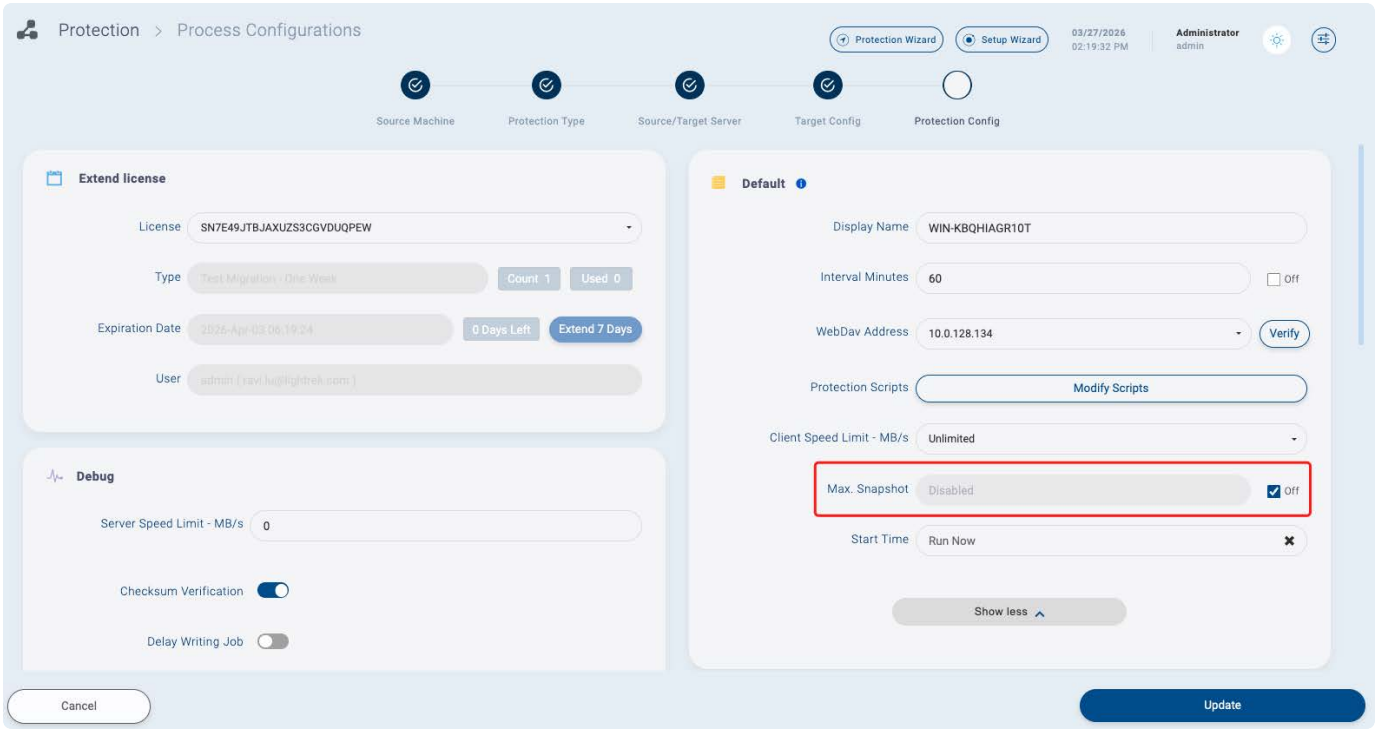
1. When the storage is `ceph type` or `ZStone type`, a snapshot will be created of the target machine according to the `number of copies` during synchronization.
    - If you don’t know about `number of copies`, you can refer to the knowledge base "Task Strategy Parameters".

2. When the storage is `non-ceph type` or `non-ZStone type`, only one snapshot will be created for the target machine during synchronization.

Operation steps

Disable synchronization tasks to create target machine snapshots

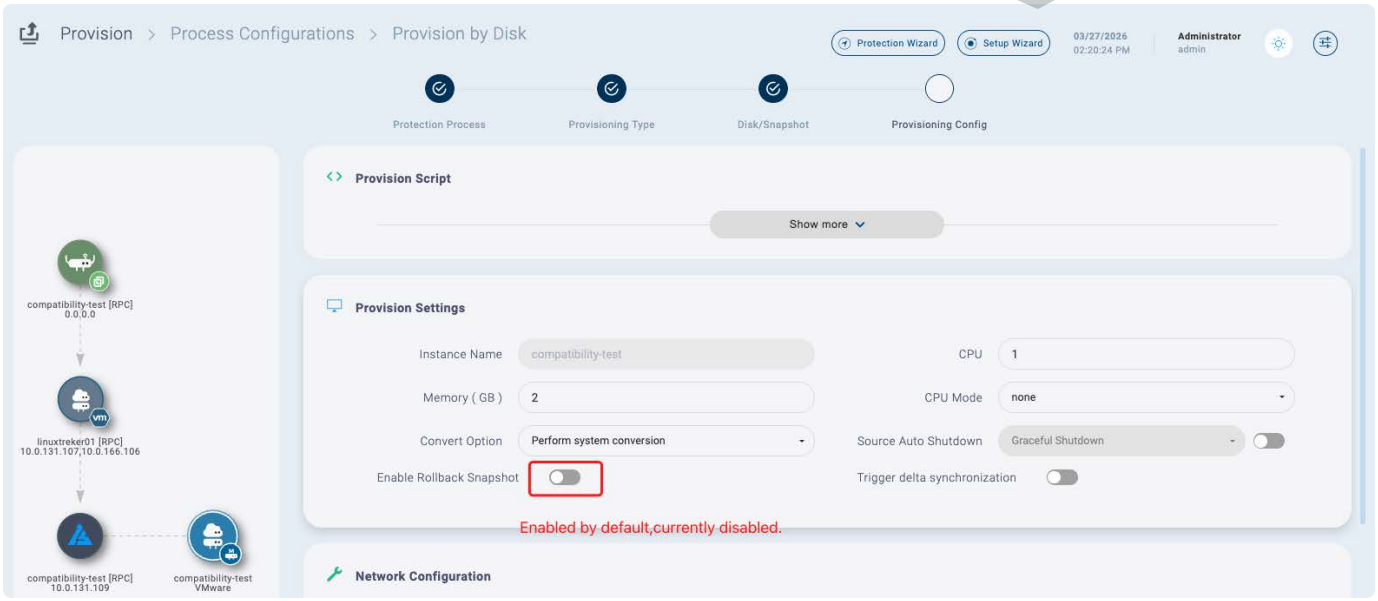
In the synchronization policy page, expand the preset more parameters and check the `Off` of `Number of copies`.



Disable switching tasks to create target machine rollback snapshots

> This function requires management console version ⩾ (greater than or equal to) version 666.

On the switching task policy page, turn off the Enable rollback snapshot button.

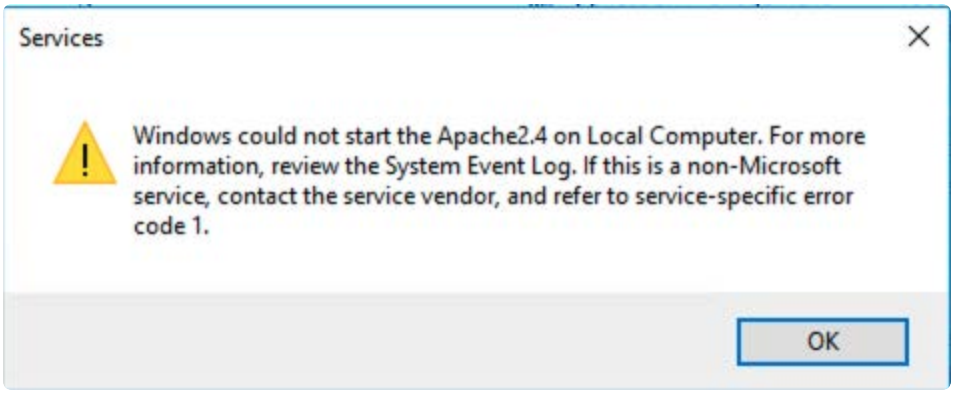

Provision > Process Configurations > Provision by Disk
Protection Wizard
Setup Wizard
03/27/2026
02:20:24 PM
Administrator
admin
Protection Process
Provisioning Type
Disk/Snapshot
Provisioning Config
compatibility-test [RPC]
0.0.0.0
linuxtreker01 [RPC]
10.0.131.107,10.0.166.106
compatibility-test [RPC]
10.0.131.109
compatibility-test
VMware
Provision Script
Show more
Provision Settings
Instance Name
compatibility-test
CPU
1
Memory (GB)
2
CPU Mode
none
Convert Option
Perform system conversion
Source Auto Shutdown
Graceful Shutdown
Enable Rollback Snapshot
Trigger delta synchronization
Enabled by default,currently disabled.
Network Configuration

Apache failed to start, PID of port 80=4

Document Category: Third Party Related Experience

Problem description

After installing the management console, apache failed to start. Checking the occupation of port 80 showed PID=4.




```
PS C:\Users\Administrator> netstat -ano|findstr "80"
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       580
  TCP    10.2.2.235:50138       152.195.38.76:80       TIME_WAIT       0
  TCP    127.0.0.1:50078        127.0.0.1:50080        ESTABLISHED     4716
  TCP    127.0.0.1:50080        127.0.0.1:50078        ESTABLISHED     4716
  TCP    [::]:80                [::]:0                 LISTENING       4
  TCP    [::]:49669             [::]:0                 LISTENING       580
PS C:\Users\Administrator>
```

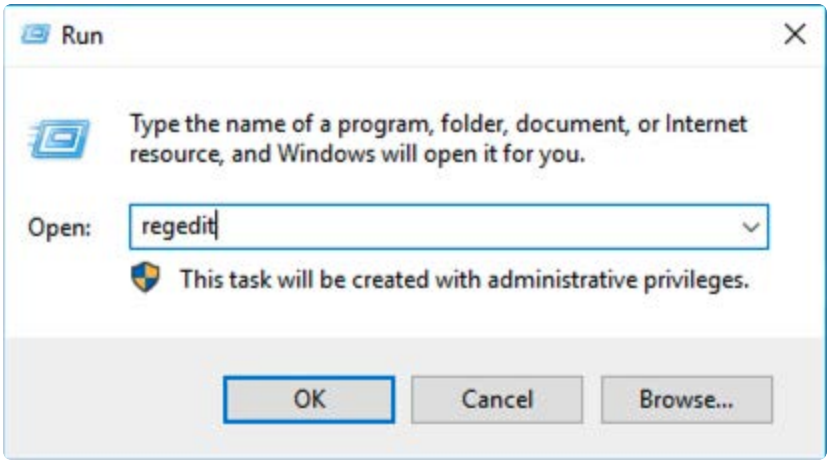
```
1   netstat -ano|findstr "80"
```

Problem analysis

PID=4, 4 means that the system occupies port 80, not IIS. You need to turn off the system's occupation of port 80.

Solution

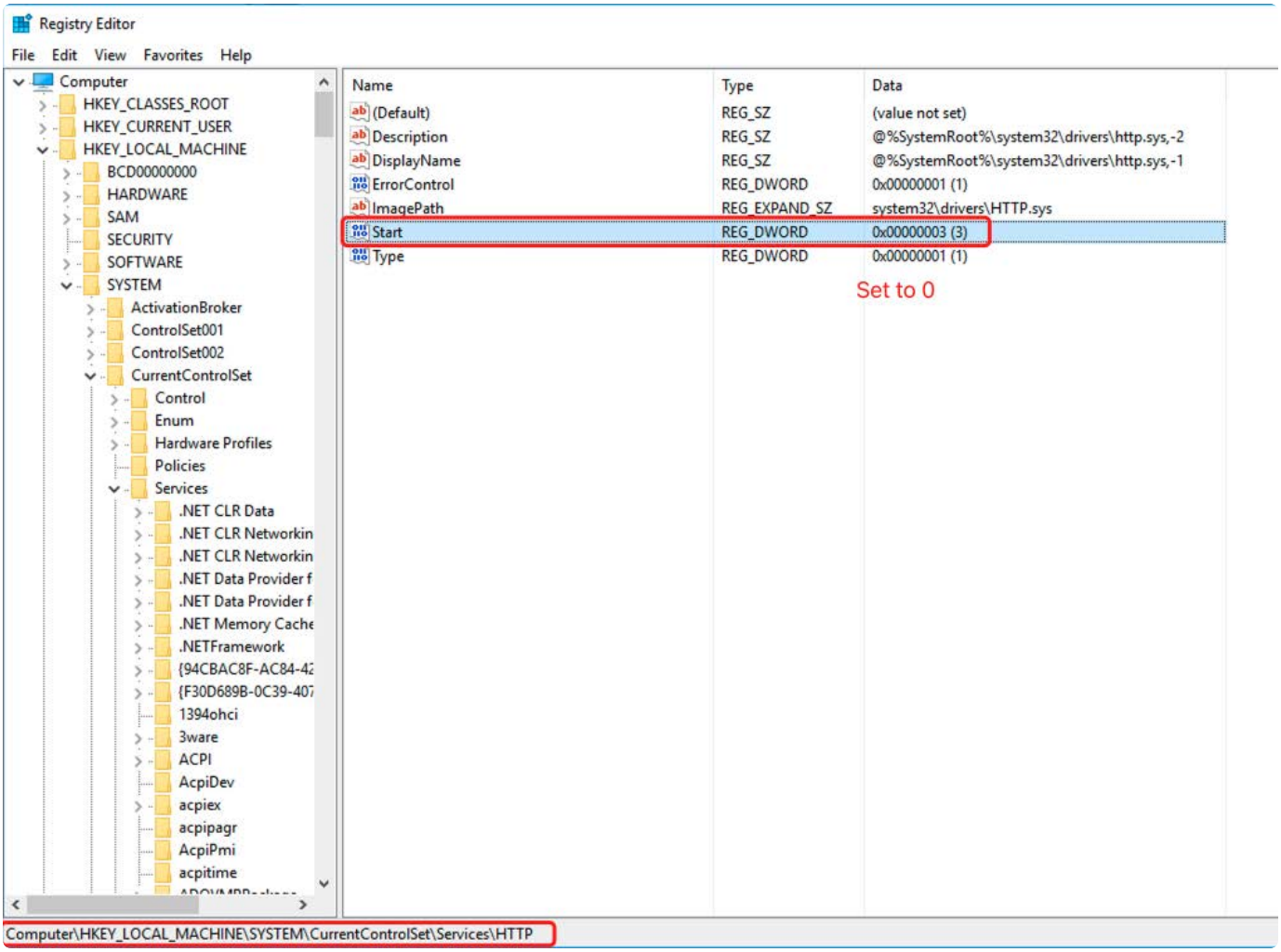
1. Open the registry and run regedit.



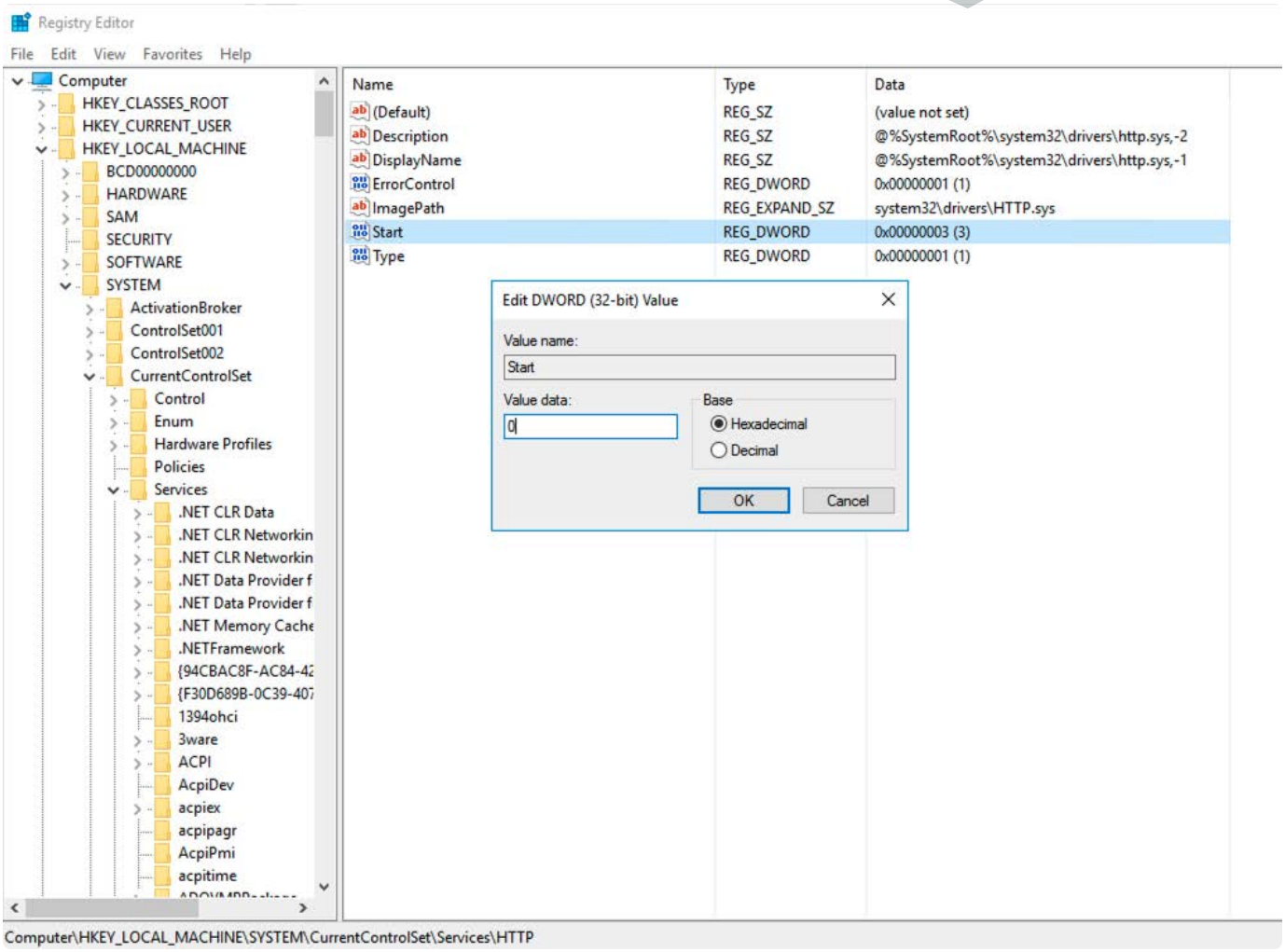
2. The registry opens in sequence

- If CurrentControlSet is not found, modify ControlSet001** and **ControlSet002.

```
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP
```



3. Change HTTP Start to 0.

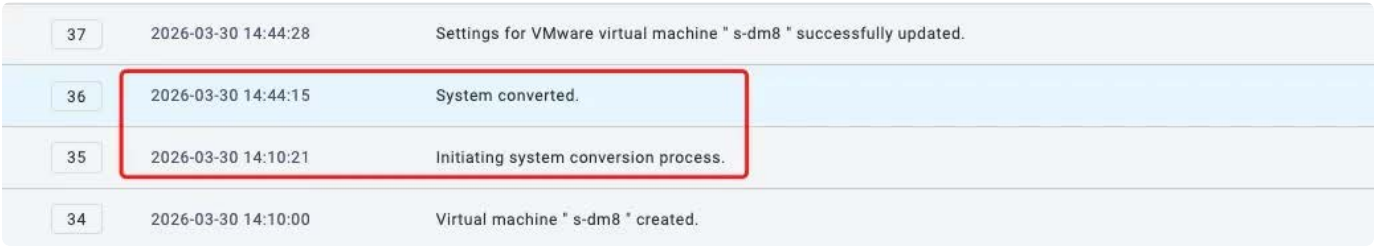


4. Just close the registry and restart the server.

Optimize Linux convert speed of VMware Win Data Gateway

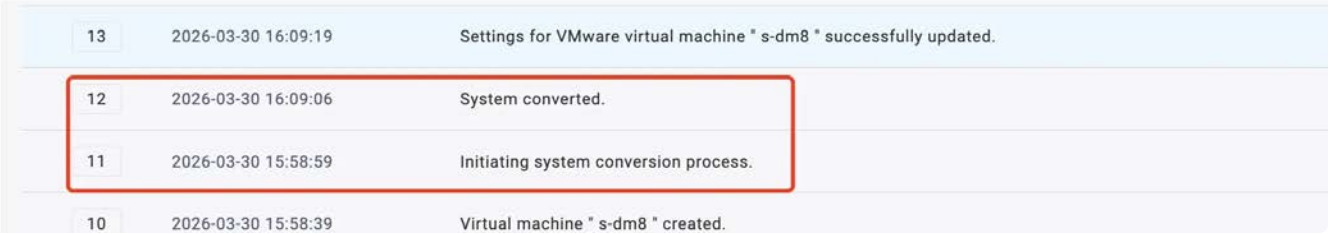
Internal test results

Before optimization: 34 minutes



37	2026-03-30 14:44:28	Settings for VMware virtual machine " s-dm8 " successfully updated.
36	2026-03-30 14:44:15	System converted.
35	2026-03-30 14:10:21	Initiating system conversion process.
34	2026-03-30 14:10:00	Virtual machine " s-dm8 " created.

After optimization: 11minutes



13	2026-03-30 16:09:19	Settings for VMware virtual machine " s-dm8 " successfully updated.
12	2026-03-30 16:09:06	System converted.
11	2026-03-30 15:58:59	Initiating system conversion process.
10	2026-03-30 15:58:39	Virtual machine " s-dm8 " created.

Necessary conditions

1. Only supports Intel CPU;
2. Number of CPU cores ⩾ 2.

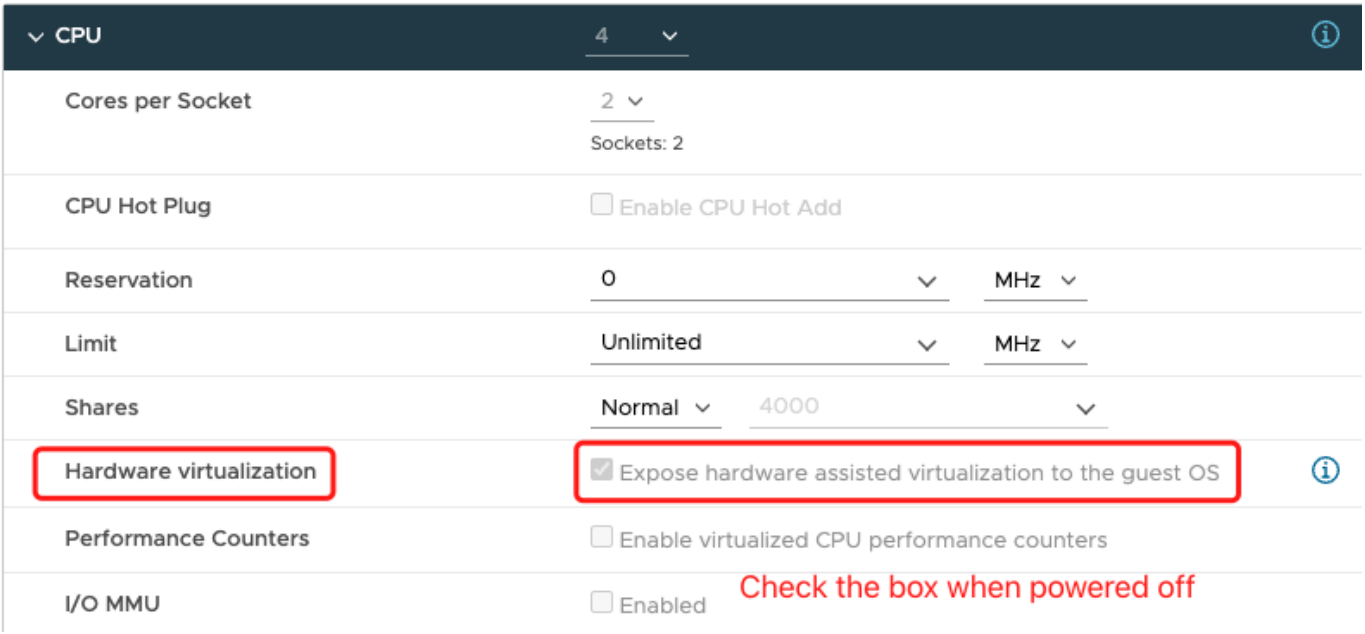
Preparation

haxm-windows: https://github.com/intel/haxm/releases

- The version used during testing was 7.8.

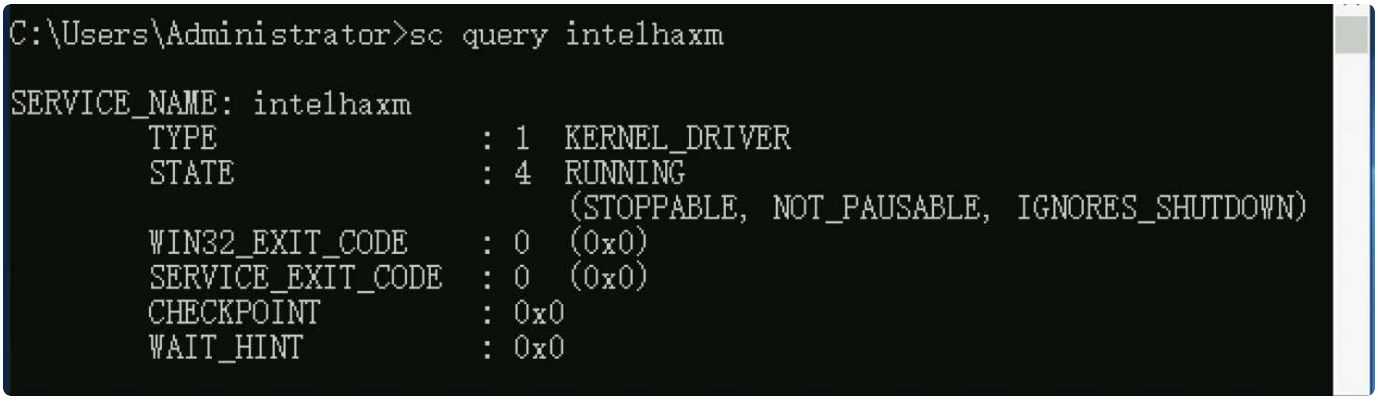
Operation steps

1. Shut down the Windows Data Gateway (Treker) virtual machine on VMware.
2. Edit the virtual machine settings and check `Hardware virtualization`.



3. Start the data gateway (Treker) virtual machine, upload intelhaxm, and install intelhaxm.
4. Restart the data gateway (Treker) virtual machine.
5. Query the running status of intelhaxm.

```
#query intelhaxm status
sc query intelhaxm
```



6. After that, switching the migration task of the Linux source host through this data gateway (Treker) will speed up the process.
    - The specific effect is affected by the performance of VMware storage, CPU and other hardware, and varies, but in the same environment, enabling it is significantly better than not enabling it.

Optimize synchronization speed

Document Category: Product Related Experience

Applicable scenarios

Hope to improve the transmission speed of synchronization tasks.

Factors affecting speed

> The Linux ext3 file system is relatively old. The performance of the ext3 file system in dispersing data is poor. The slow synchronization speed is a limitation of the file system.
>
> If you are particularly pursuing speed, consider upgrading the ext3 file system to ext4 before running the synchronization task.

1. Disk performance of the source machine, transit data gateway, and target machine;
2. The bandwidth of the source machine, transit data gateway, and target machine;
3. Network card performance of the source machine, transit data gateway, and target machine (very little).

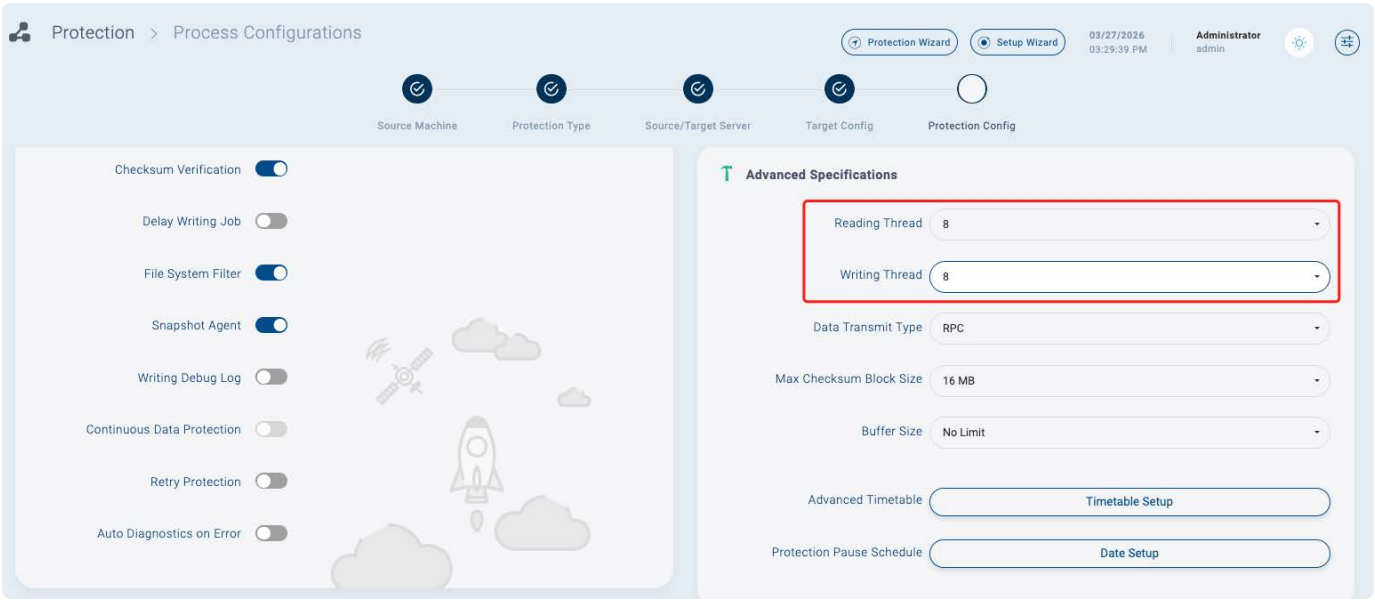
Transfer time calculation formula

Calculate the transmission time and follow the principle of the barrel effect:

- Disk performance is the bottleneck:
  - Data volume ÷ disk throughput = transfer time.
- Bandwidth is the bottleneck:
  - Data volume ÷ bandwidth speed = transfer time.
- Network performance is the bottleneck (rarely):
  - Data volume ÷ network throughput = transmission time.

Optimization plan

1. Migrate using Agent.
2. Add read and write threads for synchronization tasks (the default read and write threads are 4, and the maximum can be set to 8).
    - Adding read and write processes will consume a little more CPU resources.



3. In the scenario of installing Agent, you can turn on `client compression`.
    - If there are many text files in the system, the transmission time will be significantly reduced.
    - If the system is full of video, picture, and audio files, the transmission time will not change significantly.
4. In the scenario of installing Agent, you can turn off `client intelligent filtering`.
    - In scenarios with many small files and discrete files, the speed will be significantly improved.
5. If the replication architecture does not use a transit data gateway, you can add a transit data gateway.
6. Optimize disk performance and network bandwidth.

Offline solution

If the source machine can be shut down for migration, you can use offlinekit for offline migration, which does not rely on the file system. The theoretical speed can run to full disk and bandwidth.

For details, please refer to the knowledge base "OfflineKit Offline Migration".

Fixed the problem of graphics not displaying after SuSE10 migration

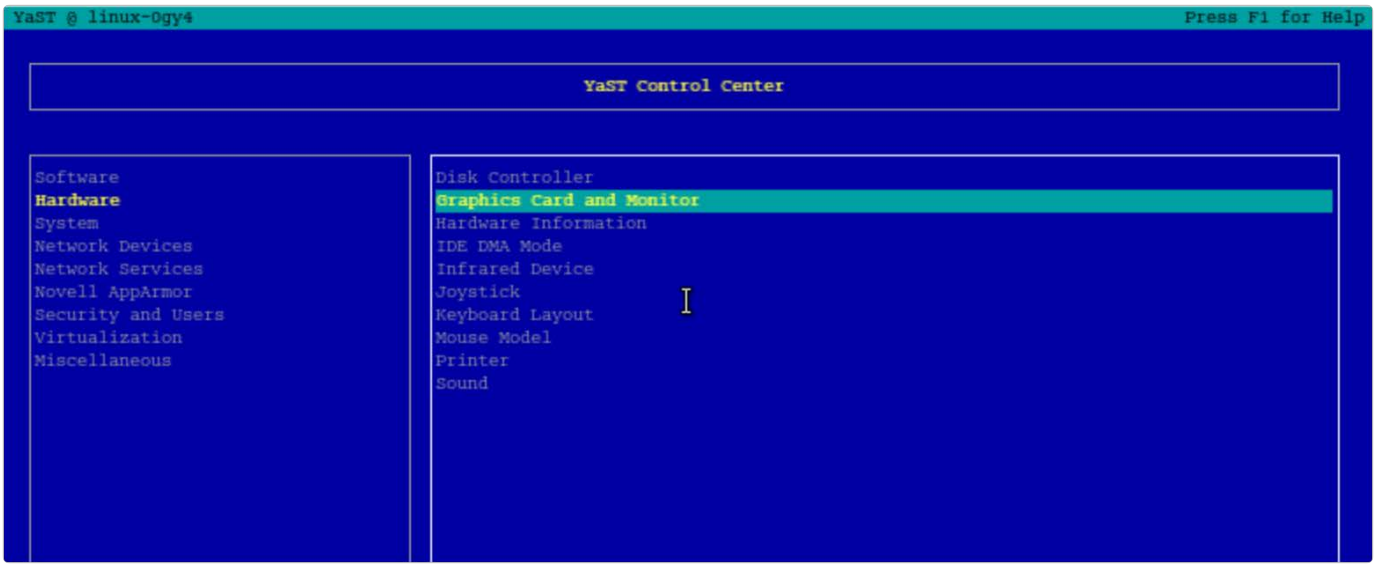
Document Category: Third Party Related Experience

Operation steps

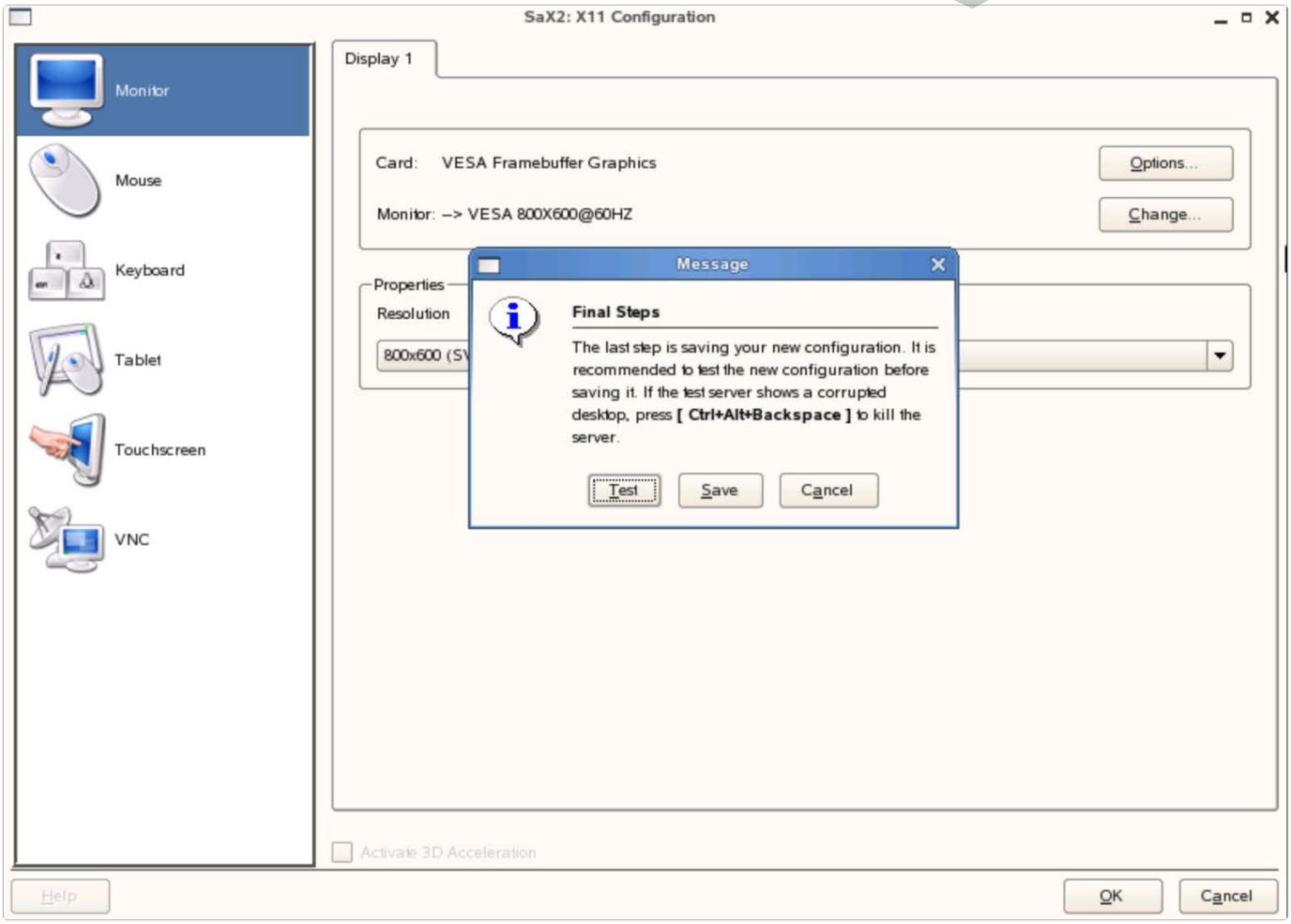
1. Open yast in terminal

```
yast
```

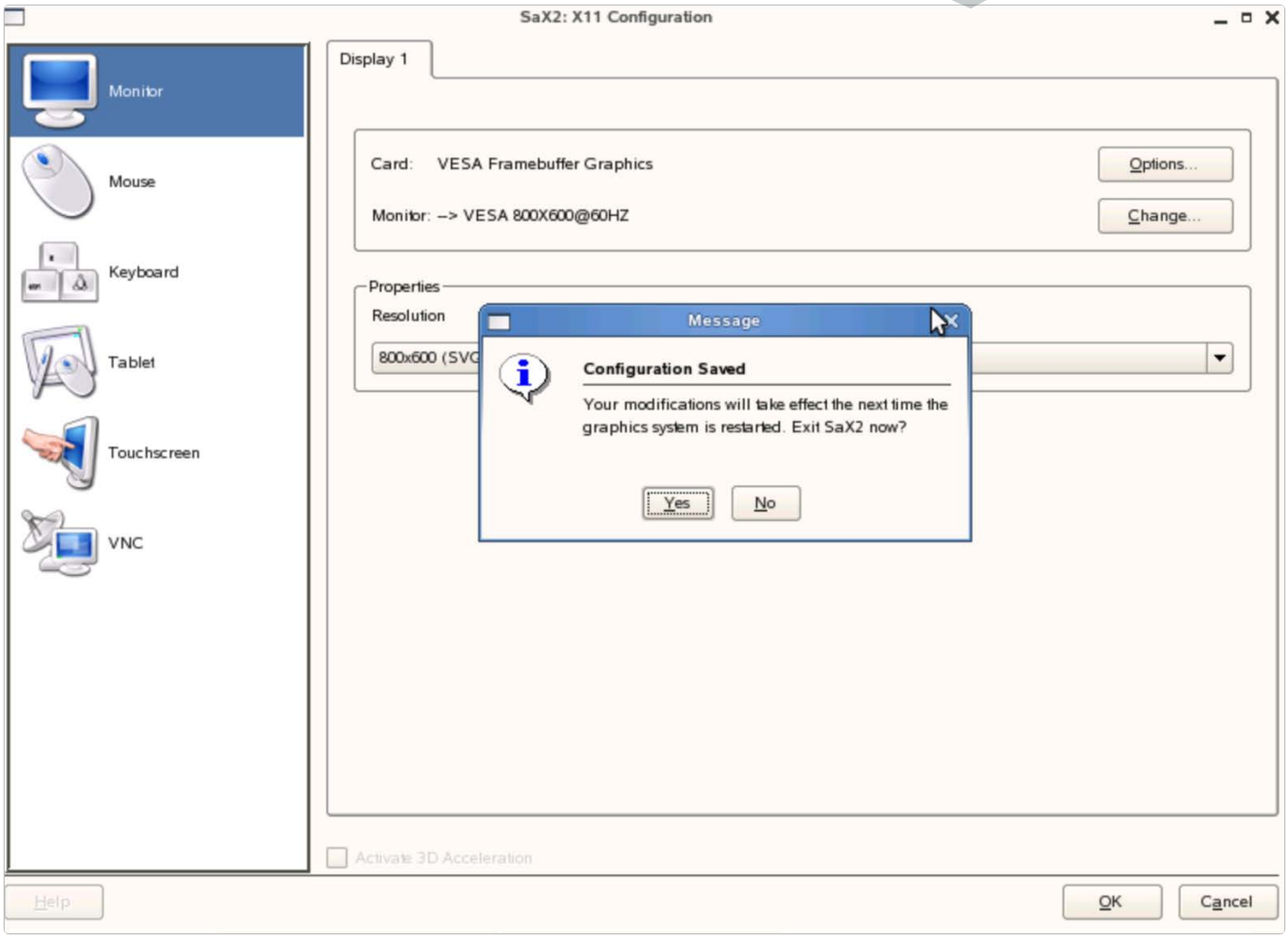
2. Select Hardware, Graphic Card and Monitor



3. Select OK, Save


SaX2: X11 Configuration
Monitor
Mouse
Keyboard
Tablet
Touchscreen
VNC
Display 1
Card: VESA Framebuffer Graphics
Options...
Monitor: --> VESA 800X600@60HZ
Change...
Properties
Resolution
800x600 (SV
Message
Final Steps
The last step is saving your new configuration. It is recommended to test the new configuration before saving it. If the test server shows a corrupted desktop, press [Ctrl+Alt+Backspace] to kill the server.
Test
Save
Cancel
Activate 3D Acceleration
Help
OK
Cancel

4. Choose yes



5. Restart the system

```
1   reboot
```

Fixed the problem of graphics not displaying after SuSE11 migration

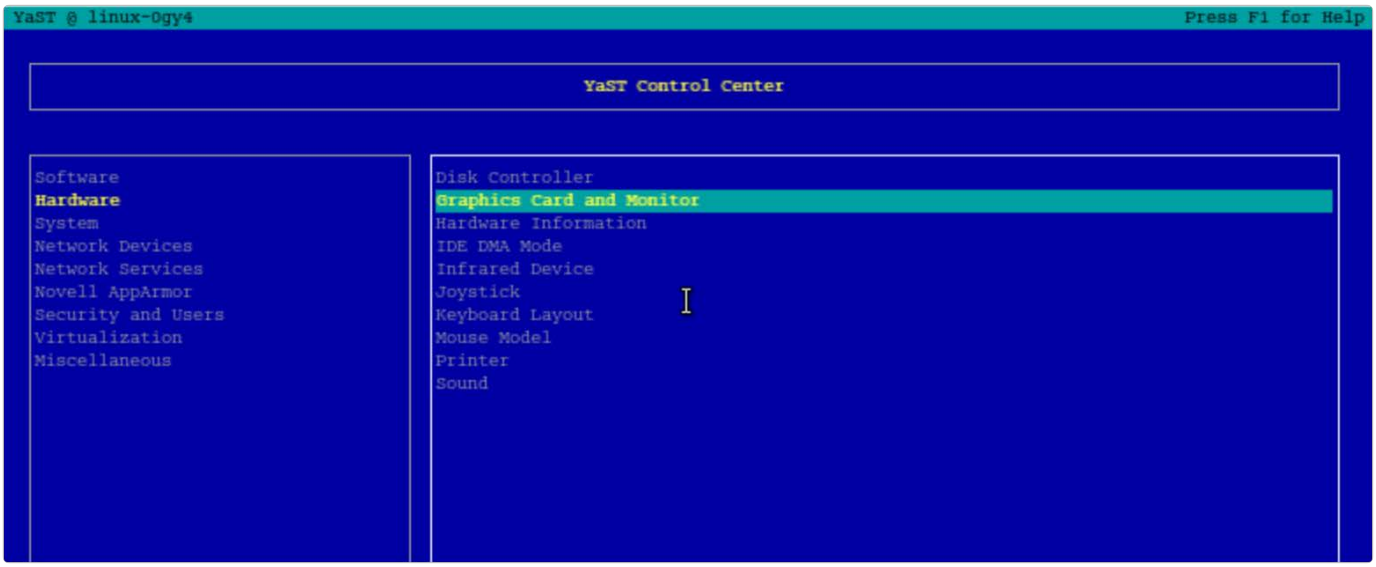
Document Category: Third Party Related Experience

Operation steps

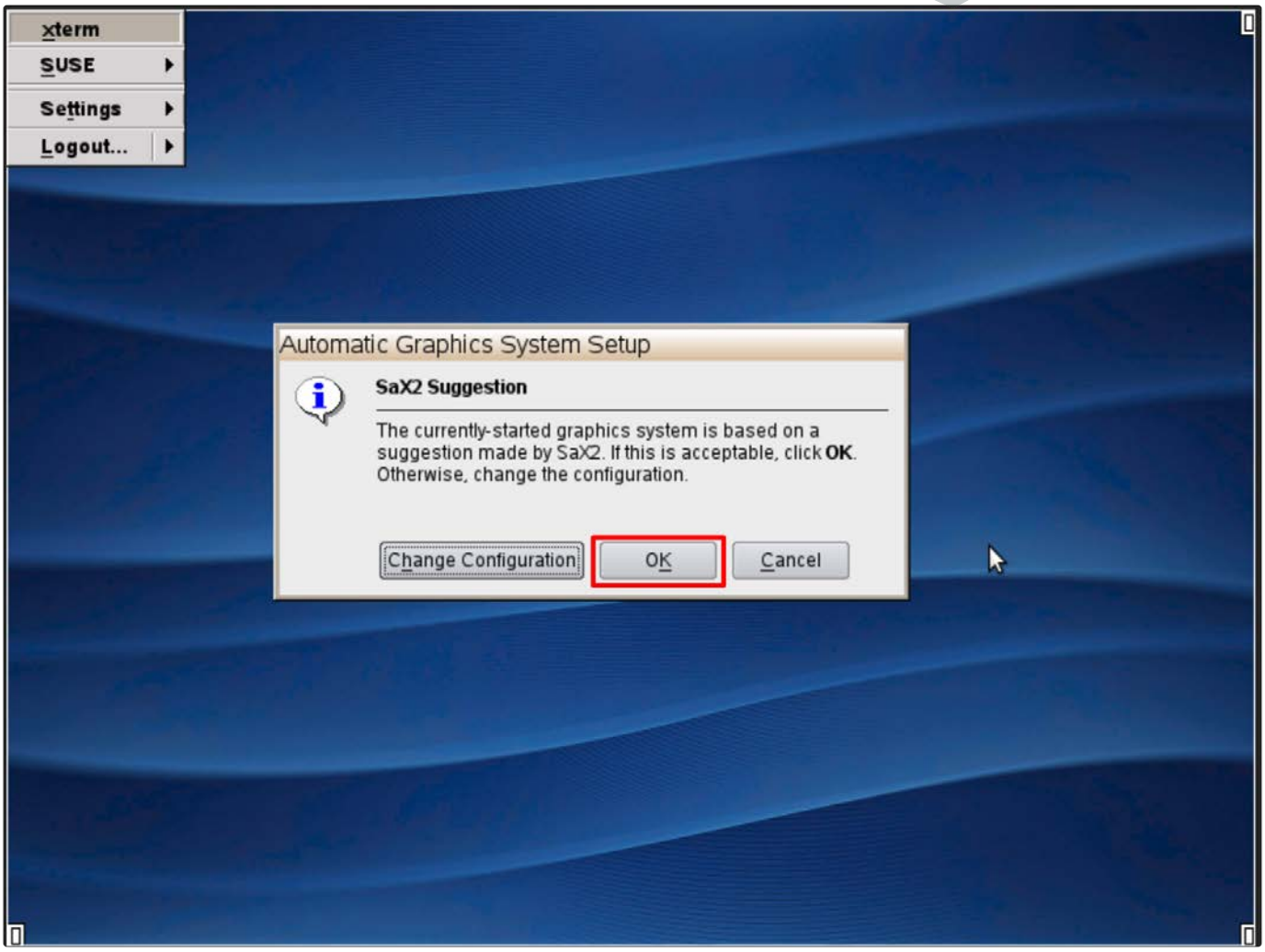
1. Open yast in terminal

```
yast
```

2. Select Hardware, Graphic Card and Monitor

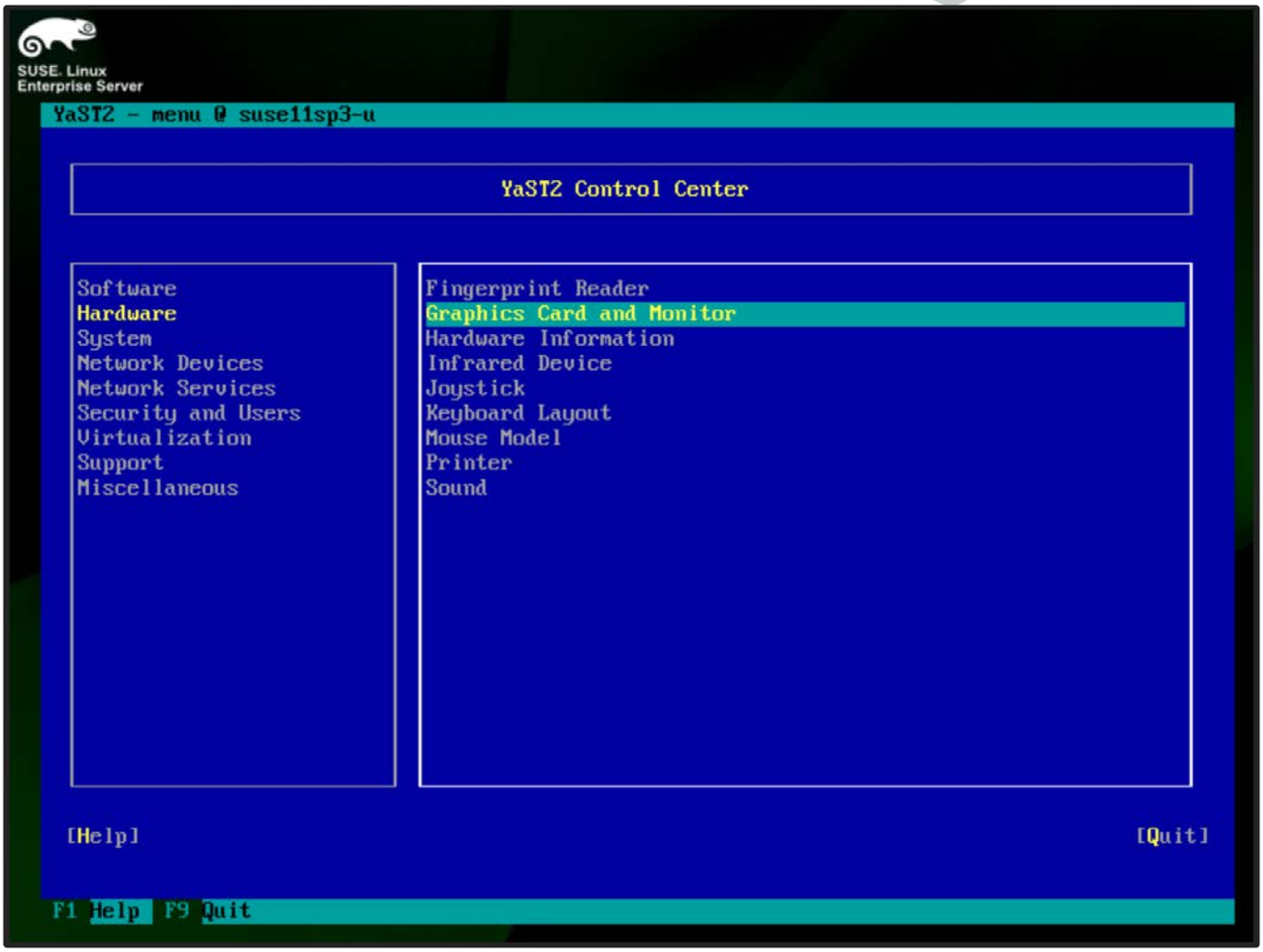


3. Select OK


xterm
SUSE
Settings
Logout...
Automatic Graphics System Setup
SaX2 Suggestion
The currently-started graphics system is based on a suggestion made by SaX2. If this is acceptable, click OK. Otherwise, change the configuration.
Change Configuration
OK
Cancel

4. F9 to exit

NEXAVM



5. Restart the system

```
1   reboot
```

Fix SuSE10sp4 that cannot enter the system after migration

Document Category: Third Party Related Experience

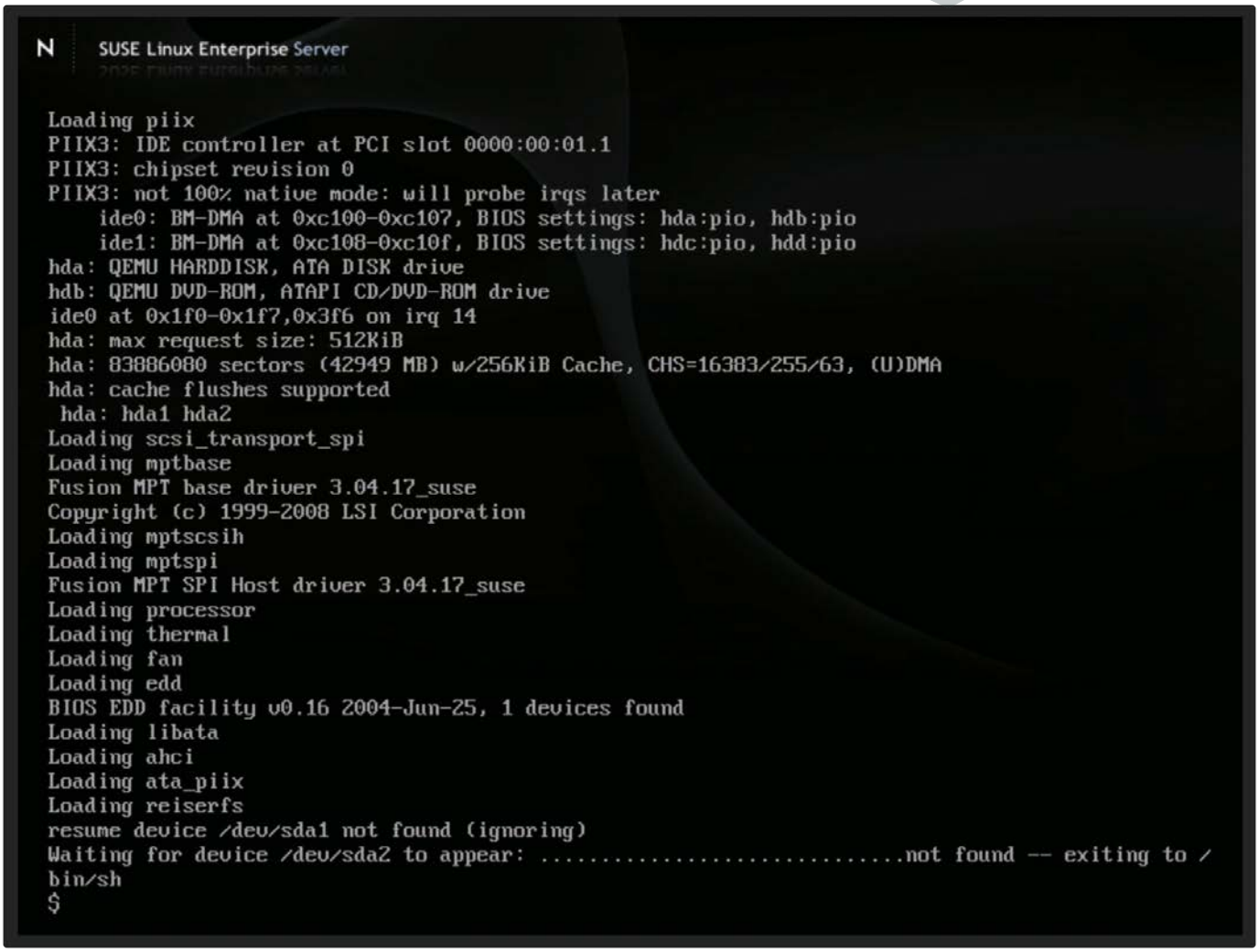
Applicable scenarios

After migration, the system cannot be entered normally due to the change of disk device name.

Boot interface

```
Loading ata_piix
Loading reiserfs
resume device /dev/sdal not found (ignoring)
Waiting for device /dev/sda2 to appear: ........not found -- exiting to /bi
n/sh
$
```

NEXAVM

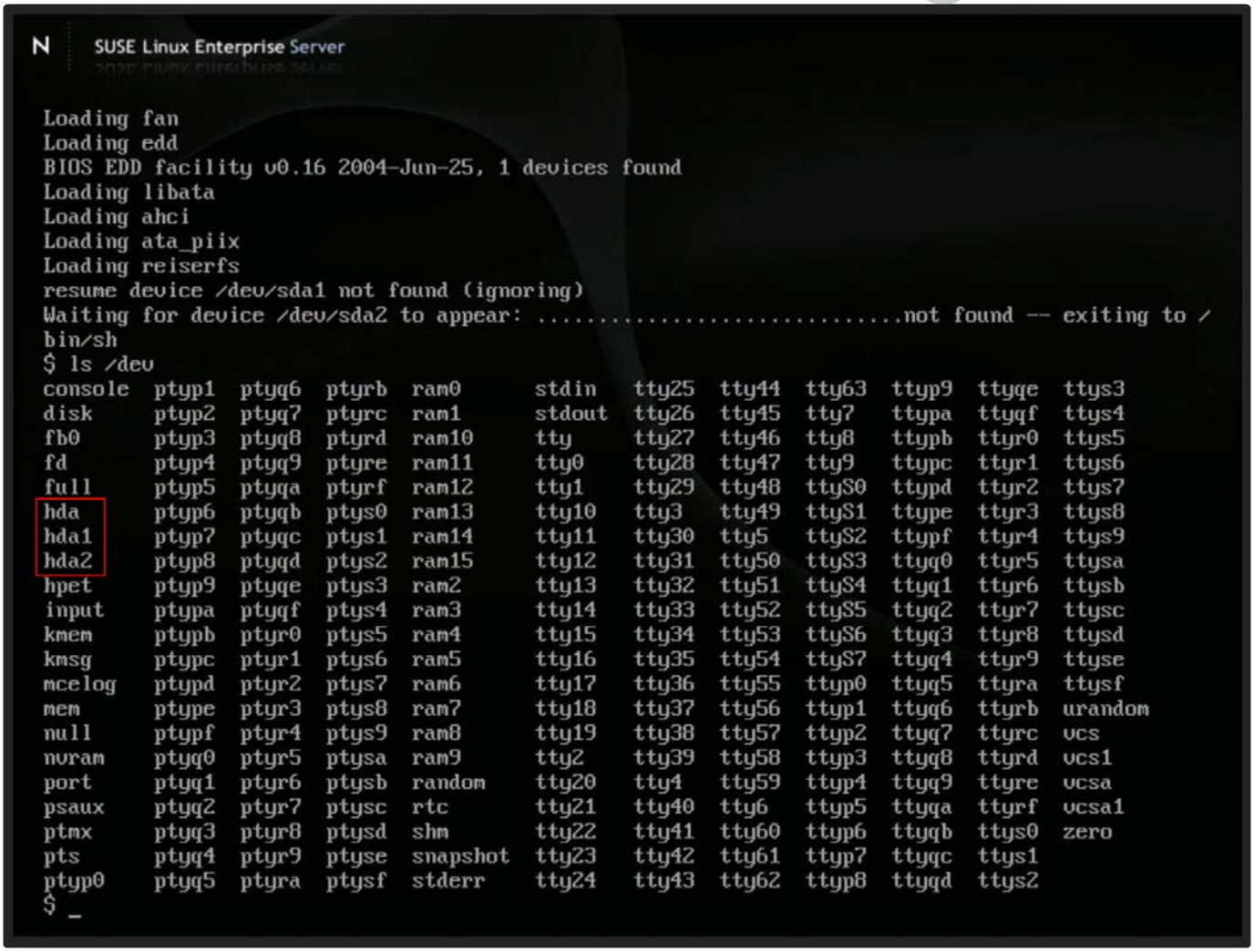


Operation steps

1. Check the new device name.
    - The device names before migration are sda, sda1, sda2
    - You can see that after migration, they are hda, hda1, and hda2.

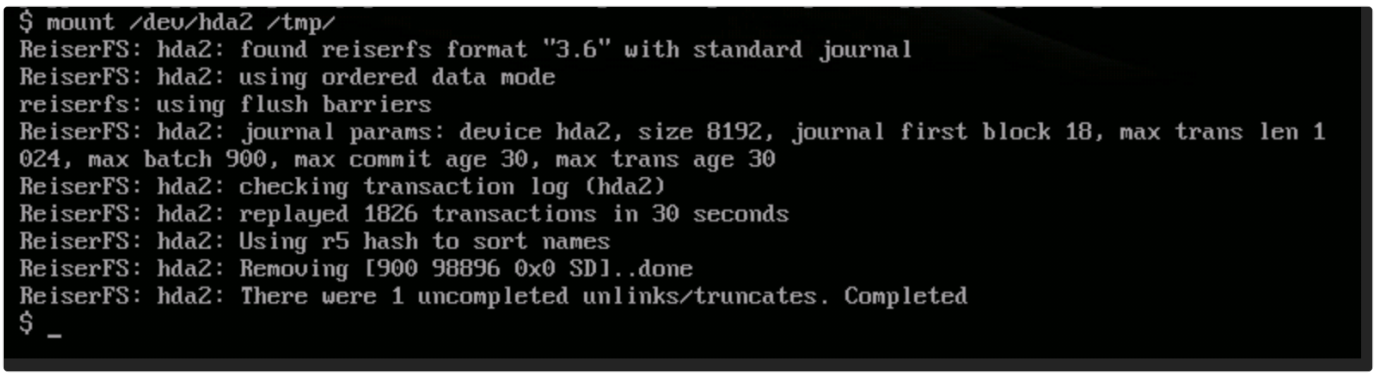
```
1   ls /dev
```

NEXAVM



2. Mount the root directory to tmp
    - If fsck is enabled for the root directory in fstab, the mounting time may be slightly longer.

```
1   mount /dev/hda2 /tmp
```



3. Use ls to check whether it is the root directory and whether the boot directory is in the root directory.
    - Flexibility is required here. If the boot directory is not in the root directory, find the boot partition and mount it in the root directory.

NEXAVM

```
ls /tmp
ls /tmp/boot
```

```
$ ls /tmp/
bin   dev  home  lib64  mnt  proc  sbin  sys  usr
boot  etc  lib   media  opt  root  srv   tmp  var
$ ls /tmp/boot/
System.map-2.6.16.60-0.85.1-smp  message
backup_mbr                       symsets-2.6.16.60-0.85.1-smp.tar.gz
boot                             symtypes-2.6.16.60-0.85.1-smp.gz
config-2.6.16.60-0.85.1-smp      symvers-2.6.16.60-0.85.1-smp.gz
grub                             vmlinux-2.6.16.60-0.85.1-smp.gz
initrd                           vmlinuz
initrd-2.6.16.60-0.85.1-smp      vmlinuz-2.6.16.60-0.85.1-smp
$
```

4. Modify relevant configuration files.
    - BIOS:
        - /etc/fstab (can be skipped if mounted with uuid)
        - /boot/grub/device.map
        - /boot/grub/menu.list
    - UEFI: (Tentative 2 files)
        - /etc/fstab (can be skipped if mounted with uuid)
        - /boot/efi/efi/SuSE/elilo.conf
    - Use sed instead (minimized environment without vi).
        - Take replacing sda with hda as an example.

NEXAVM

```
#Backup
cp /tmp/etc/fstab /tmp/etc/fstab.LT
#Preview the execution result
sed "s/sda/hda/g" /tmp/etc/fstab
#Use -i parameter to update
sed -i "s/sda/hda/g" /tmp/etc/fstab

#Backup
cp /tmp/boot/grub/device.map /tmp/boot/grub/device.map.LT
#Preview the execution result
sed "s/sda/hda/g" /tmp/boot/grub/device.map
#Use -i parameter to update
sed -i "s/sda/hda/g" /tmp/boot/grub/device.map

#backup
cp /tmp/boot/grub/menu.list /tmp/boot/grub/menu.list.LT
#Preview the execution result
sed "s/sda/hda/g" /tmp/boot/grub/menu.list
#Use -i parameter to update
sed -i "s/sda/hda/g" /tmp/boot/grub/menu.list
```

5. Restart

```
reboot -f
```

Modify VMware agentless parallel number

Document Category: Product Related Experience

Background

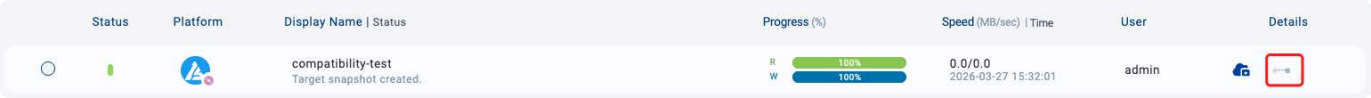
1. **Default VADP replication task, the same ESXi can only run one replication job. **
2. **This setting is to limit the number of vadp concurrencies and avoid affecting production business. Communication with users is required before modification. **
3. **ESXi version ⩽ (less than or equal to) 5.5 version. It is not recommended to modify the number of concurrencies, nor is it recommended to increase the number of transit Trekkers to achieve multiple concurrencies.**

Applicable scenarios

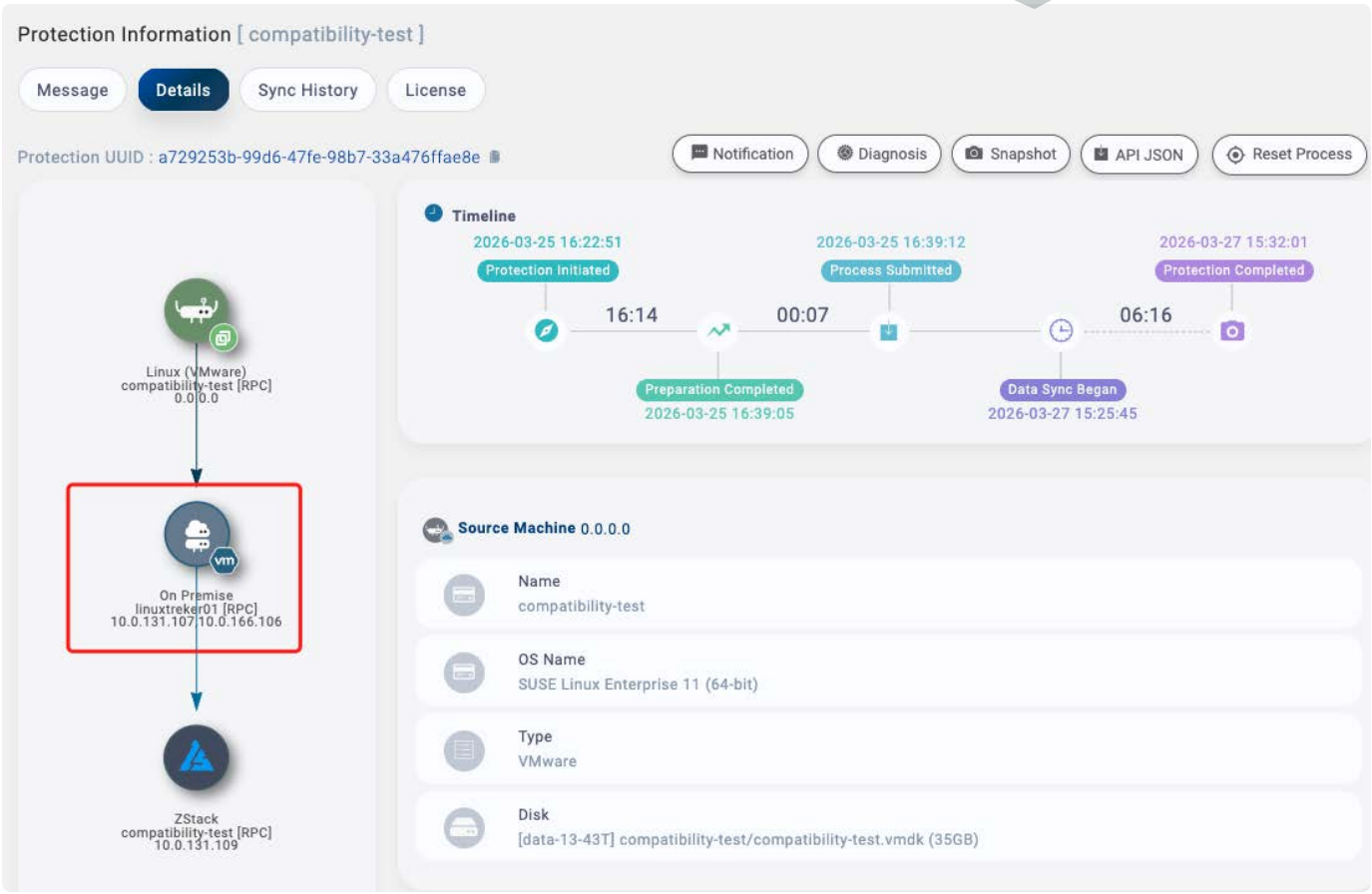
- The number of concurrent VADP needs to be increased.

Confirm the modification of the number of concurrent data gateways (Treker)

1. Click on the details icon of this protection task



2. Click on the information in the details to see the topology diagram. The one in the middle of the topology is the data gateway that needs to be modified for concurrency.



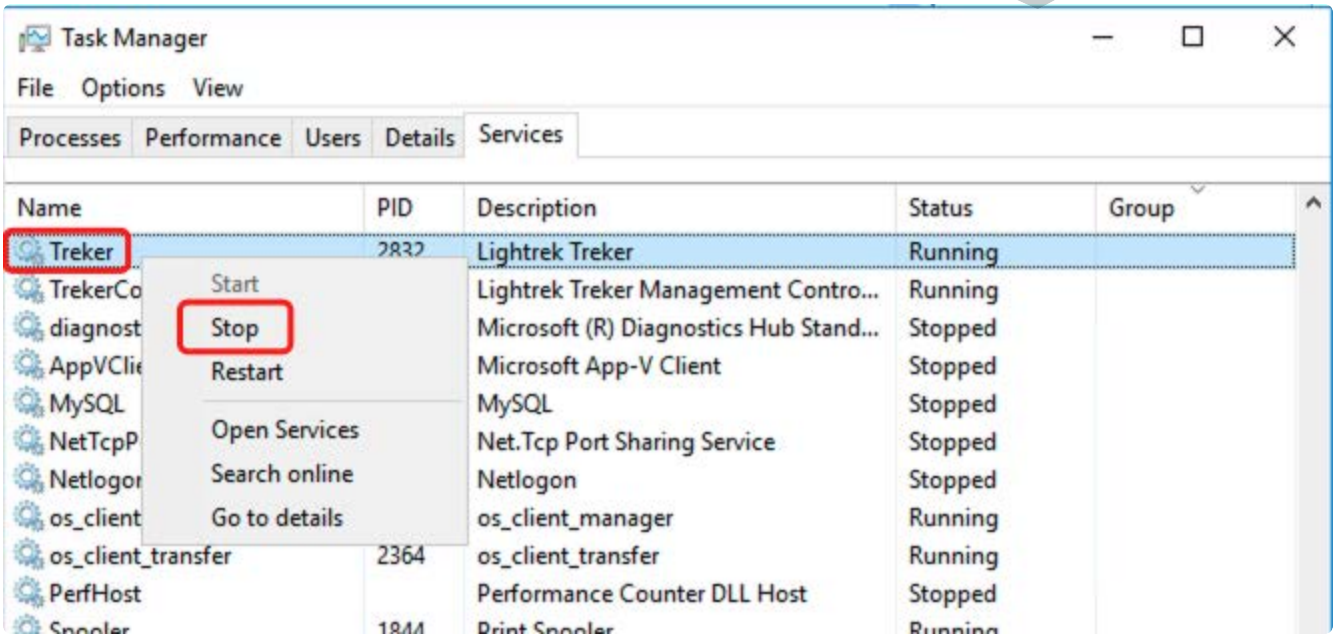
Operation steps

> If the source platform is VADP reading, modify the registry of the relay Trekker (refer to the topology above).
>
> If the target platform is VADP writing, modify the registry of the target Trekker (the last data gateway in the topology).
>
> Both the source and target platforms use VADP for reading and writing, so modify the registry of the source and target Trekkers.

Windows Data Gateway

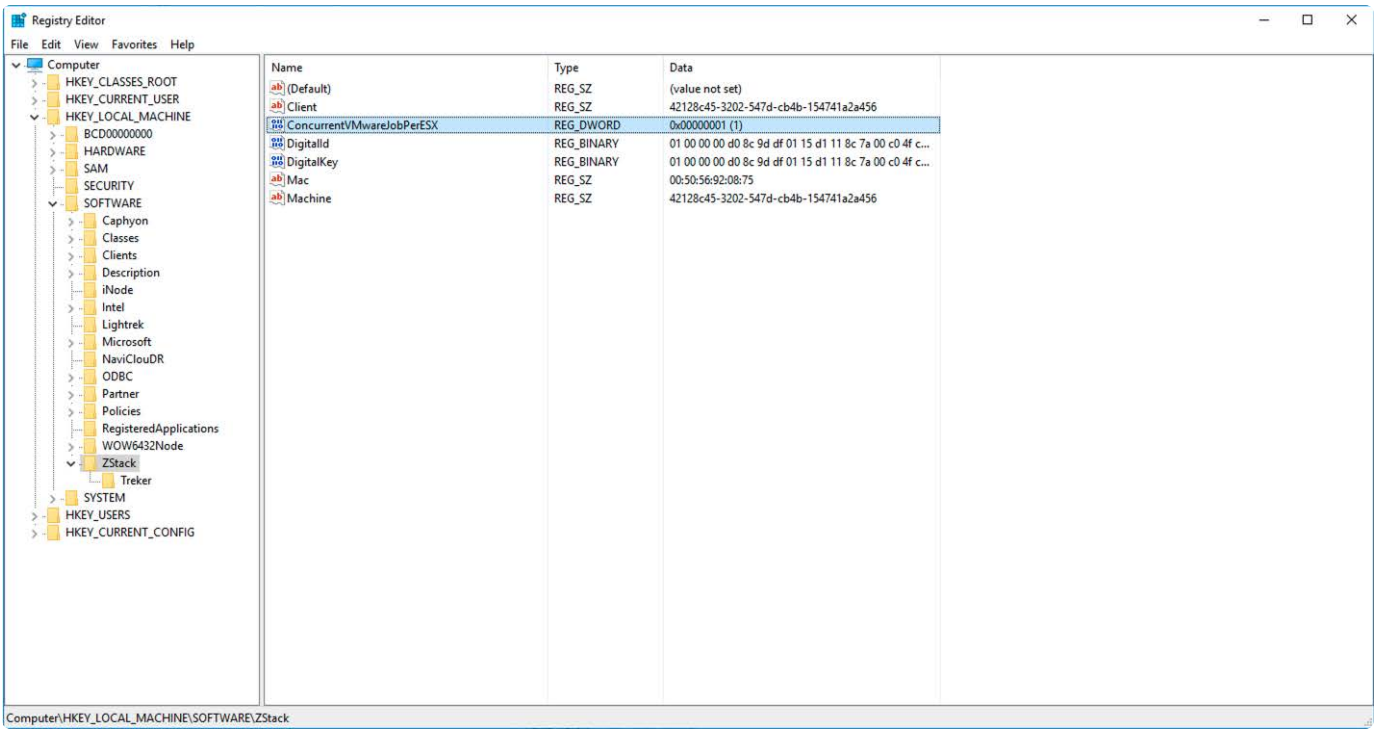
1. Stop Treker.service.

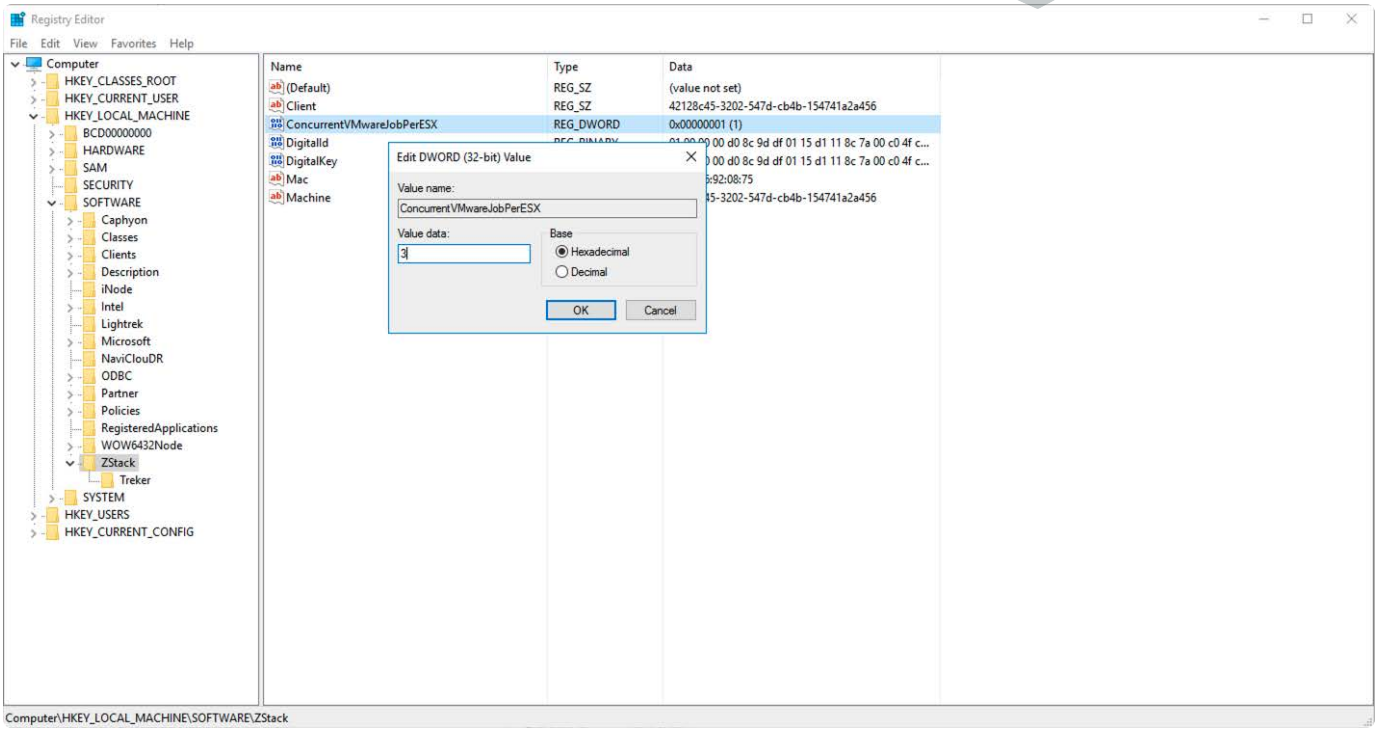
NEXAVM

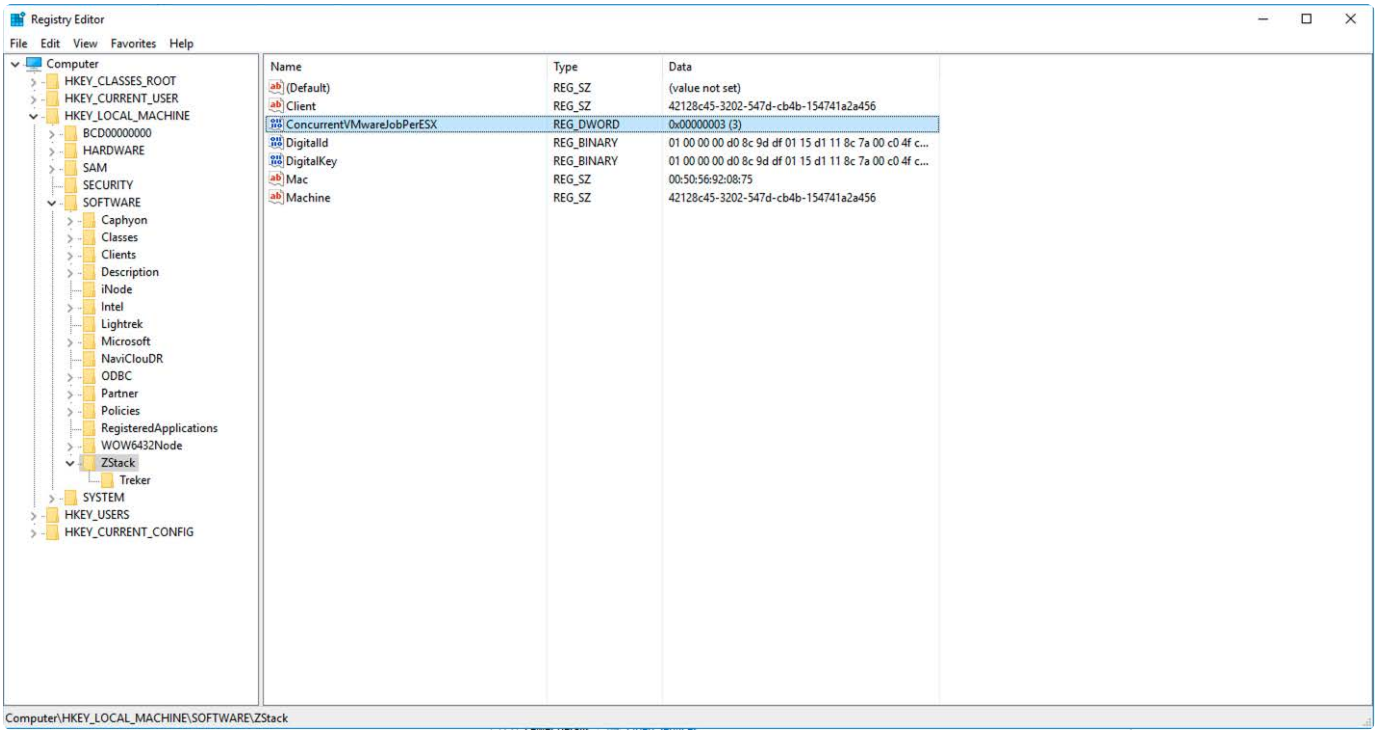


2. Modify the registry and change the key value of the number of concurrent tasks `ConcurrentVMwareJobPerESX` from 1 to custom (it is recommended not to exceed 5).

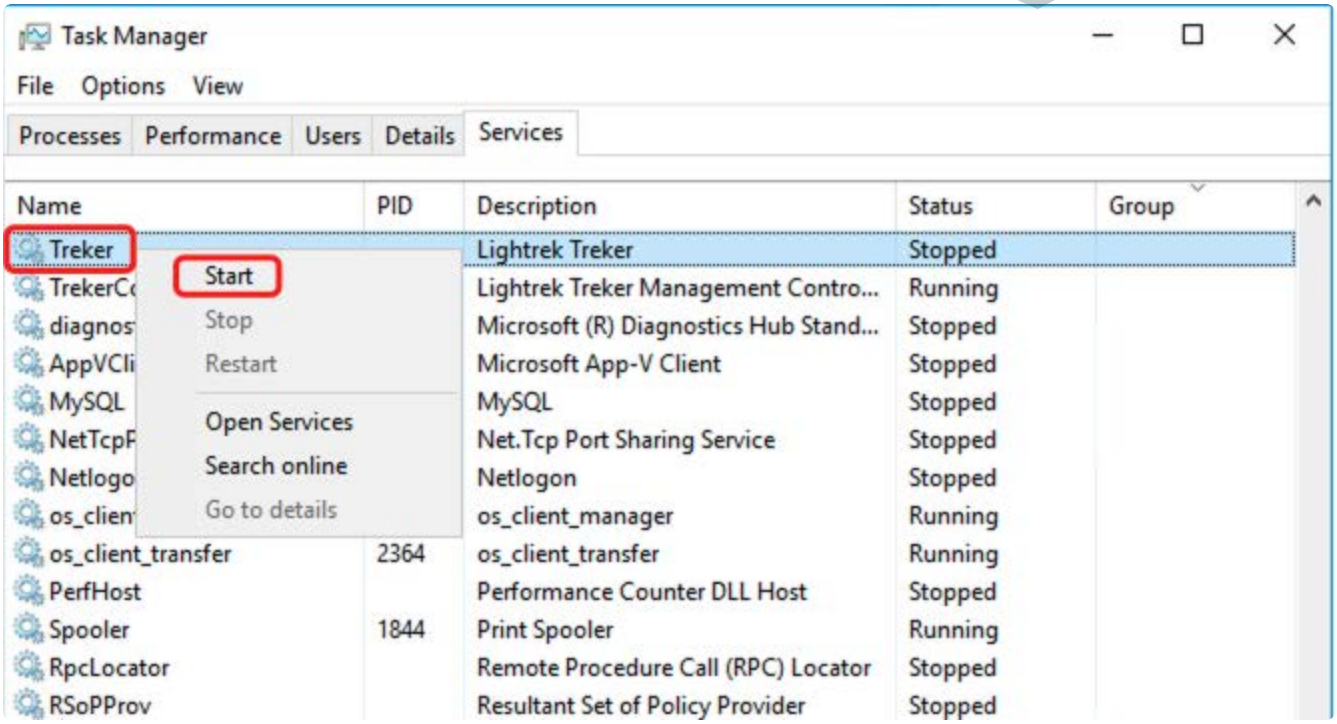
```
regedit PATH: HKEY_LOCAL_MACHINE\SOFTWARE\ZStack\ConcurrentVMwareJobPerESX
```







3. Start Treker.service.



Linux data gateway

> After executing the following command, the number of concurrency will be automatically configured based on the number of CPU cores.

```
docker exec treker touch concurrent_reading_job_number
docker exec treker touch concurrent_vmware_job_per_esx
docker restart treker
```

Modify the number of times the synchronization task waits for the target disk and API debugging

Document Category: Product Related Experience

Applicable scenarios

Modify the waiting times: When NexaVM storage performance is poor, the target machine starts slowly.

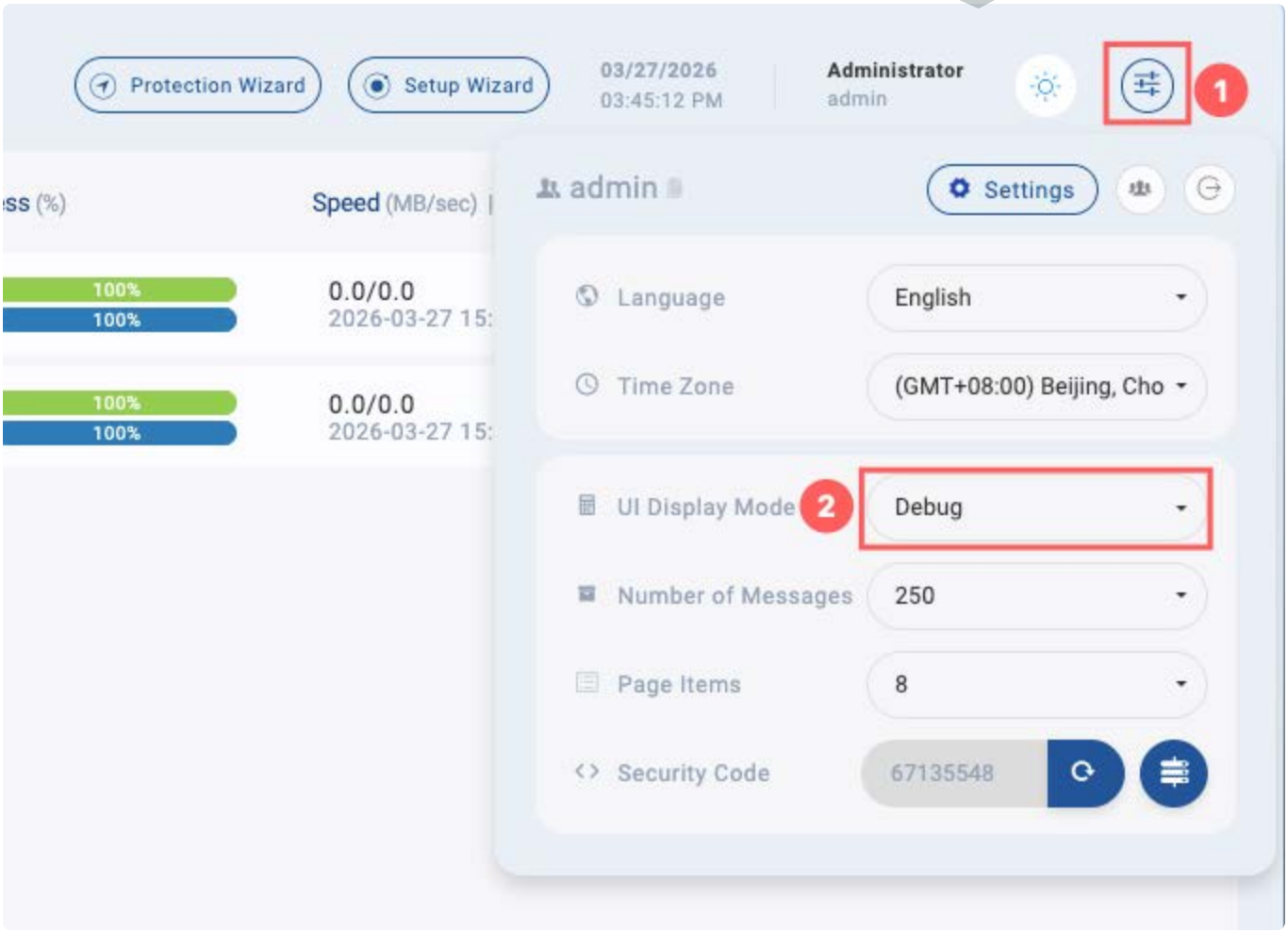
Turn on API Debug: When you need more detailed NexaVM API logs to troubleshoot problems.

Version requirements

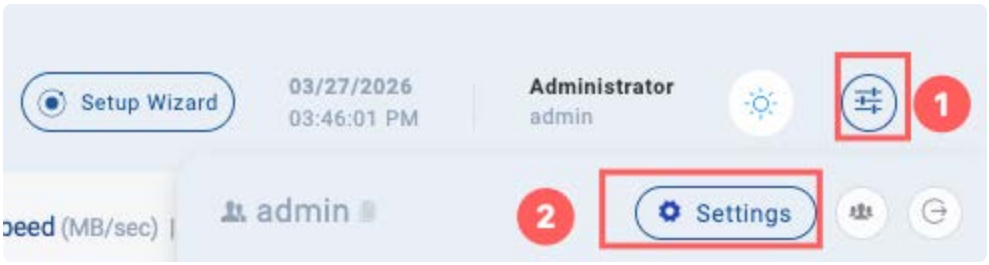
This page will only be available if the management console version is ⩾ (greater than or equal to) version 666.

Operation steps

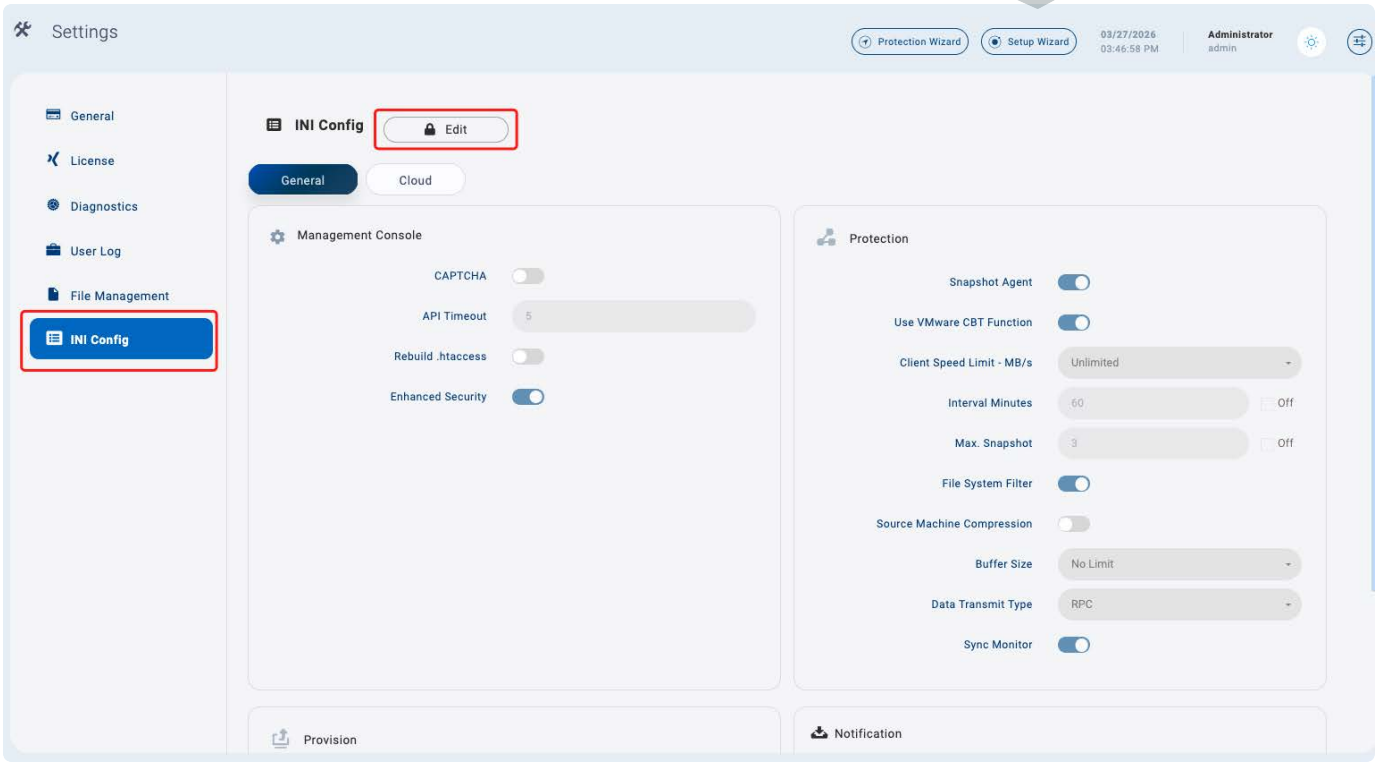
1. Set the configuration status of the management console to `Troubleshooting`.

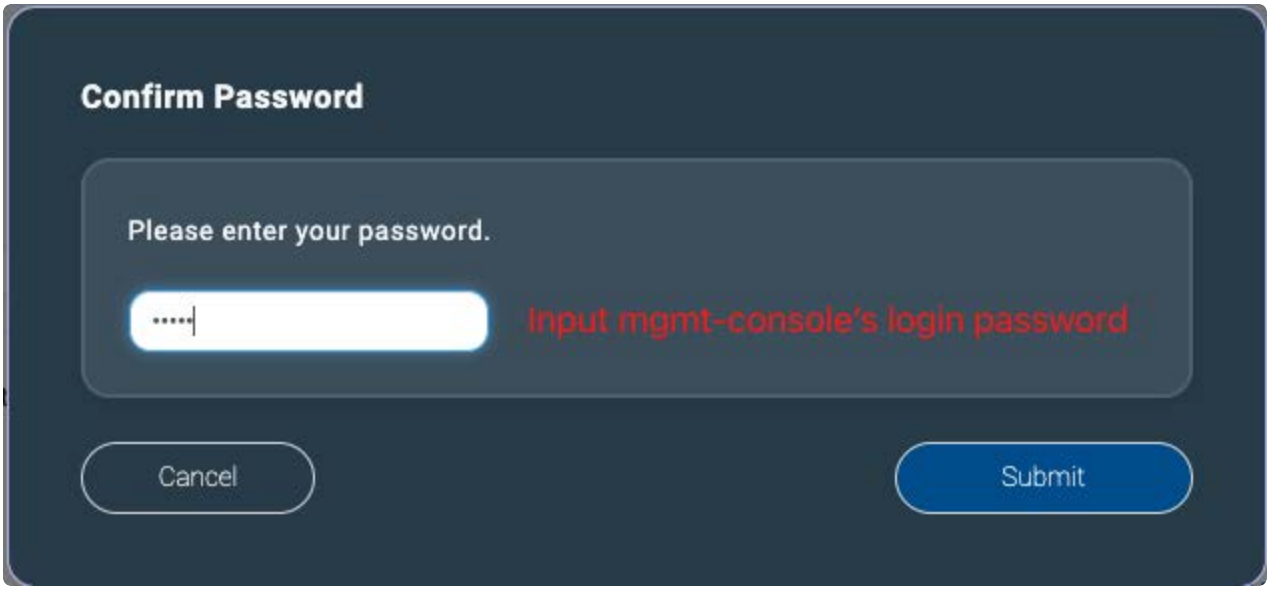


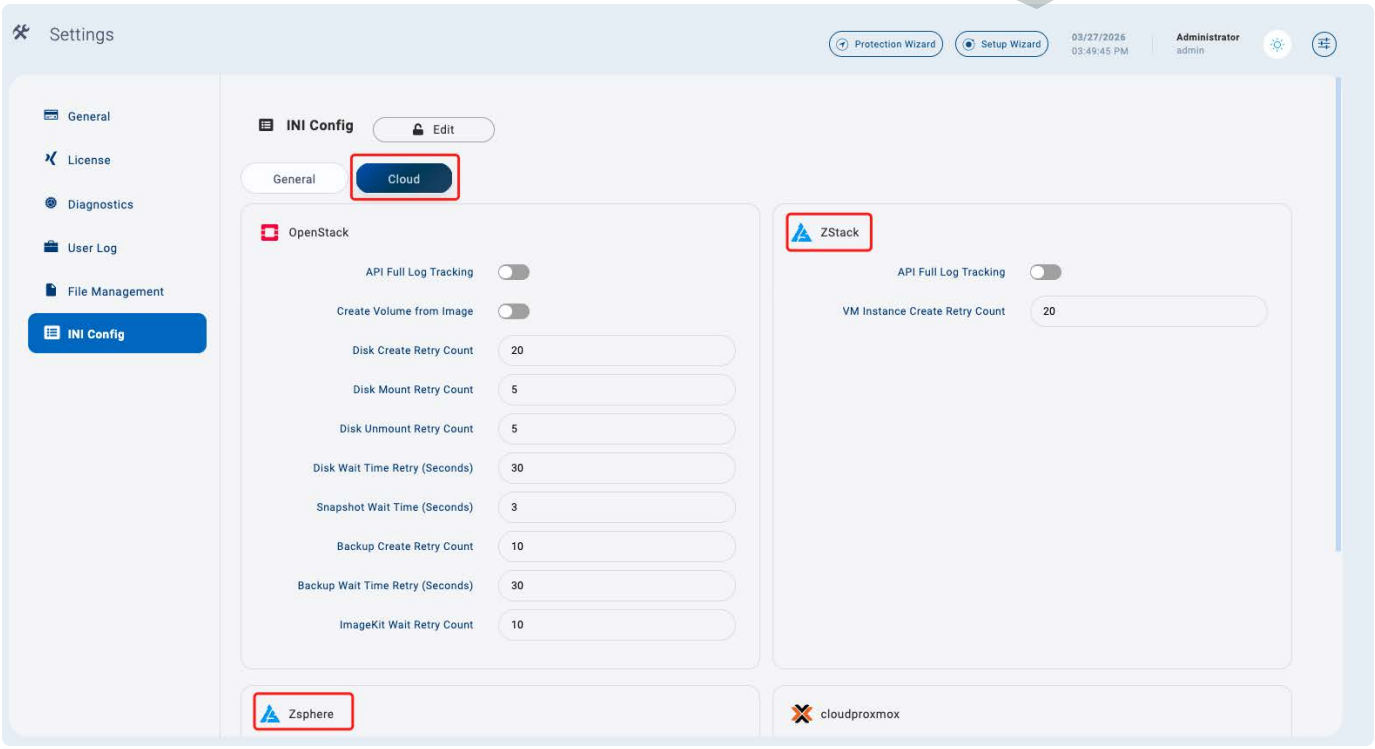
2. Settings –-> Profile Management.
    - This page can only be seen if the configuration status is set to debugging.



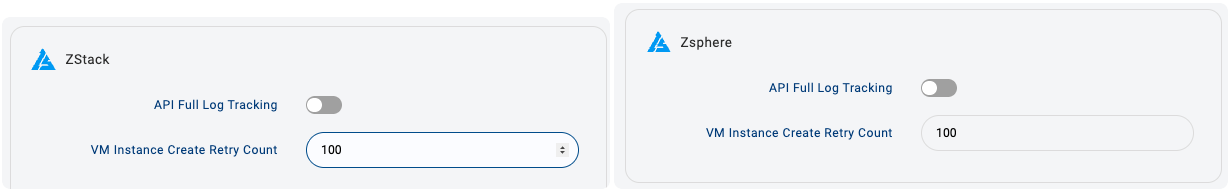
3. `Unlock` configuration.


Settings
Protection Wizard
Setup Wizard
03/27/2026
03:46:58 PM
Administrator
admin
General
License
Diagnostics
User Log
File Management
INI Config
INI Config
Edit
General
Cloud
Management Console
CAPTCHA
API Timeout
5
Rebuild .htaccess
Enhanced Security
Protection
Snapshot Agent
Use VMware CBT Function
Client Speed Limit - MB/s
Unlimited
Interval Minutes
60
Off
Max. Snapshot
3
Off
File System Filter
Source Machine Compression
Buffer Size
No Limit
Data Transmit Type
RPC
Sync Monitor
Provision
Notification

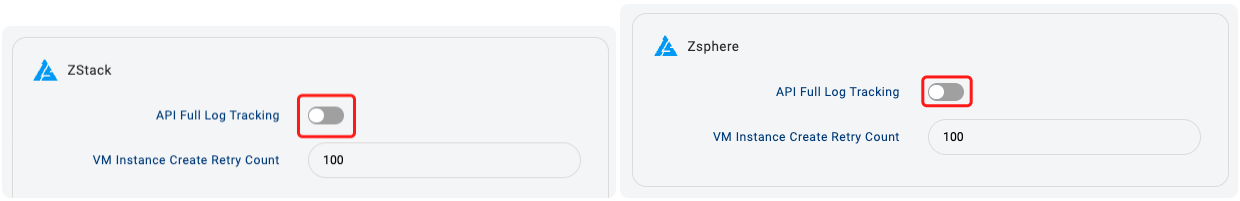

Confirm Password
Please enter your password.
Input mgmt-console's login password
Cancel
Submit



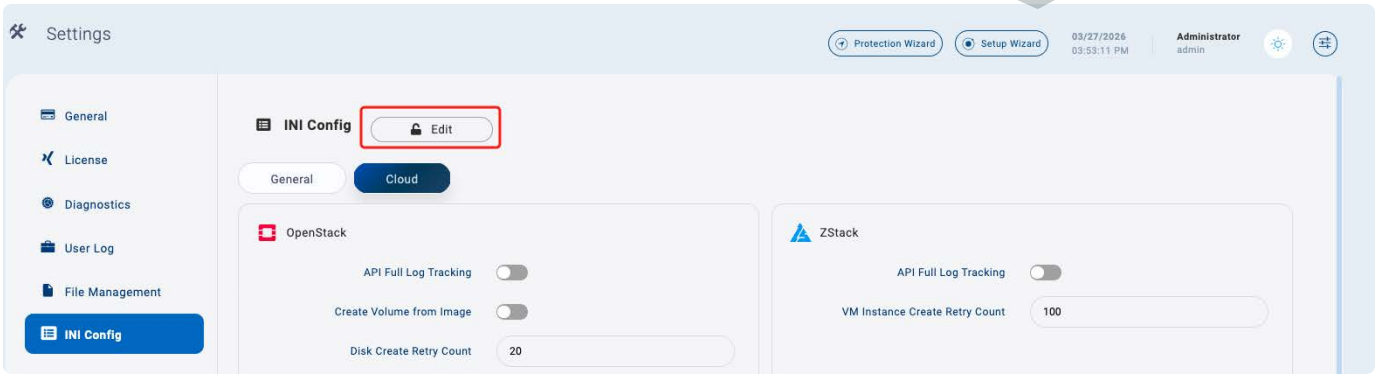
4. Modify the `number of waits` according to the type of target platform (maximum does not exceed 100):
   - When the target is NexaVM, modify NexaVM's `number of cloud host creation retries` .
   - When the target is NexaSphere, modify NexaSphere's `number of cloud host creation retries` .



5. Modify `API debug` according to the type of target platform:
   - When the target is NexaVM, open NexaVM `API full log capture` .



6. `Lock the configuration page` .



7. Rebuild the synchronization task.
8. It is recommended to change the configuration state to `Simple`.

Modify the IP address of the management console

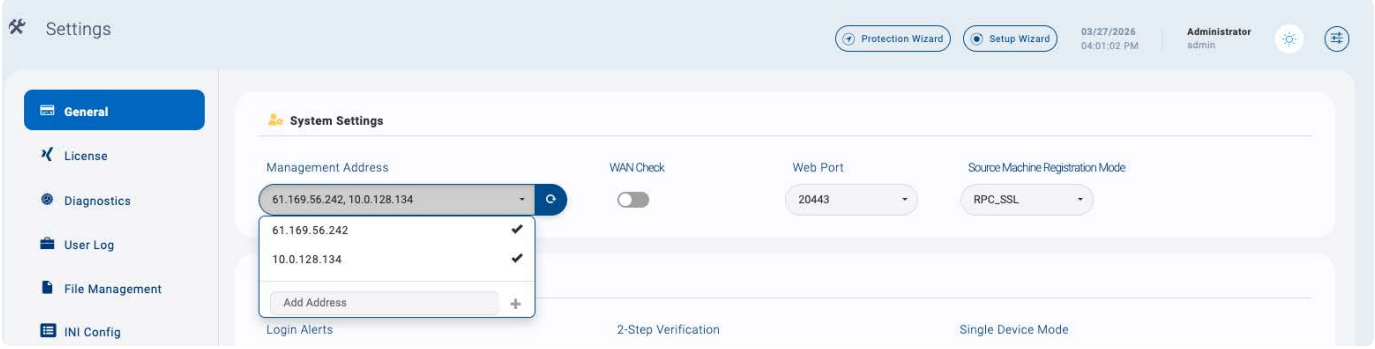
Document Category: Product Related Experience

Prerequisites

1. It only changes the IP, not the management console copied by other environments through mirroring, cloning, etc.
2. There are no synchronization tasks in the management console. If there are, please delete all synchronization tasks.
    - Synchronization tasks that have completed migration can be retained.
    - If you want to retain completed migration tasks, it is recommended to deploy a new migration console.

Operation steps

1. Modify the IP within the system.
2. Log in to the management console, go to the `setting icon` in the upper right corner --> Settings --> `Basic Settings` --> `Central Control Address Settings`, and replace the previous IP with the new IP.
    - Uncheck the previous IP.
    - A new IP has been identified, please select the new IP directly.
    - If the new IP is not automatically recognized, enter the new IP, click `+` and check it.



NEXAVM

3. Delete the cloud platform, data gateway, and source host in the `Resources` of the management console and add them again.
4. Finish.

Switch VDDK to the specified version

Document Category: Third Party Related Experience

Applicable situations

- VADP write failed.
- VMware VDDK is not compatible with VMware ESXi versions.

Compatibility list

> Some versions may have compatibility errors, which can be solved by replacing them with the corresponding version of VDDK.

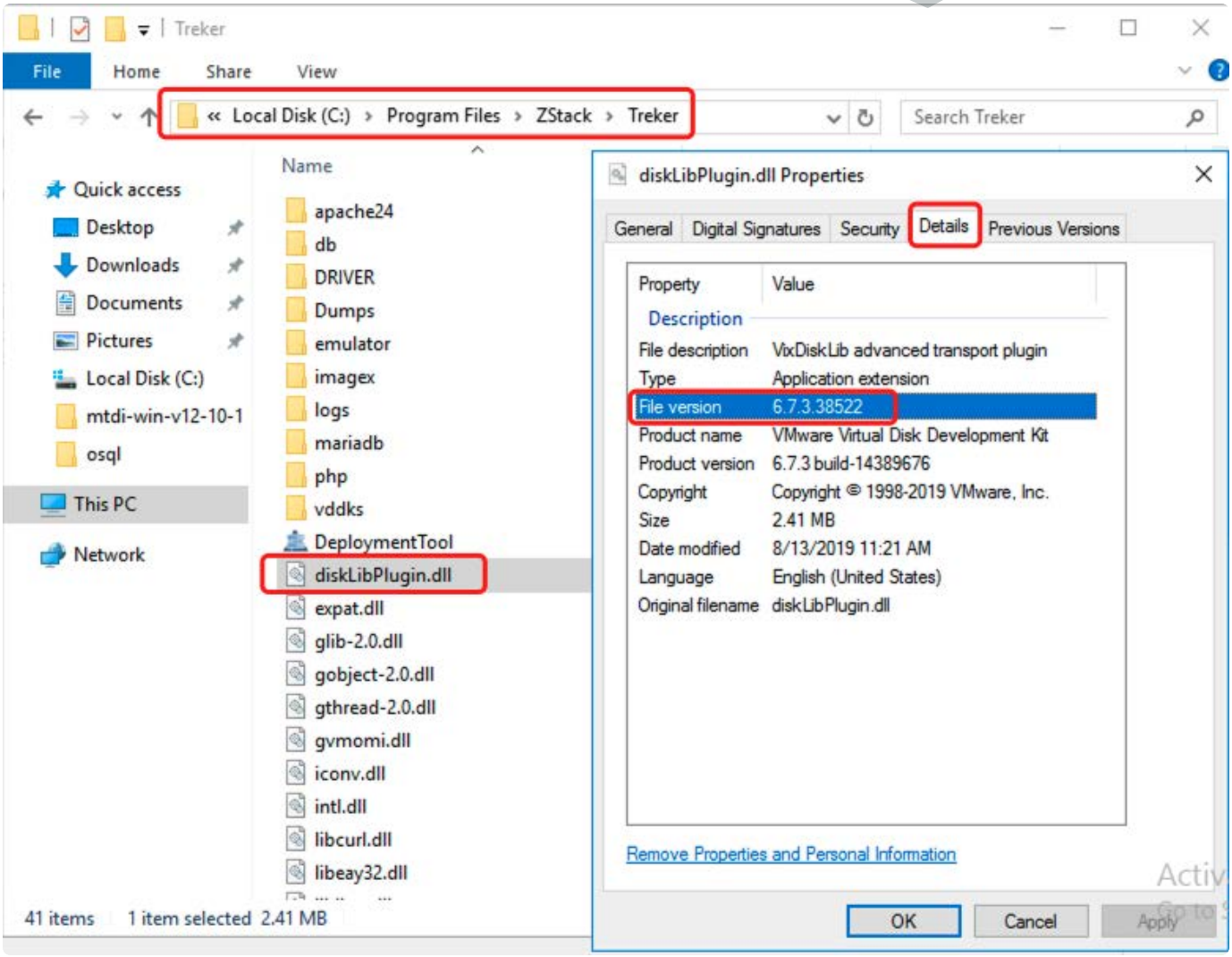
VDDK version	ESXi version
7.0	6.5, 6.7, 7.0, 8.0
6.7	6.0, 6.5, 6.7, 7.0.3, 8.0
6.5	81);">
6.0	81);">

- Verify that VDDK7.0 supports ESXi 8.0.
- Verified VDDK6.7 supports ESXi 7.0 & 8.0.
- Verify VDDK6.7 supports ESXi 7.0.3.

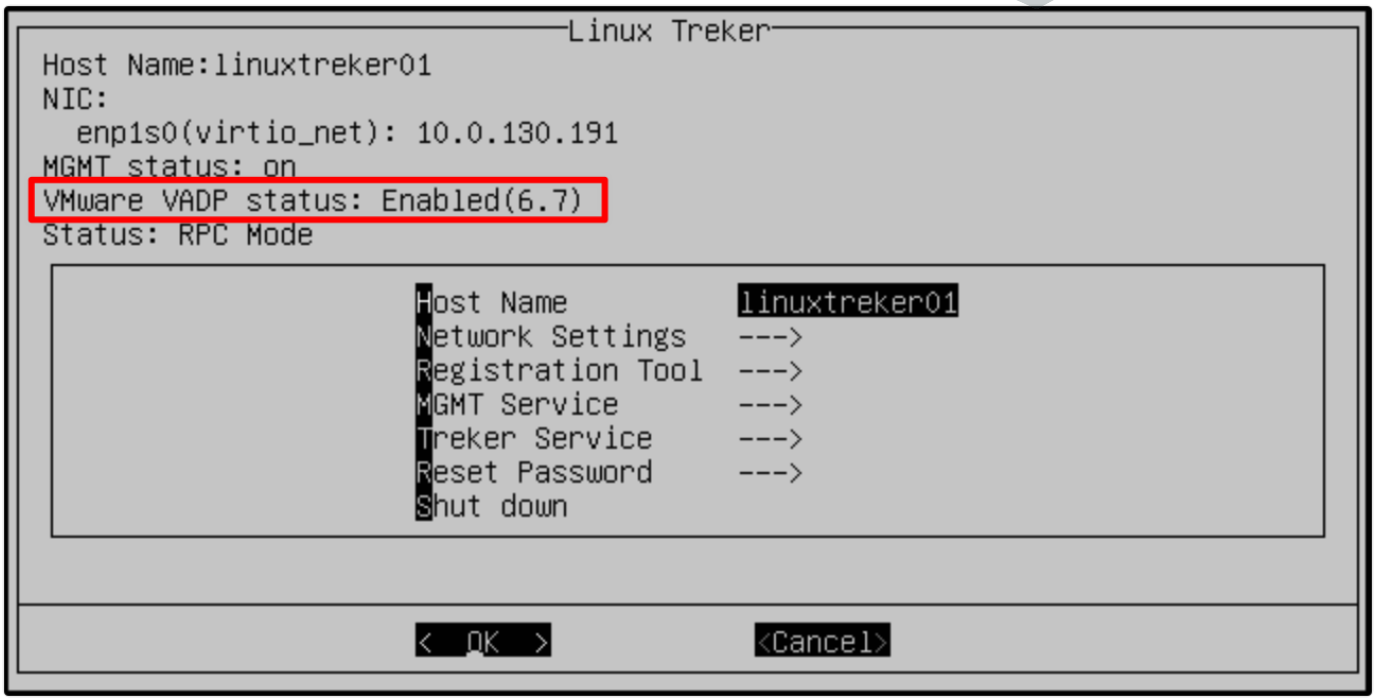
Check VDDK version

Windows Data Gateway

1. Log in to the data gateway that requires VDDK replacement, and switch to the installation directory of Treker.
    - e.g. C:\Program Files\ZStack\Treker\
2. Just view the detailed information of **diskLibPlugin.dll**.



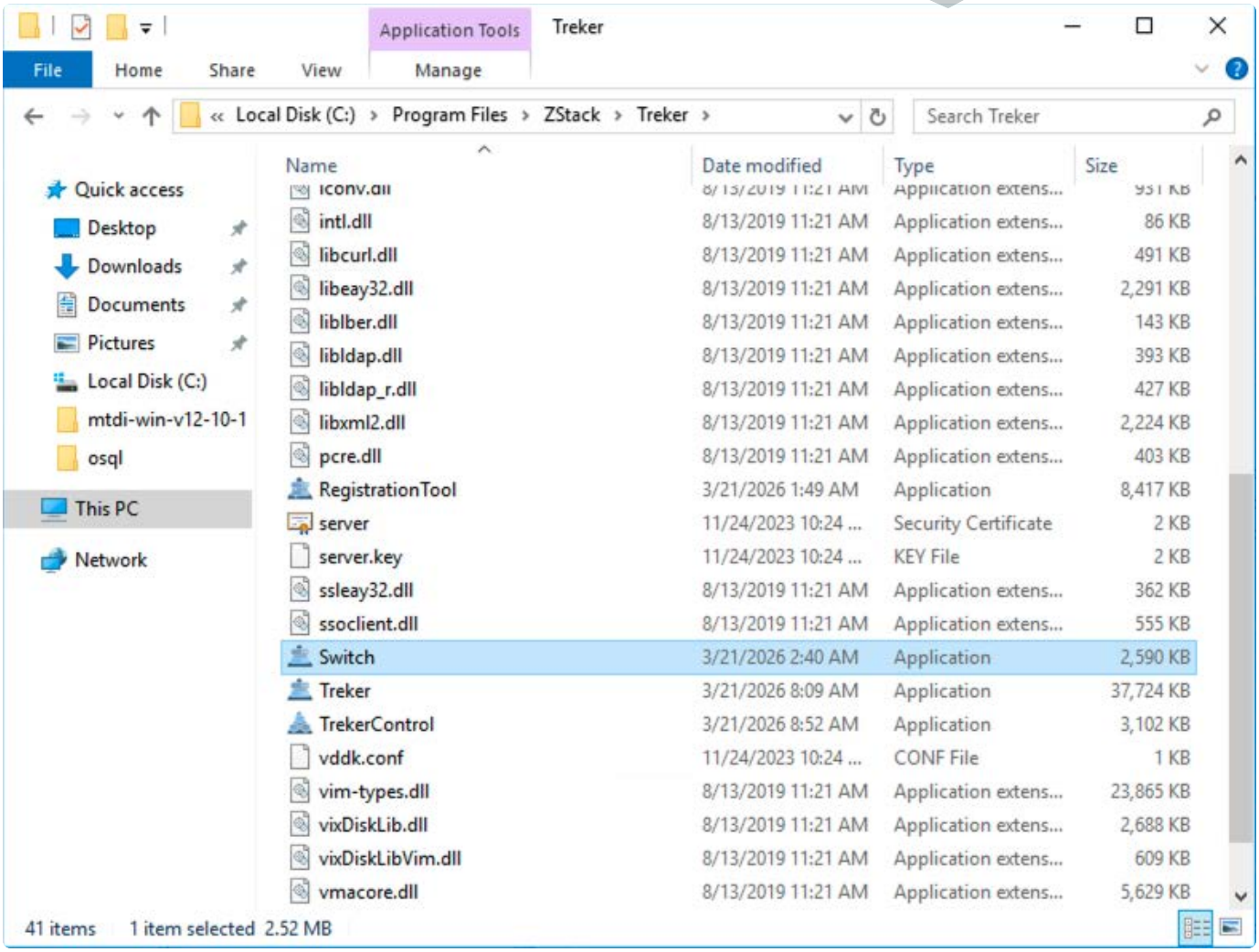
Linux data gateway



Switching steps

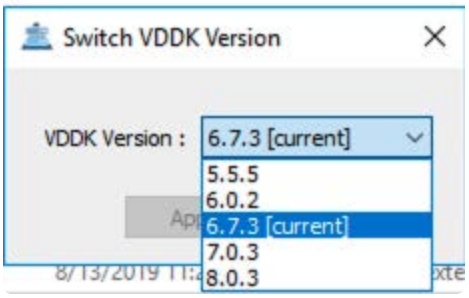
Windows Data Gateway

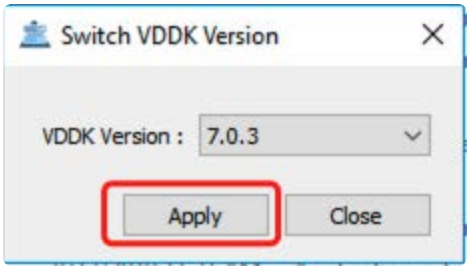
1. Log in to the data gateway that needs to replace VDDK and switch to the Treker installation directory.
    - For example: C:\Program Files\ZStack\Treker\
2. Find the application named Switch.



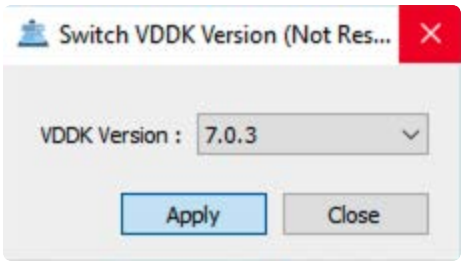
3. Just switch the VDDK version you want to change in Switch.







4. If there is no response, please wait patiently.



5. Switching completed.

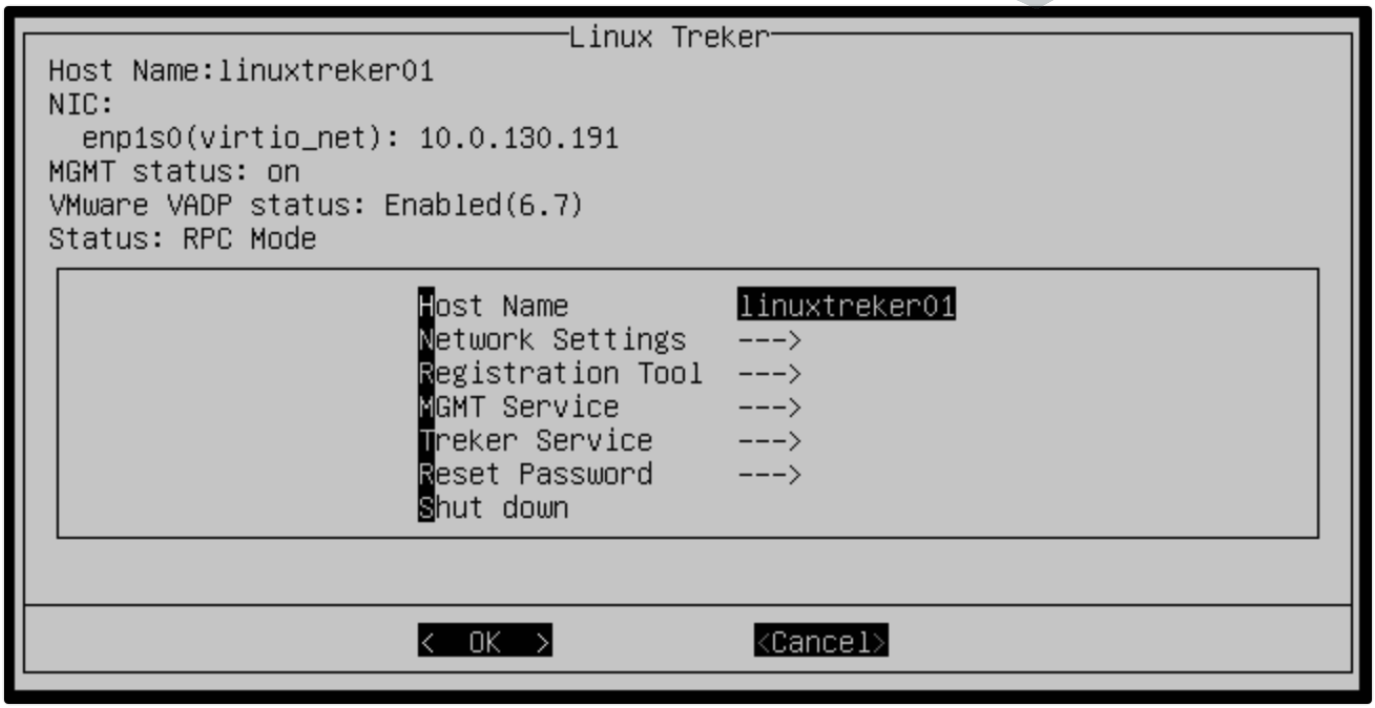


Linux data gateway

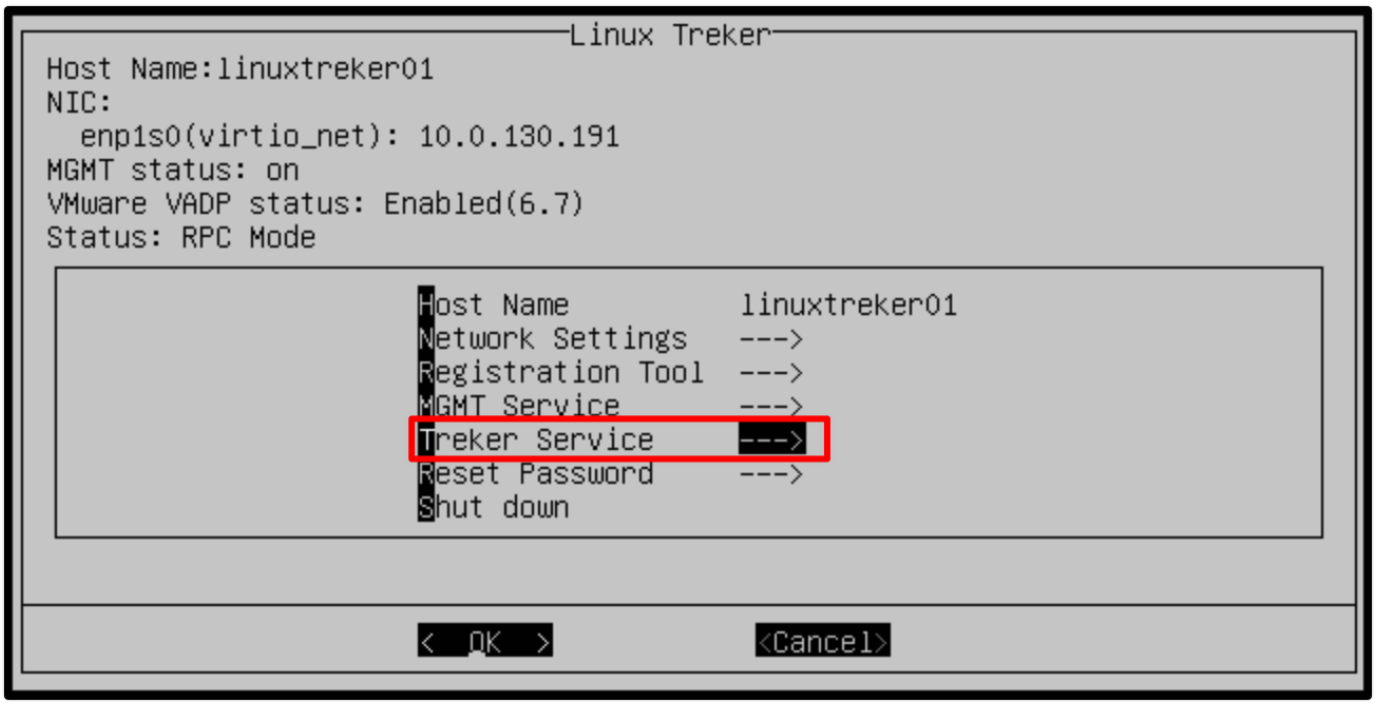
> The Linux version only supports VDDK6.7 and 8.0.

1. Open the LinuxTreker console, you may need to enter the lock password, the default is admin.

NEXAVM

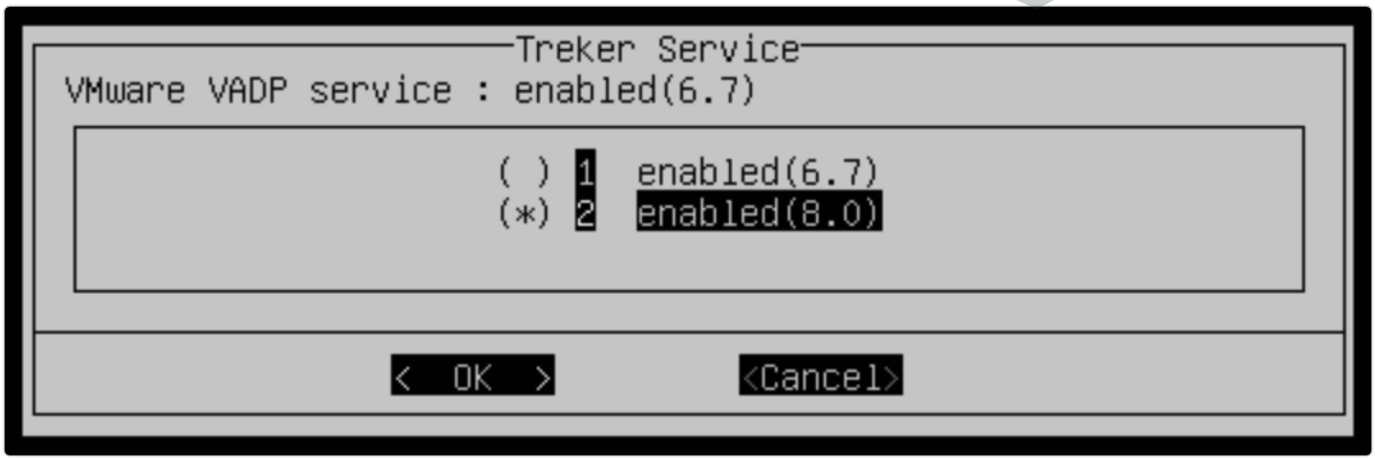


2. Select `Treker Service` and press Enter to confirm.

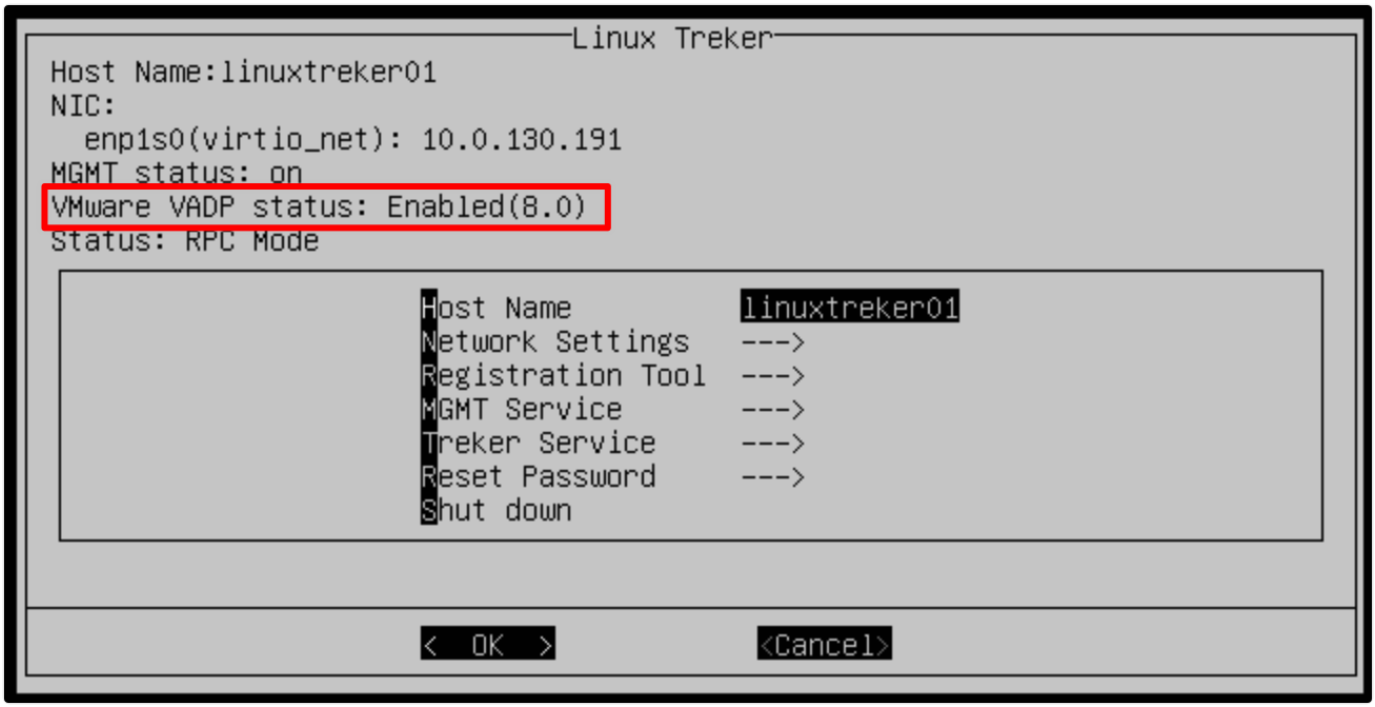


3. Select the VDDK version you want to replace, use the `space bar` to select it, and press Enter to confirm.

NEXAVM



4. Switching completed.



Upgrade VMware virtual machine compatibility

Document Category: Third Party Related Experience

Background

This document copies the content of "Scheduling Compatibility Upgrade of a Single Virtual Machine" from the official website.

VMware Official Documentation：Scheduling compatibility upgrades for individual virtual machines

VMware Official Documentation：Scheduling compatibility upgrades for virtual machines

Prerequisites

- Create a backup or snapshot of a virtual machine.
- Upgrade to the latest version of VMware Tools. On a Microsoft Windows virtual machine, if you upgrade the compatibility level before upgrading VMware Tools, the virtual machine might lose its network settings.
- Confirm all `.vmdk`Whether the file is available to the ESX/ESXi host on a VMFS5 or NFS datastore.
- Confirm whether the virtual machine is stored on a VMFS5 or NFS datastore.

process

1. Right-click the virtual machine and select **Compatibility > Schedule virtual machine compatibility upgrade**.
2. In the**Schedule virtual machine compatibility upgrade**dialog box, click **Yes**Confirm that you want to schedule a compatibility upgrade.
3. From the **Compatible with** drop-down menu, select the compatibility you want to upgrade to. Virtual machine compatibility will be upgraded the next time the virtual machine is restarted.

NEXAVM

4. **(Optional)** To upgrade compatibility when performing regularly scheduled guest maintenance, select **Upgrade only after a graceful shutdown of the guest operating system**.

result

Virtual machine compatibility will be upgraded, and the new version will appear in the virtual machine's Summary tab.

Start and stop related services

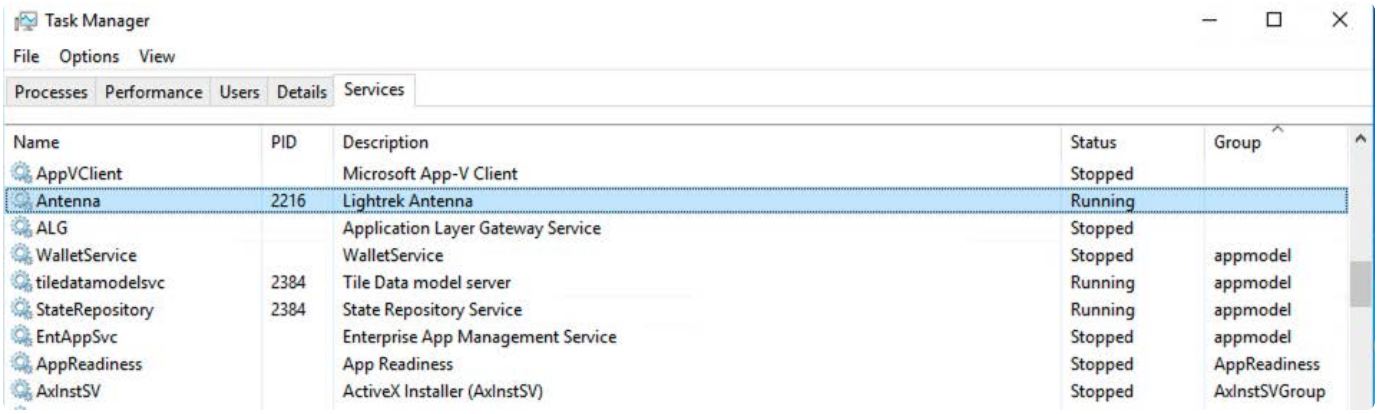
Document Category: Product Related Experience

Source host

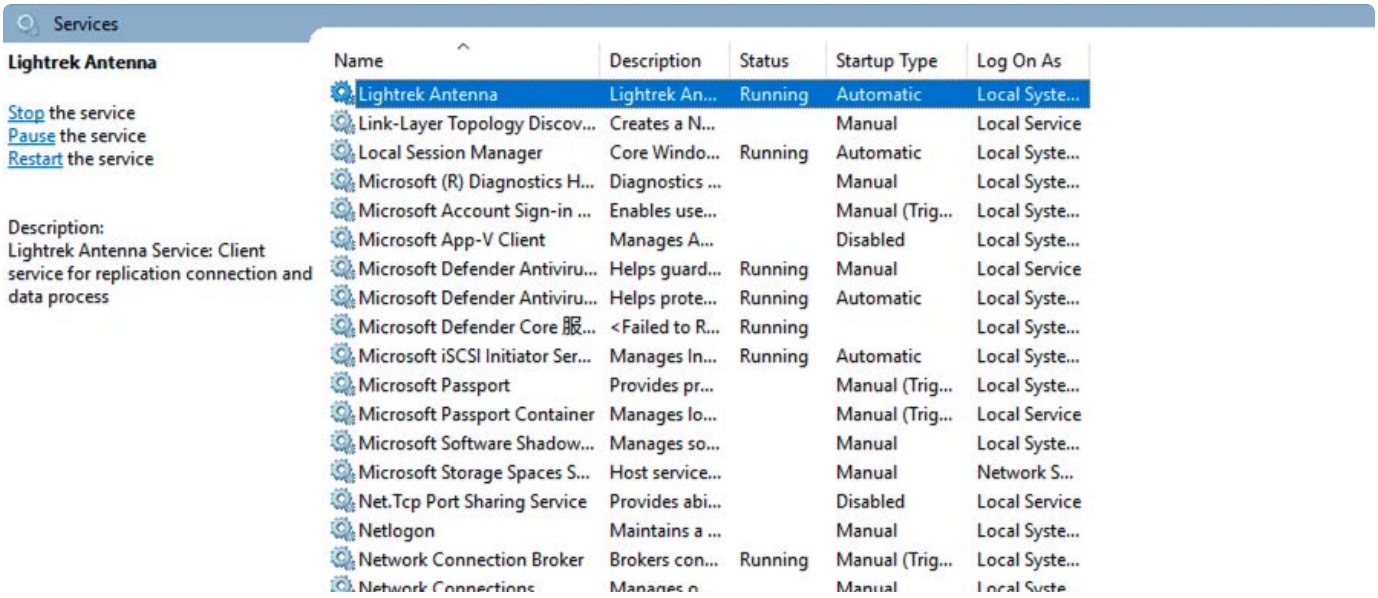
1 service: Antenna

Source host–Windows version

Method 1. Check in the service of the task manager: `Right-click to stop, start, restart`



Method 2. Check in system services: `Right-click to stop, start, restart`



Source host–Linux version

Method 1. Use `systemctl` to manage services:

```
#start Antenna service
systemctl start antenna

#restart Antenna service
systemctl restart antenna

#stop Antenna service
systemctl stop antenna

#check Antenna status
systemctl status antenna

#disable Antenna auto start when OS booting
systemctl disable antenna
```

Method 2. Use `Antenna's parameters` to manage the service in the installation directory:

```
#start Antenna service
/usr/local/antenna/init_service.sh

#stop Antenna service
/usr/local/antenna/stop_service.sh

#restart Antenna service.It is recommended to combine ps -ef | grep antenna to check if the PID has changed.
/usr/local/antenna/antenna --restart
```

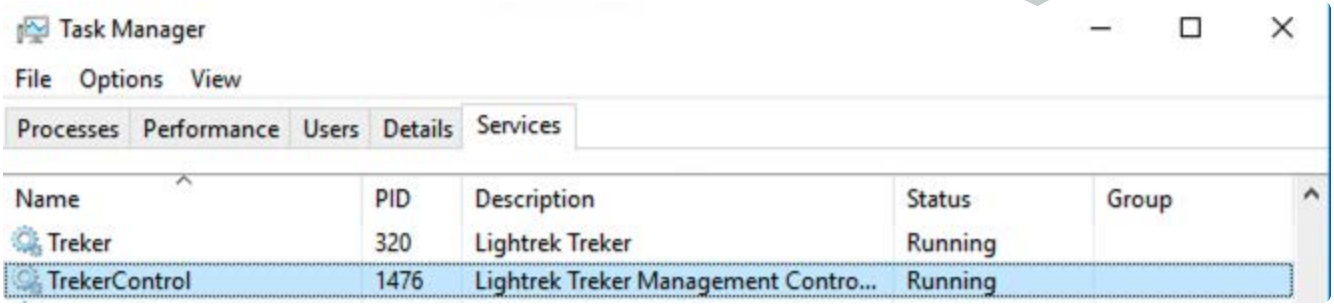
Data gateway

2 services: TrekControl, Treker.

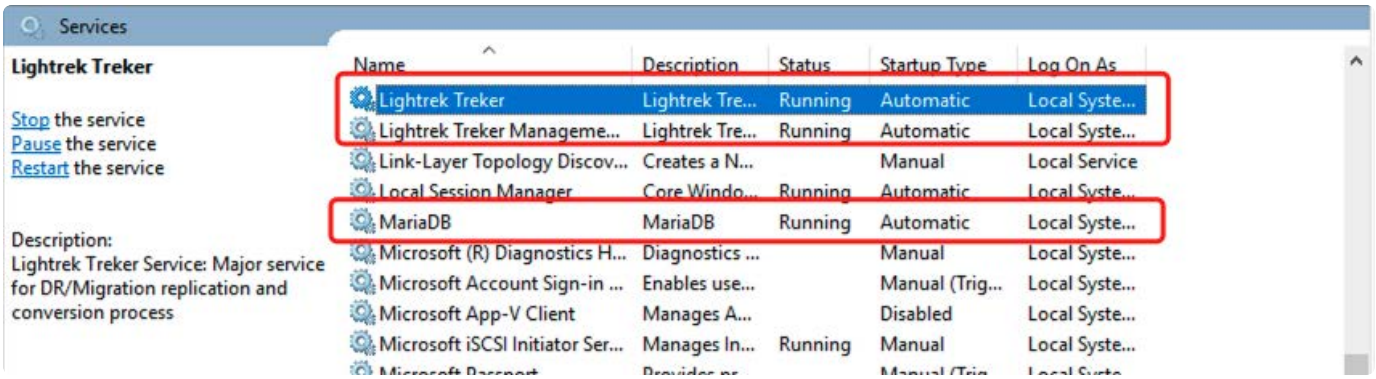
Data Gateway–Windows version

Method 1. Check in the service of the task manager: `Right-click to stop, start, restart`

NEXAVM



Method 2. Check in system services: `Right-click to stop, start, restart`



Data Gateway–Linux version

**After logging in to the guest, sudo to the root user, or use the sudo command. **

```
root@linuxtreker01:~# docker ps -a
CONTAINER ID   IMAGE              COMMAND                  CREATED        STATUS                    PORTS     NAMES
0201eaaad9e8   convert:673        "/usr/local/convert/…"   2 months ago   Up 2 months                         convert
771589f140c7   trekercontrol:673  "/usr/local/trekerco…"   2 months ago   Up 2 months (healthy)               trekercontrol
e3774781fbd6   treker18:673       "/usr/local/treker/t…"   2 months ago   Up 2 months (healthy)               treker
b57fe476cea8   mariadb:10.11.6    "docker-entrypoint.s…"   2 months ago   Up 2 months                         mariadb
048cd278ad5c   php:7.4.33-apache  "docker-php-entrypoi…"   2 months ago   Up 4 weeks                          mgmt
```

```
#restart apache
docker restart mgmt

#restart apache and treker
docker restart mgmt treker
```

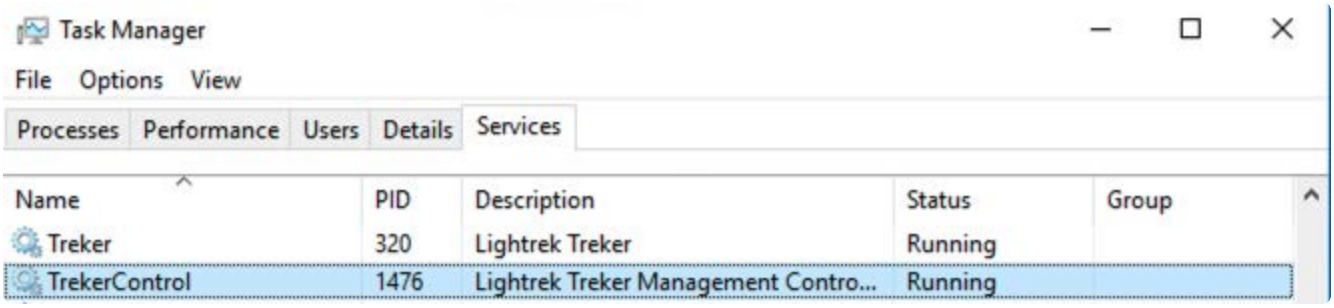
```
root@linuxtreker01:~# docker restart mgmt
mgmt
root@linuxtreker01:~# docker restart mgmt treker
mgmt
treker
```

Management console

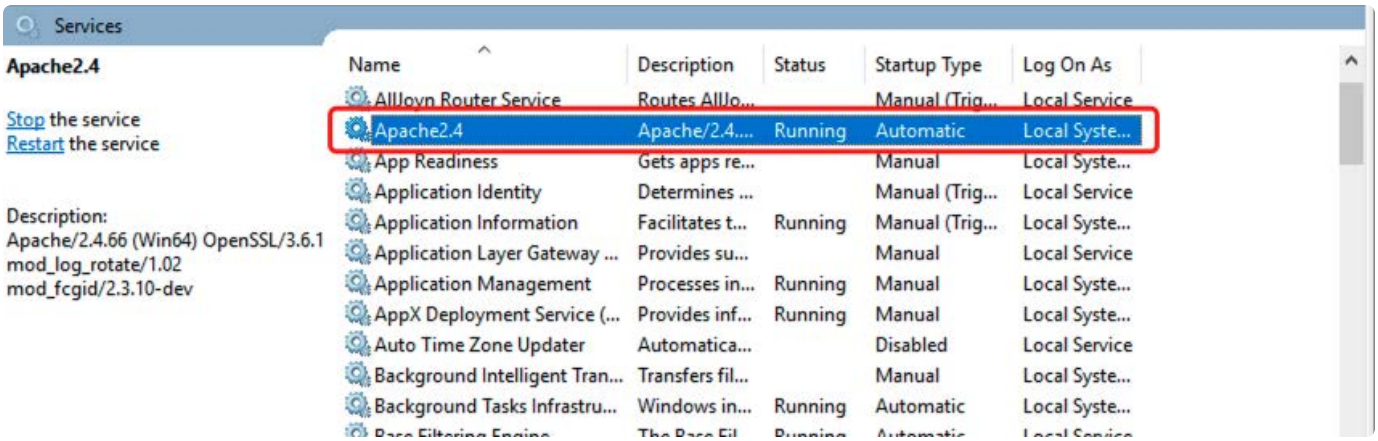
4 services: MariaDB, TrekerControl, Treker, Apache2.4.

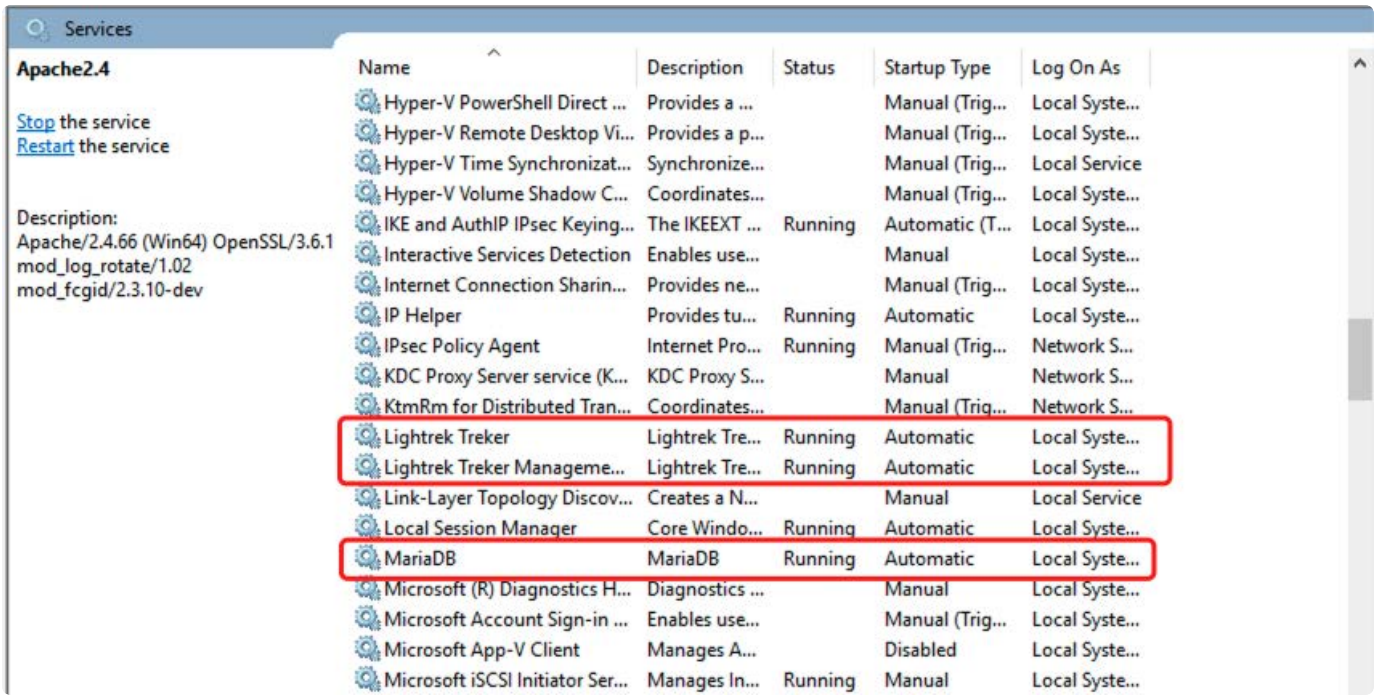
Management Console – Windows version

Method 1. Check in the service of the task manager: `Right-click to stop, start, restart`



Method 2. Check in system services: `Right-click to stop, start, restart`





Management Console–Linux version

NEXAVM

**After logging in to the guest, sudo to the root user, or use the sudo command. **

```
root@linuxtreker01:~# docker ps -a
CONTAINER ID   IMAGE                COMMAND                  CREATED        STATUS                    PORTS     NAMES
0201eaaad9e8   convert:673          "/usr/local/convert/…"   2 months ago   Up 2 months                         convert
771589f140c7   trekercontrol:673    "/usr/local/trekerco…"   2 months ago   Up 2 months (healthy)               trekercontrol
e3774781fbd6   treker18:673         "/usr/local/treker/t…"   2 months ago   Up 2 months (healthy)               treker
b57fe476cea8   mariadb:10.11.6      "docker-entrypoint.s…"   2 months ago   Up 2 months                         mariadb
048cd278ad5c   php:7.4.33-apache    "docker-php-entrypoi…"   2 months ago   Up 4 weeks                          mgmt
```

```
1  #restart apache
2  docker restart mgmt
3
4  #restart apache and treker
5  docker restart mgmt treker
```

```
root@linuxtreker01:~# docker restart mgmt
mgmt
root@linuxtreker01:~# docker restart mgmt treker
mgmt
treker
```

Limit the speed of protection tasks - at the cloud platform level

Document Category: Product Related Experience

Applicable scenarios

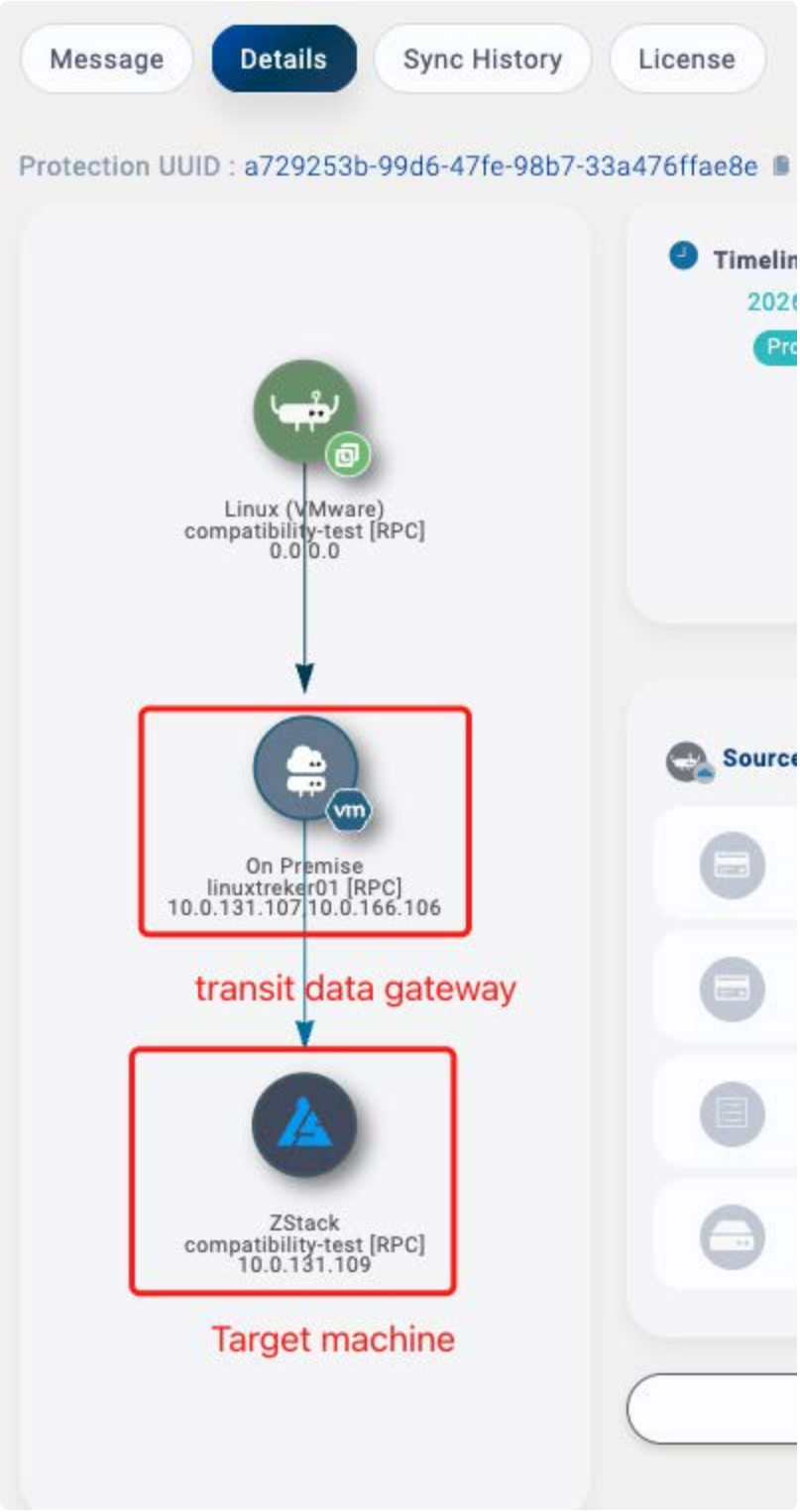
Users do not want protection tasks to occupy too much bandwidth to avoid affecting their business.

Implementation method

Modify the cloud host network card QoS of the NexaVM platform.

solution

1. View the topology diagram of the protection task and confirm the transit data gateway and target node.



2. Find the transit data gateway and configure network card QoS.
    - The network card QoS of the transit data gateway determines the overall speed of all protection tasks passing through the transit data gateway.
    - Under normal circumstances, just modify the QoS of the network card of the transit data gateway.
3. [Optional] Find the target machine and configure network card QoS.

Limit the speed of protection tasks - at the source host level

Document Category: Product Related Experience

Applicable scenarios

Users do not want protection task to occupy too much bandwidth to avoid affecting their business.

Speed limit logic

Antenna's speed limit is a speed limit at the network level, so you need to specify the next hop of the network. If there are multiple IP addresses in the next hop, fill in the IP address that can communicate with the source host when limiting the speed.

There is a structure of transit data gateway, and the next hop is the transit data gateway.

There is no architecture for transferring data gateway (the source host goes directly to the target machine), and the next hop is the target machine.

Force deletion of protection or provision tasks

Document Category: Product Related Experience

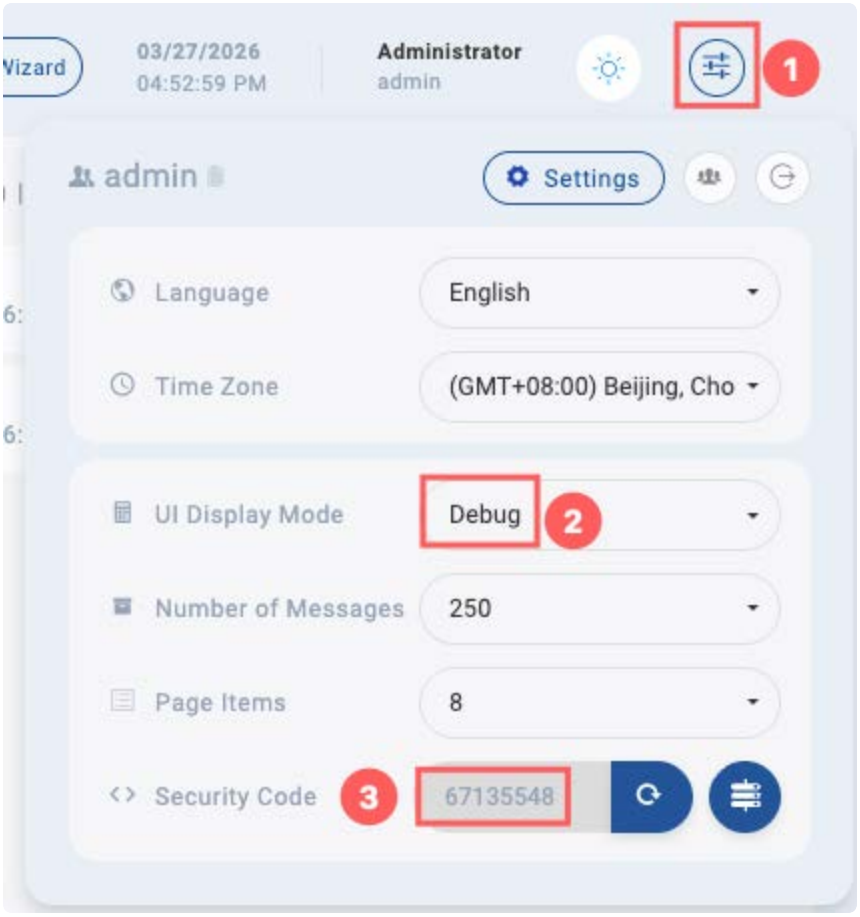
Applicable scenarios

Delete protection tasks or get stuck provison tasks.

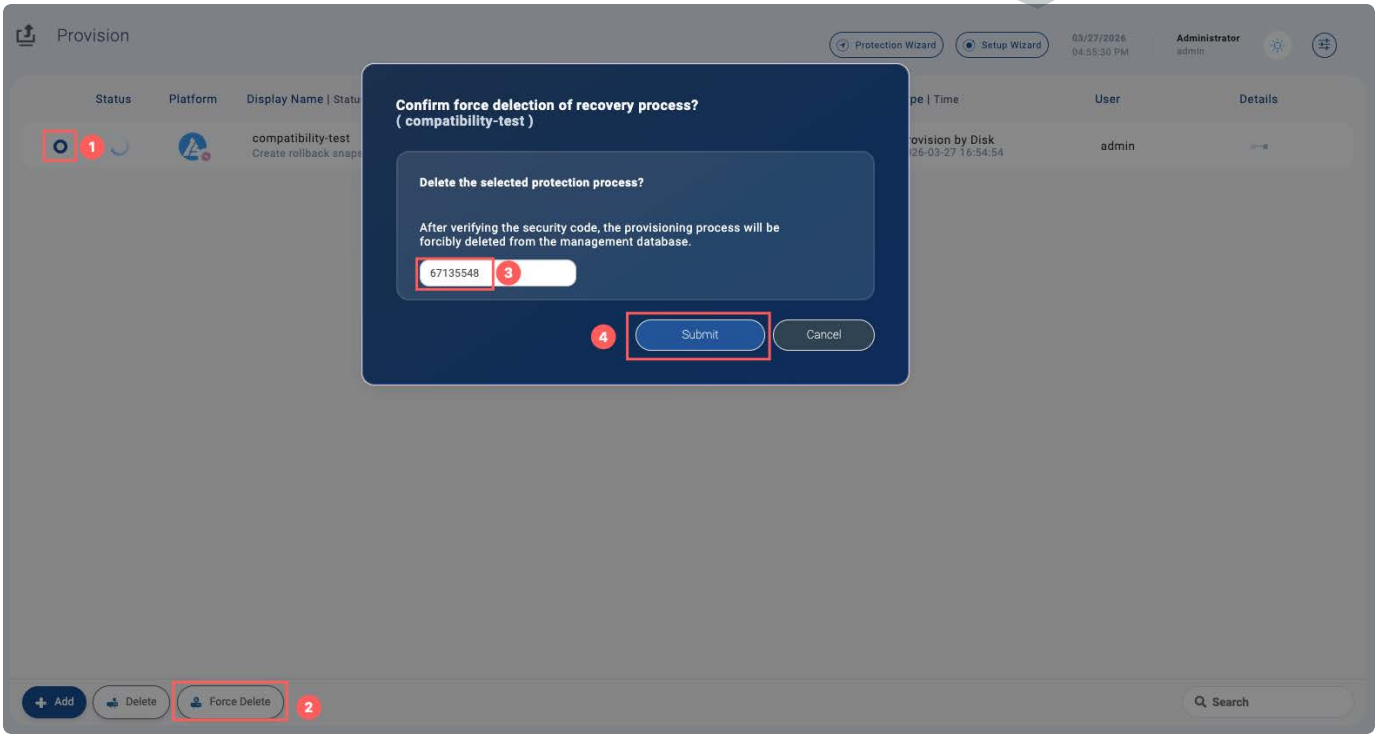
- Please confirm with Support first whether forced deletion is required.

Operation steps

1. Set the configuration mode of the management console to troubleshooting and copy the verification code.



2. Select the task, click "Force Delete" and enter the verification code.

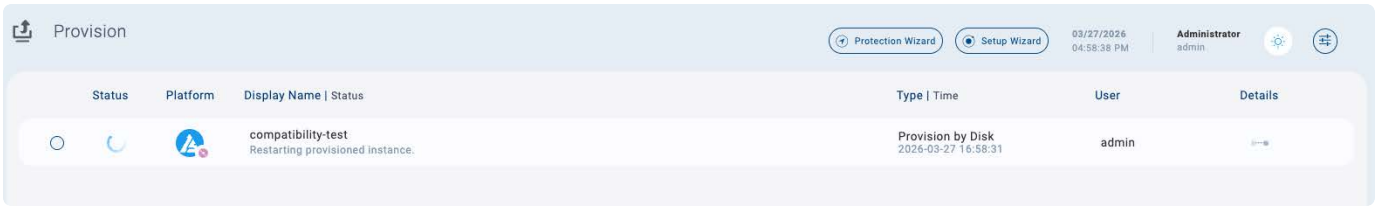


3. Deleted successfully.

Force the Provision task progress to 100%

Document Category: Product Related Experience

Progress description



Progress 100%:**In most cases, after the provision task is completed, the task displays "Successfully started the operating system." **

- Successfully started the operating system: This information is fed back to the management console when the target machine is powered on for the first time after provision.
  - The network configured when the target machine is powered on for the first time after provision can communicate with the management console, and the management console can get this information.
  - The openssl version of some systems is too low to communicate with the https protocol (port 443 or 20443) of the management console, and Netcom cannot get this information.
    - Openssl version compatibility issue. Communication with the http protocol (port 80) of the management console has been supported. Port 80 of the management console needs to be released to the target machine.

The progress is 72% or 81%:**In some cases, after the provision task is completed, the task displays "Restart target enable host". **

- Reboot the target and enable the host: This is after the switch, and the boot command has been issued to the target machine. In theory, the switch is completed here.
  - The network configured for the first power-up after the target machine is switched cannot communicate with the management console, and the management console cannot get the "operating system started successfully" information, so it will be stuck here.
  - The openssl version of some systems is too low to communicate with the https protocol

NEXAVM

of the management console, and Netcom cannot get "Successfully started the operating system", so it will get stuck here.

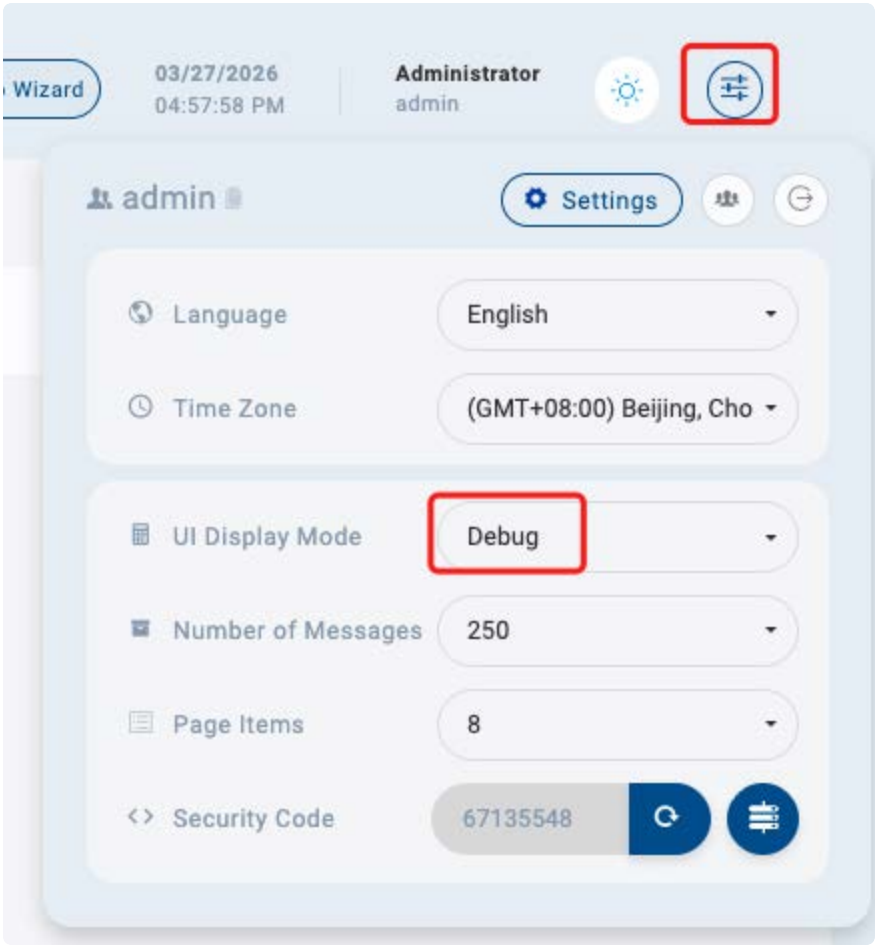
Applicable scenarios

**Version requirements: Management console version ⩾ (greater than or equal to) 676. **

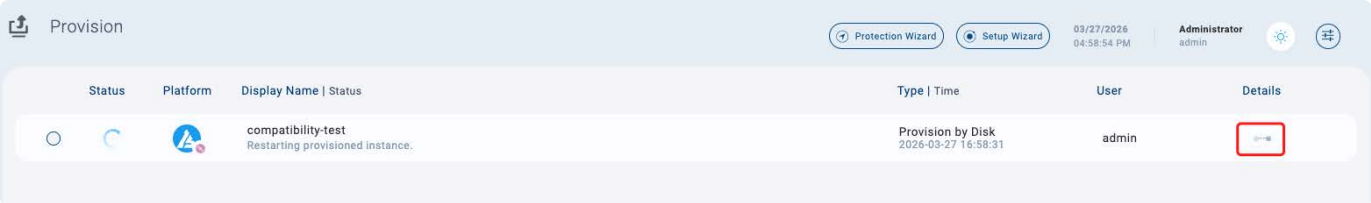
1. The progress is 72% or 81% (restart the target to enable the host), and check that the target machine has entered the system normally.
2. Skip system conversion and check that the target machine has entered the system normally.
3. The system conversion fails, and Support manually performs the post-system conversion tasks.

Operation steps

1. Change the `configuration state` of the management console to `Debug`.
    - Upper right corner: Settings --> Configuration state --> Debug.

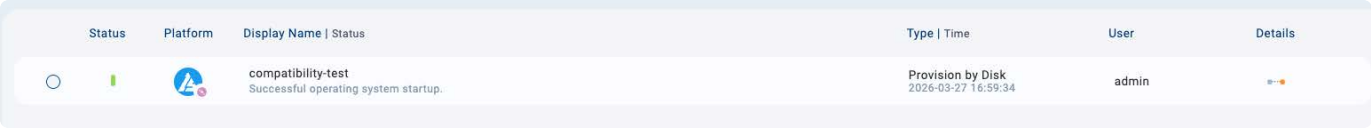


2. Find the provision task that needs to be forced to set 100%, and click `Information`.



3. Click ☑ and wait for a few seconds, "Operating system started successfully" will be displayed.





Manual BootImage (TL) mode for verification testing

Document Category: Product Related Experience

Prerequisites

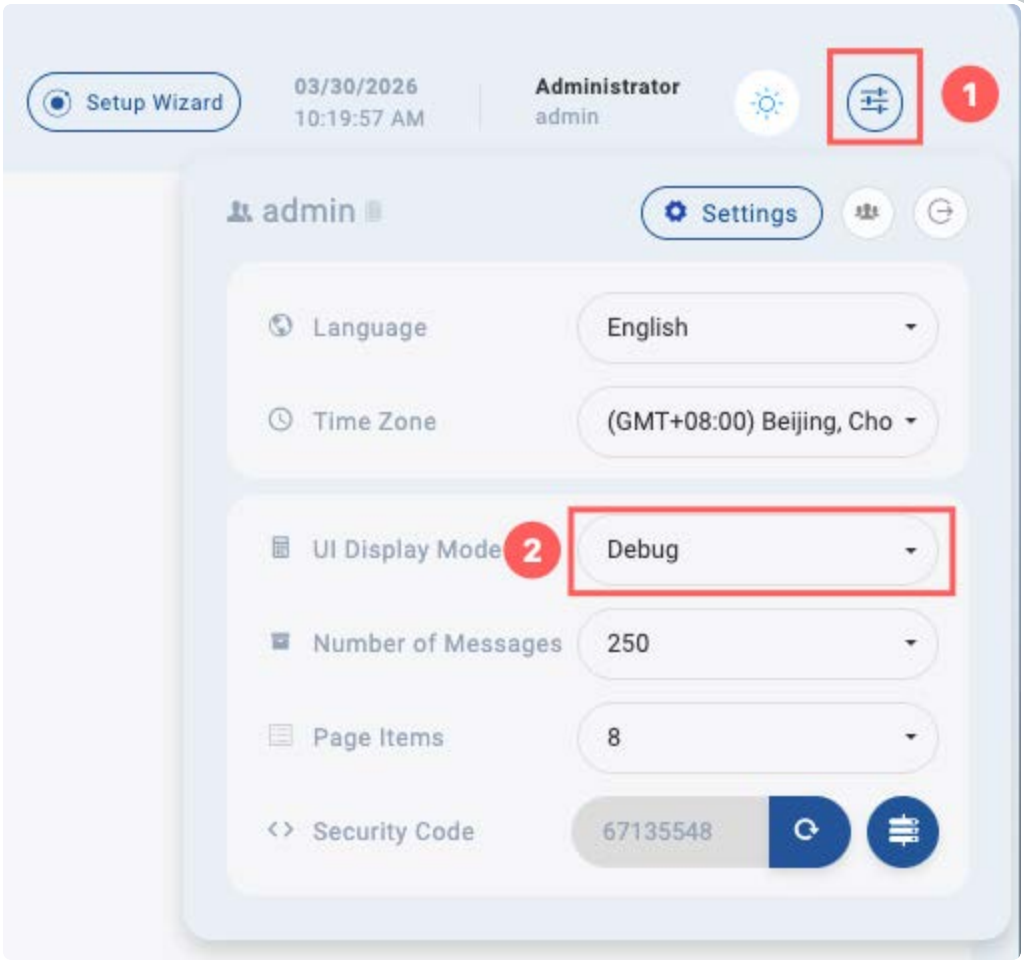
- The target cloud supports manual snapshots, and cloud hosts can be created from snapshots.

or

- The target cloud platform supports cloning cloud hosts.

Operation steps

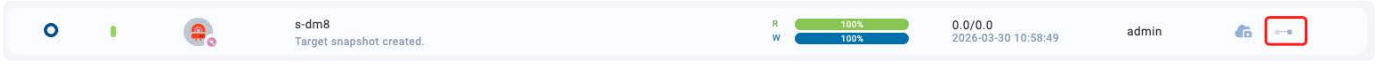
1. Adjust the configuration status of the management console to `Debug`.

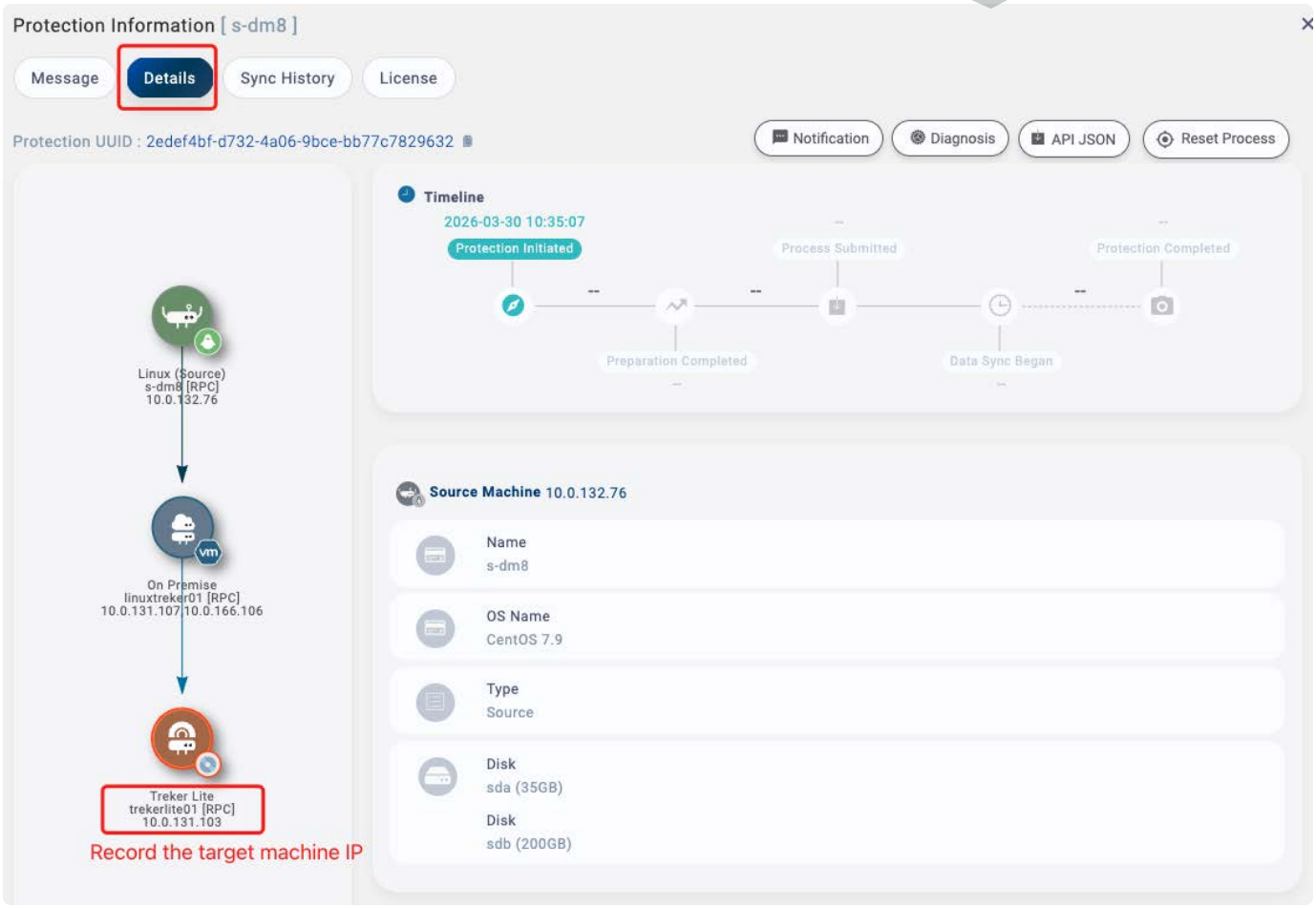


2. Confirm that the current increment is completed and the task information is "Target snapshot created".



3. Confirm the target machine based on the IP address in the topology map.

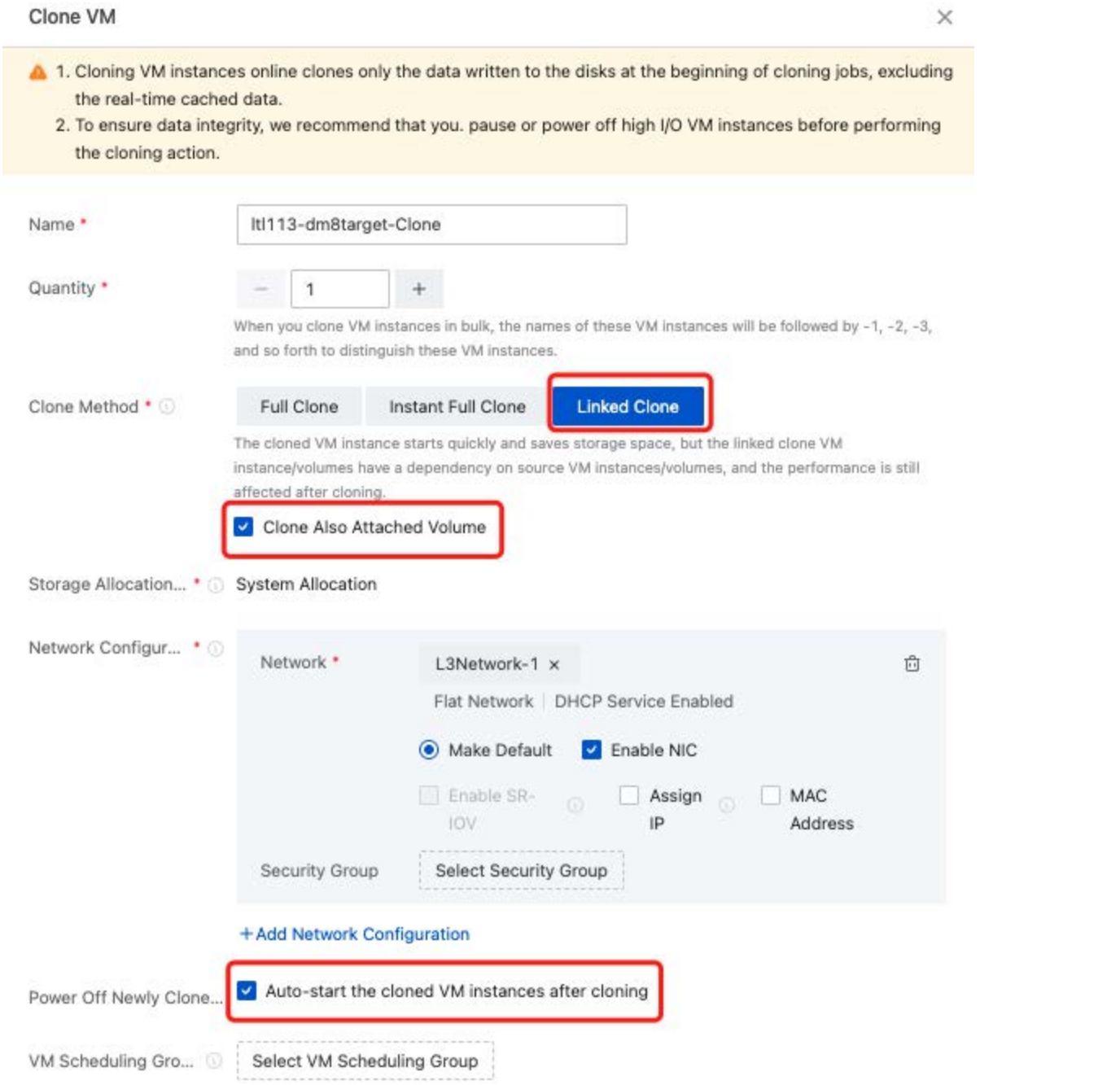


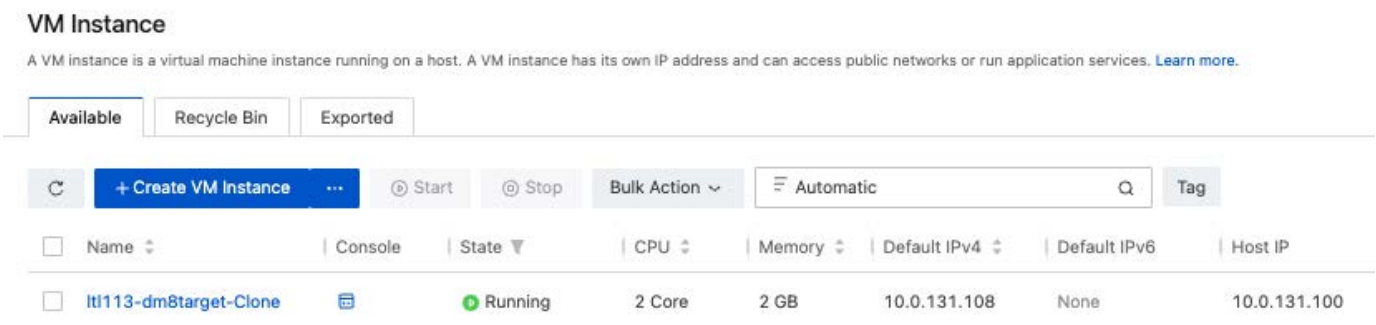


4. Go to the NexaCloud platform to find the target machine and clone the target machine.



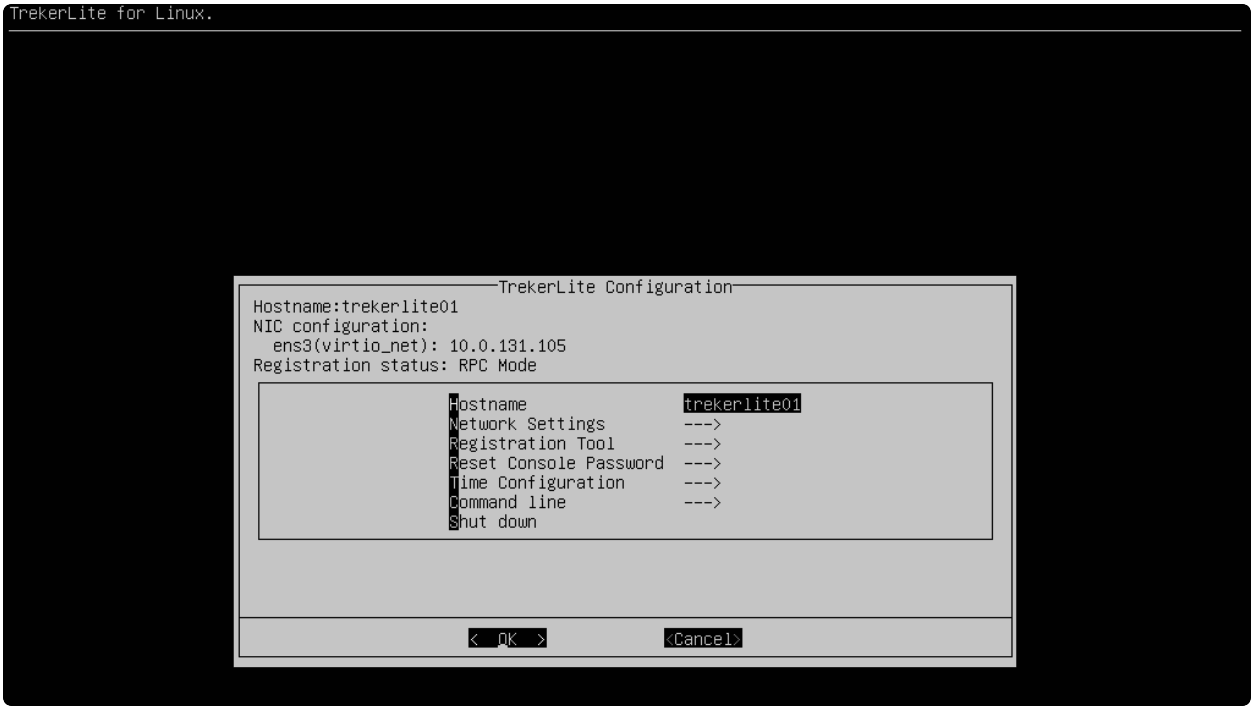
NEXAVM



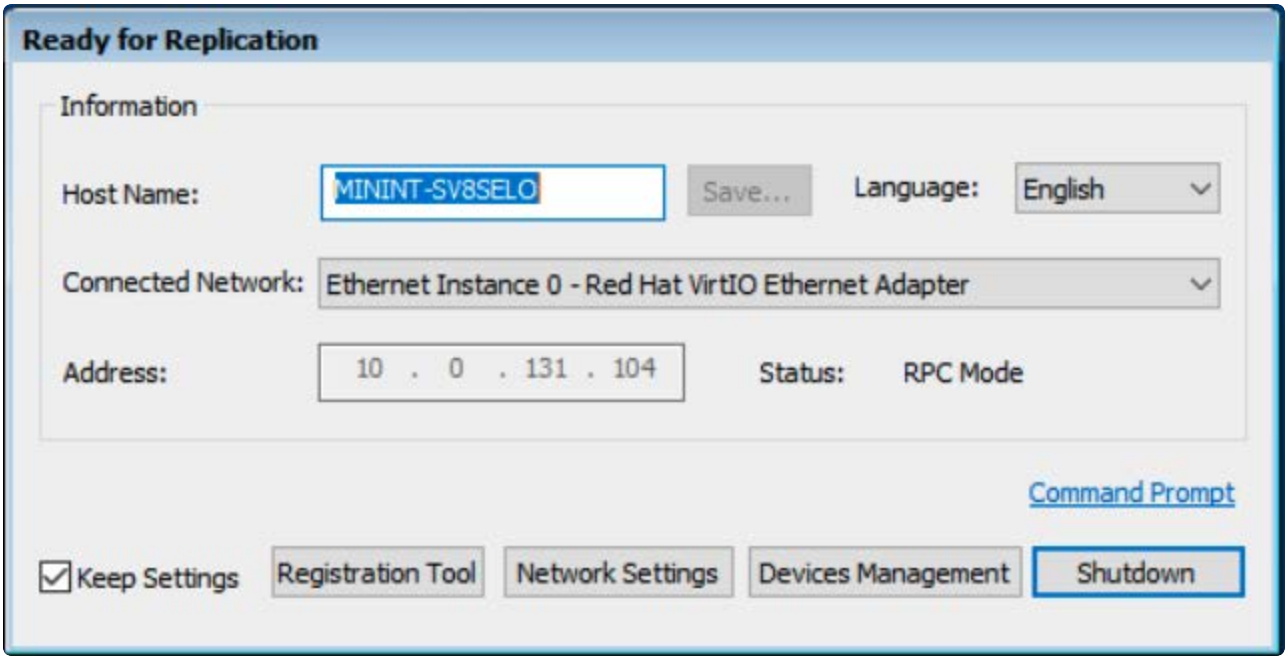


5. Record the IP address of the cloned target machine, and wait for the target machine to boot up and enter the configuration interface.

Configuration interface of Linux target machine

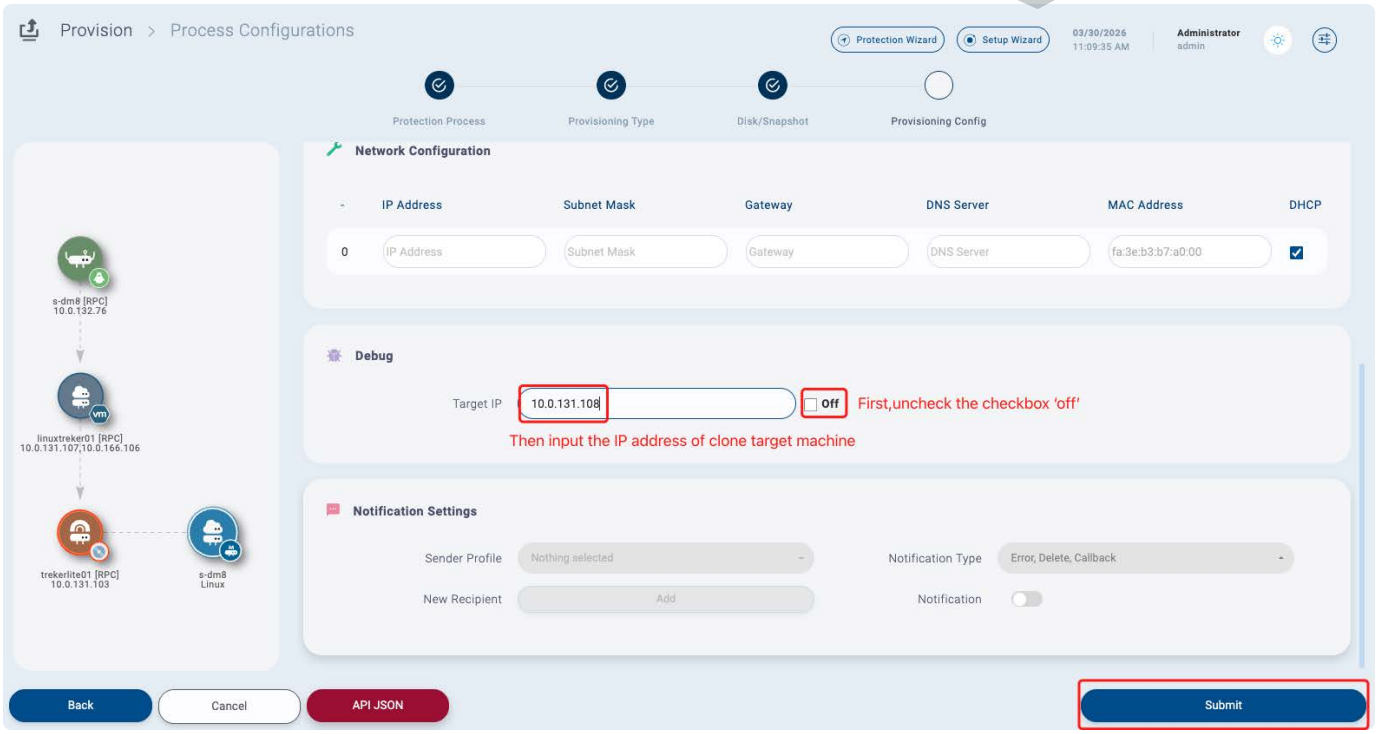


Configuration interface of Windows target machine



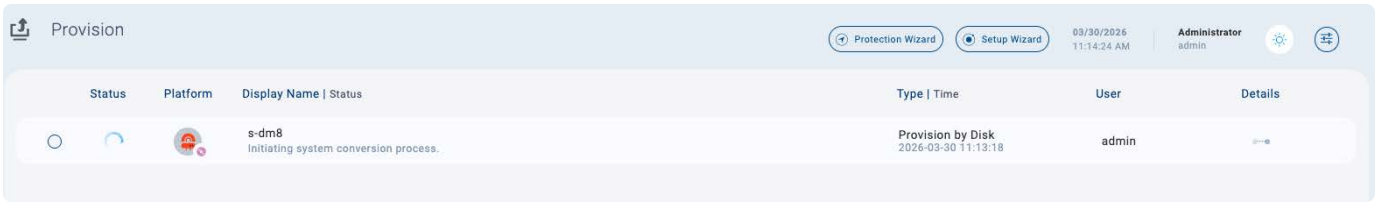
6. Create a provision task, uncheck Target IP's 'Off', and enter the IP address of the clone target machine.

- Be sure to wait until the target machine enters the configuration interface in step 5 before performing this operation!
- Must not add the clone target machine to the data gateway!

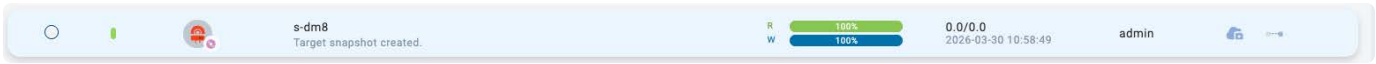


7. Wait for the provision task to complete, and you can observe that the protection task is still functioning normally.

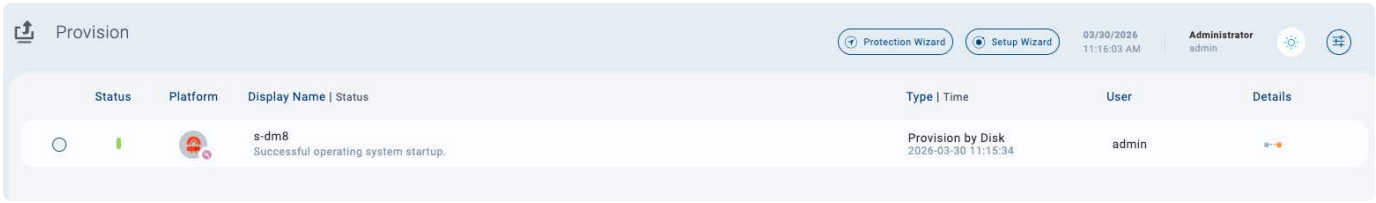
Submitted provision tasks:



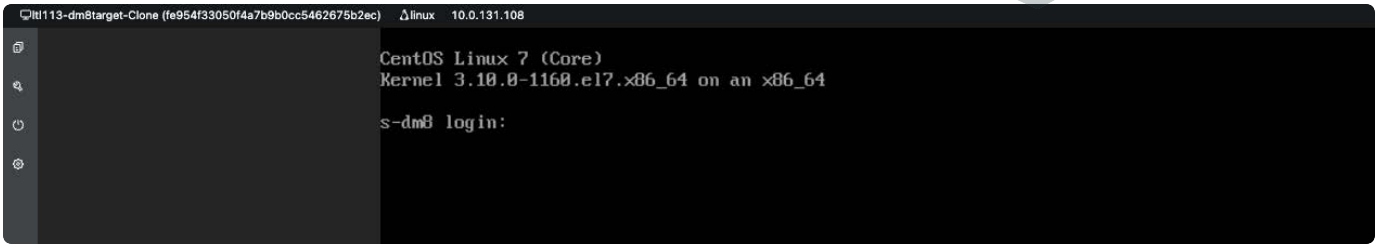
Normally functioning sync tasks:



8. The provision task has been completed.

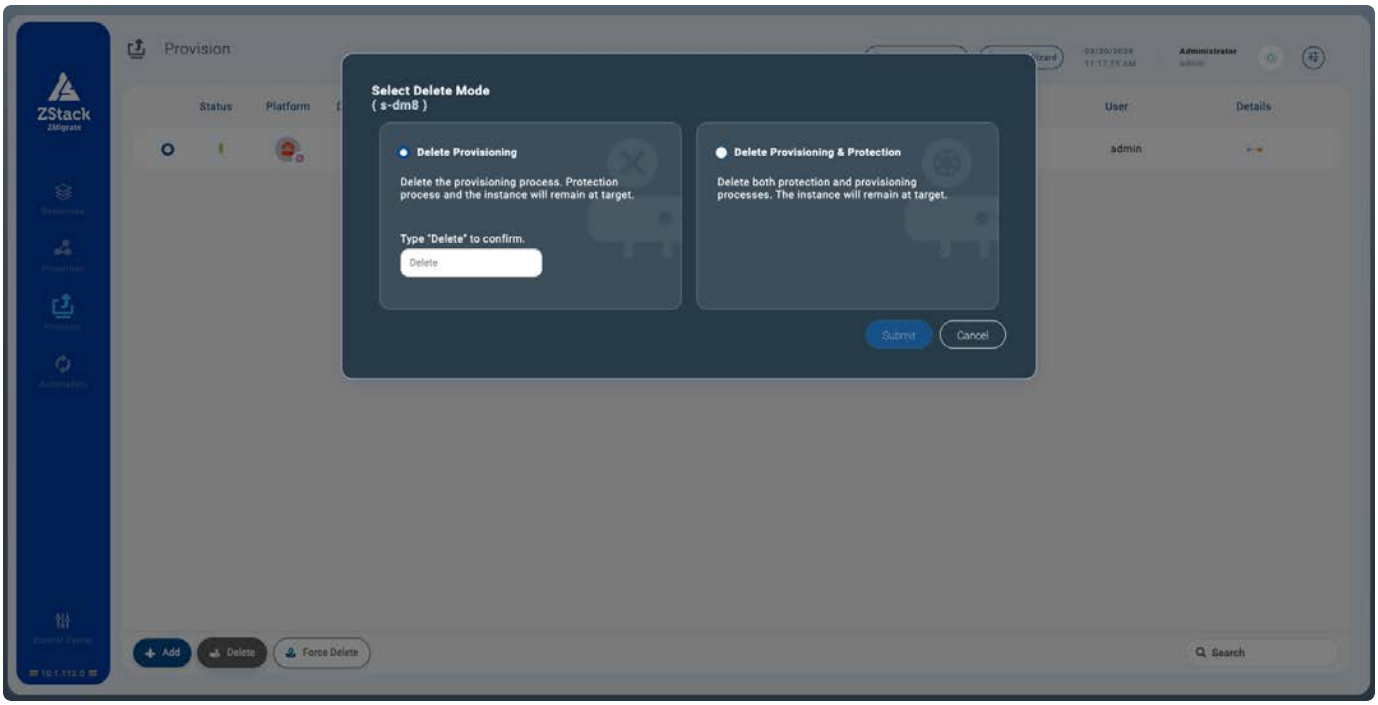


9. Log in to the NexaCloud platform to check that the clone target machine has been successfully switched to the business system.



10. After the test verification is completed, delete the provision task as needed and manually delete the target cloud host from the cloud platform.

Delete a task:Select the option on the left. (Delete the provisioning process. Protection process and the instance will remain at target.)



11. Test verification completed.

Manually install Windows Antenna

Document Category: Product Related Experience

Notes

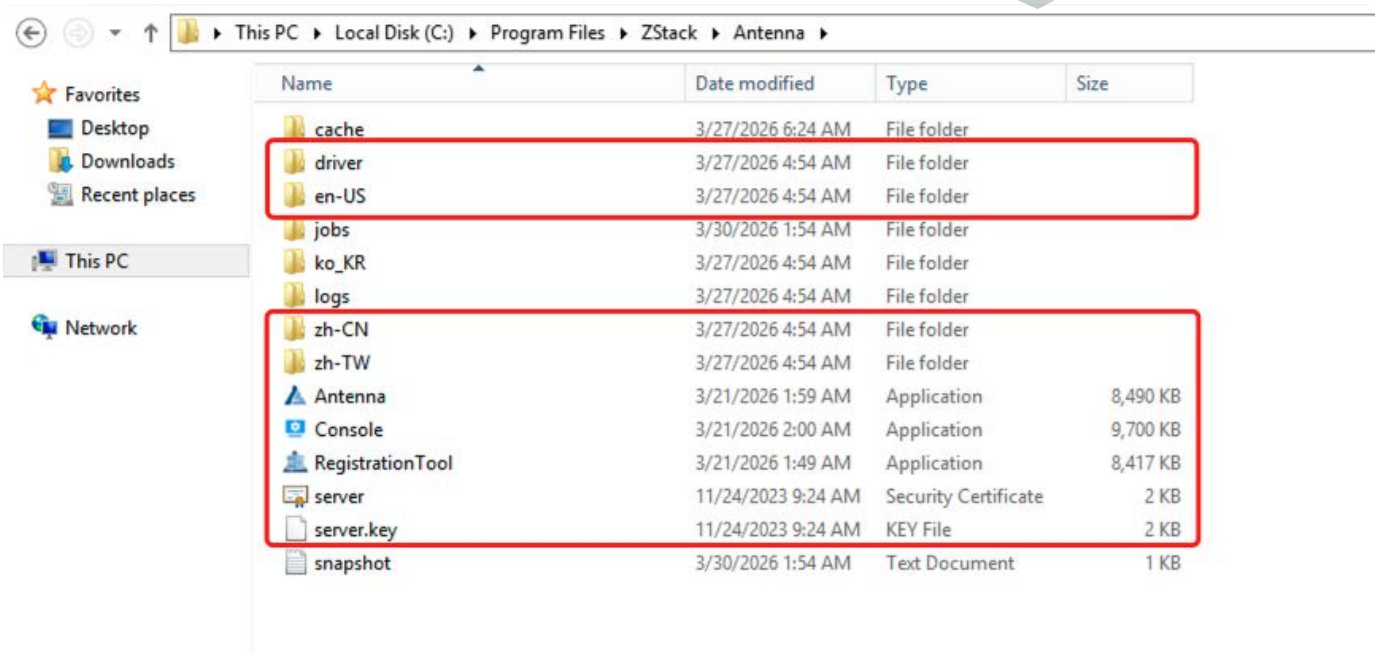
1. Windows 2003 does not require a KB, so do not use this method.
2. This method can be used for non-2003 versions, but you need to pay attention to the system number and system version requirements.
    - System bit requirements:
        - 32-bit systems copy files in 32-bit systems.
        - 64-bit systems copy files in 64-bit systems.
    - System version requirements:
        - Antenna directories and files are common to Win7, Win8, Win10, Win11, Win2008, Win2008 R2, Win2012, Win2012 R2, Win2016, Win2019, Win2022, etc.

Scenario where the source machine does not have Microsoft KB and does not want to install KB - the increment is checksum

Steps to install Antenna

Note: Each increment is cheksum (contrast differential transmission), which is slower than normal increments.

1. Copy the Antenna directory from other server A with the same system version (same as x64 or same as x32) to the system of the source host (server B).



2. Use the command line to install the Antenna service:

```
cd <Antenna installation path>
Antenna.exe -i
```

3. Use the command line or service to start the Antenna service:

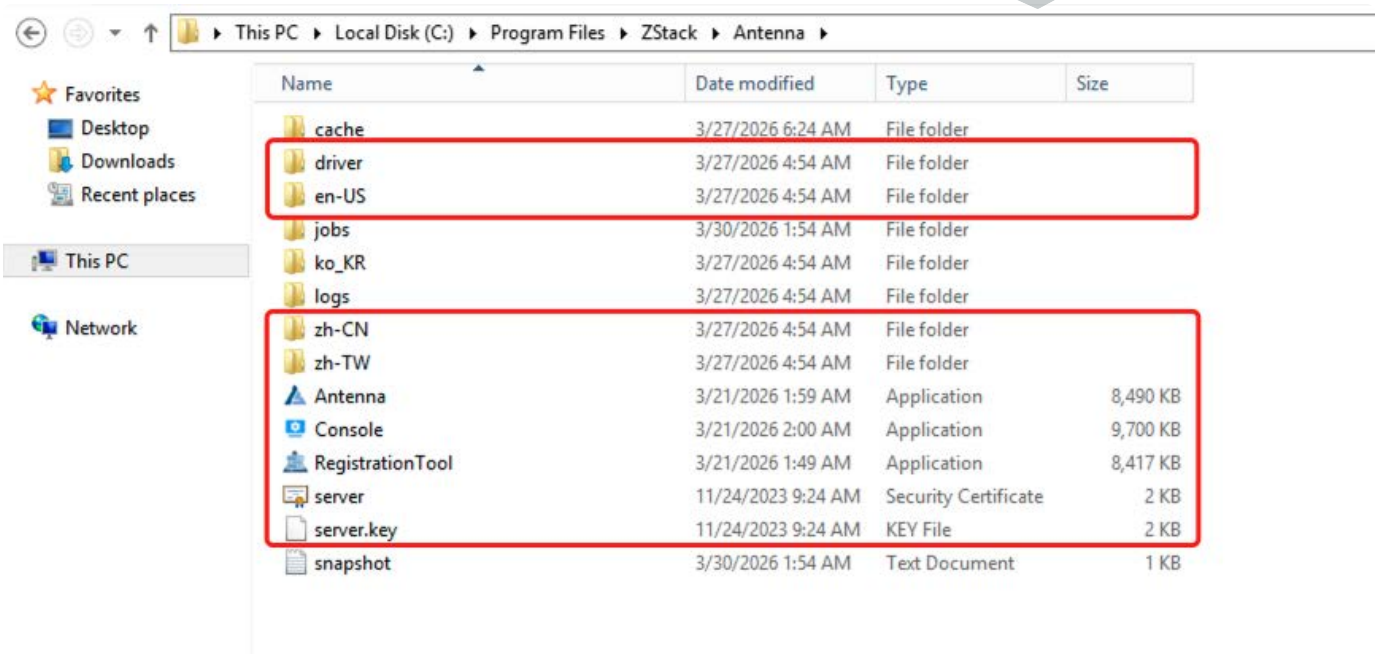
```
sc start antenna
```

4. Just register to the management console normally.

Source machine has Microsoft KB but cannot detect the KB scenario – it can be incremented normally

Steps to install Antenna

1. Copy the Antenna directory from other server A with the same system version (same as x64 or same as x32) to the system of the source host (server B).



2. Right-click in the Antenna/drivers directory in server B to install the ltbj.inf driver file.
3. Use the command line to install the Antenna service:

```
cd <Antenna installation path>
Antenna.exe -i
```

4. Use the command line or service to start the Antenna service:

```
sc start antenna
```

5. Check that the registry upfilter has automatically added ltbj. (You can skip this step if you don't understand)
6. Just register to the management console normally.

Uninstallation steps

1. Uninstall Antenna's service.

```
cd <Antenna installation path>
Antenna.exe -u
```

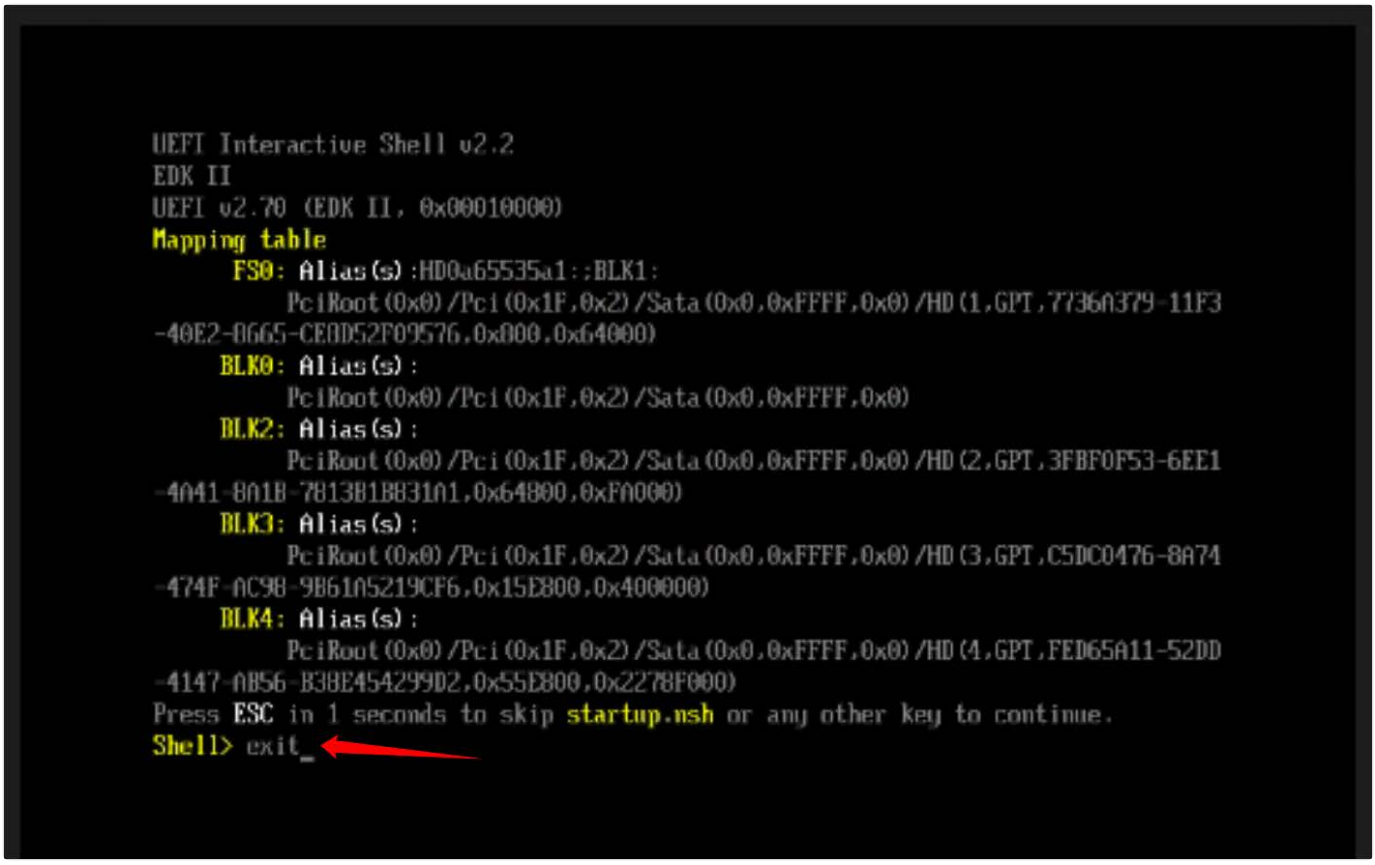
2. Delete the entire Antenna directory.

Manually specify UEFI boot files

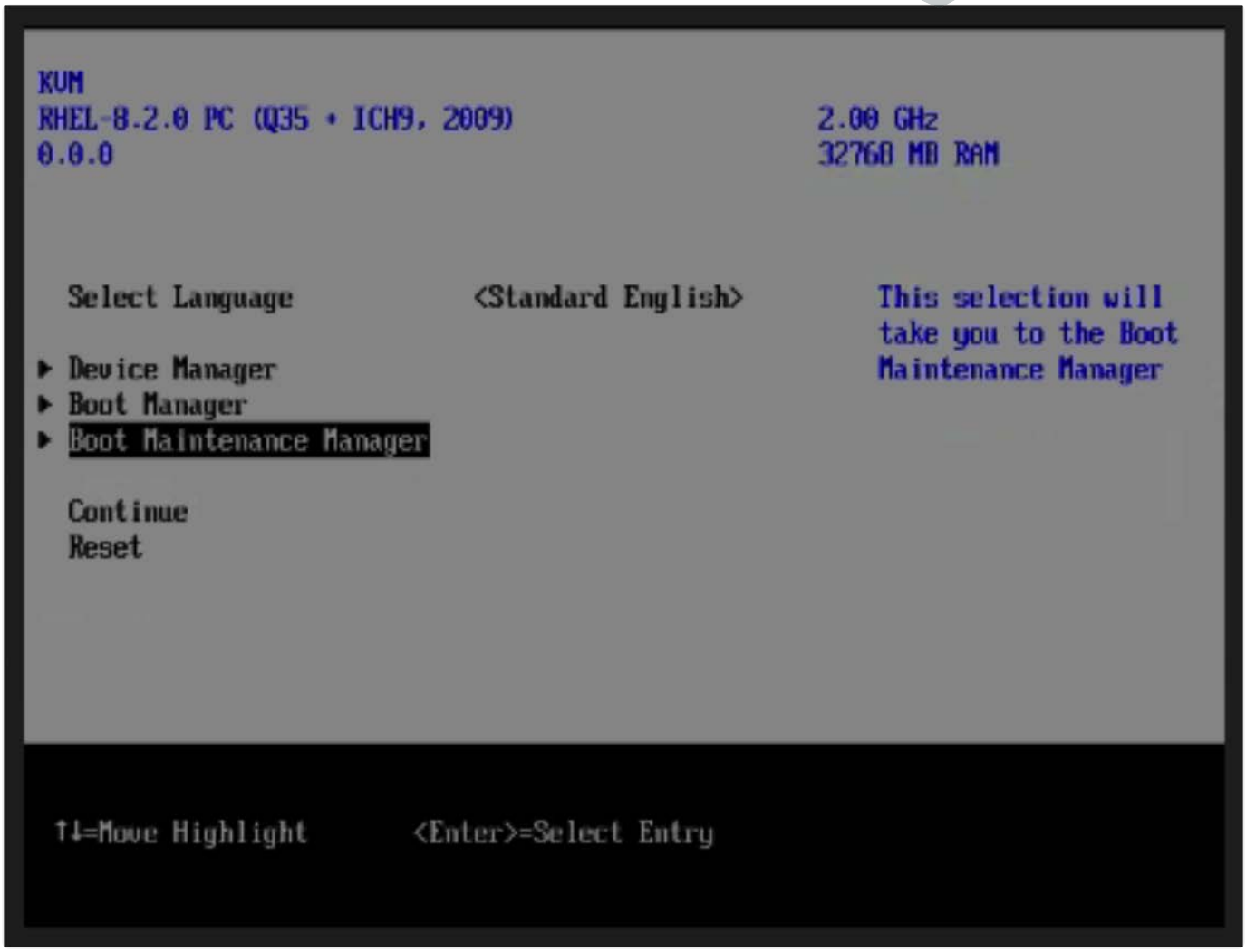
Document Category: Third Party Related Experience

Operation steps

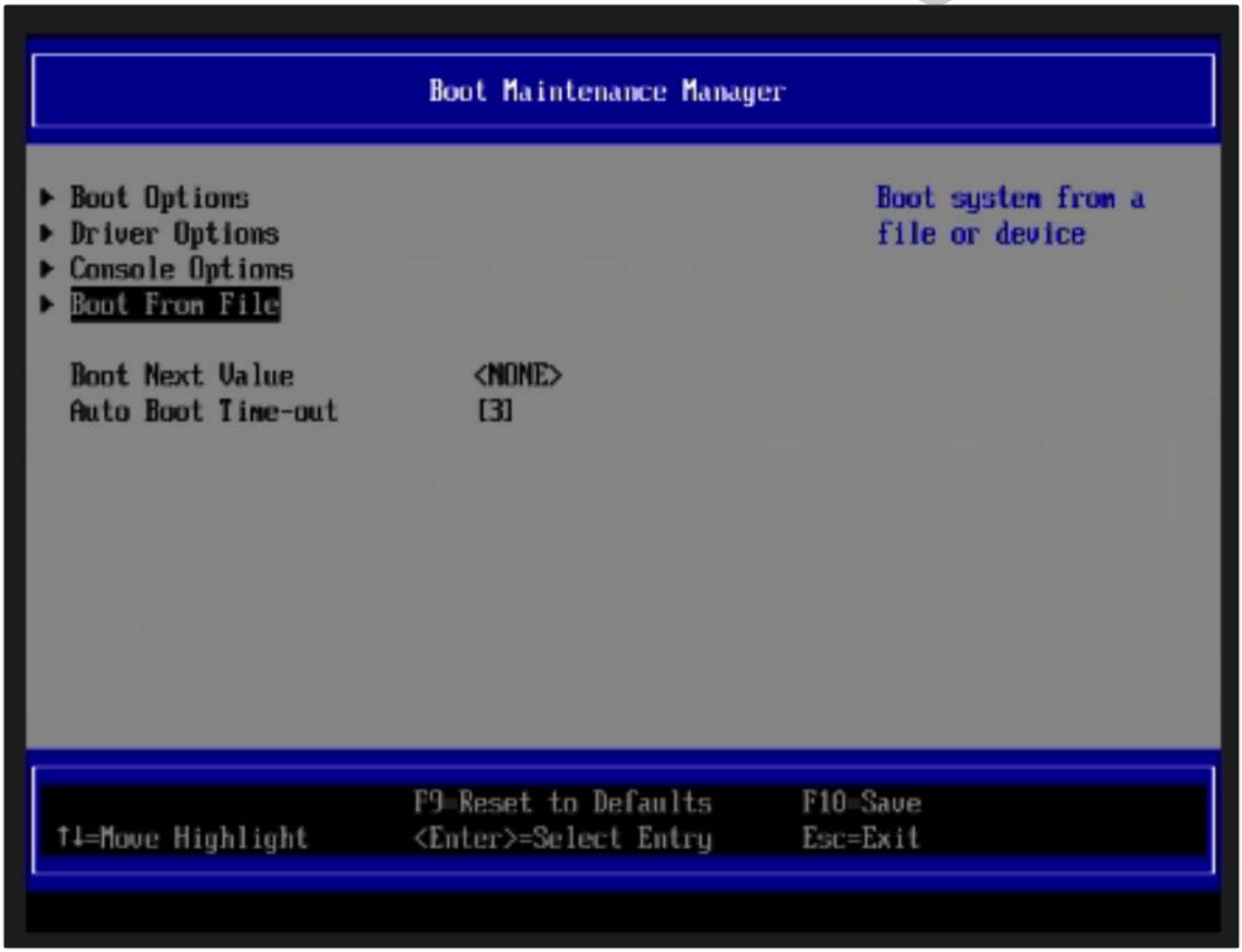
1. Enter `exit` in the UEFI Shell.



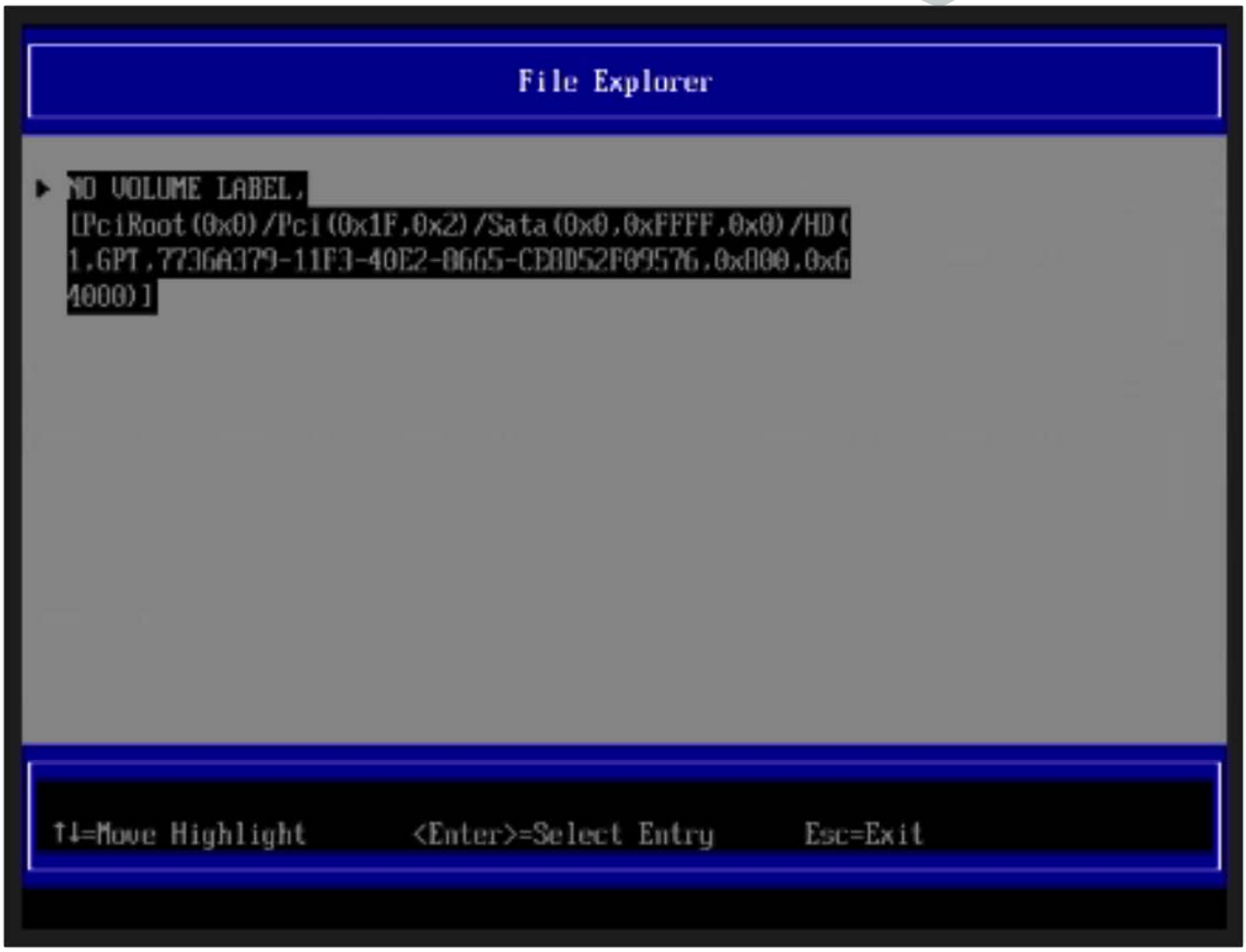
2. Select `Boot Maintenance Manager`.



3. Select `Boot From File`.



4. Select the disk listed.



5. Select the `EFI` directory.



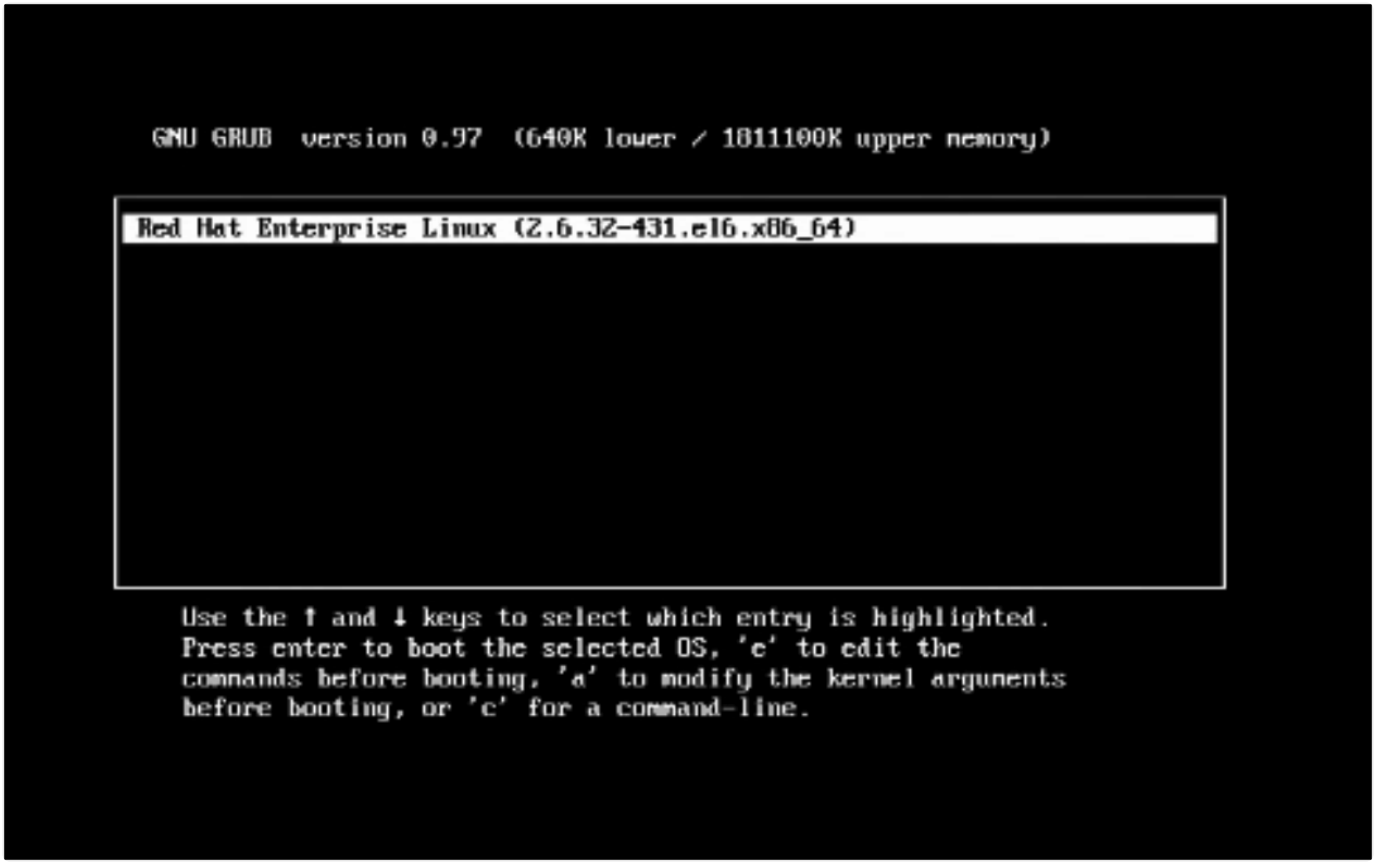
6. Continue to select the loaded directory.



7. Select `grub.efi`. If there are multiple efis, you can try them one by one.

NEXAVM


File Explorer
NEW FILE
NEW FOLDER
<.>
<..>
grub.efi
↑↓=Move Highlight
<Enter>=Select Entry
Esc=Exit


GNU GRUB version 0.97 (640K lower / 1011100K upper memory)
Red Hat Enterprise Linux (2.6.32-431.el6.x86_64)
Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the
commands before booting, 'a' to modify the kernel arguments
before booting, or 'c' for a command-line.

Improve WindowsTreker's Linux convert speed

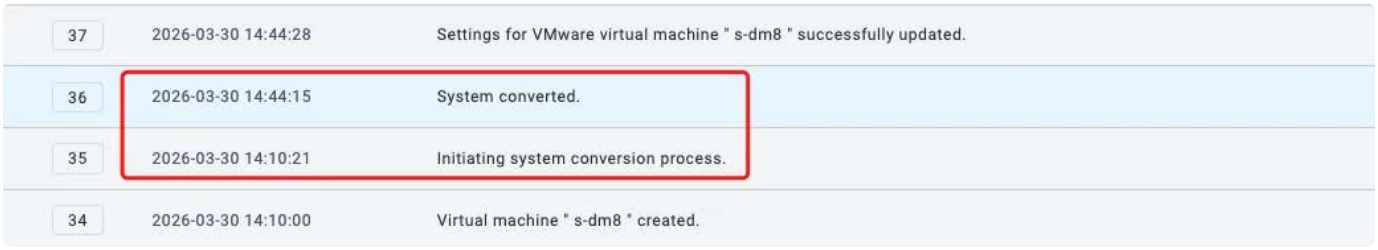
Document Category: Product Related Experience

Applicable scenarios

1. The source machine is Linux, and it is migrated to the VMware platform through API mode or disaster recovery.
2. The source machine is Linux and is migrated to NexaVM platforms through disk mode or disaster recovery.

Test effect comparison

Before optimization: 34 minutes



After optimization: 11 minutes



Necessary conditions

1. Only supports Intel CPU;
2. CPU core number ⩾ 2.

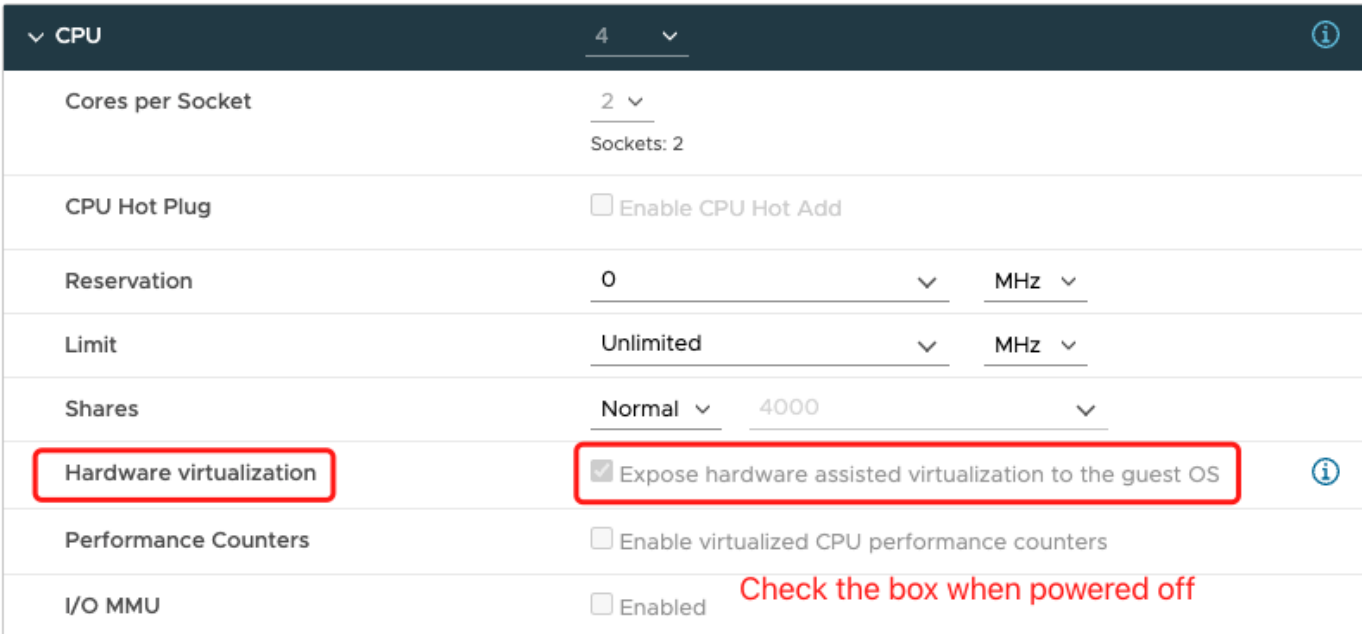
Preparation

haxm-windows：https://github.com/intel/haxm/releases

- The version used during testing is 7.8.

Operation steps

1. Shut down the data gateway (Treker) virtual machine.
2. Edit the virtual machine settings and open the cloud host's `Hardware virtualization`.
    - On the VMware platform, `hardware virtualization` is checked.




```
On NexaVM platform , change CPU mode to 'Host-Passthrough'.
```



3. Start the data gateway (Treker) virtual machine, upload intelhaxm, and install intelhaxm.
4. Restart the data gateway (Treker) virtual machine.

NEXAVM

5. Query the running status of intelhaxm.

```
#query intelhaxm status
sc query intelhaxm
```

```
C:\Users\Administrator>sc query intelhaxm

SERVICE_NAME: intelhaxm
        TYPE               : 1  KERNEL_DRIVER
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

6. After that, switching the migration task of the Linux source host through this data gateway (Treker) will speed up the process.
    - The specific effect is affected by the performance of cloud platform storage, CPU and other hardware, and varies. However, in the same environment, there is a significant improvement when it is turned on compared to not turning it on.

Changing VMware Agentless Transit Data Gateway

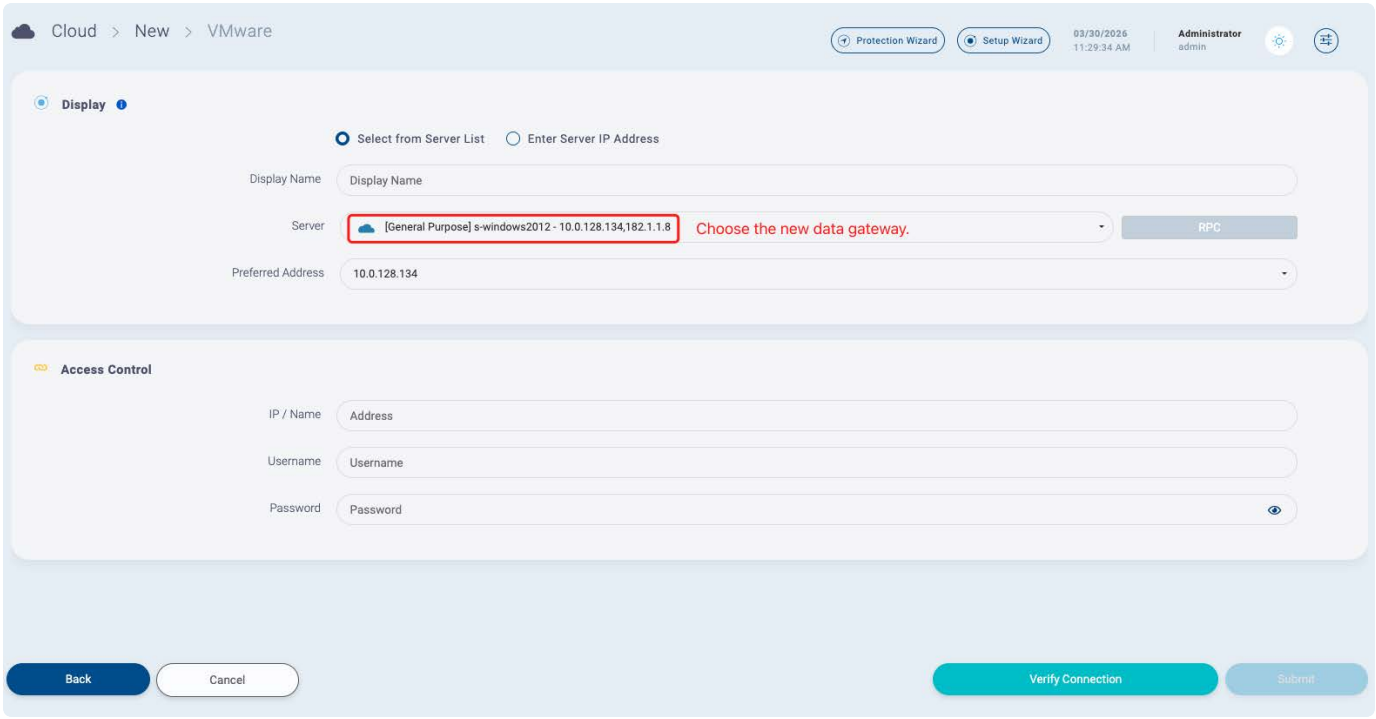
Document Category: Product Related Experience

Background

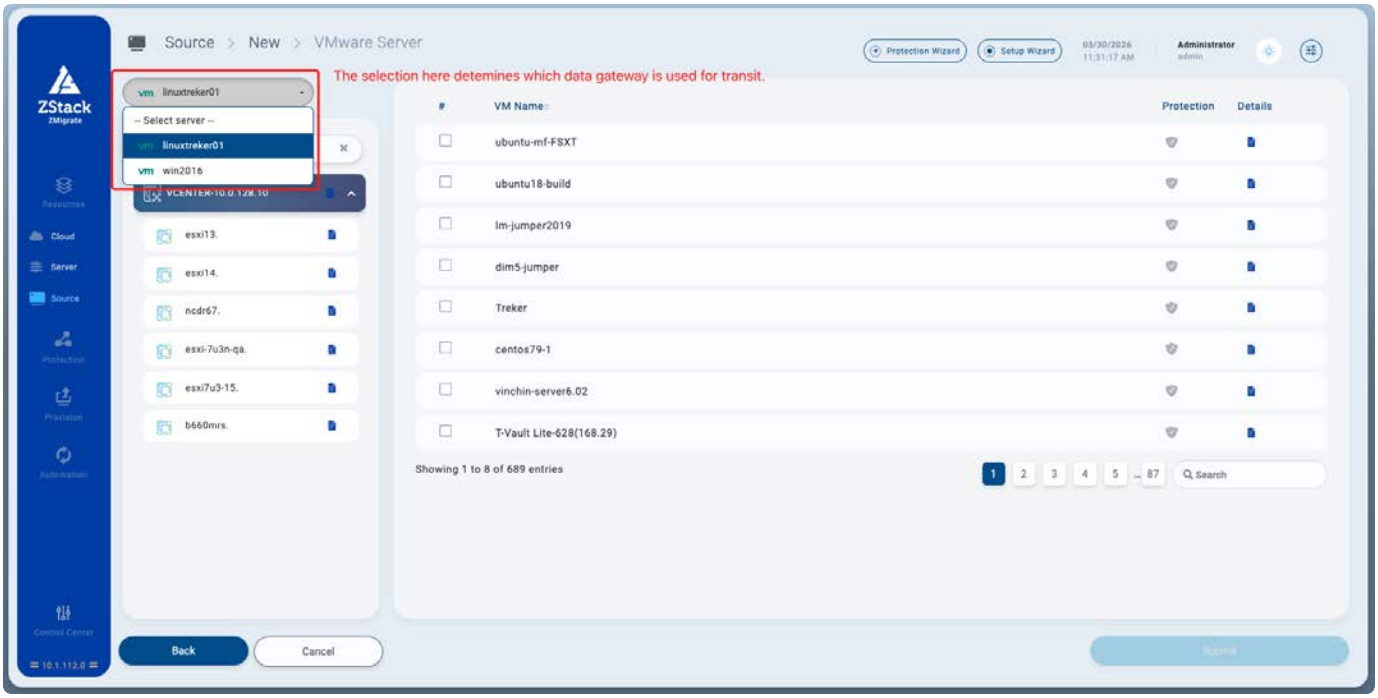
The agentless transit data gateway is determined when adding the source host. Therefore, changing the agentless transit data gateway requires re-adding the source host.

Operation steps

1. If a synchronization task has been created, delete the synchronization task first.
2. Delete the added source host.
3. Add the new data gateway to the management console.
4. To add a VMware cloud platform again, it is recommended to distinguish the name from the previous VMware cloud platform and choose to bind a new data gateway.



5. Add the source host.



6. Select the source host to add to the management console.

7. Create a synchronization task.

Change NexaVM agentless transit data gateway

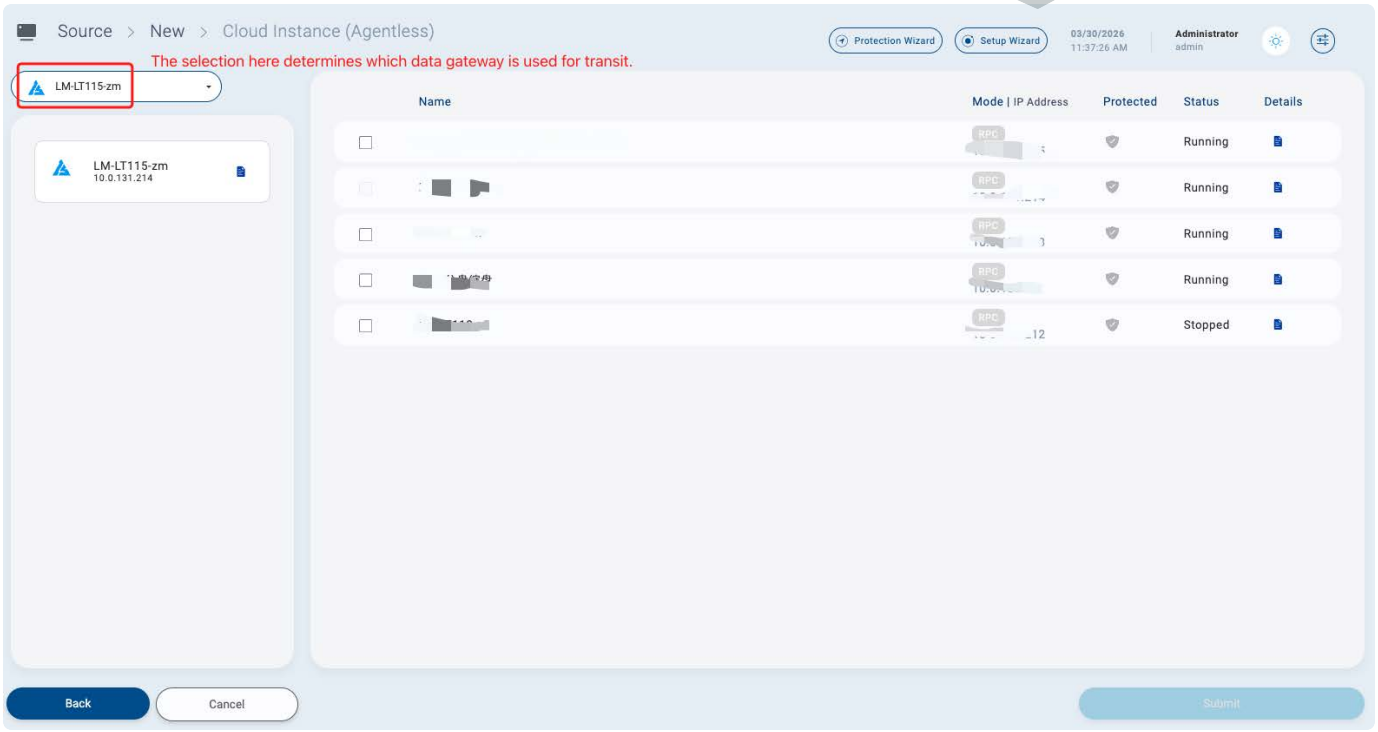
Document Category: Product Related Experience

Background

The agentless transit data gateway is determined when adding the source host. Therefore, changing the agentless transit data gateway requires re-adding the source host.

Operation steps

1. If a synchronization task has been created, delete the synchronization task first.
2. Delete the added source host.
3. Add the new data gateway to the management console in `hanging mode`.
4. Add the source host and select `NexaVM Cloud host (no agent)`.
5. Select the newly added data gateway and select the source host to add to the management console.

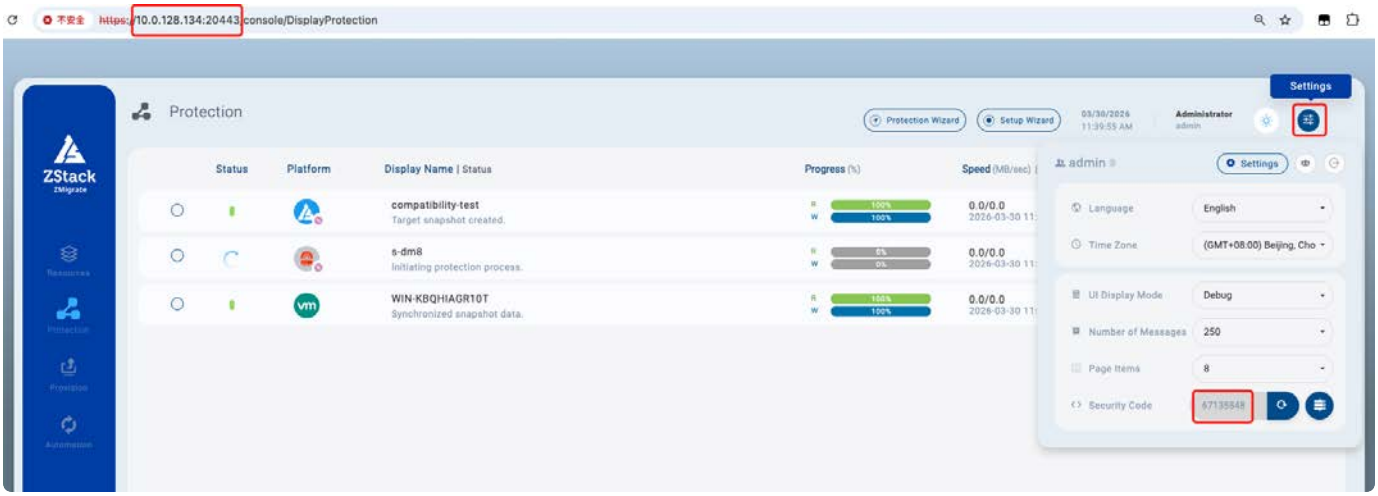


6. Create a synchronization task.

The source host is registered to the management console using HTTPS.

Document Category: Product Related Experience

Record MGMT information



According to the screenshot, you can see (according to the information record of the actual project)

- IP address: 10.0.128.134
- Port: 20443. If no port is specified, the default port is 443.
- Verification code: 67135548

Register to MGMT

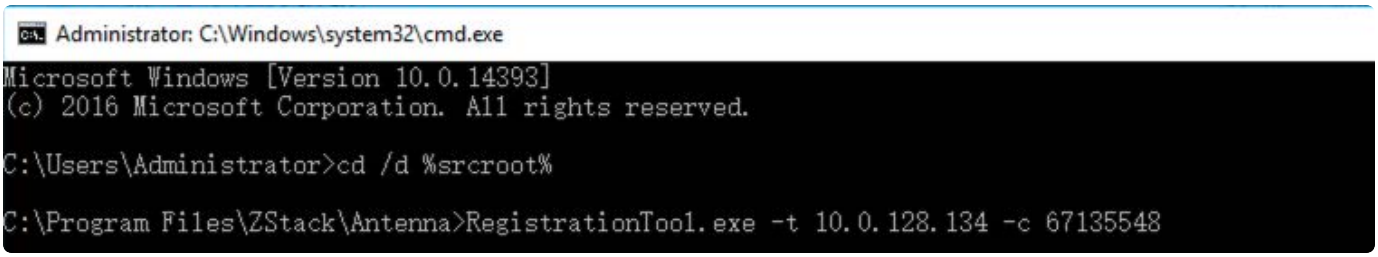
Windows

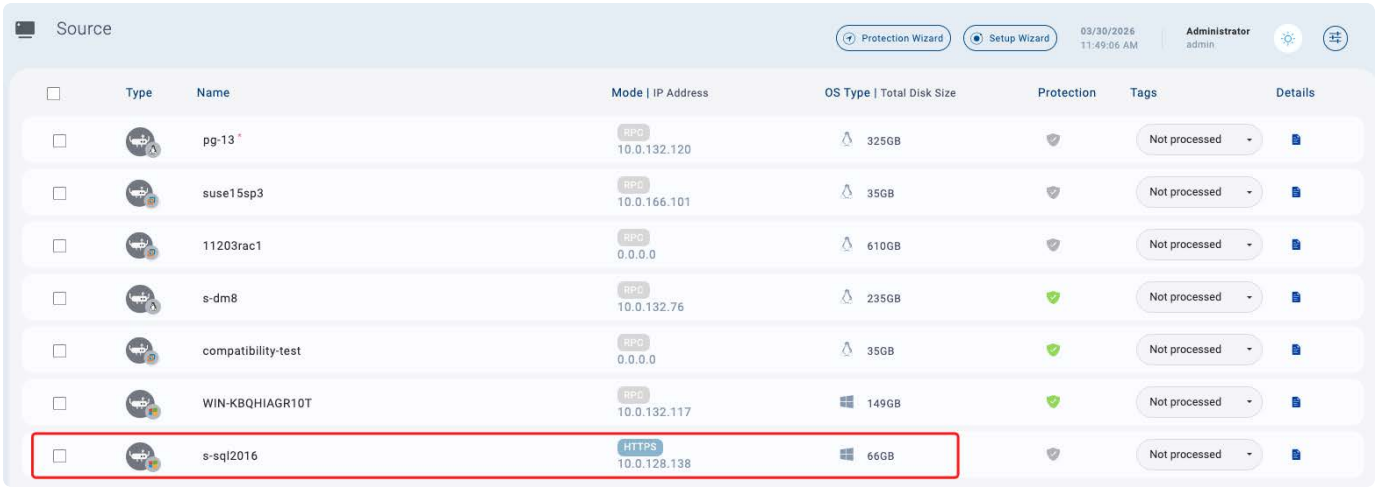
command mode

```
#Switch to the software installation directory.The /d parameter allows changing directories across partitions.
cd /d %srcroot%

#Use the command to register with MGMT,replacing with the actual IP,port,and authentication code used in the project.
RegistrationTool.exe -t 10.0.128.134:20443 -c 67135548

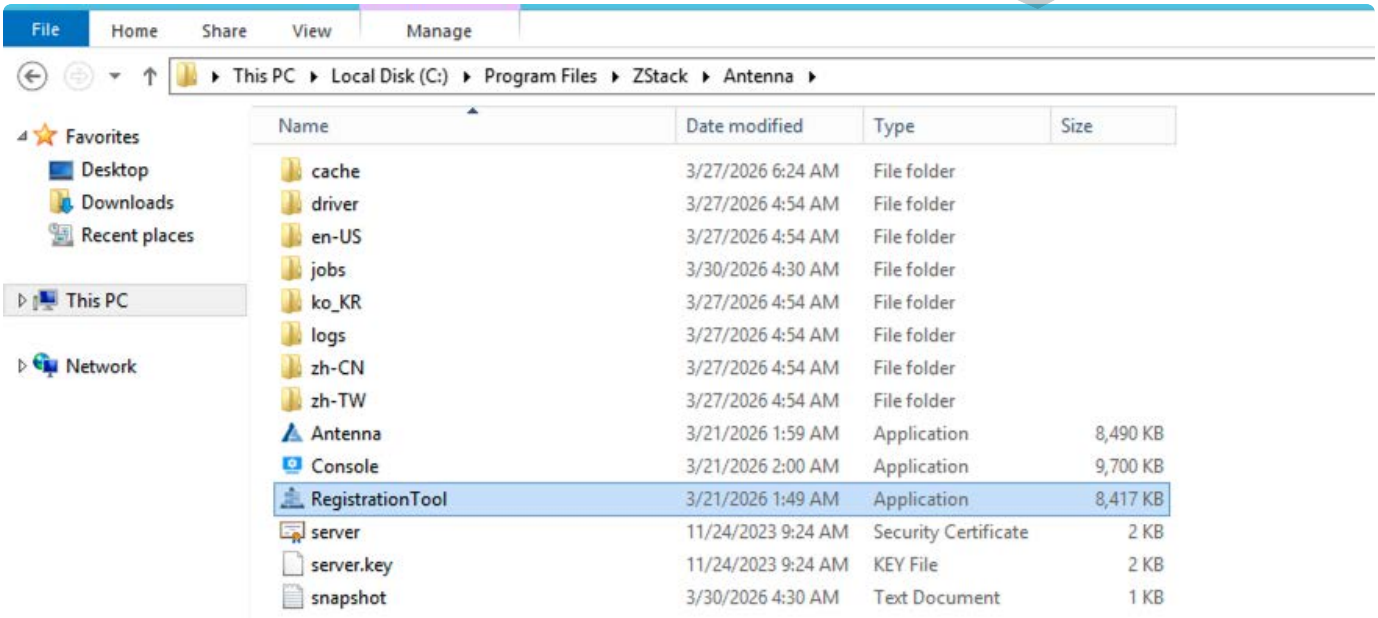
#After registration is complete, check on MGMT to verify successful registration.
```





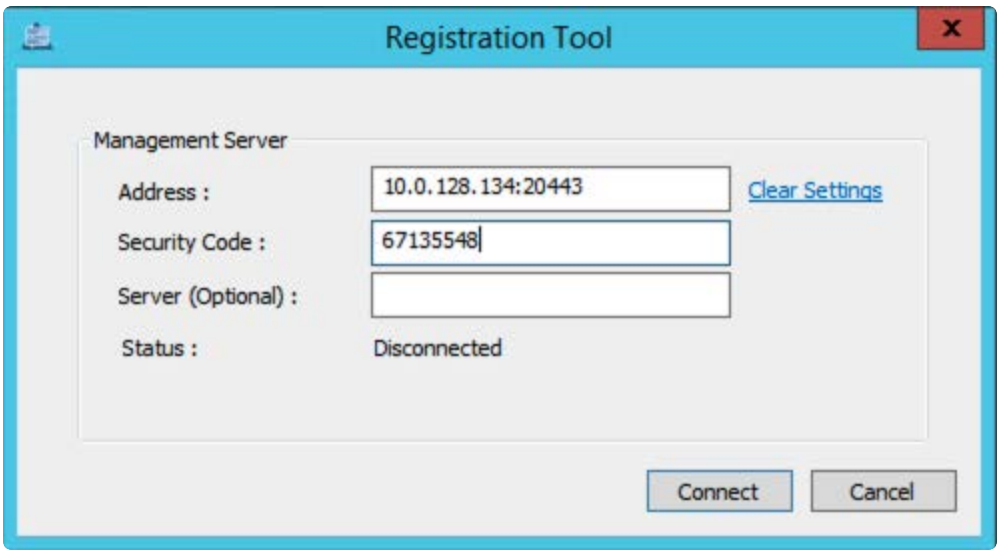
Graphical mode

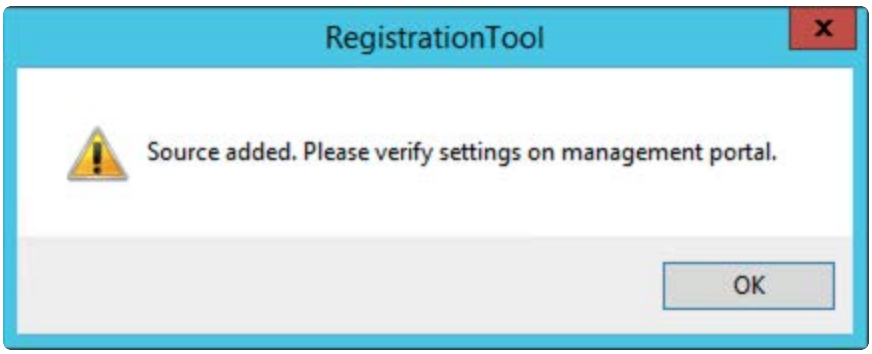
1. Navigate to the Antenna installation directory



2. Execute RegistrationTool.exe to register.

> After clicking "Online", the registration tool will become unresponsive for a short time, which is normal. Just wait until it is completed.





3. Go to MGMT to check whether the registration is successful.

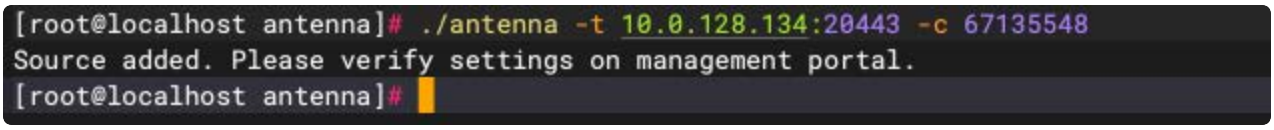


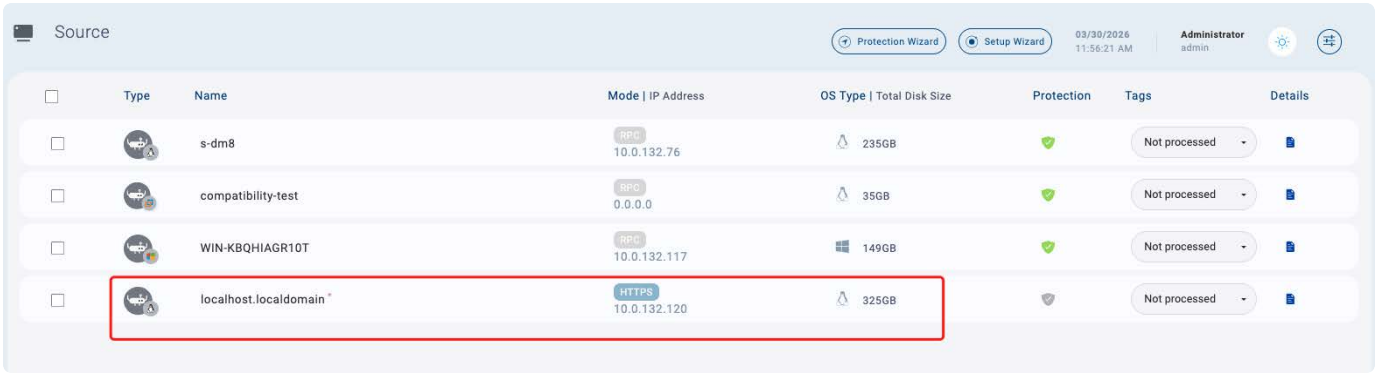
Linux

```
#Switch to the software installation directory.
cd /usr/local/antenna/

#Use the command to register with MGMT,replacing with the actual IP,port,and authentication code used in the project.
./antenna -t 10.0.132.171:20443 -c 91554508

#After registration is complete, check on MGMT to verify successful registration.
```





How to confirm whether Antenna is adapted to the specified Linux kernel

Document Category: Product Related Experience

Knowledge points

Linux Antenna is divided into small packages and large packages.

Packet

Definition: Only applicable to the Antenna installation package of the specified system version and specified kernel version.

**Name format: **antenna__.tgz

**Name example: **antenna_CentOS_Linux_release_7.9.2009_(Core)_3.10.0-1160.6.1.el7.x86_64.tgz

Large package

Definition: All system versions and kernel versions that have been compatible before (inclusive) the compilation date.

**Name format: **all_antenna-..tar.gz

**x86 architecture name example: **all_antenna-10.0.614.20250416.tar.gz

**arm architecture name example: **all_antenna_arm-10.0.621.20250926.tar.gz

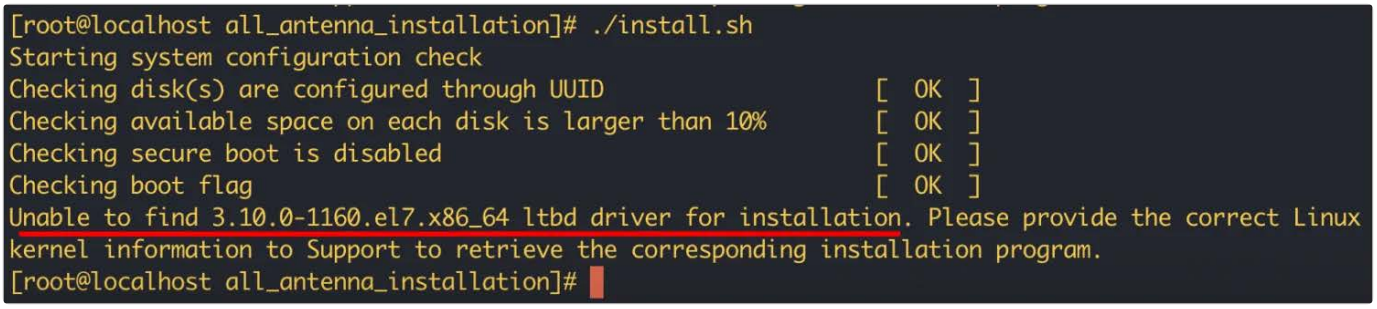
Method 1. Query the compatibility list

Query the compatibility list directly, **There is a delay in compatibility and cannot be updated in real time**.

NEXAVM

Method 2. Install using the latest large package

Directly upload the latest Antenna package to the user's Linux system for installation. If it is not compatible, an error will be reported.




```
Unable to find <kernel-version> ltd driver for installation.
Please provide the correct Linux kernel information to Support to retrieve the corresponding installation program.
```

Method 3. Unzip the latest large package and view it

Decompress the large package directly, the decompression path level of the large package:

```
all_antenna_installation/
├── driver/                          # dirver directory
│   └── [OS type]/                   # e.g. CentOS
│       └── [major version]/         # e.g. 7
│           ├── [kernel version]/    # e.g. 3.10.0-1062.el7.x86_64
│           │   └── [System Architecture]/      # e.g. x86_64
│           │       └── ltbd-*.rpm  # driver installation rpm package
│           └── *.rpm                # Common dependencies
├── install.sh                       # Installation script
└── uninstall.sh                     # Uninstallation script
```

Patch the management console

Document Category: Product Related Experience

write in front

1. The management console is divided into two versions: Linux and Windows;
2. Patches are common across Linux and Windows management consoles.
3. Patch is bound to the version number and only takes effect for the specified version.

Example:

The user installed version 676 of the management console and encountered a problem that required patch compatibility.

Then users can use it whether it is a Windows management console or a Linux management console, as long as it is version 676.

Preparation

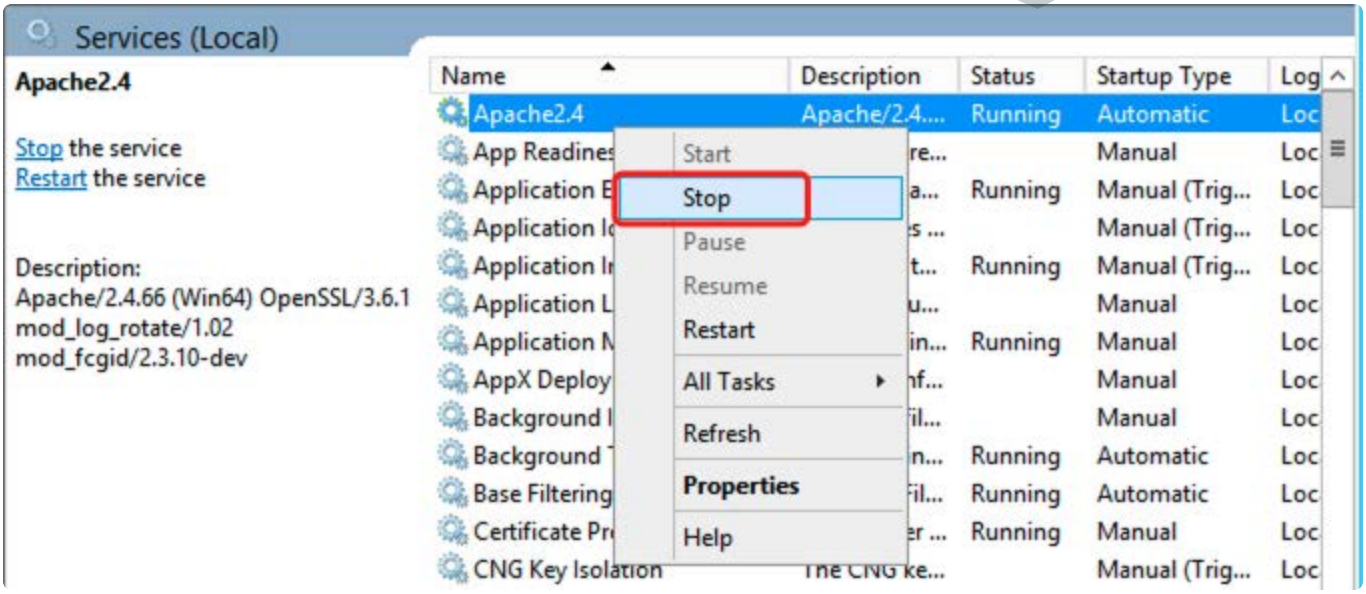
Confirm There is no synchronization task currently being synchronized in the current management console**. If there is a task to be synchronized again, please wait for the task synchronization to be completed before patching.

Operation steps

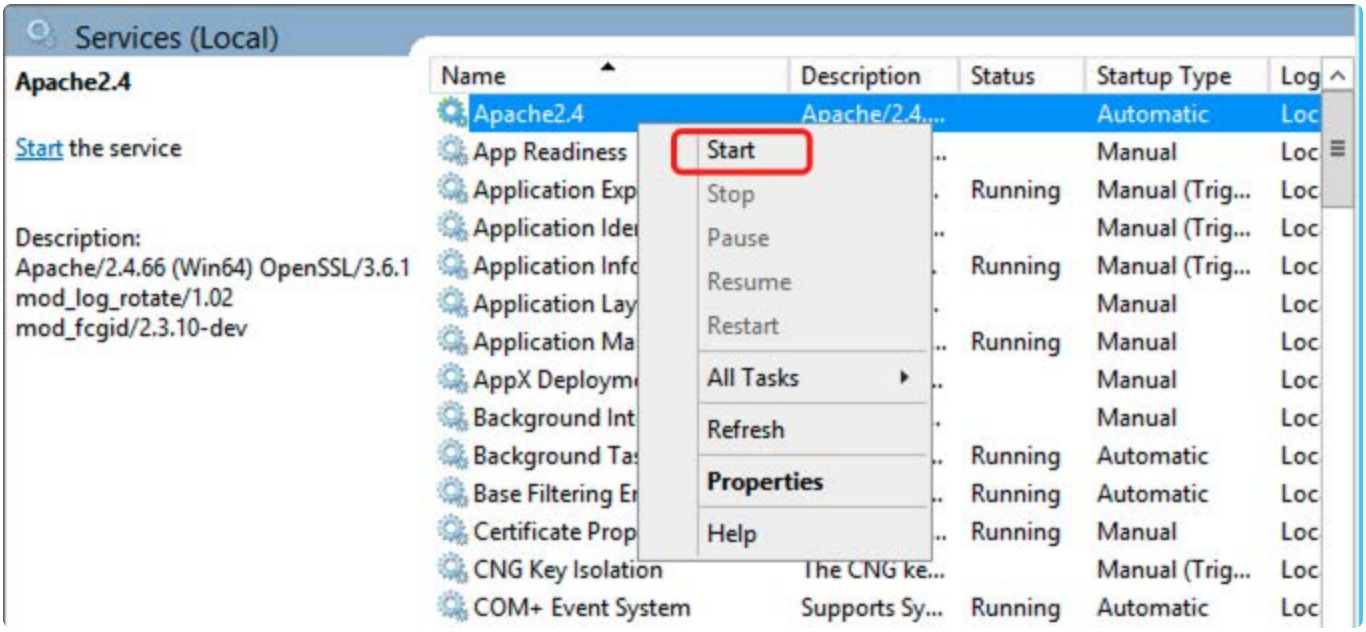
Confirm the patch path with technical support.

Windows Management Console

1. Stop the apache service.



2. Back up the original file.
3. Replace patch.
4. If patching multiple files at once, repeat steps 2 and 3 (backup and replacement).
5. Start apache.



Linux management console

Use the guest user to switch to root and execute the command, or the guest uses sudo to execute the command.

NEXAVM

```
# Stop apache service
docker stop mgmt

# Back up the original file
cp <original_file_path> <original_file_path>.bak

# replace patch
cp <patch_file_path> <original_file_path>

# set permissions
chmod 644 <original_file_path>

# If patching multiple files at once, repeat the above three steps (backup, replace, set permissions), then proceed to the next step.

# start apache
docker start mgmt
```

Skip system conversion

Document Category: Product Related Experience

Applicable scenarios

1. System conversion failed due to some special reasons.
2. Some source host systems are not compatible with system conversion.

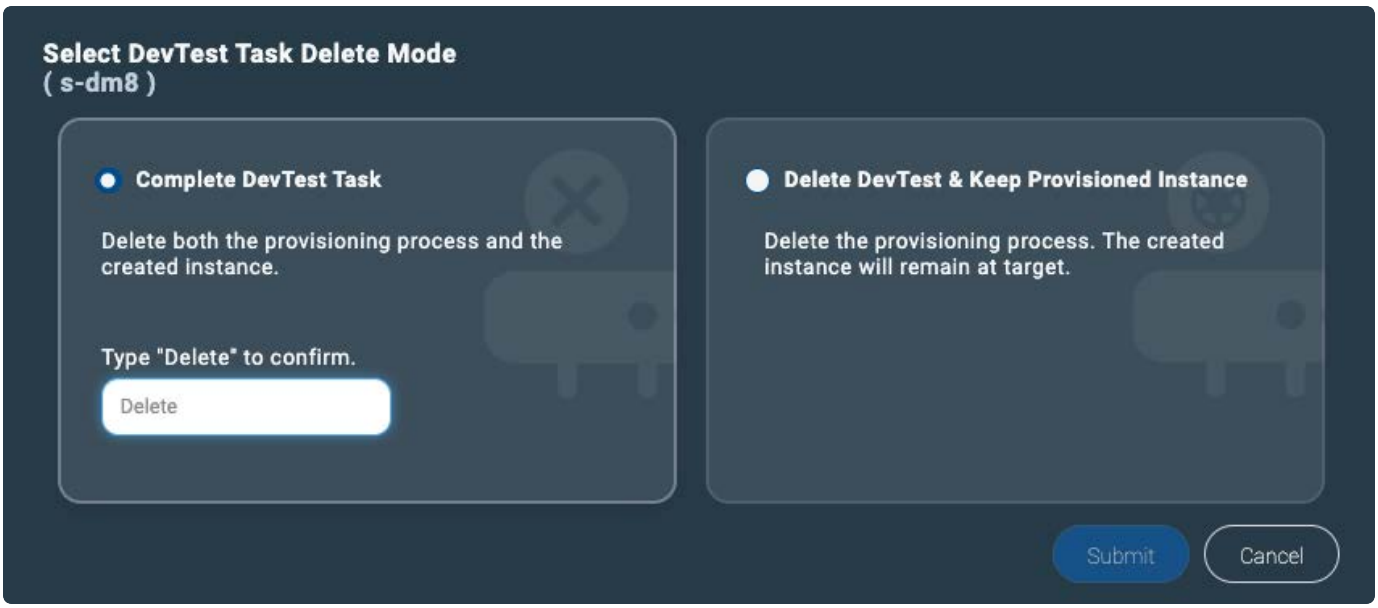
Notes

Skip system conversion:

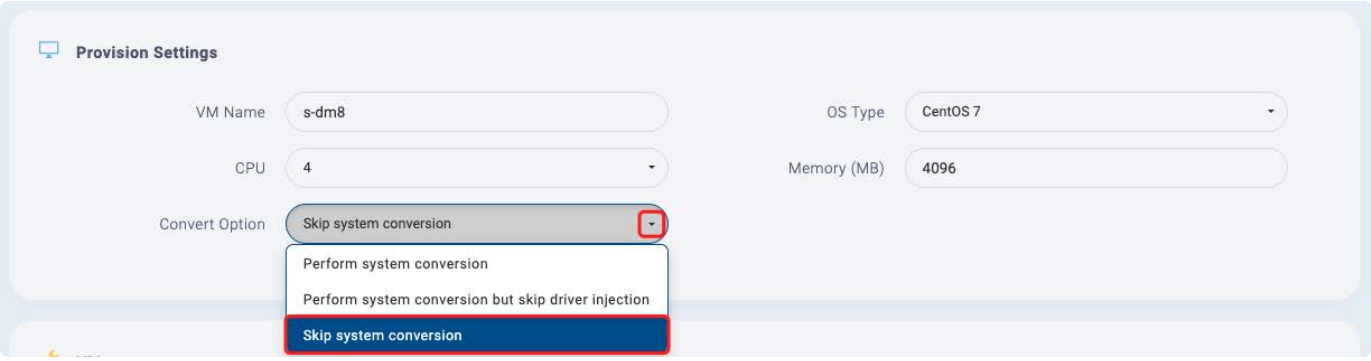
1. **The network card name, IP address and other information will not be configured on the target machine after switching. You need to log in to the target machine system to modify it manually.**

Operation steps

1. If a switching task has been created, delete the switching task first.
    - Select `Delete enabled task and re-execute` on the left.



2. Re-create the switching task and select `Skip system conversion` from the drop-down menu.



3. Wait for the switching task to complete.
4. Log in to NexaVM to check whether the target machine has entered the system normally.
   - If you do not enter the system, see `Step 5`.
   - If you have already entered the system, see `Step 6`.
5. Stop the cloud host, close the cloud host virtio, restart it, log in to the system, and manually configure the IP.
   - It is recommended to manually install the performance optimization tool, shut down the computer, enable virtio and then restart the computer.
6. Log in to the system and manually configure the IP.
   - It is recommended to manually install the performance optimization tool, shut down the computer, enable virtio and then restart it. If virtio is enabled, keep it enabled.

Things to note when migrating to 2003

Document Category: Product Related Experience

Background

For 32-bit operating systems, after installing Antenna, needs to be restarted first, and then registered to the management console for migration.

- If you do not restart, each increment will be the full amount.

For 64-bit operating systems, after installing Antenna, you can directly register to the management console for migration.

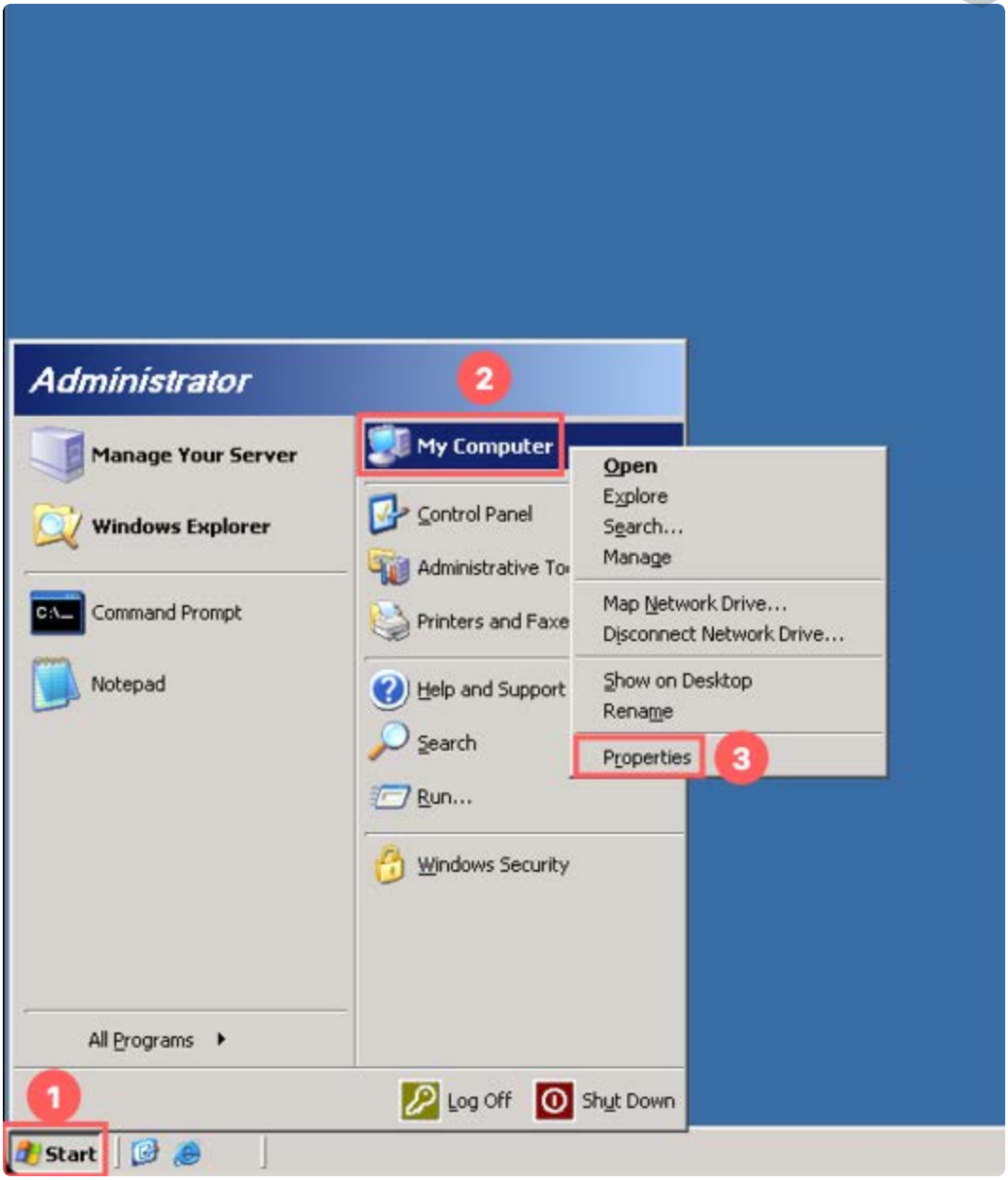
- Because the system is too old, each increment is a checksum.

Recommended actions

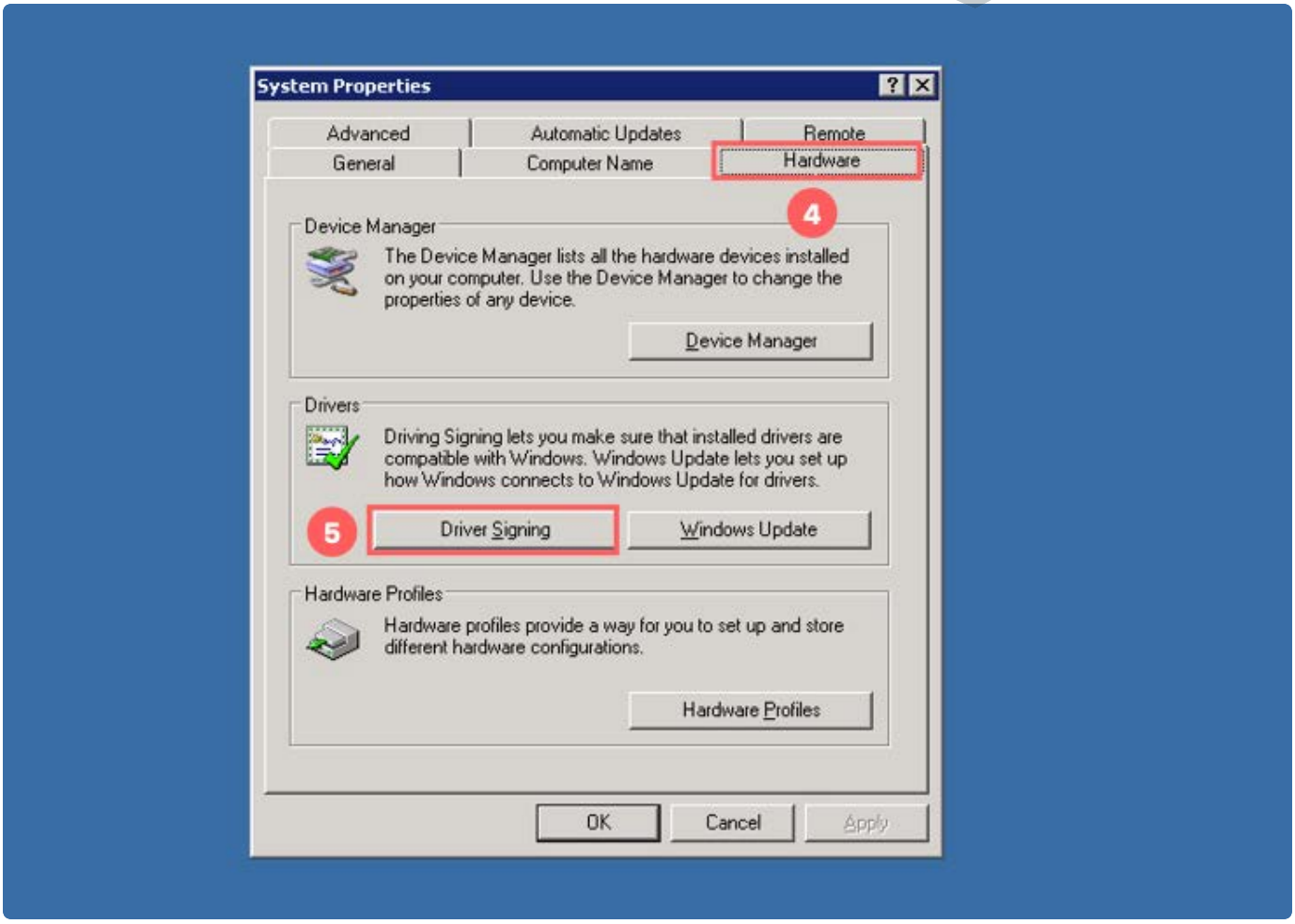
> Non-required operation. After configuration, the driver wizard window will be reduced and manual interaction will be reduced when the target machine is turned on.

- It is recommended to change the driver signature to **ignore**.

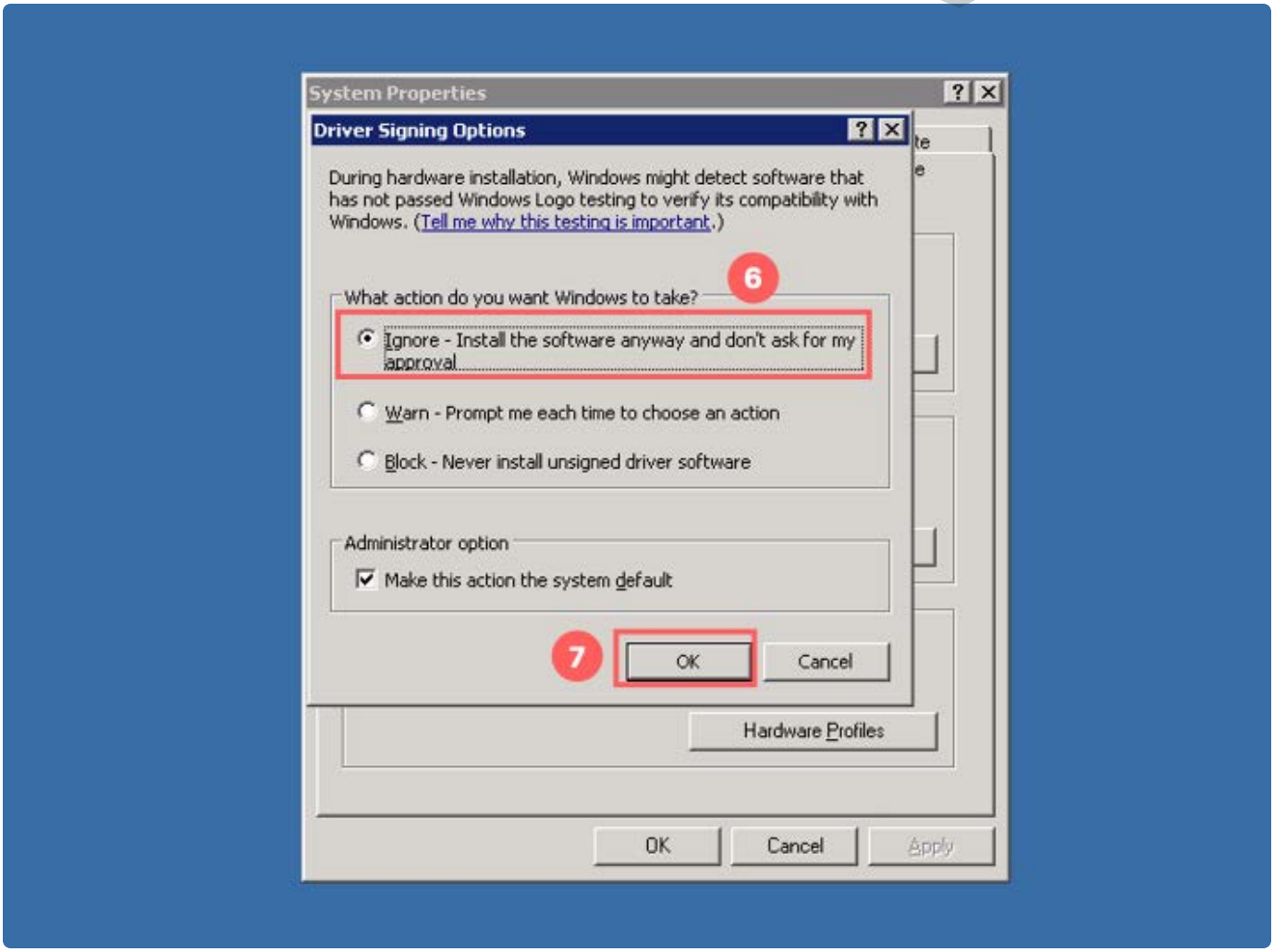
NEXAVM


Administrator
2
Manage Your Server
Windows Explorer
Command Prompt
Notepad
All Programs
My Computer
Control Panel
Administrative To
Printers and Faxe
Help and Support
Search
Run...
Windows Security
Open
Explore
Search...
Manage
Map Network Drive...
Disconnect Network Drive...
Show on Desktop
Rename
Properties
3
1
Log Off
Shut Down
Start

NEXAVM


System Properties
Advanced
Automatic Updates
Remote
General
Computer Name
Hardware
4
Device Manager
The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.
Device Manager
Drivers
Driving Signing lets you make sure that installed drivers are compatible with Windows. Windows Update lets you set up how Windows connects to Windows Update for drivers.
5
Driver Signing
Windows Update
Hardware Profiles
Hardware profiles provide a way for you to set up and store different hardware configurations.
Hardware Profiles
OK
Cancel
Apply

NEXAVM

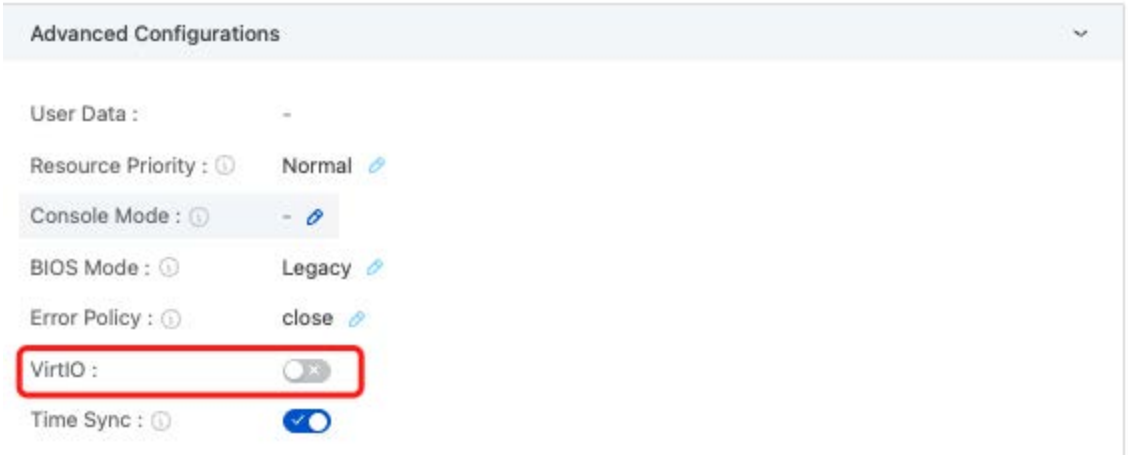


After the migration, the operations on the target machine upon entering the system

If the blue screen displays 0x000007B when booting

Please stop the target machine, close virtio, and then turn it on again.

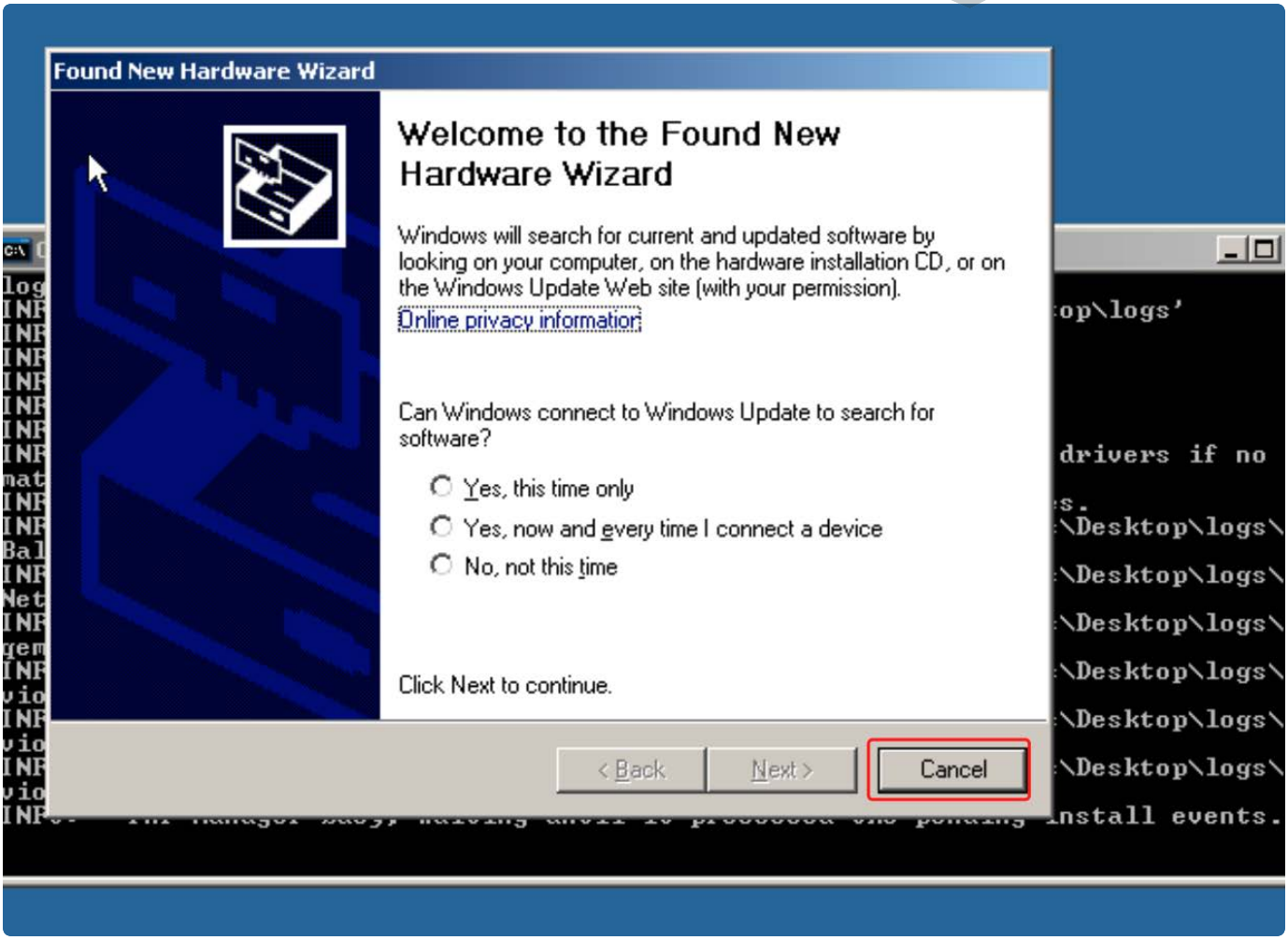
NEXAVM



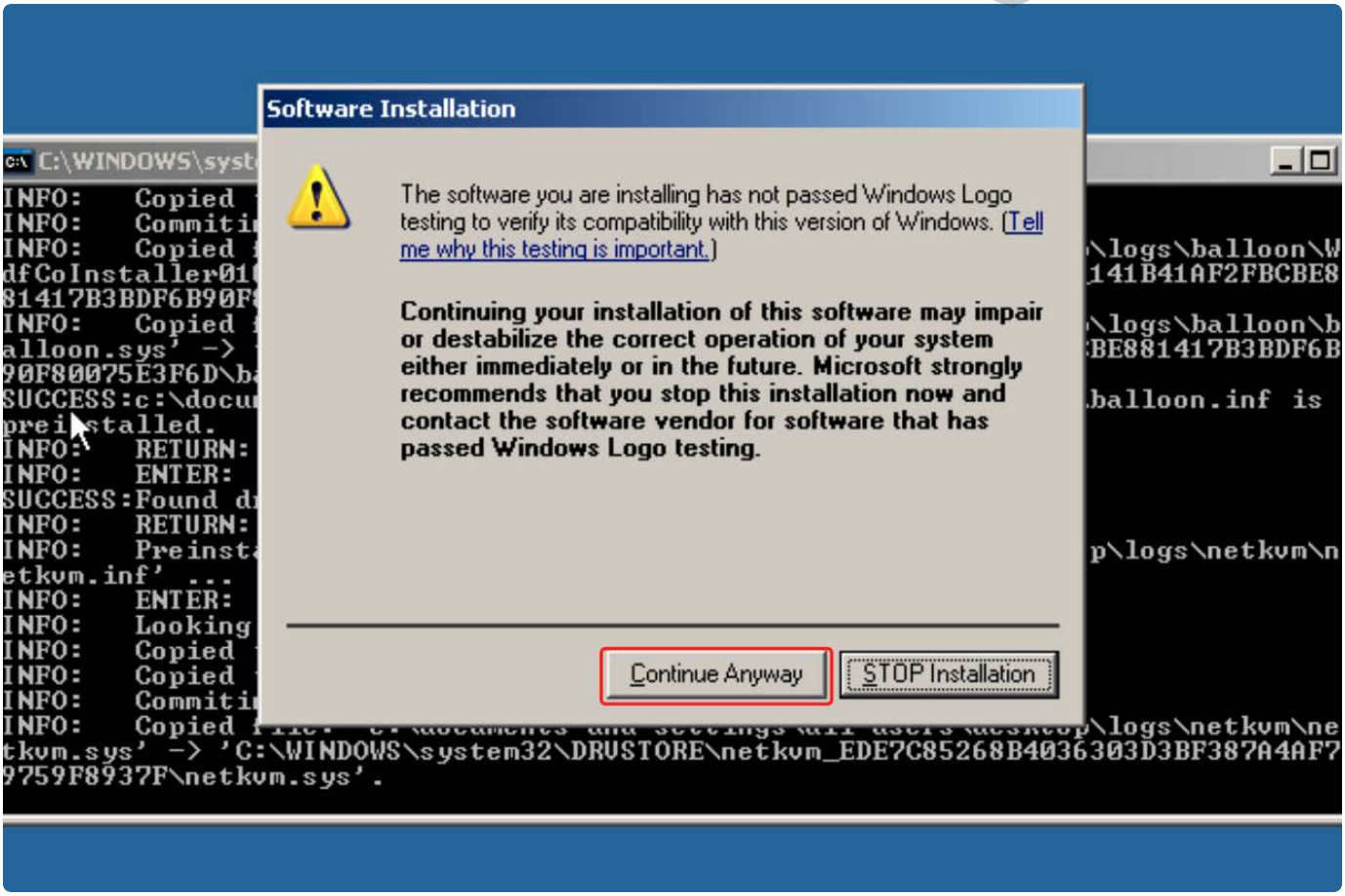
Close the installation driver wizard window

Multiple driver installation wizard windows pop up, close them one by one manually.

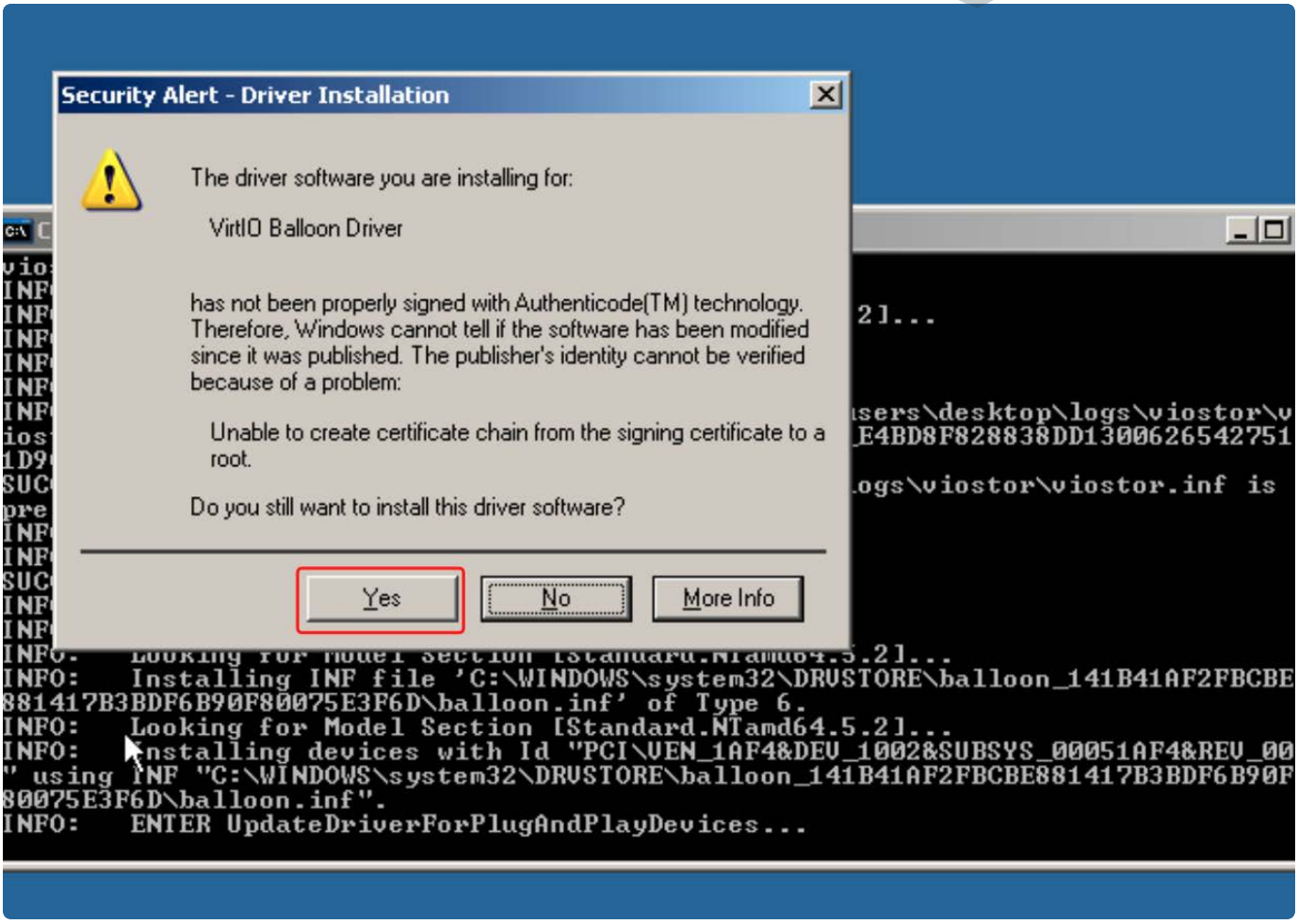
- If the black window of cmd is stuck on a certain command, it may be that the "Find New Hardware Wizard" is behind the cmd window. Switch the "Find New Hardware Wizard" to the foreground, and then click `Cancel` one by one.



A software installation window will pop up, select **Install anyway**. (may appear multiple times)



For driver installation, select **Yes**. (may appear multiple times)



If there is no network card driver

Please execute the script to install the driver:

- Double-click the script ending with .cmd in the logs directory on the desktop to install the driver.

Things to consider when migrating SuSE10 or SuSE11

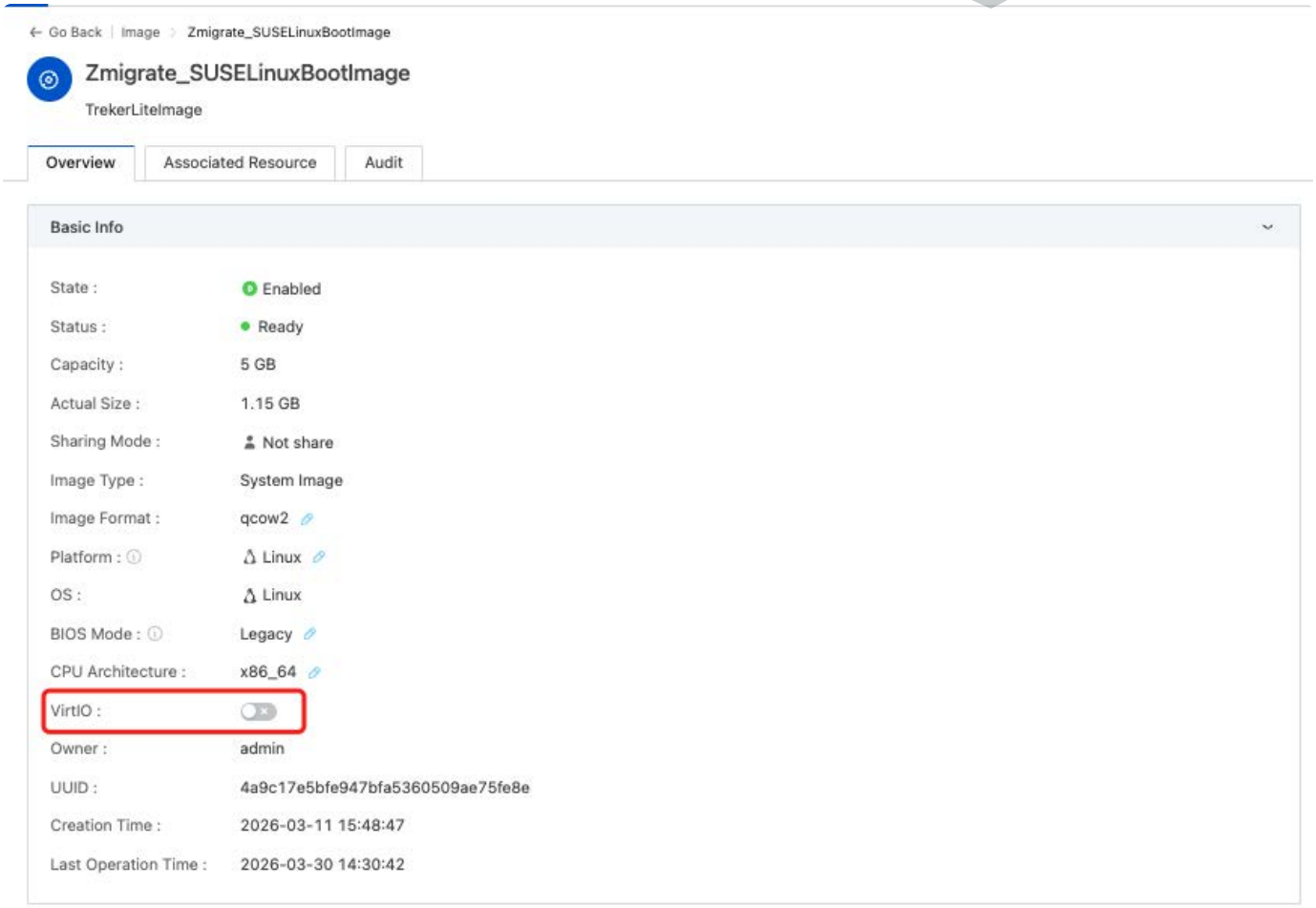
Document Category: Product Related Experience

Background

Due to the kernel mechanism problem of SuSE10 or SuSE11, the virtio driver cannot be inserted offline. Therefore, only the network is configured during system conversion and the virtio driver will not be inserted.

Notes

1. Please upload LinuxBootImage (LinuxTrekerLite) separately for SuSE10 or SuSE11,** and turn off virtio. **
    - It is recommended to upload Legacy and UEFI separately for source hosts corresponding to the two startup modes.



2. If you want to use virtio after migration, please install the performance optimization tool of the NexaVM platform.
    - Note: After installing the performance optimization tool, you will be asked to restart the operating system. Please arrange the restart time appropriately.

Windows repeatedly restarts or enters safe mode after migration

Document Category: Product Related Experience

Applicable scenarios

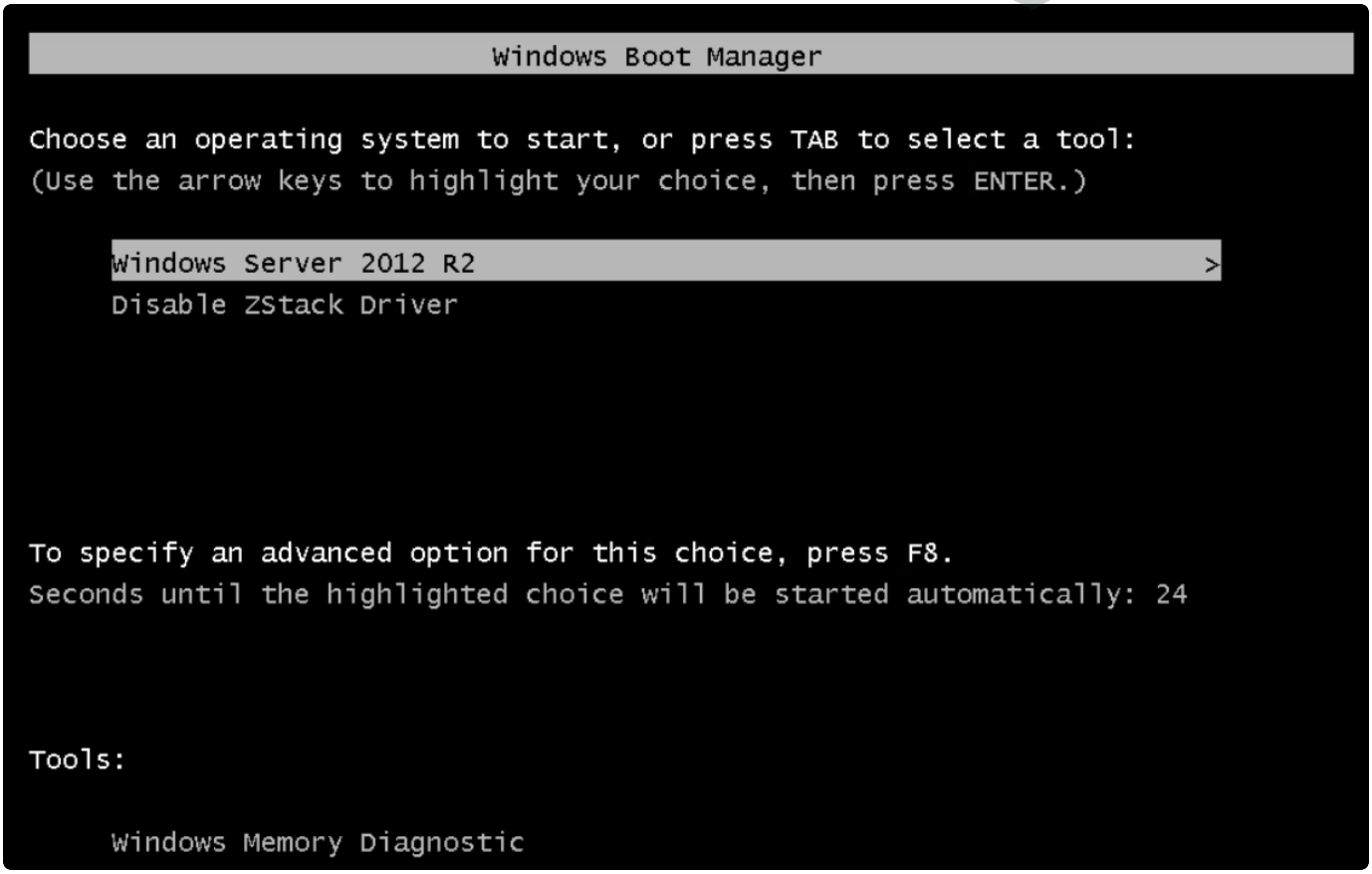
The first boot after recovery will enter the system recovery/repair mode, and it will also enter the system recovery/repair mode after restarting.

Reason

1. The system has secure boot enabled: Some Windows will enter secure boot after driver conversion.
2. To migrate from Intel CPU to Haiguang CPU, you need to modify the CPU mode.
3. For Windows 2008 in UEFI mode, CSM needs to be enabled on the NexaVM platform to enter the system normally.
4. After switching, the safe mode is entered by default for the first time. Some Windows safe modes cannot be loaded normally, resulting in repeated restarts.

Solution 1. System has secure boot enabled

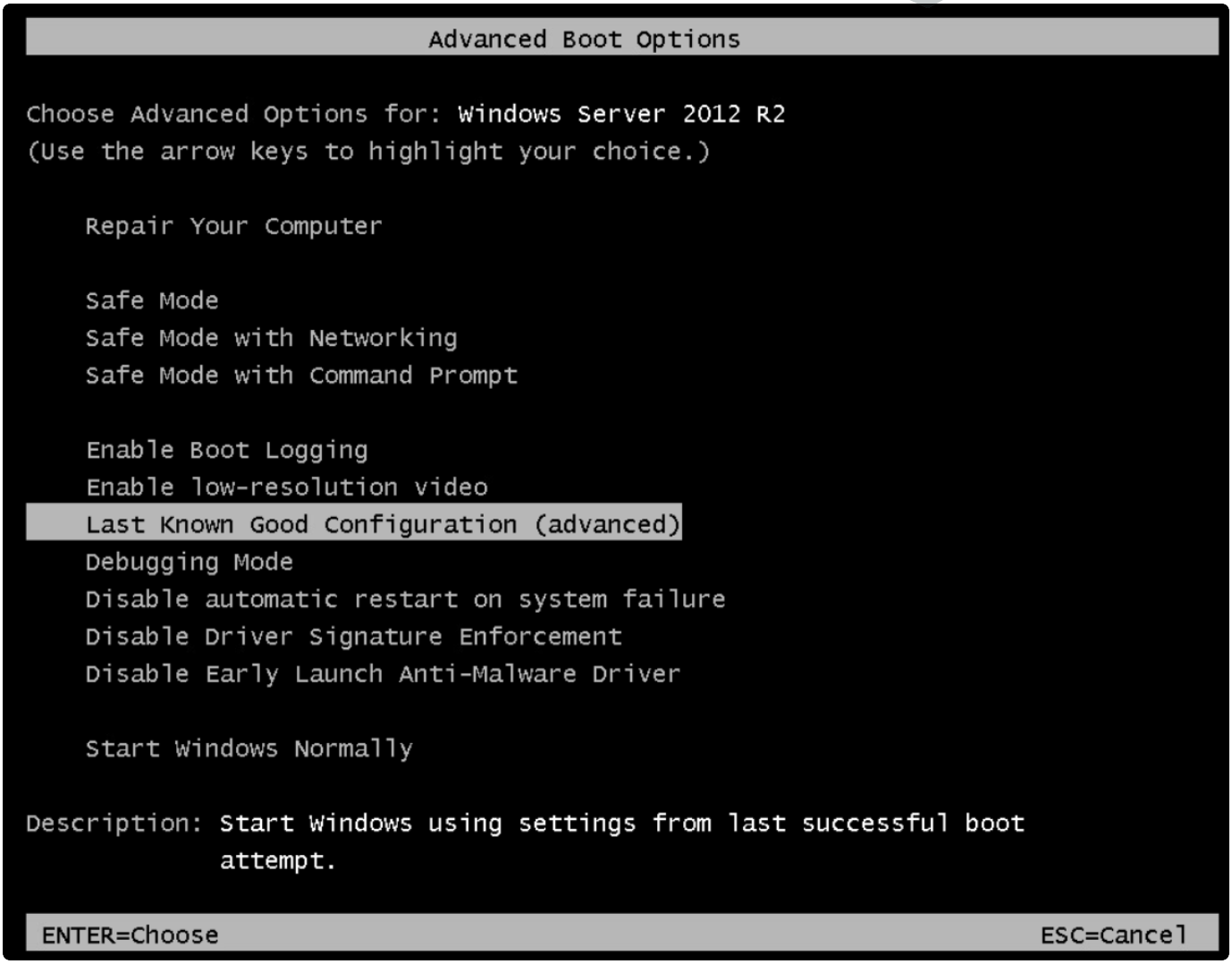
1. While booting into Windows Startup Manager, press F8.



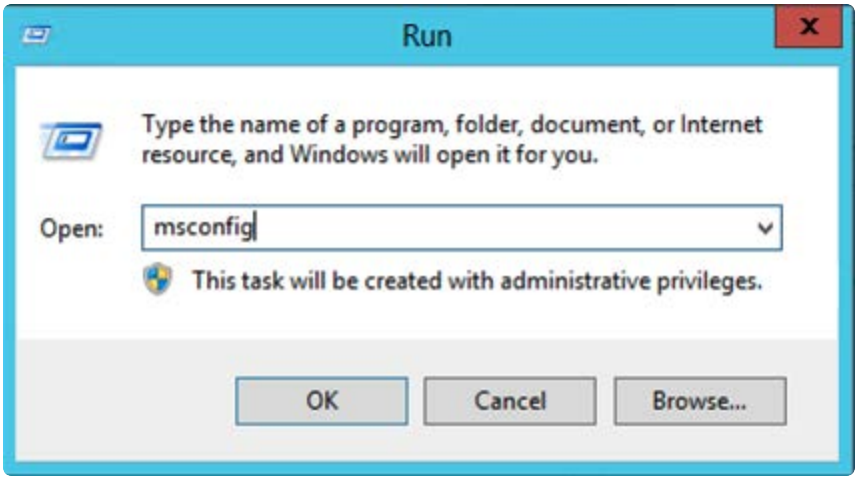
2. Select "Last Known Good Configuration (Advanced)"

> If you do not successfully enter the system, you can try to select "Safe Mode".

NEXAVM

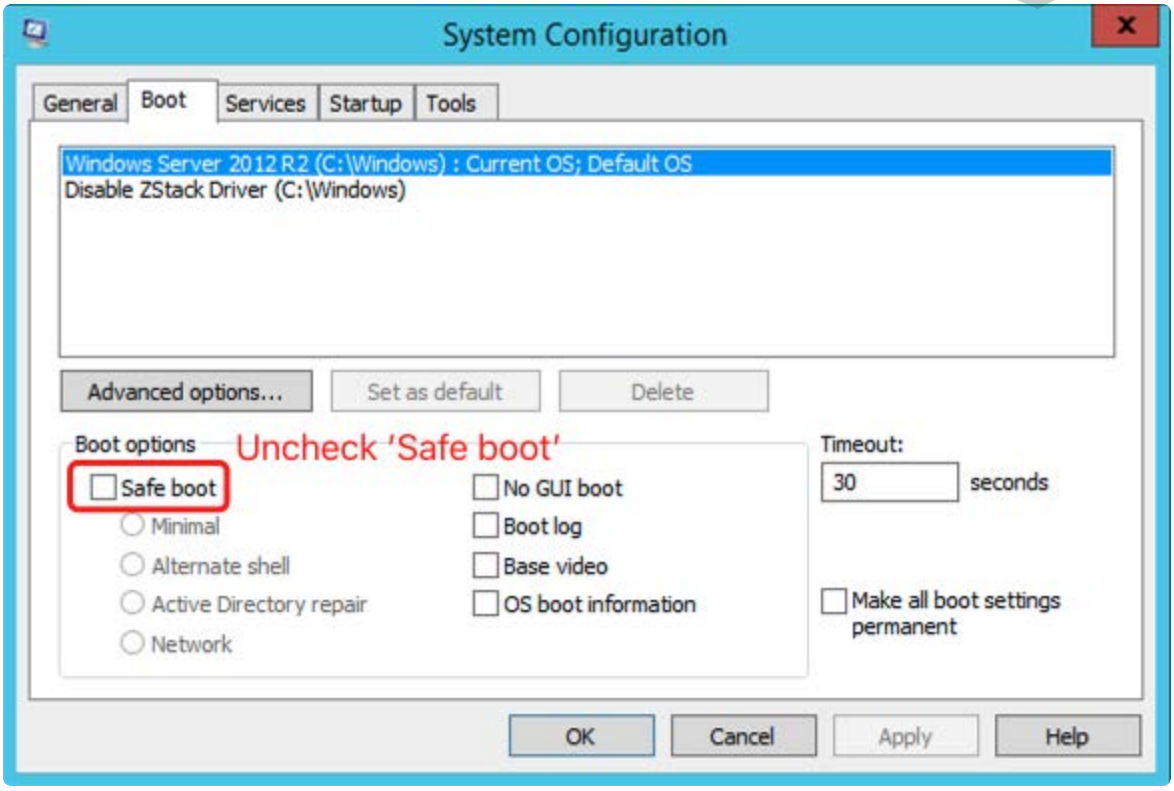


3. After entering the system, run –-> msconfig to open the system configuration.

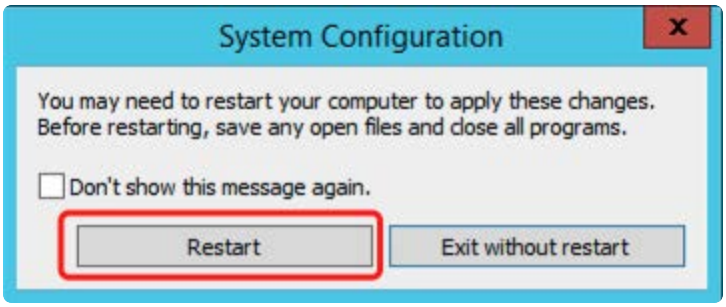


4. In the boot options of the system configuration**uncheck Safe Boot** and click OK.

NEXAVM

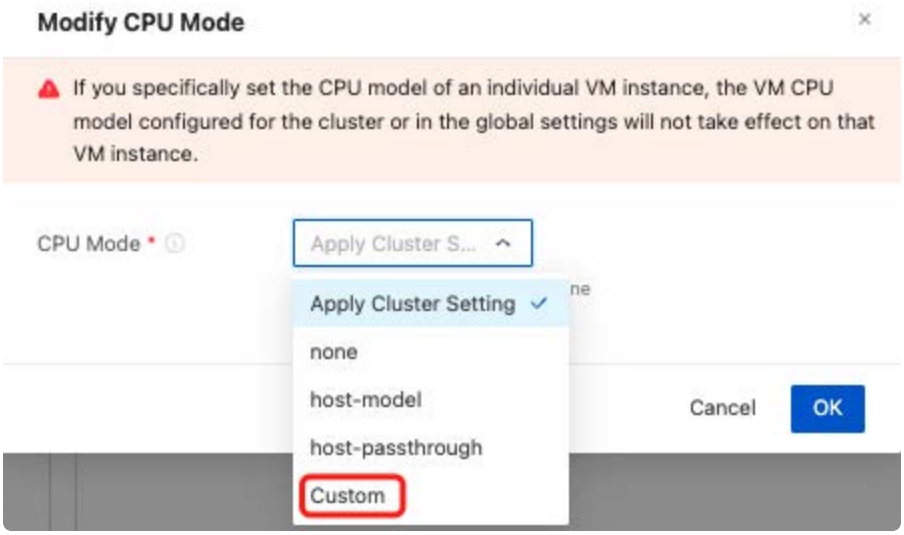


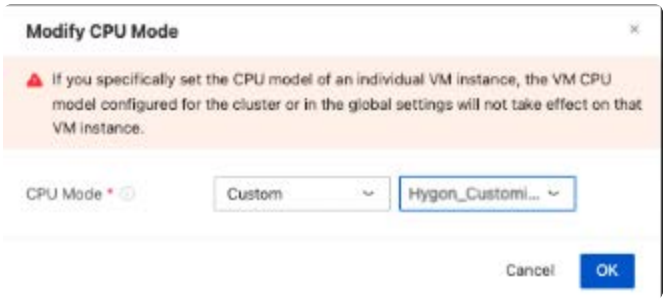
5. A pop-up window will ask you to restart the server, just select Restart.



Solution 2. CPU mode is incompatible

1. Stop the cloud host.
2. Modify the CPU mode to `Hygon_Customized` or `host-passthrough` or `host-model`.
   - In most cases, changing it to `Hygon_Customized` will enable normal booting.
   - In a small number of cases, you need to try the other 2 CPU modes.



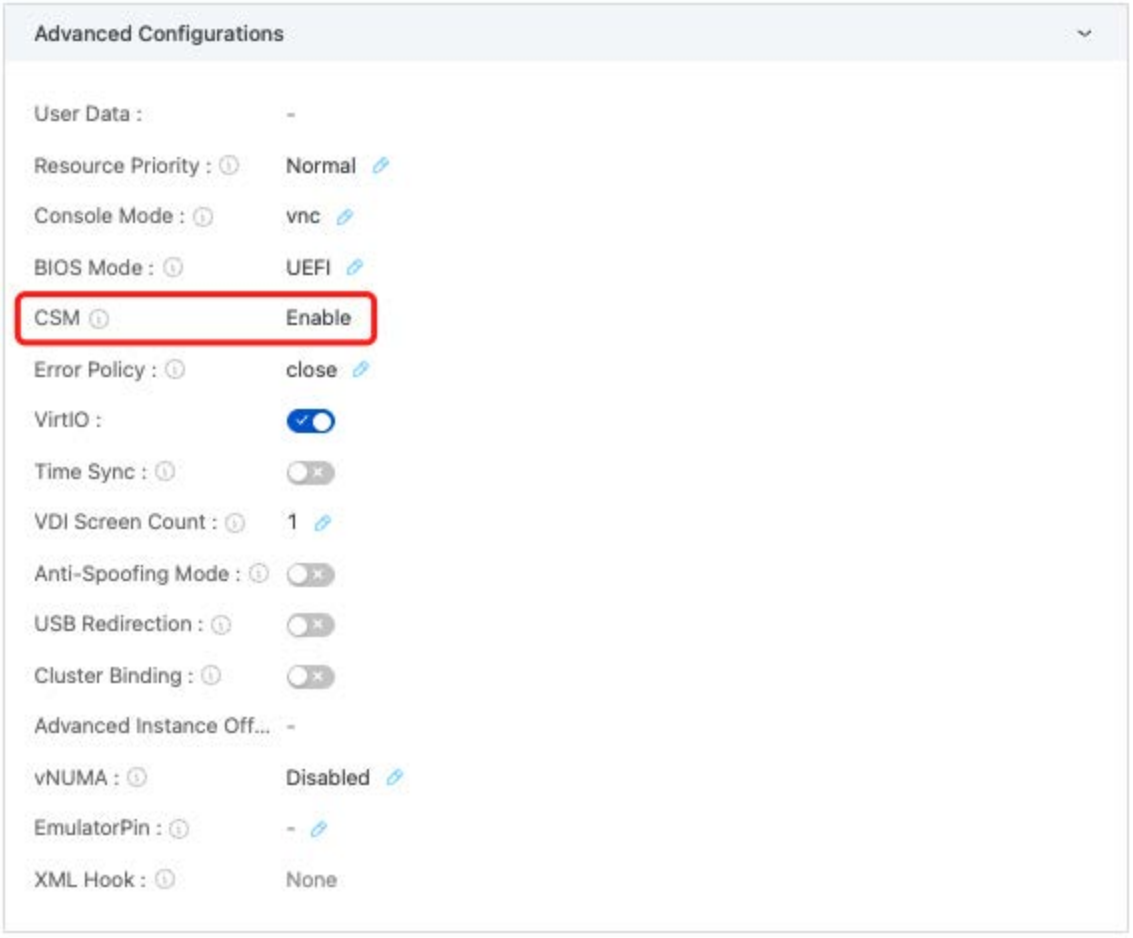


3. Start the cloud host.

Solution 3. UEFI mode is incompatible

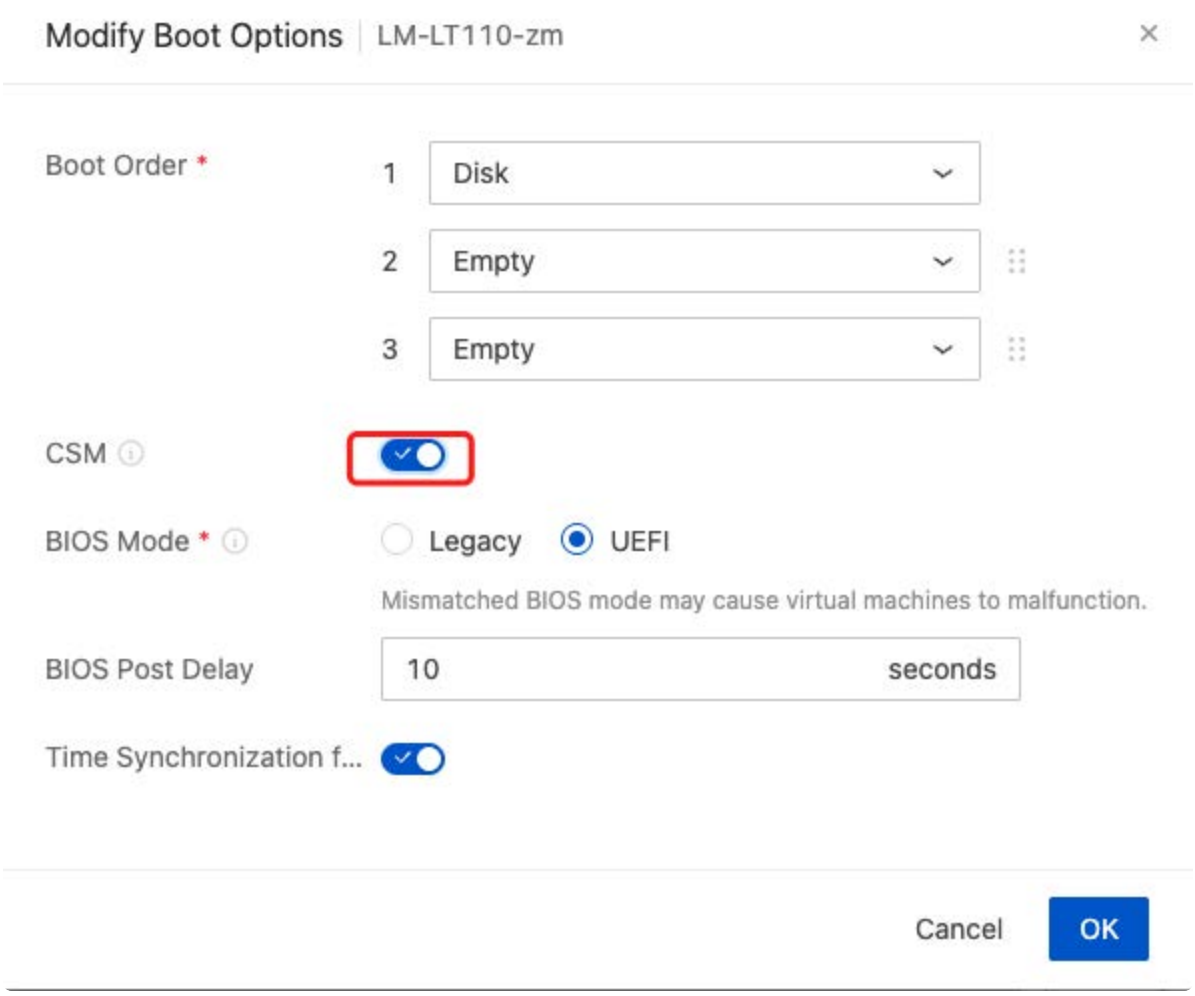
1. Confirm that the system is Win7, Win 2008, or Win 2008 R2.
2. Confirm that the booted BIOS mode is UEFI.
3. Shut down the target system.
4. Turn on the CSM function of UEFI.

NexaVM


Advanced Configurations
User Data :
-
Resource Priority :
Normal
Console Mode :
vnc
BIOS Mode :
UEFI
CSM
Enable
Error Policy :
close
VirtIO :
Time Sync :
VDI Screen Count :
1
Anti-Spoofing Mode :
USB Redirection :
Cluster Binding :
Advanced Instance Off...
-
vNUMA :
Disabled
EmulatorPin :
-
XML Hook :
None

ZSphere

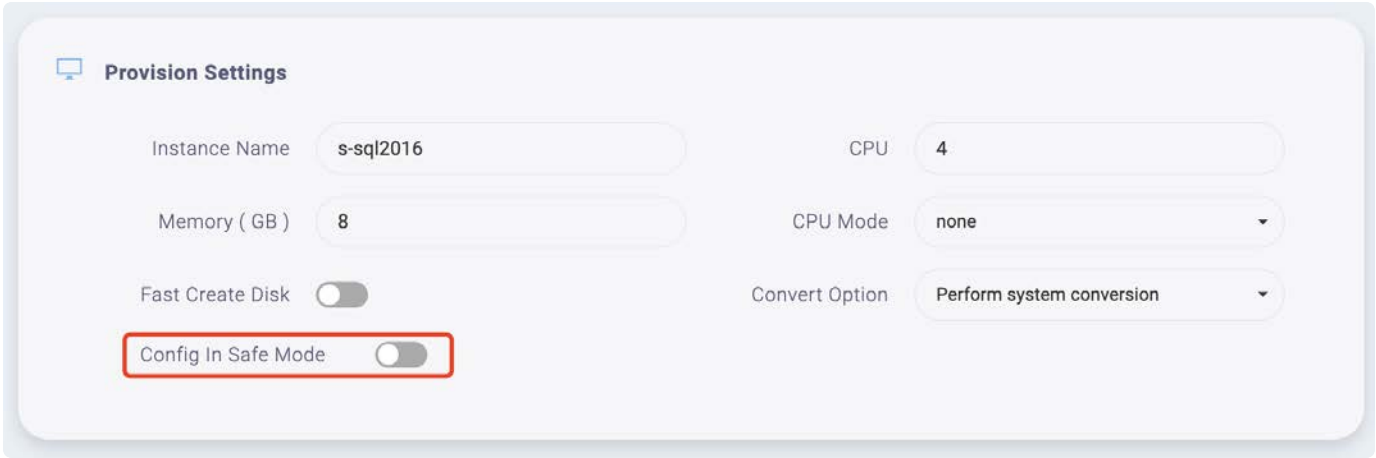
NEXAVM



5. Power on the target machine.

Solution 4. Skip Safe Mode

1. Delete switching tasks.
    - Select the Reswitch option on the left.
2. Re-create the switching task, Close `Configured by Safe Mode` .



3. Wait for the switching task to be completed and observe whether the target machine has entered the operating system normally.

Ignore disk errors when migrating

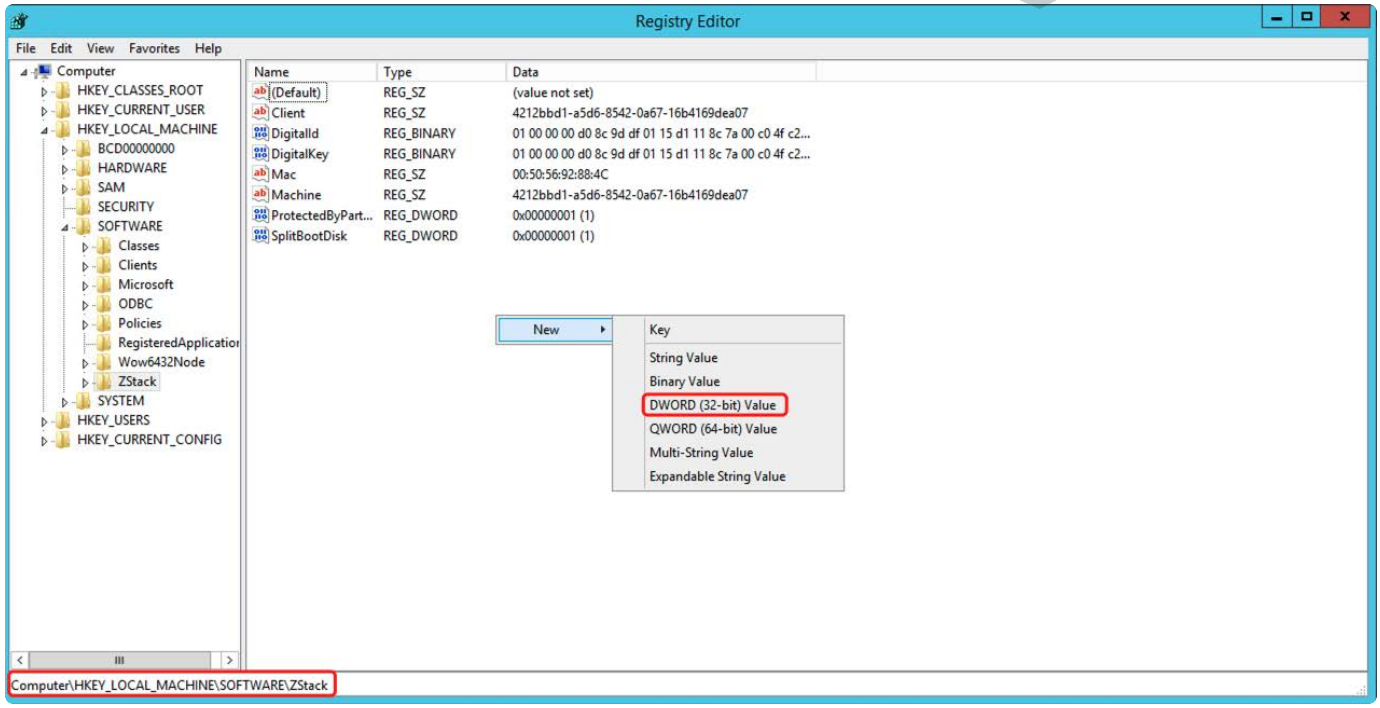
Document Category: Product Related Experience

Background (very important)

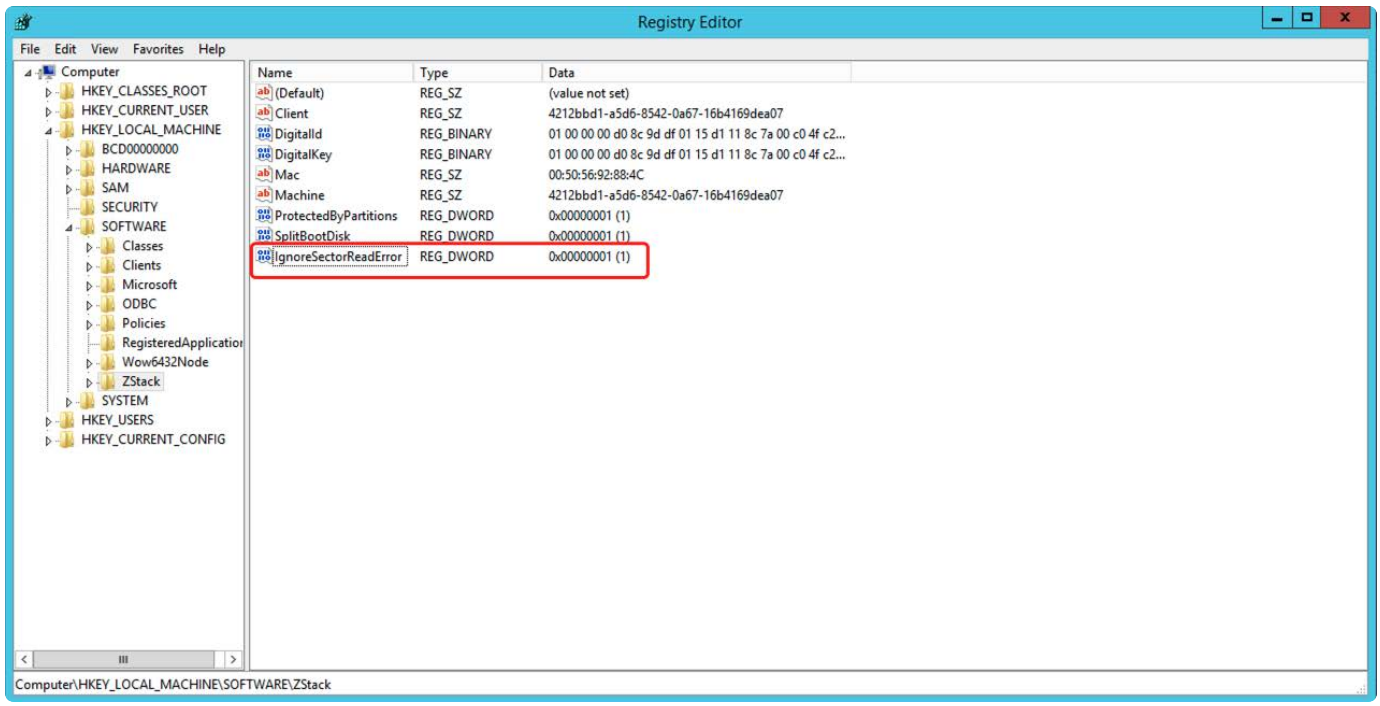
1. After a disk error occurs, it is recommended to communicate with the user to fix the disk error before migrating.
2. If the user insists on not repairing the problem, he or she can use the knowledge base's methods to ignore the bad blocks.
    - If the system disk error is serious, ignoring the disk error may cause the system conversion to fail, and the user needs to be informed in advance.
    - If the data disk error is serious, if the disk error is ignored, the migrated business may not be able to run normally, and the user needs to be informed in advance.

Windows source host configuration skip disk error

1. Stop the synchronization task.
2. Open the registry
    - Run --> regedit
3. Locate \HKEY_LOCAL_MACHINE\SOFTWARE\ZStack and create new --> **DWORD (32-bit) value (D)**



4. Name: IgnoreSectorReadError, value: 1.



5. Initiate synchronization.

Linux source host configuration skips Superblock error

1. Stop the synchronization task.

NEXAVM

2. Configure to ignore disk errors (Superblock errors).

```
cd /usr/local/antenna/config
touch ignore_sector_read_error
```

3. Restart antenna.

```
cd /usr/local/antenna/
./antenna --restart
```

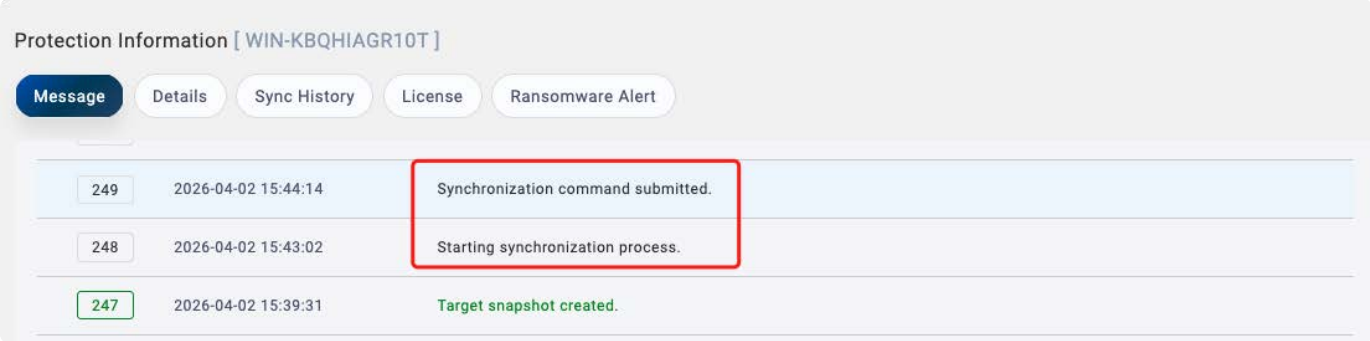
4. Initiate synchronization.

Reset program - processing Protection task stuck

Document Category: Product Related Experience

Applicable situations

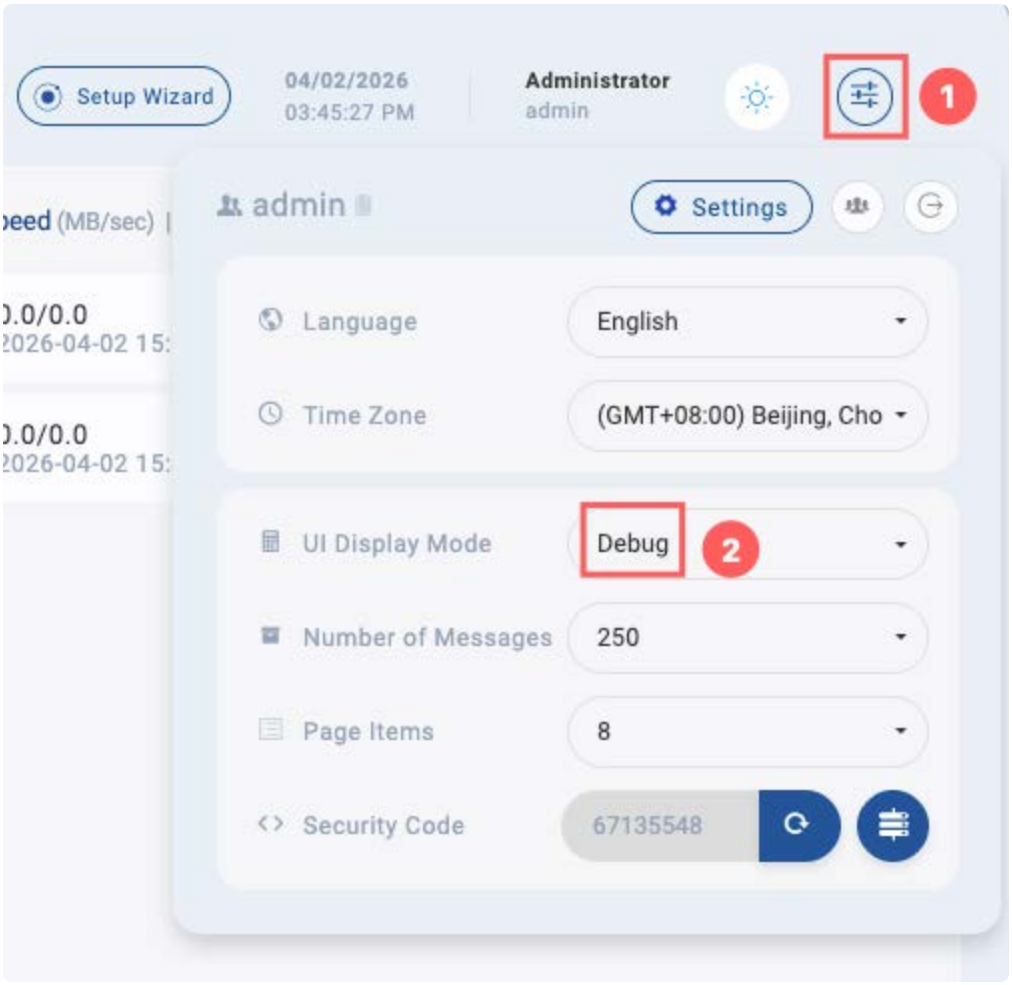
The synchronization task is stuck at "Synchronization command submitted."



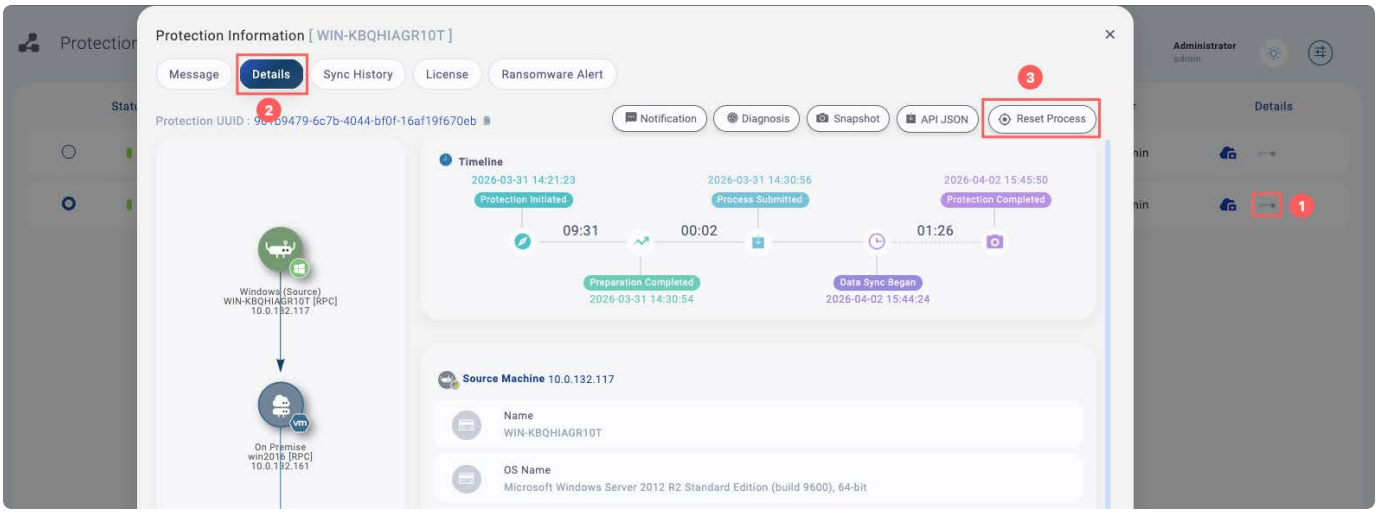
[Recommended]Reset procedure on the management console web page

Operation steps

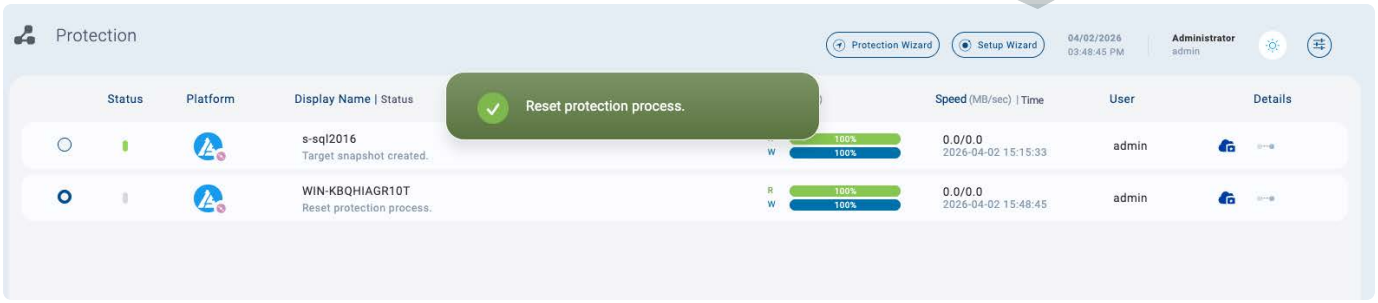
1. Change the configuration status of the management console to `Debug` .

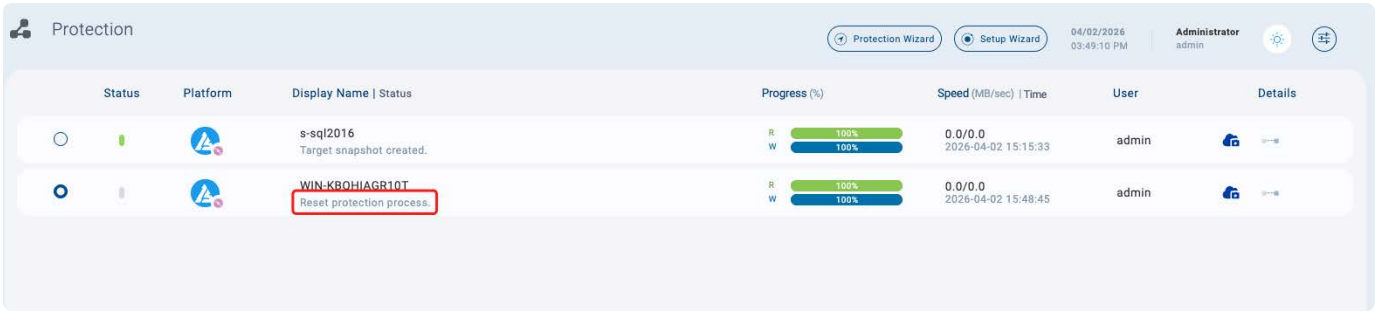


2. Click on sync task details –-> Details –-> Reset Process.

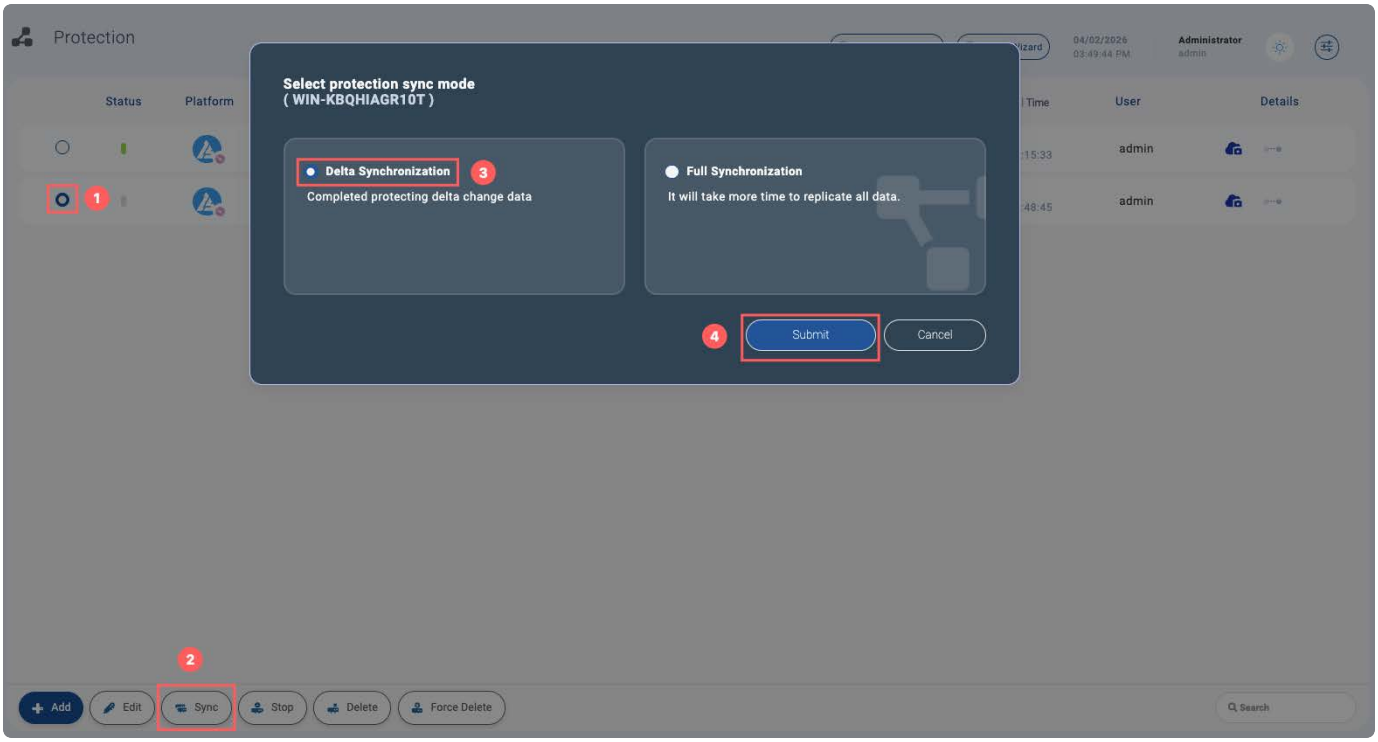


3. Wait for the reset task to complete.

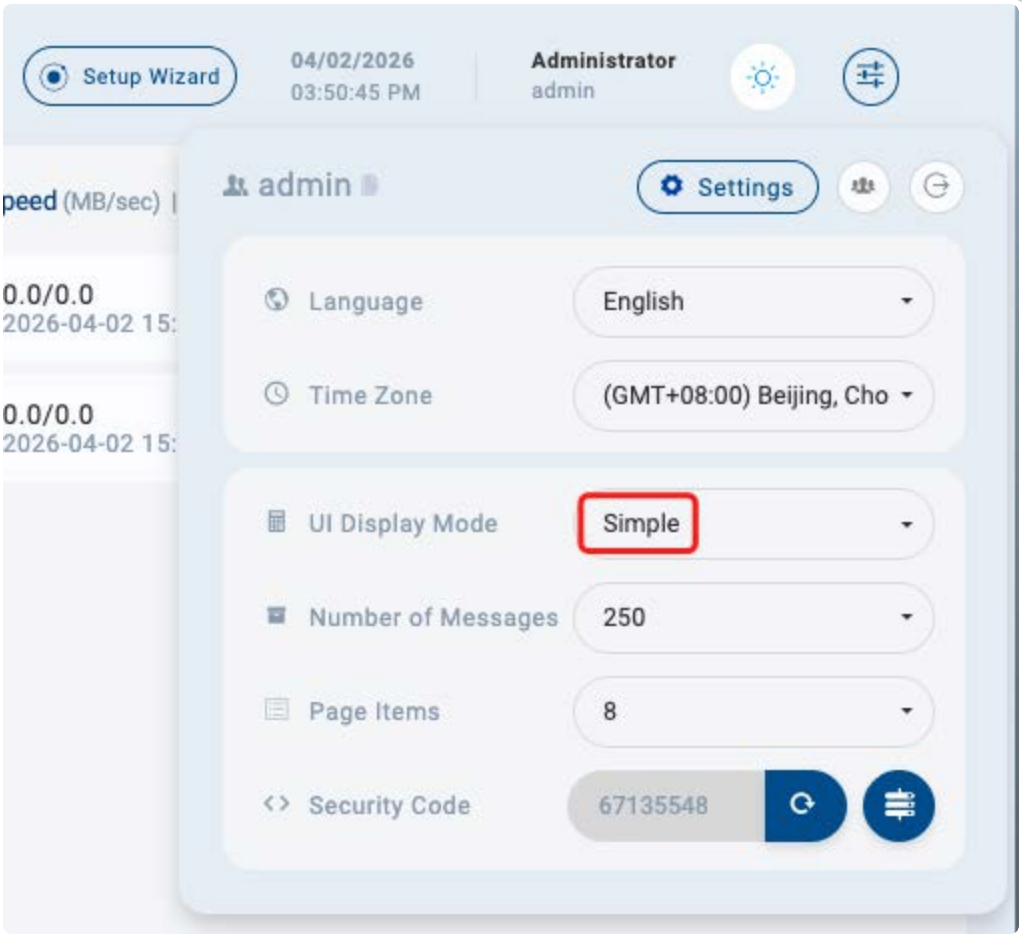




4. Manually synchronize tasks.



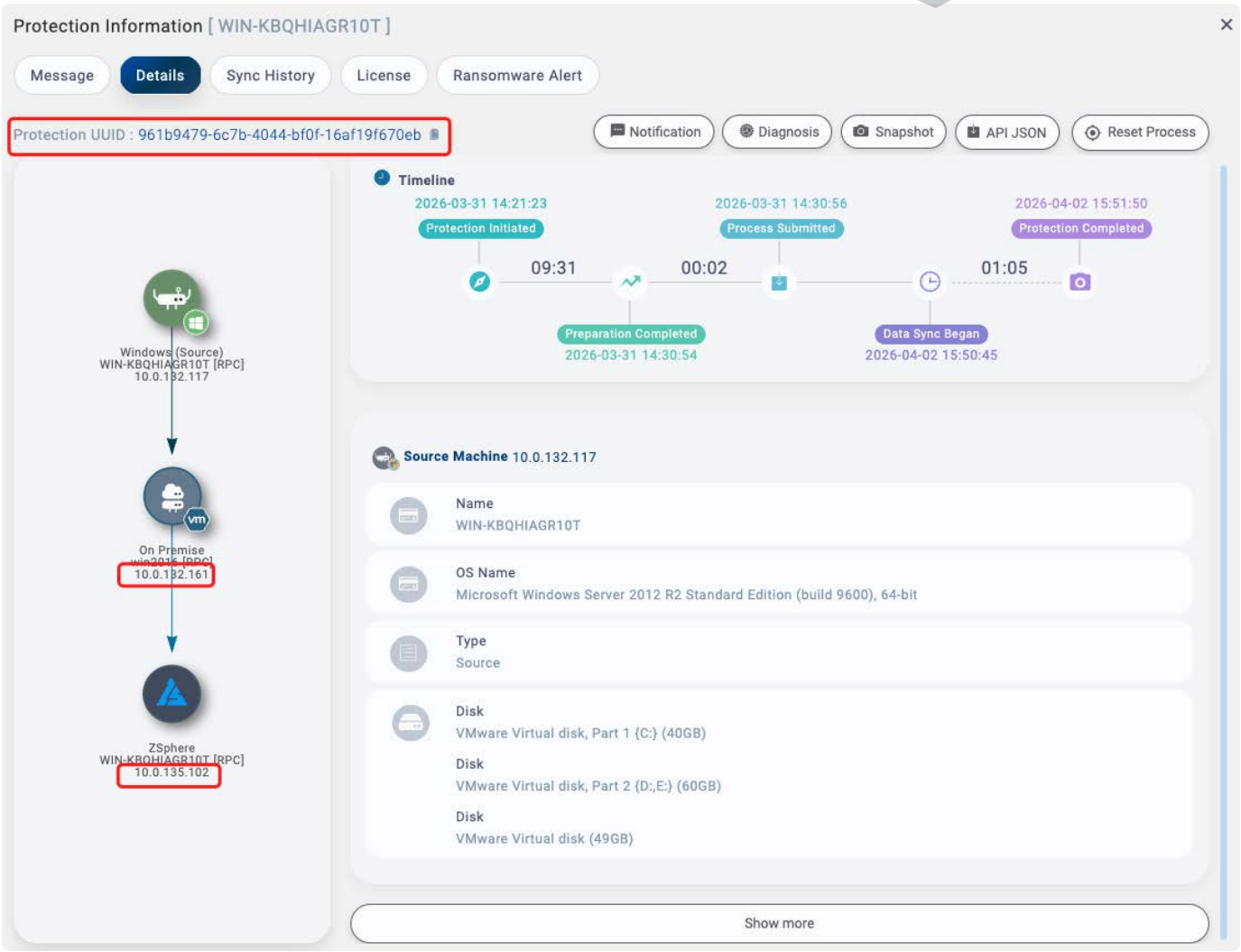
5. **[Recommendation]**Change the configuration state of the management console back to `Simple`.



[Not recommended] Manually reset the program through commands – Windows Management Console

Operation steps

1. Log in to the remote desktop of the management console.
2. Record the UUID of the protection task, the transit data gateway, and the IP address of the target machine.



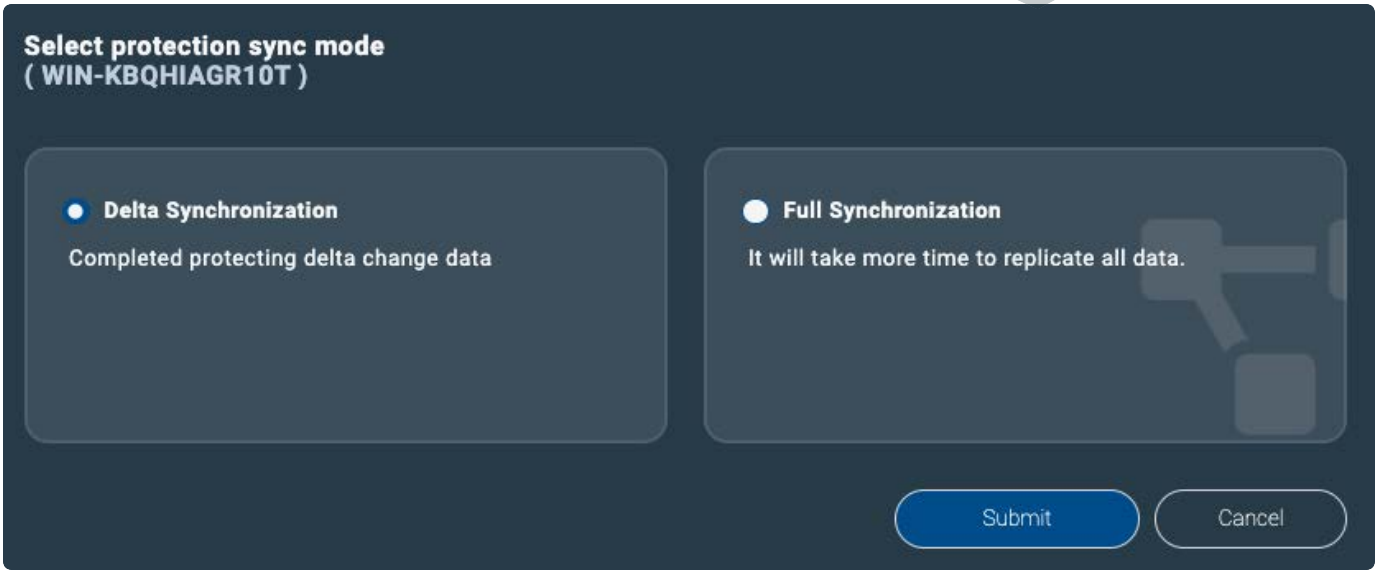
3. Run --> cmd --> Use cd to switch to the Treker installation directory.
4. Execute the Reset Job command.

> If there is no transfer data gateway, both the transfer data gateway_IP and the target machine_IP fill in the target machine_IP.

```
#Enter the treker installation directory.
cd /d %webroot%

#Execute the Reset Job command. When entering,do not include the angle brackets <>.
TrekerControl.exe --reset <Protection UUID> --server <DataGateway IP>
TrekerControl.exe --reset <Protection UUID> --server <TargetMachine IP>
```

5. Select the protection task and click Sync (select the first item: Delta synchronization).

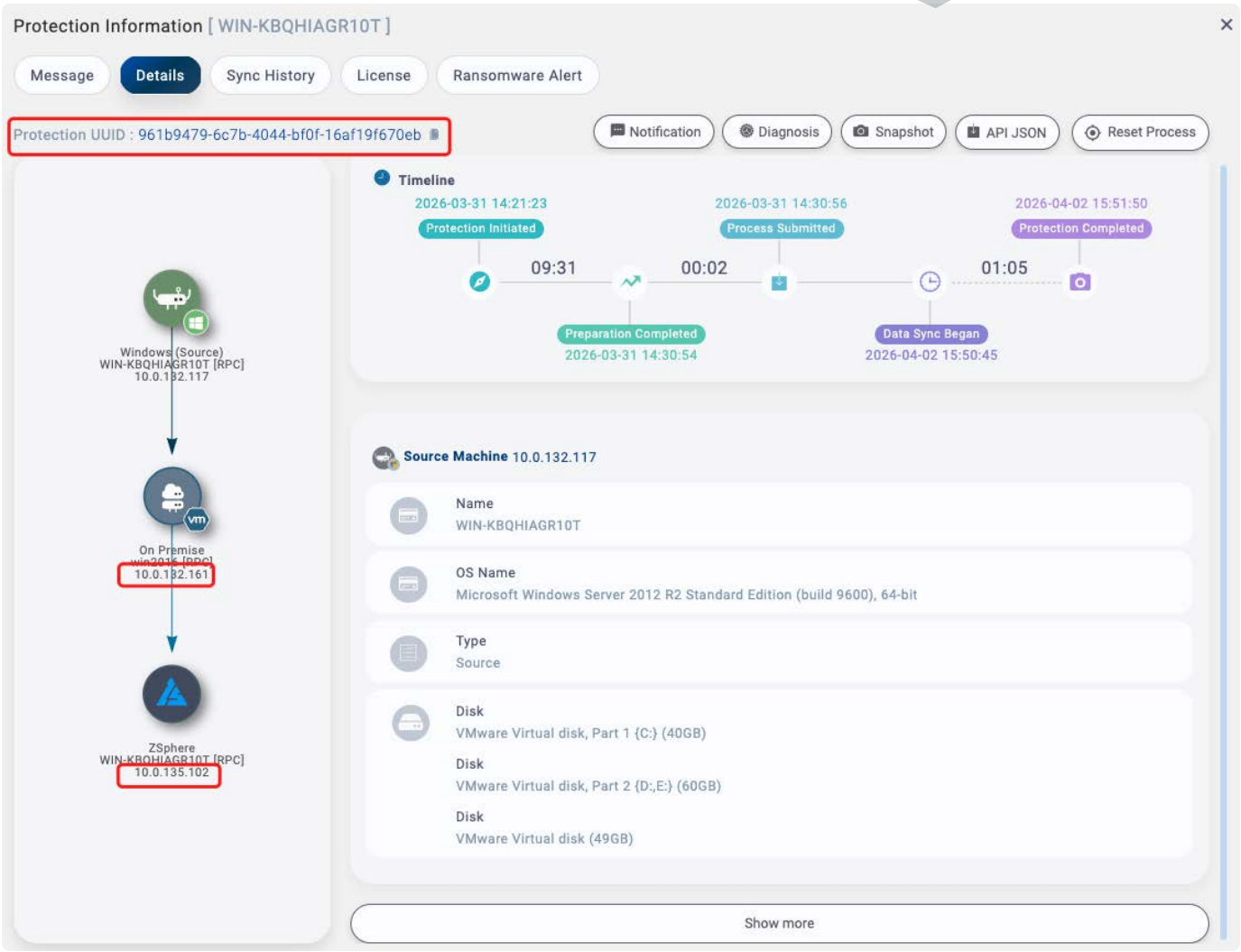




[Not recommended] Manually reset the program through commands–Linux Management Console

Operation steps

1. Log in to the remote desktop of the management console.
2. Record the UUID of the protection task, the IP address of the transit server and the target server.

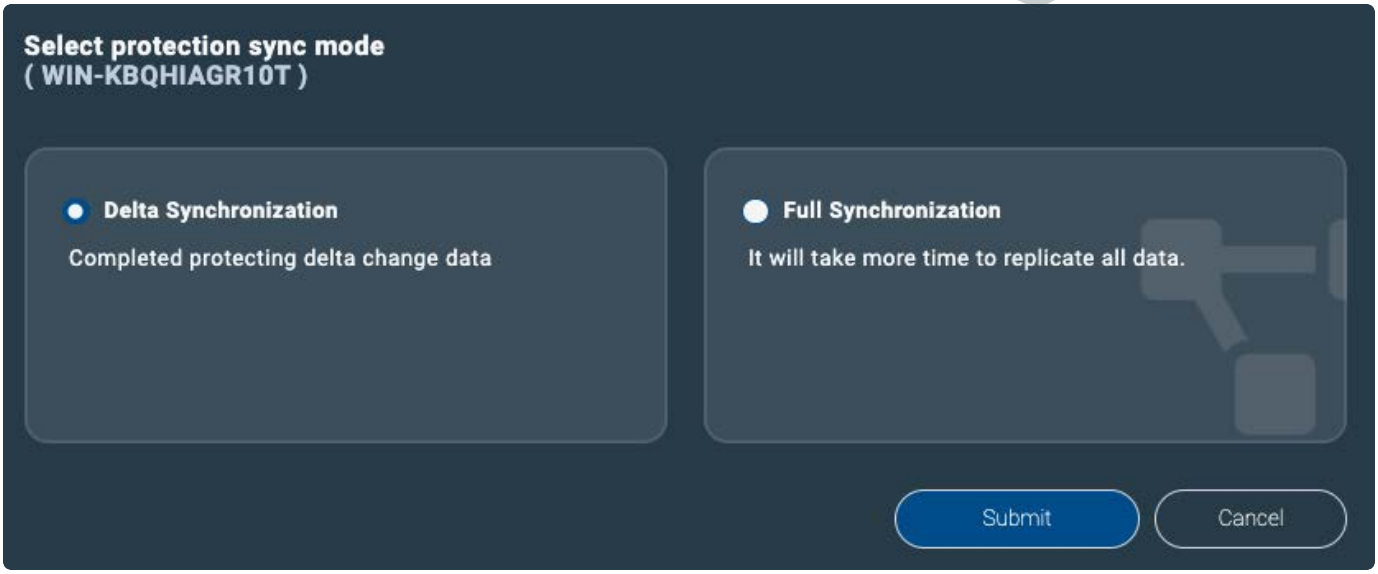


3. Log in to the LinuxTreker system. It is recommended to log in via ssh to facilitate copying and pasting the UUID and Server IP.
4. Execute the Reset Job command.

> If there is no transfer data gateway, both the transfer data gateway_IP and the target machine_IP fill in the target machine_IP.

```
#Execute the Reset Job command. When entering,do not include the angle brackets <>.
docker exec trekercontrol --reset <Protection UUID> --server <DataGateway IP>
docker exec trekercontrol --reset <Protection UUID> --server <TargetMachine IP>
```

5. Select the protection task and click Sync (select the first item: Delta synchronization).



Protection Information [WIN-KBQHIAGR10T]

Message | Details | Sync History | License | Ransomware Alert

232	2026-04-02 15:50:50	Protection size of disk 0-1 is 3.86 MB .
231	2026-04-02 15:50:49	Calculating replication size of disk 0-1 .
230	2026-04-02 15:50:37	Initiating protection process.
229	2026-04-02 15:50:35	Synchronization command submitted.
228	2026-04-02 15:50:34	Starting synchronization process.

Stagger the schedule of Protection tasks

Document Category: Product Related Experience

Schedule planning

From the perspective of optimal performance, if there are many parallel protection tasks at the same time, it is recommended to stagger the time of protection tasks.

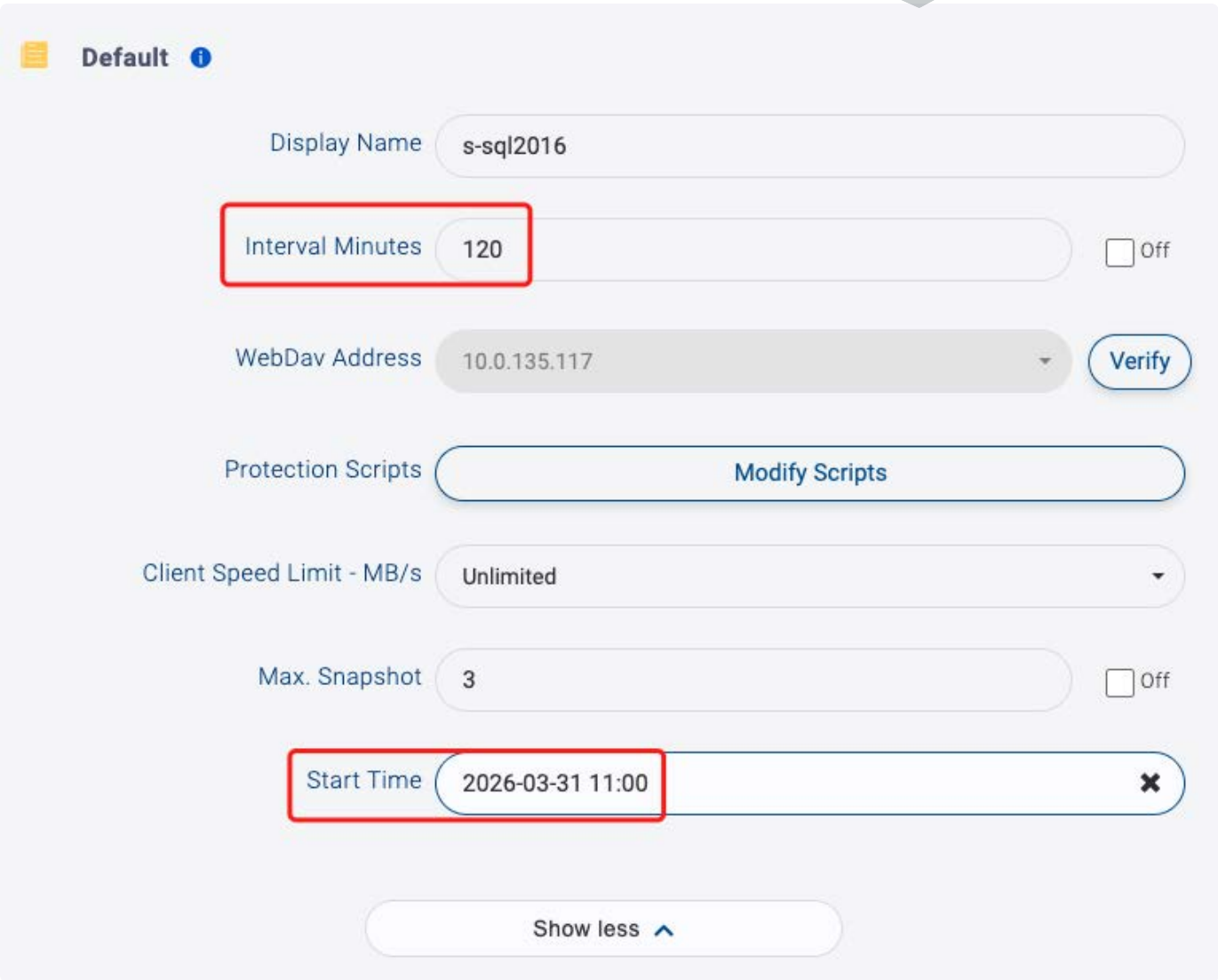
like:

Assume that the replication interval is one hour and 20 tasks

- 5 tasks start synchronizing at 11:00;
- 5 tasks start synchronizing at 11:15;
- 5 tasks start synchronizing at 11:30;
- 5 tasks start syncing at 11:45.

Supplementary knowledge

For example, when creating a migration task, set the "Startup window" to 11 o'clock and the "Incremental synchronization frequency" to 120 minutes:



The first replication starts at 11 o'clock and is synchronized every 2 hours. Then the incremental synchronization time is 13 o'clock, 15 o'clock, 17 o'clock, 19 o'clock, and continues backward.

If the task is already running and the start time of the task is modified, such as 11:45, then the next increment will be synchronized at 11:45, and the next time will be 13:45, and will be postponed in sequence.