Sangfor Cloud Migration Platform

User Manual

Product Version	2.0
Document Version	V1.2
Released on	March. 15, 2022

Disclaimer

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

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is used for reference only, and all statements, information, and recommendations therein do not constitute any express or implied warranties.

Technical Support

For technical support, please visit: https://www.sangfor.com/en/about-us/contact-us/technical-support

Send information about errors or any product related problem to tech.support@sangfor.com.

About This Document

This document describes the user manual of the Sangfor Cloud Migration Platform(SCMP) User Manual.

Intended Audience

This document is intended for:

- System / Network Administrator
- Technical Users

Note Icons

English Icon	Description
	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
	Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.
	Indicates a hazardous situation, which if not avoided, could result in settings failing to take effect, equipment damage, or data loss. NOTICE addresses practices not related to personal injury.
	Calls attention to important information, best practices, and tips. NOTE addresses information not related to personal injury or equipment damage.

Change Log

Date	Change Description
Mar. 15, 2022	SCMP User Manual.

Contents

1 Overview

Use the Sangfor Cloud Migration Platform (SCMP) to perform P2V and V2V migration of customer production virtual machines, including point-to-point migration, backup migration, and HA backup migration.

1.1 Introduction to Platform

SCMP provides the function of fully migrating the host (X86 server or virtual machine of another specific virtualization platform) systems to the Sangfor HCI platform to ensure smooth and stable production migration.

NOTE

The Sangfor Cloud Migration Tools(SCMT) installation package is intended for the Sangfor Cloud Migration Platform (SCMP).

1.2 Key features

SCMP supports both agentless migration and agent-based migration. Depending on different environments and business requirements, the migration mode supports point-to-point migration, HA backup migration, and backup migration:

- **Point-to-point (agentless)**: The VMware platform supports the source machine's migration without the agent's installation and uses the VMware VADP interface to obtain VM data. After migrating to the HCI destination machine, it supports automatic compatibility processing (injection of vmtools). There is no need to back up the source system, and the source system data is transferred to the destination virtual machine through the Sangfor Cloud Migration platform.
- **Point-to-point migration (agent-based)**: It uses the migration function to directly transfer the source data to the destination machine to migrate the source as a whole to the destination machine. There is no need to back up the source system, and the source system data is transferred to the destination virtual machine on the HCI platform.

- **HA backup migration**: The source system data is continuously backed up to the Sangfor Cloud Migration Platform using the function of CDP backup and then synchronized to the destination virtual machine. In this way, data from the source system is synchronized to the destination in real-time through CDP, which minimizes the migration and switching time.
- **Backup recovery mode**: Use the backup function to back up the source system data to the Sangfor Cloud Migration platform. Then, restore the system to the destination virtual machine through the backup file saved on the server. Compared with point-to-point migration and HA backup migration, longer business downtime is required.

1.3 Platform Architecture

SCMP comprises the **Sangfor Cloud Migration Platform(SCMP)**, **Migration Agent** for the source system, and **Bare Metal Restore** for the destination virtual machine. The functions of these three parts are as follows:

1. Sangfor Cloud Migration Platform(SCMP)

- Connect the source and destination machine and also issue the migration tasks.
- For agentless migration, connect to the source virtualization platform to obtain source virtual machine data.
- Connect to the HCI platform management and call the HCI platform API interface to create the destination virtual machine automatically.

2. Migration Agent

- It is installed on the source host or virtual machine to connect to the SCMP and obtain the migration tasks issued by the SCMP.
- Obtain the data of the source host or virtual machine and transfer it to the destination virtual machine or SCMP.

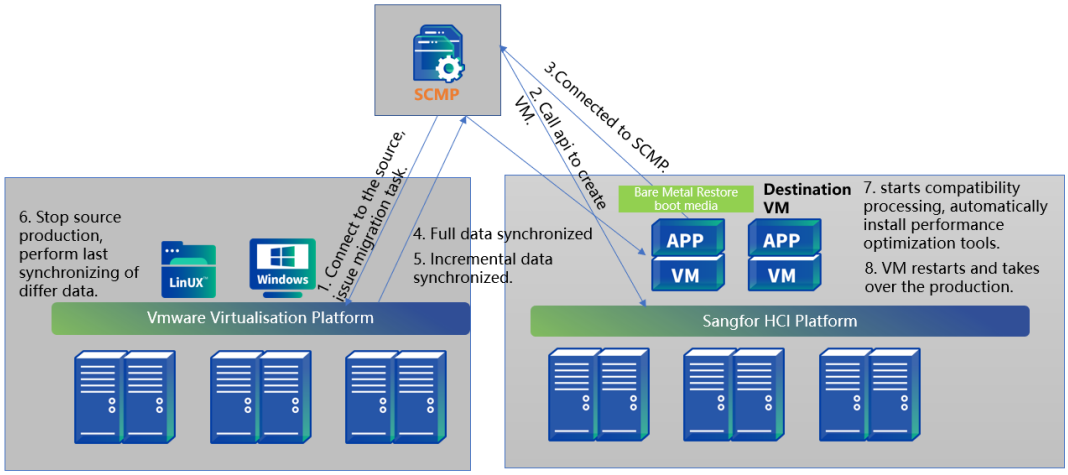
3. Bare Metal Restore

- The destination virtual machine will first boot from the bare metal and connect to the SCMP.
- Accept the migration tasks issued by the SCMP.

- Receive the data transmitted by the source host or virtual machine, or receive the data restored by the SCMP.

Different migration modes have different product networking architectures. The following are the networking architectures of Sangfor Cloud Migration Platform under different migration modes:

1.3.1 Agentless Point-to-point Migration



In the agentless point-to-point migration mode, the migration process of the Sangfor Cloud Migration Platform is as follows:

1. The Sangfor Cloud Migration Platform connects to the source VMware virtualization platform, obtains the virtual machine list of the source VMware virtualization platform, and issues migration tasks.

2. Sangfor Cloud Migration Platform calls HCI's API interface to create the destination virtual machine and automatically loads the bare-metal restore to power on.

3. After modifying the bare metal restore IP address, the destination virtual machine actively connects to the Sangfor Cloud Migration Platform, obtains the migration task through the SCMP, and receives the data transmitted from the source VMware virtualization platform.

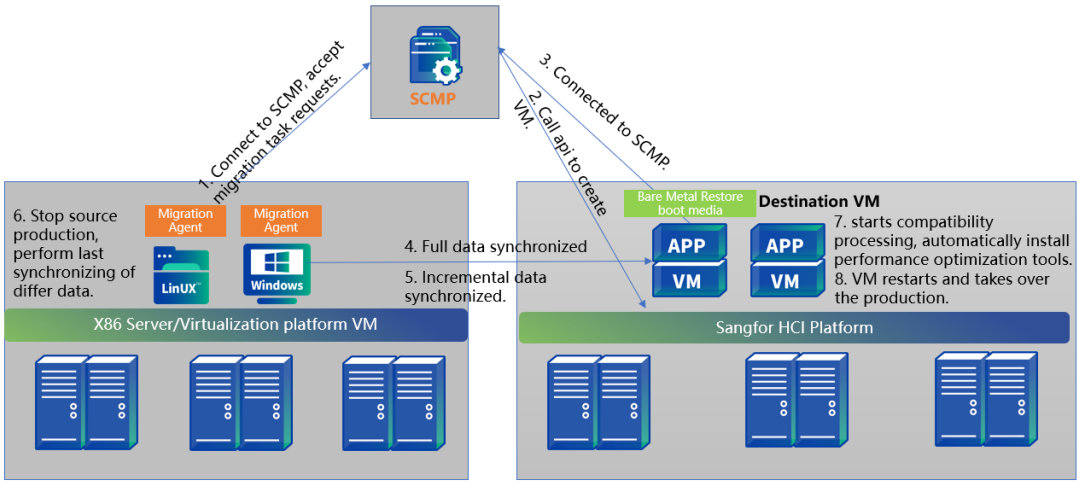
4. The source and destination machines are synchronized with full and incremental data through the SCMP.

5. Stop the source production and perform production switching after synchronizing the last difference data.

6. The destination virtual machine starts compatibility processing and automatically installs a performance optimization tool(vmtool).

7. The destination virtual machine restarts and takes over the production.

1.3.2 Agent-based Point-to-point Migration



The migration process for Agent-based Point-to-point Migration mode in Sangfor Cloud Migration Platform is as follows:

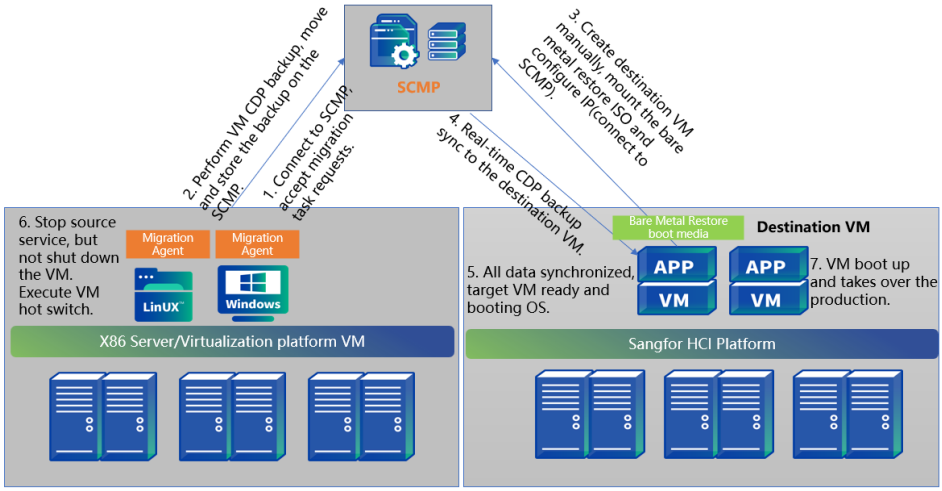
1. The source machine installs the migration agent, and the migration tool has two modes: **active** and **passive**.

- In the active mode, the migration agent at the source actively connects to the SCMP and receives tasks issued by the SCMP.
- In the passive mode, SCMP will take the initiative to connect the source machine migration agent to issue migration tasks.

2. SCMP calls HCI's API interface to create the destination virtual machine and automatically loads the bare-metal restore to start.
3. After modifying the bare metal restore IP address, the destination virtual machine actively connects to the SCMP, obtains the migration task through the SCMP, and receives the data transmitted from the source machine migration agent.

4. Full data synchronization.
5. Incremental data synchronization.
6. Stop the source production, and perform production switching after synchronizing the last difference data.
7. The destination virtual machine starts compatibility processing and automatically installs performance optimization tools(vmTools).
8. The destination virtual machine restarts and takes over the production.

1.3.3 HA Backup Migration



The migration process of the HA backup migration mode in SCMP is as follows:

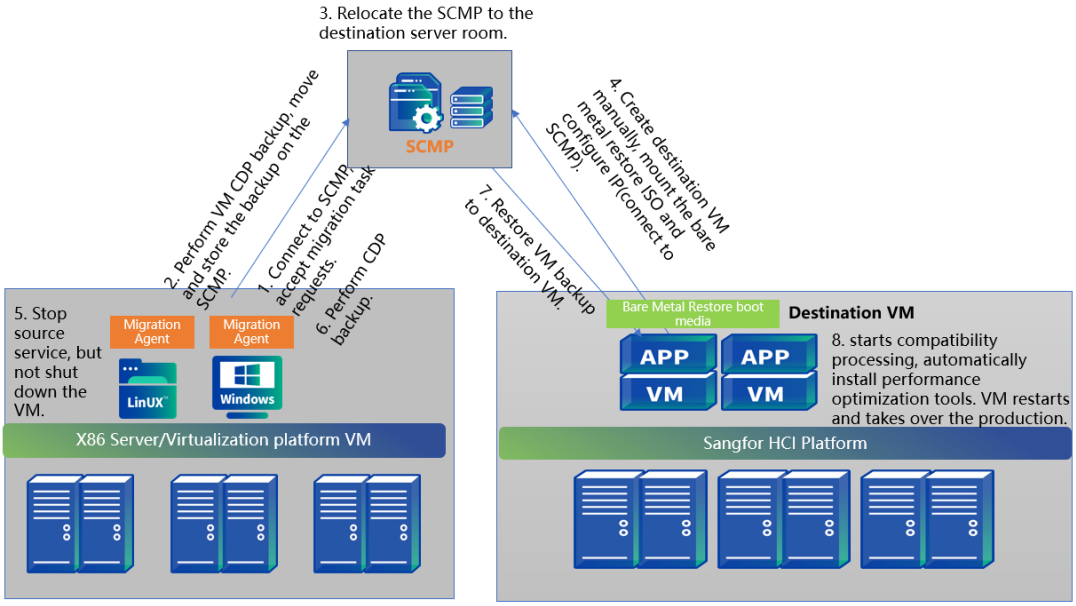
1. The source host installs the migration agent, and the migration tool has two modes: **active** and **passive**.

- In the active mode, the migration agent at the source actively connects to the SCMP and receives tasks issued by the SCMP.
- In the passive mode, SCMP will take the initiative to connect the source machine migration agent to issue migration tasks.

2. Perform CDP backup on the entire source machine and store the backup on the SCMP.
3. Manually create the destination virtual machine, manually mount the bare metal restore ISO file and power on the VM. Configure the IP address to connect to the SCMP.
4. Create a CDP backup plan, and SCMP will sync the source machine's CDP backup to the destination virtual machine in real-time.

5. After synchronizing the data, the destination machine is ready and booting OS.
6. Stop the source application service, but do not shut down, and execute the HA backup switch plan.
7. The destination virtual machine starts compatibility processing and automatically installs performance optimization tools(vmTools).
8. The destination virtual machine restarts and takes over the production.

1.3.4 Backup Migration



The migration process of the backup migration mode in SCMP is as follows:

1. The source host installs the migration agent, and the migration tool has two modes: **active** and **passive**.

- In the active mode, the migration agent at the source actively connects to the SCMP and receives tasks issued by the SCMP.
- In the passive mode, SCMP will take the initiative to connect the source machine migration agent to issue migration tasks.

2. Perform a full backup of the source machine to the storage of the SCMP.
3. Relocate the SCMP to the destination server room.
4. Manually create the destination virtual machine, mount the bare metal restore ISO file, and boot it. Configure the IP address to connect to the SCMP.

5. Stop the source machine application service, but not shut down the host.
6. Perform incremental backup of the source machine.
7. Restore the backup to the destination virtual machine.
8. The destination virtual machine performs compatibility processing and automatically installs the performance optimization tool(vmTools). The VM will be restarted after installing vmTool and will take over the business normally.

2 Migration Constraints

2.1 Migrate Network Constraints

1. During the migration process, the network latency between the source and the HCI platform(where the destination is located) must be within 50ms, and the packet loss rate is within 5%.
2. To meet the migration requirements of different network environments, the migration agent of the SCMP supports two connection modes:

- For the **Actively Connected Agent** migration mode, point-to-point migration will connect to ports 80 and 20000-20047 of the SCMP. While for HA backup or backup migration, it will connect the ports 80 and 20000-20003 of the SCMP. If there is a firewall or DNAT in the connection link, it is necessary to allow these ports to be accessed.
- For the **Passively Connected Agent** migration mode, it will be the SCMP access to the port of the migration agent. The default port for **Connected TCP Port** is **3345**, and it can be changed when downloading the migration agent. If there is a firewall or DNAT in the connection link, it is necessary to allow access to these ports.

3. For agentless VMware migration, the network needs to meet the following requirements:

- SCMP needs to be able to access the TCP port 443 of VMware vCenter and the TCP port 902 of the ESXi server.
- The network between the source VMware vCenter and SCMP must be reachable.

- The network between the source VMware ESXi host and SCMP must be reachable.
- If the ESXi host uses a domain name to connect to vCenter, the domain name of the ESXi host must be able to be resolved by SCMP.
- The VMware account used needs permission to back up the virtual machine.

2.2 Compatibility List

2.2.1 Platform Compatibility

The SCMP agentless migration mode supports the migration of virtual machines on the VMware platform to the Sangfor HCI. The supported VMware versions are shown in the following table.

Source platform	Destination platform
VMware vSphere 5.5	HCI 6.0.0 R5, 6.3.0, and later versions support automatic creation of the destination virtual machine and load the bare metal restore to start. After the migration is completed, it supports the automatic installation of a performance optimization tool(vmTools). Other HCI versions doest not support the automatic creation function. It is required to manually create the destination virtual machine and load the bare metal restore ISO file. After the migration is complete, you need to check whether the performance optimization tool is installed.
VMware vSphere 6.0	
VMware vSphere 6.5	
VMware vSphere 6.7	
VMware vSphere 7.0	

Agentless migration of VMware virtual machines does not support virtual machines with RDM disks, independent disks, and network card pass-through scenarios. If you need to migrate virtual machines in the above scenarios, agent-based migration is required.

2.2.2 Operating System Compatibility

1. Agent-based migration supports the migration of Windows and Linux 32/64-bit operating systems.
2. The following file systems are supported for migration:

- ext2, ext3, ext4, xfs.

- FAT, FAT32, NTFS, Refs.

3. The following file device formats are supported for migration:

- LVM, GPT, MBR, dynamic volume, spanned volume, striped volume.

Please refer to the **SCMP Compatibility List-20211214** for detailed compatibility information.

2.2.3 Production Compatibility

Migration of cluster applications, such as Oracle RAC, SQL Server failover clusters, and other applications are not supported. Only standalone applications can be migrated.

2.3 Migration Specification Restrictions

Name	Specification
Maximum concurrent migration tasks	No limitation. When the system resources of the Sangfor Cloud Migration Platform are insufficient, there will be a queuing mechanism for migration tasks. The pending migration tasks will continue the switching when there are sufficient resources. As the number of migration tasks switched at the same time increases, the switching duration will be increased accordingly.
Migration speed	Depending on the migration network bandwidth and storage performance, the measured migration rate can be up to 110MB/s with an agent in a 1G network environment and 300MB/s with an agent in a 10G network environment 35MB/s without an agent. The block size of the data migrated by the migration tool is 64k sequential read and write, and the block size can evaluate the storage performance of the source and destination.

2.4 Production Interruption Time Reference

The following is the switching time of different operating systems in different migration modes (excluding the service startup time of the business). In the case of production service startups, the start time will be vary depending on the production type.

Under normal circumstances, the production downtime for different migration mode is as follow:

1. Point-to-point migration mode: 5-10 minutes.
2. HA backup migration mode: around 1 minute.
3. Backup migration mode: around 15 minutes.

Operating System	Migration Method	Production switching-switch successful
Windows Server 2016	Point-to-point Migration	3 minutes 27 seconds
	Point-to-point Migration (Agentless)	5 minutes 7 seconds
	HA Backup Migration	01 minute 22 seconds
	Backup Migration	16 minutes and 16 seconds
Linux	Point-to-point Migration	4 minutes 6 seconds
	Point-to-point Migration (Agentless)	2 minutes 51 seconds
	HA Backup Migration	01 minute 13 seconds
	Backup Migration	8 minutes 22 seconds

Table 1: Service switching time reference table

2.5 System Changes After Migration

The system configuration will also change accordingly since the physical or virtual machine's operating platform has changed after the migration. The specific changes are shown in the following table.

Category	Details
CPU	The total number of CPU cores is the same as the source machine by default.
	The total number of CPU cores can be changed. The minimum number of cores is 1.

Memory/RAM	The memory size is the same as the source machine by default.
	The memory size can be changed, and the changed memory cannot be less than 2G.
Disk	After the Windows dynamic disk is migrated, it becomes a basic disk.
	The disk driver may be changed after the migration (virtio driver is used by default).
	The disk partition size will change after the migration (when the remaining disk space is less than 1G, the remaining space will be automatically allocated to the last partition).
	Disks that are not in GPT and MBR format will be converted to GPT or MBR format.
	When the system disk is not the first disk, it will be automatically adjusted as the first disk.
Network Configuration	Virtio driver will be used by default for Windows2003 and above.
	Linux kernel 2.6.18-128 and above use virtio (For other kernel versions, ide+e1000 will be used).
	The MAC and IP of the network card will be changed (consistent with the migration task switching parameters).
System configuration changes	The UUID of the OS changes and applications that rely on the UUID of the system need to be re-authorized, such as Windows license, EDR license, etc.
Performance optimization tools(vmTools)	According to HCI rules, performance optimization tools will be installed on the following OS: 1. Windows 2003 and above 2. Linux 2.6.18-128 and above.

3 Platform Deployment

This chapter mainly explains the process, precautions, preparations, and operation steps of the platform installation process.

3.1 Installation Preparation

Tool/Material Name	Main Content	Download link

Sangfor Cloud Migration Platform User Manual	Introduce the applicable scenarios and usage guidance of the SCMP	https://community.sangfor.com/
SangforCloudMigrationPlatform.iso	The ISO installation package for the Sangfor Cloud Migration Platform. After configuration, it can be installed and used on a physical machine or another virtualization platform.	Contact Sangfor Technical Support to obtain
SangforCloudMigrationPlatform.vma	The virtual machine template for Sangfor Cloud Migration Platform. Support direct import into HCI without OS installation.	https://community.sangfor.com/plugin.php?id=service:download&action=view&fid=47#/42/all
Compatibility list of Sangfor Cloud Migration Platform	Introduce the list of operating systems, virtualization platforms, and file systems supported by the SCMP.	Contact Sangfor Technical Support to obtain
Chrome, UltraISO, MD5		Get it online

Table 2: Files and documentation preparation

Before installation, please verify the MD5 value of the software to avoid installation failure due to incomplete download.

3.2 Hardware Specification Requirements

The hardware configuration of the SCMP directly affects the number of concurrent migrations and switching. According to the number of concurrent migrations, the specific hardware configuration requirements of the SCMP are shown in the following table.

Hardware	Minimum configuration	Recommended configuration	Notes
CPU	CPU with 4 cores and above	CPU with 16 cores and above	
Memory/RAM	16GB and above	32GB and above	SCMP itself reserves 8GB of memory, and each concurrent migration or switching occupies 2GB of memory.

System disk	200GB and above	300GB and above	During VMware agentless migration, data synchronization will go through the SCMP. The size of the system disk needs to be expanded appropriately.
Storage disk	200GB and above Evaluate based on the amount of data	300GB and above Evaluate based on the amount of data	According to the data volume of the HA backup/backup migration host, it is generally recommended to set the size to 1.5 times the data volume of the migration.

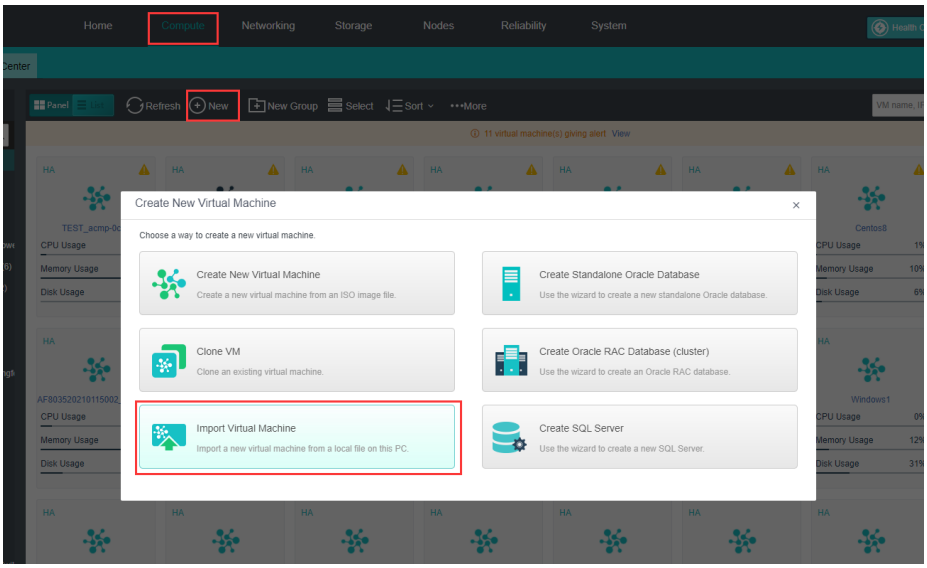
3.3 Installation and Deployment

Sangfor Cloud Migration Platform supports deployment on physical machines and HCI platforms, and there are two installation methods:

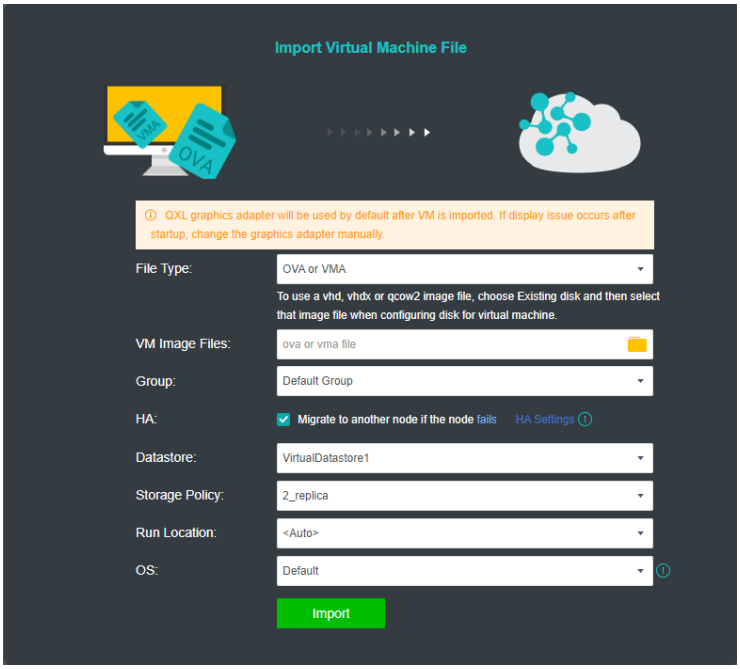
1. **Import the SCMP vma template**: This scenario is suitable for deploying the Sangfor Cloud Migration Platform on the Sangfor HCI, which simplifies the installation steps and saves installation time.
2. **Use ISO file to burn and install**: This scenario is suitable for deploying the Sangfor Cloud Migration Platform on a physical server for backup migration scenarios.

3.3.1 VMA Template Deployment

1. Enter the Sangfor HCI platform, click **Compute**, on Compute UI, click **New**, and select **Import Virtual Machine**.



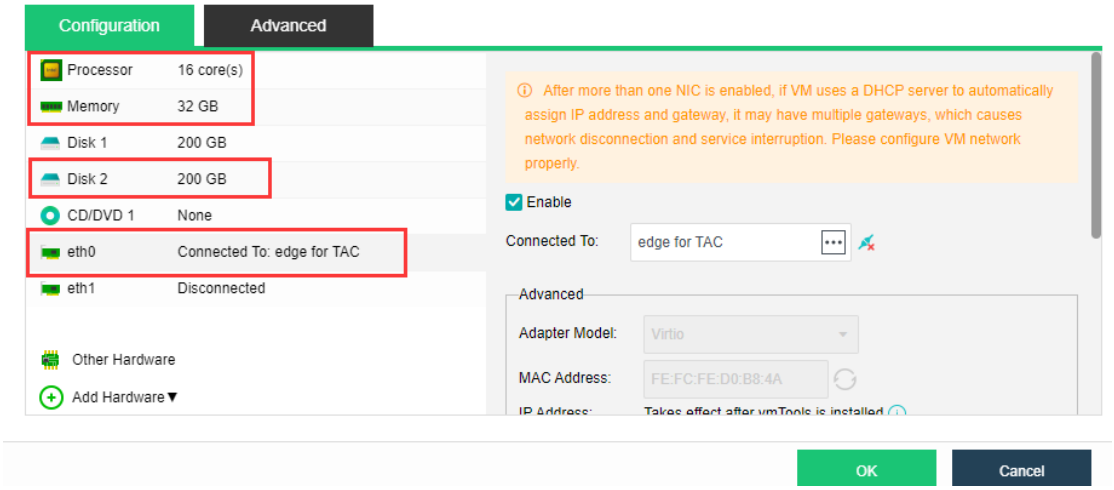
2. Select the downloaded image(.vma) of the SCMP and import it to the HCI platform.



3. After the import is complete, click **Go to Virtual Machine** to edit its hardware configuration.

- The CPU and memory will be 16 cores, 32GB, which is not required to make changes.
- Add data/storage disks to the server as needed (not required for point-to-point migration).
- Configure the NIC for the server as needed and configure the first NIC to connect to the physical outlet.

- There are two NICs by default. If there is no need for multiple NICs, delete the second one.



4. Click **OK** to finish editing the virtual machine.

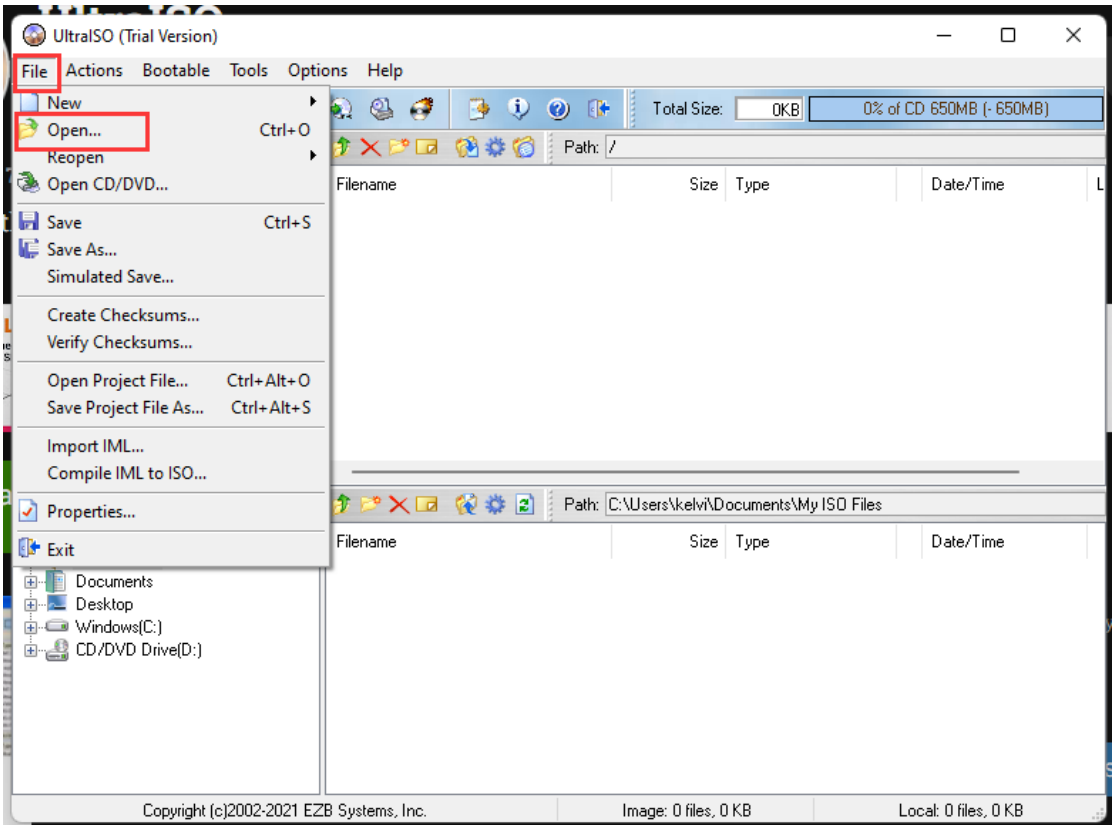
3.3.2 USB Flash Drive Burning Installation

3.3.2.1 Precautions

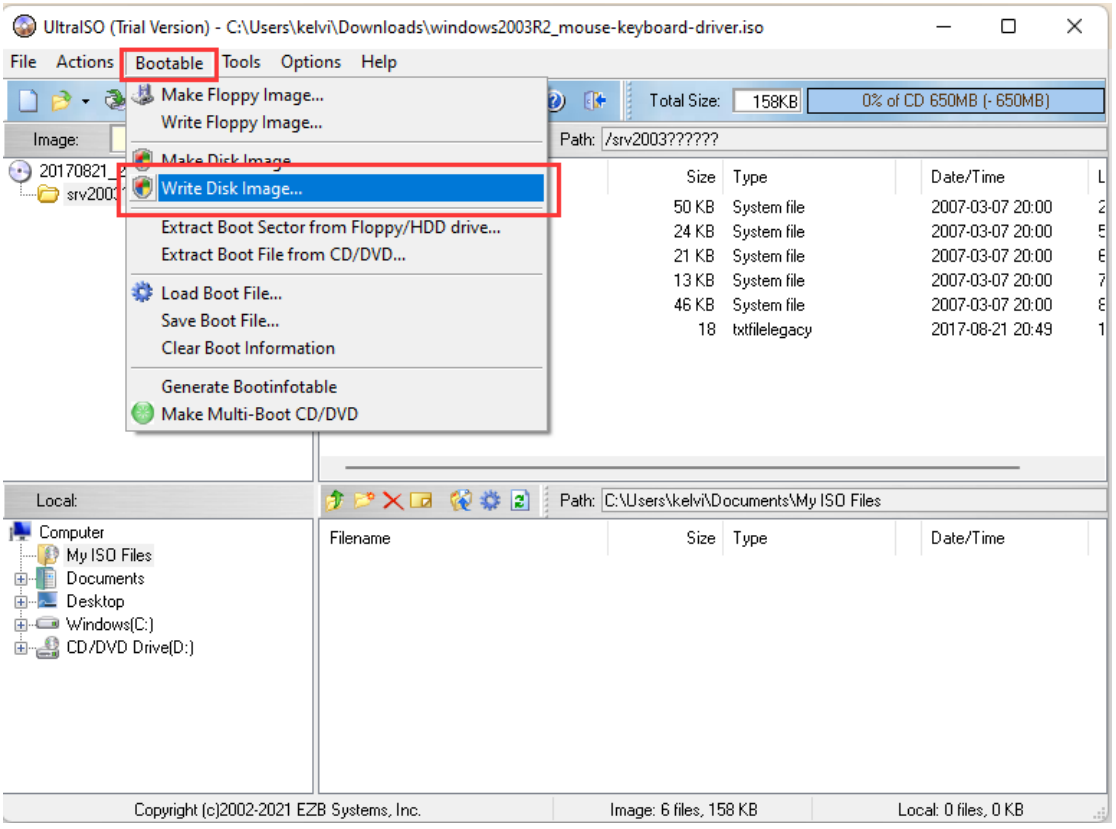
5. Please try to use the latest version of UltraISO.
6. USB-HDD or USB-HDD+ can be used as the writing format of the USB flash drive. Check the **Verify** checkbox for the burning result.
7. The total space of the USB flash drive must be larger than that of the ISO file.
8. The server configuration needs to meet the requirements in **chapter 3.2 Hardware Specification Requirements** of this manual.

3.3.2.2 Steps

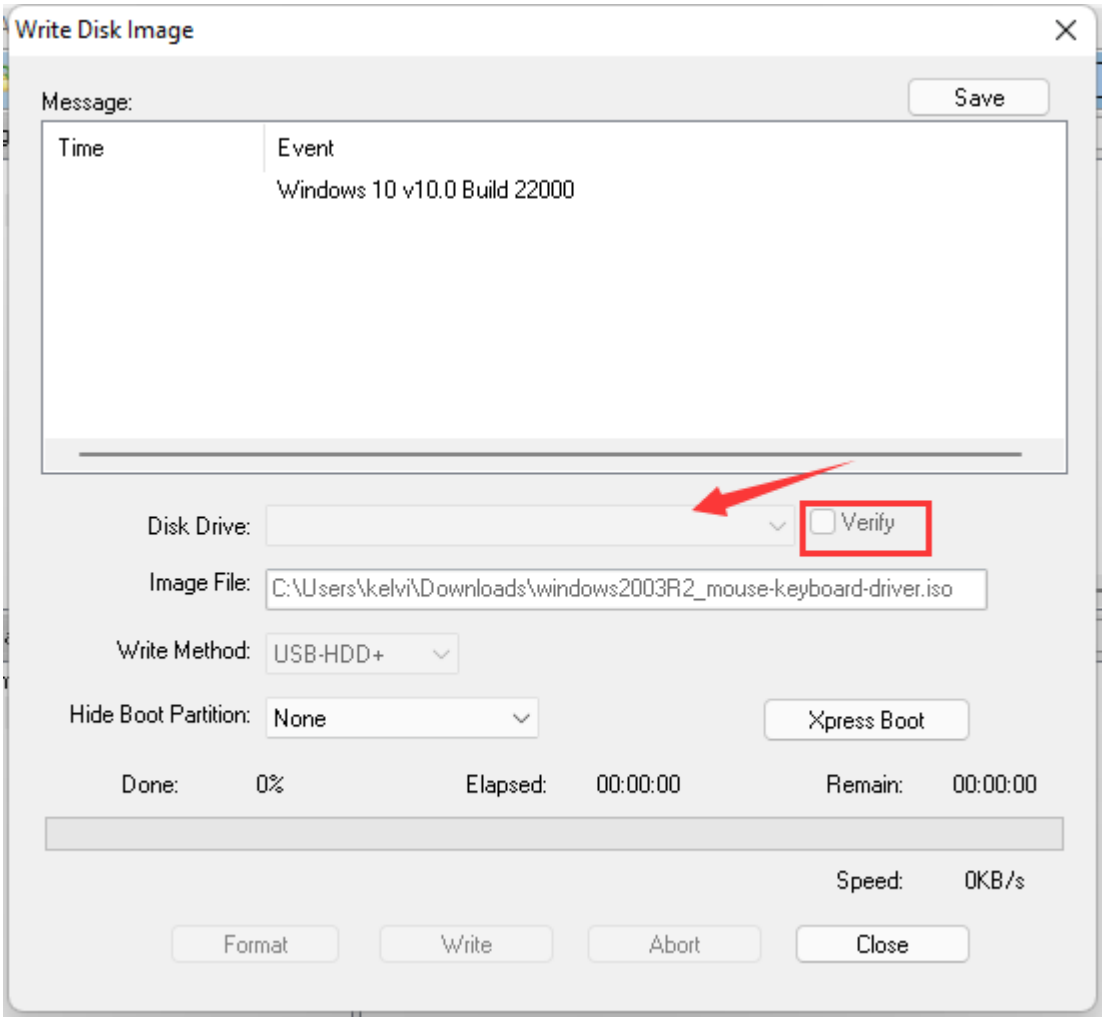
Step 1. First, insert the USB flash drive into the PC, then open the UltraISO software. Select **File** > **Open**, and load the SCMP iso file to be burned.



Step 2. Then click **Bootable** > **Write Disk Image**, and click **Write** where other options leave defaults. When finished, close the burning software and remove the USB flash drive.

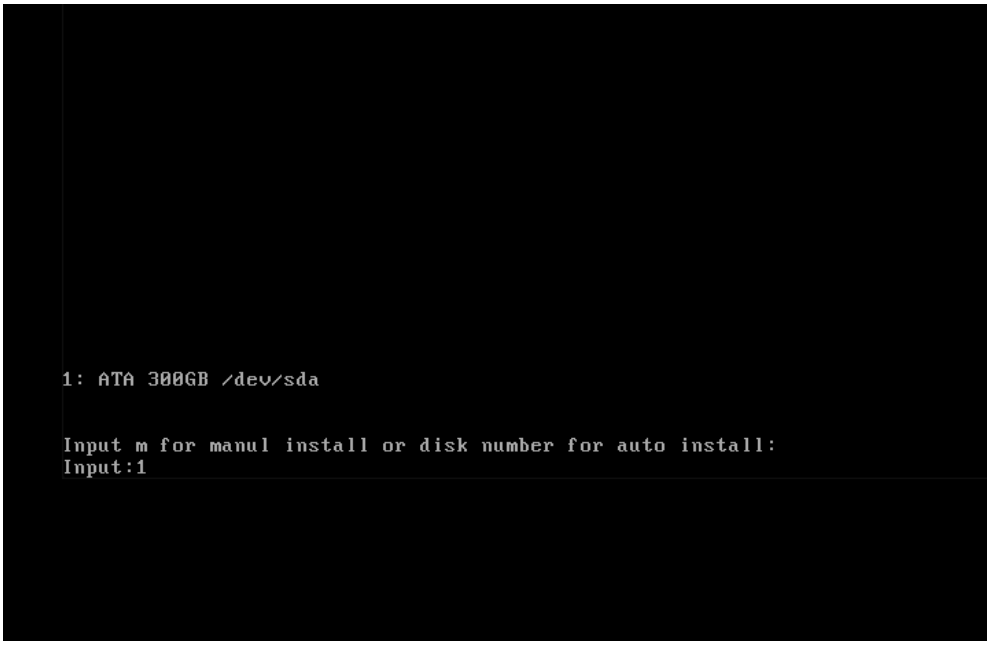


Step 3. The writing destination is a USB drive or CD. Make sure to check the **Verify** checkbox. Then, select the writing method (usually USB-HDD+) according to the USB boot type supported by the server.

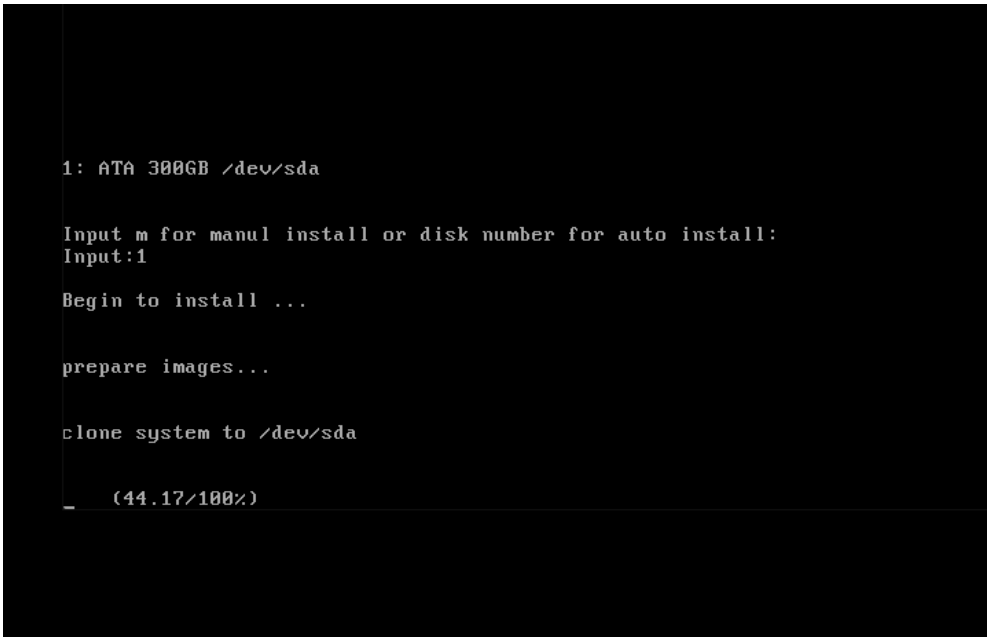


Step 4. Insert the USB flash drive into the third-party server, and set the BIOS to boot from the USB flash drive.

Step 5. Enter the disk for installing the platform. The following figure is an example, select the first 300G disk as the system disk, enter 1, and press Enter.



Step 6. The system will automatically perform the installation.



3.4 Platform Configuration

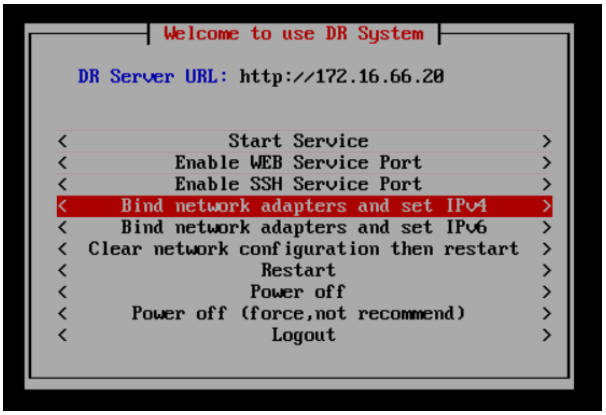
3.4.1 Network Settings

1. After the deployment is complete, you will see the **Welcome to use DR System** interface on the server console.

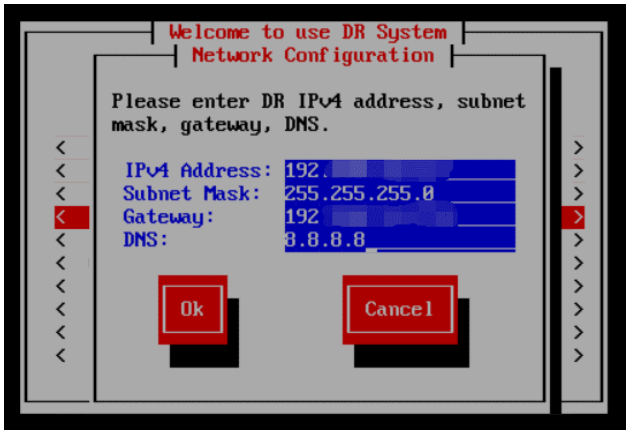
2. Enter the default password **123456** to enter the basic information configuration interface.
3. Enter the platform configuration interface. The following configuration items will be shown. Select the fourth option for IP configuration.

Configuration instructions:

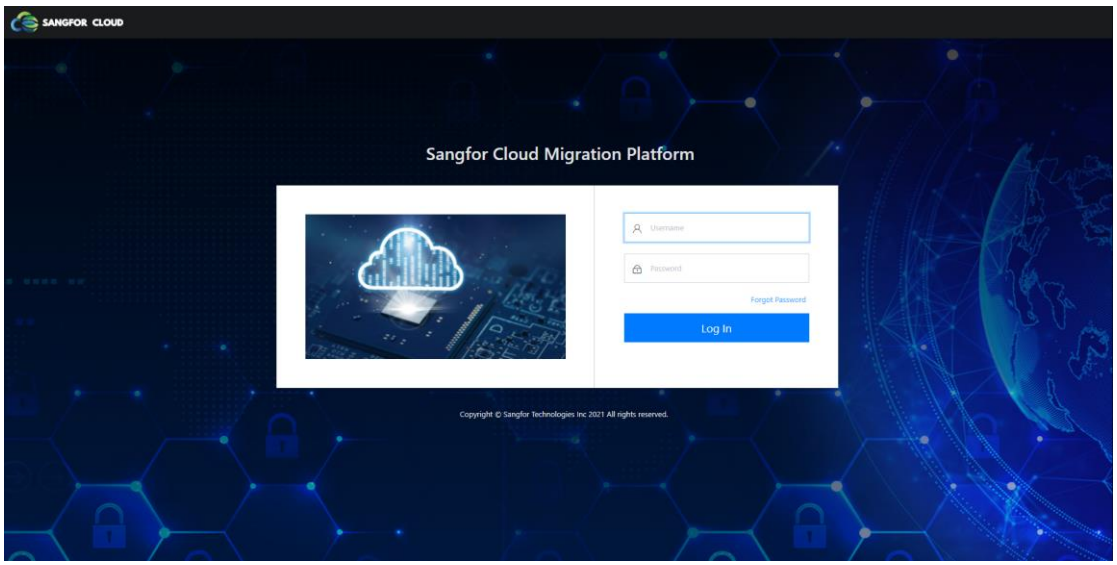
- **Start Service**: Start all services of the migration platform.
- **Enable WEB Service Port**: Enable WEB Service Port.
- **Enable SSH Service Port**: Enable SSH port.
- **Bind network adapters and set IPv4**: Configure IPv4 network adapter address.
- **Bind network adapters and set IPv6**: Configure IPv6 network adapter address.
- **Clear network configuration, then restart**: Clear existing network configuration and restart.
- **Restart**: Restart the server.
- **Power off**: Turn off the server.
- **Power off (force, not recommend)**: Force the server to shut down.
- **Logout**: log out.



4. Select the **Bind network adapters and set IPv4** to enter the IP configuration interface. Enter the planned IP address, subnet mask, gateway, and DNS.



5. After the configuration is complete, use the browser to access the SCMP through **https://ConfigureIP** to enter the management interface. The initial username/password is **admin/123456**. After successfully logging in for the first time, the password will be required to be changed.



3.4.2 Mail Server Settings (Optional)

Function Description:

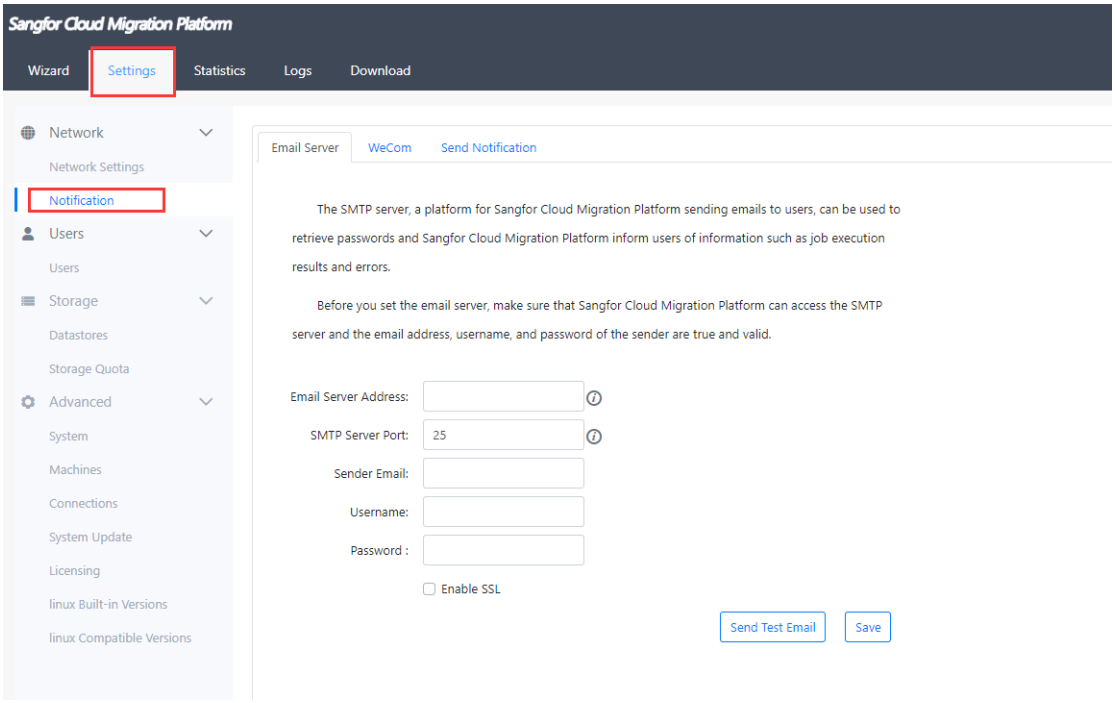
The mail server is used to send notification/warning/error information emails to inform the administrator of the real-time working status of the Sangfor Cloud Migration Platform. Besides, the SMTP server will be used to send a new password when creating a new administrator user and to retrieve the password by sending an email to the user mailbox when the password is lost/forgotten.

3.4.2.1 Precautions

The Sangfor Cloud Migration Platform needs to be able to communicate with the configured mail server normally. Otherwise, it will not be able to send the corresponding mail.

3.4.2.2 Steps

Step 1. Log in to the SCMP management console with an admin account and navigate to the **Settings** > **Notification** page to configure the email server address, SMTP server port, sender email, username, and password. After completing the settings, click **Send Test Email** to verify.



- **Email server address:** the server address where the sender's mailbox is located. Example: smtp.gmail.com
- **SMTP server port**: By default, the port of SMTP is 25. Adjust it according to your needs.
- **Sender email**: Fill in the email address of the role of sending the alarm.
- **Username**: Fill in the username of the mailbox sending the alarm.
- **Password**: Fill in the password of the mailbox that sends the alarm.

3.4.3 Create User

Function Description

The system defaults only have the admin user, which is the Super Admin. The following functions are not available to the admin account: agent download, source backup, migration, etc. To use the mentioned functions, you need to create a system administrator user and use this user to log in to the SCMP.

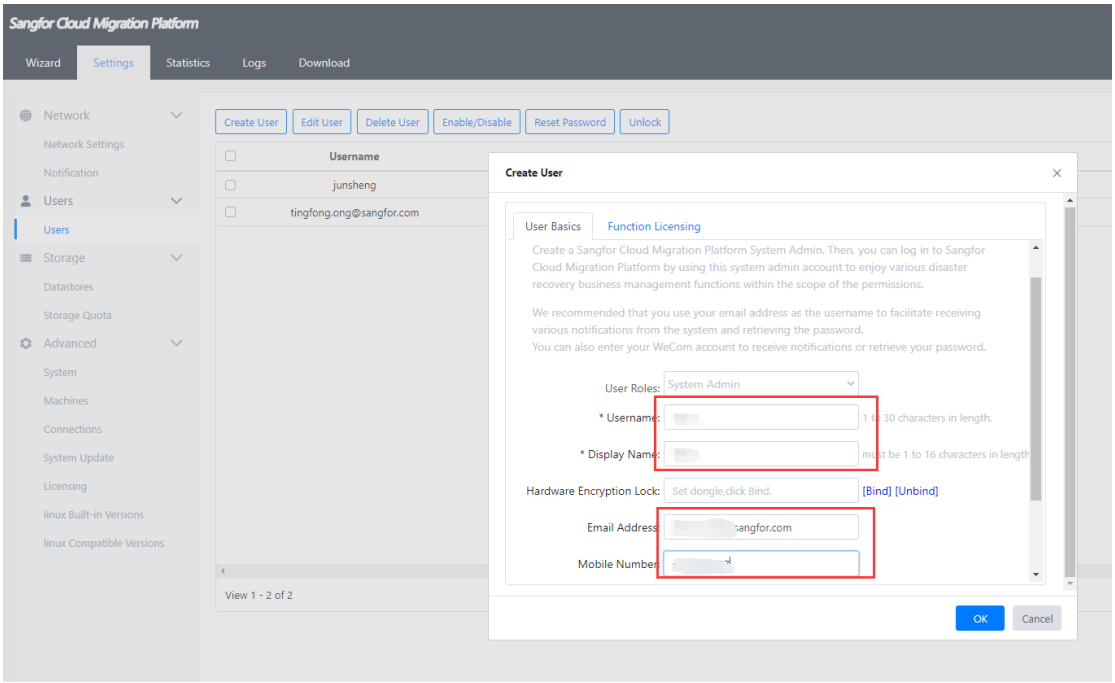
3.4.3.1 Precautions

1. The migration cannot be completed using the admin account. Only the system administrator can initiate the migration function.

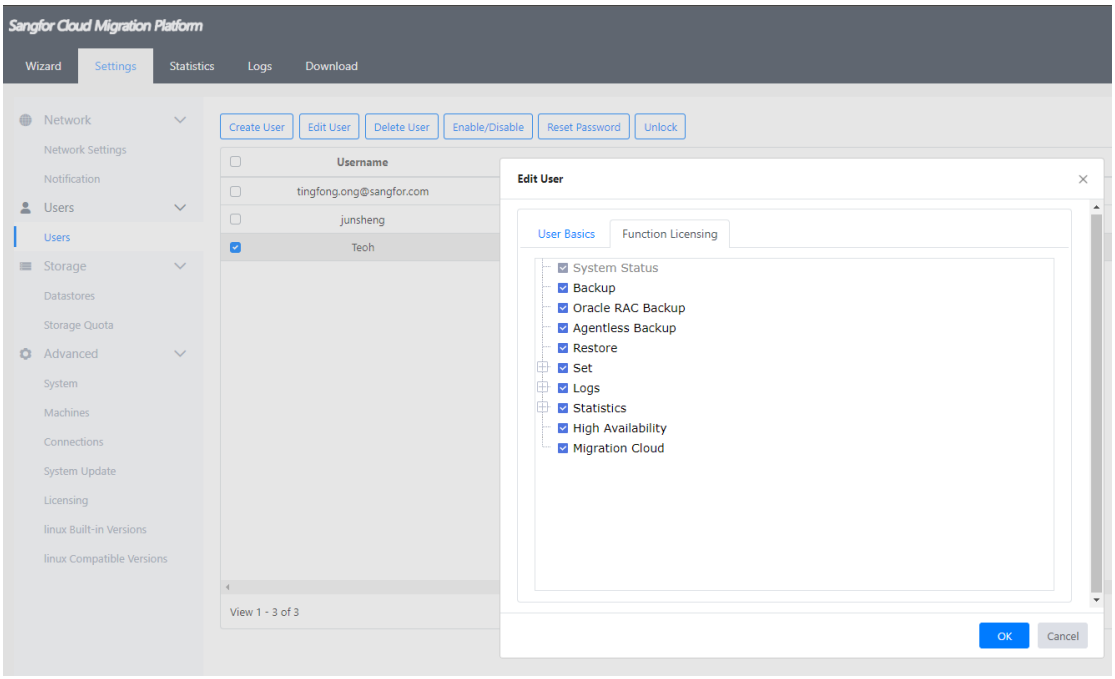
2. If the platform is configured with a mail server, you need to send an email to the user's mailbox to confirm the user's password, so it is recommended to use the email address as the username.

3.4.3.2 Steps

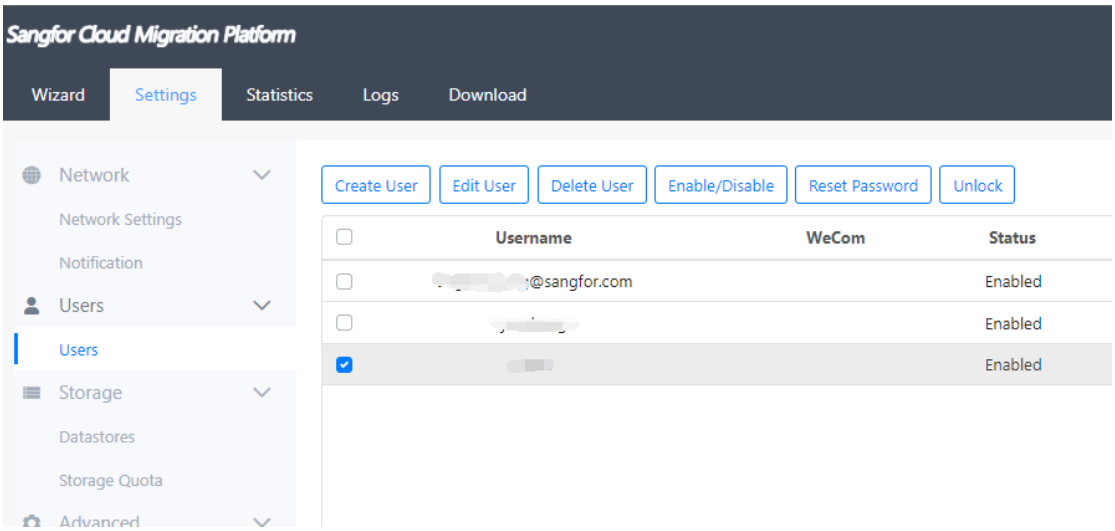
Step 1. Log in to the SCMP management console with an admin account and navigate to **Settings** > **Users** interface. Click **Create User** and enter the **Username** and **Display Name**. The default password for the newly created user is **123456**. **Email Address** and **Mobile Number** are optional, whereas the **Email Address** will be used for password confirmation and alert recipients.



Step 2. Click **Function Licensing** to configure the function permissions for users (by default, all will be selected).



Step 3. Click **OK** and the user will be created.



3.4.4 Add Storage and Storage Quota Allocation (Optional)

Function Description

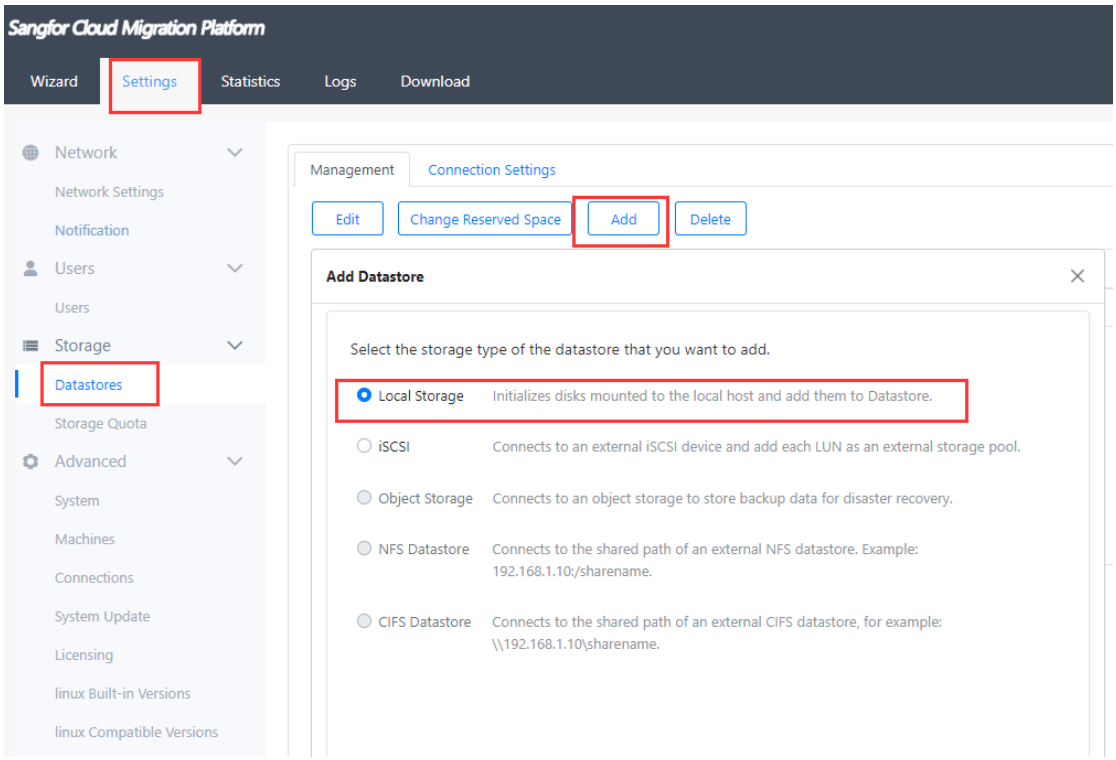
When using the HA backup migration and backup migration modes, you need to allocate storage resources for the newly created system administrator to store backup data.

3.4.4.1 Precautions

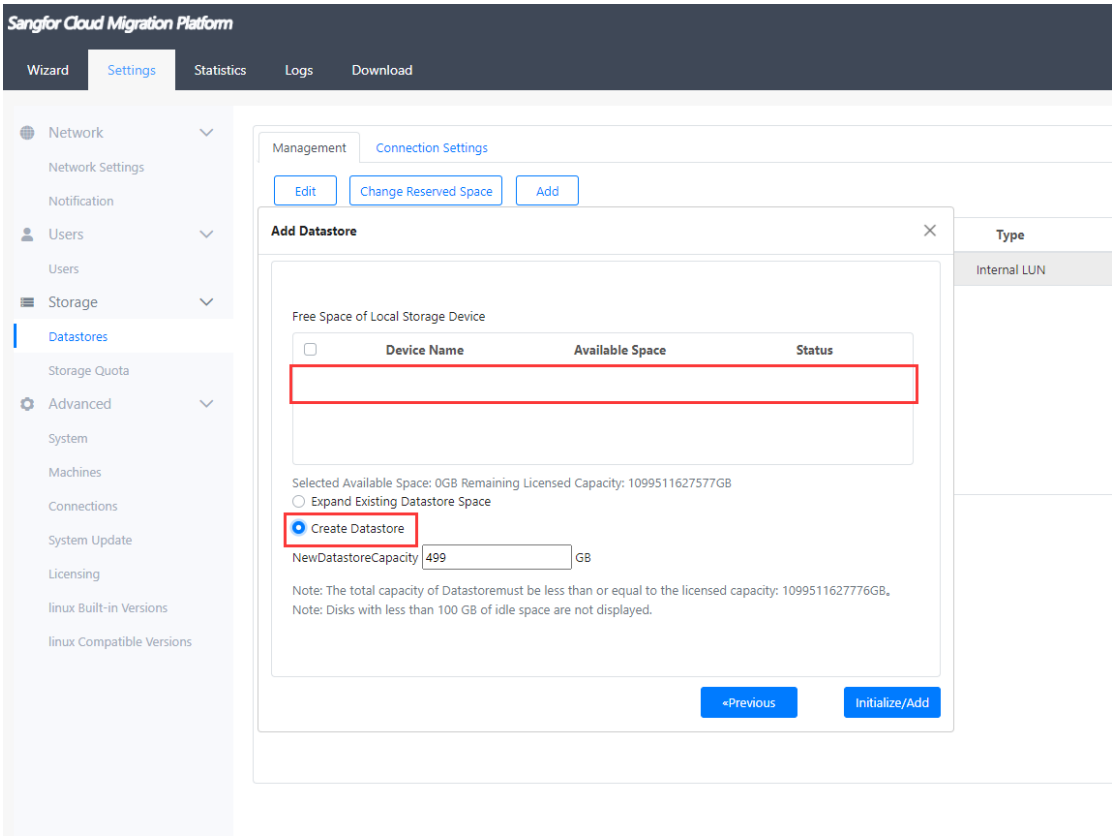
1. There is no need to allocate storage resources to the system administrator for the point-to-point migration.
2. Currently only supports adding local storage and iSCSI storage.

3.4.4.2 Steps

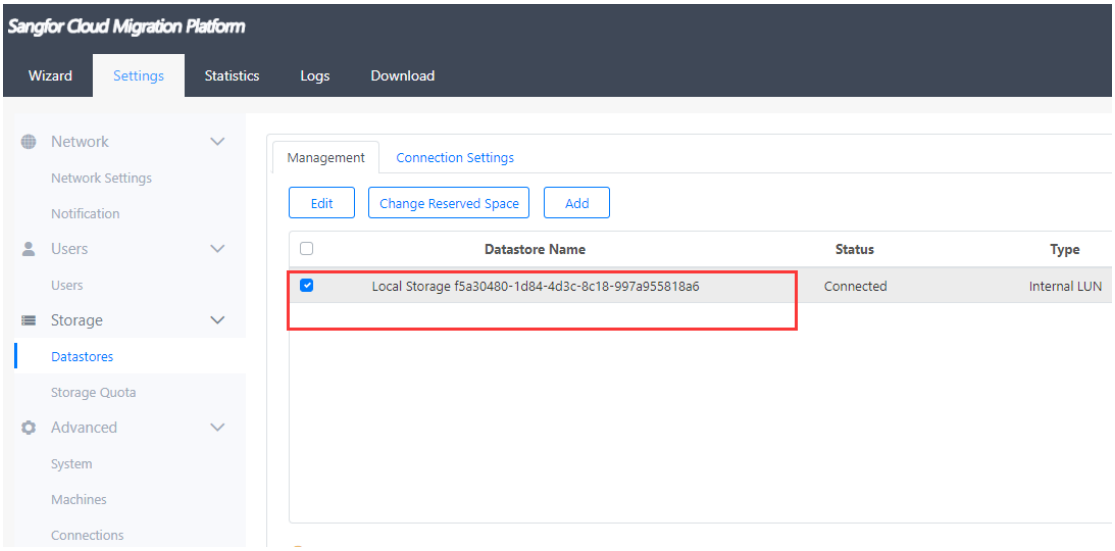
Step 1. Login to the SCMP management console with the admin account. Navigate to **Settings** > **Datastores** and click on the **Add** button to add the data disk as local storage.



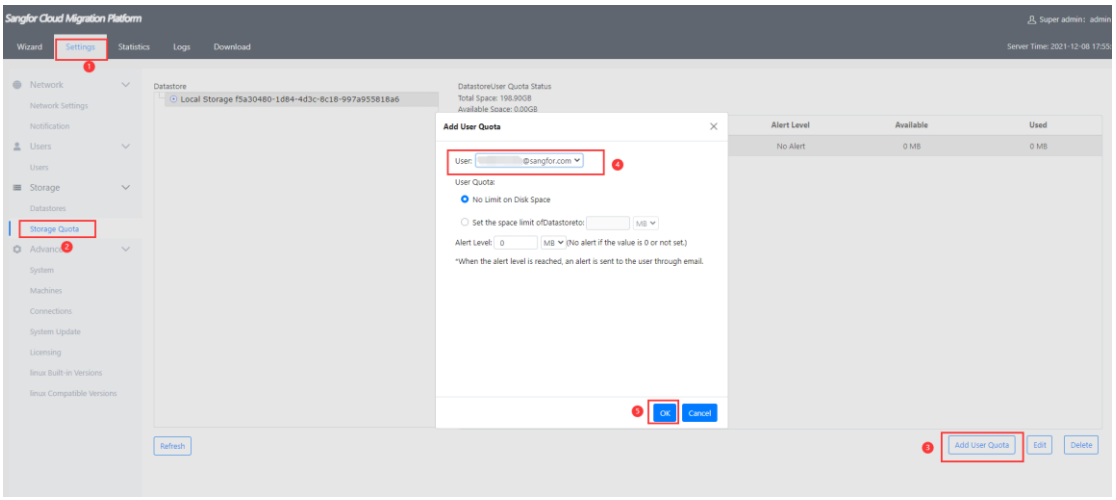
Step 2. Select **Local storage** as the storage type and click **Create Datastore** in the lower right corner.



Step 3. The local storage has been added successfully.



Step 4. Navigate to **Settings** > **Storage Quota** interface and click **Add User Quota** to add storage quotas for the created system administrators, which can be configured according to requirements.



3.4.5 Connect to the Destination HCI Platform

Function Description

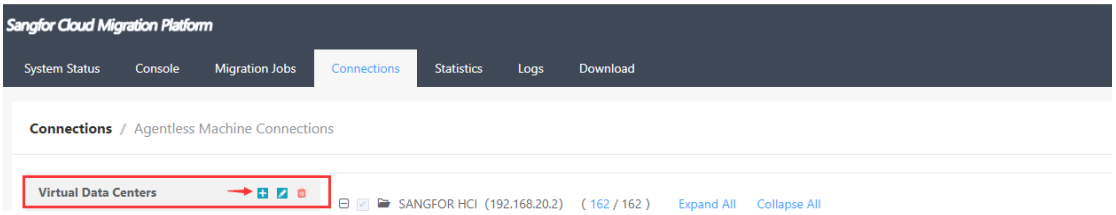
Use the Sangfor Cloud Migration Platform to connect to the Sangfor HCI. A new virtual machine will be automatically created to complete the migration when migrating to the destination machine.

3.4.5.1 Precautions

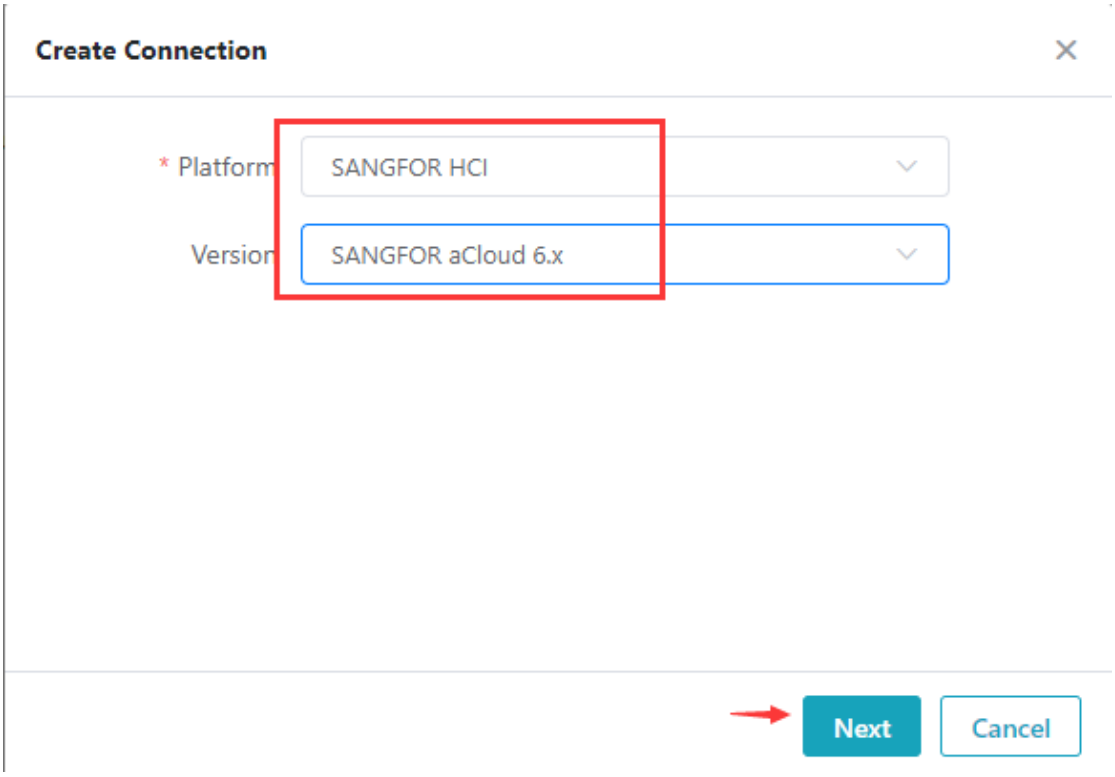
1. This function requires a complete match with the HCI version number. Please refer to the **SCMPCompatibilityList-20211214**.
2. Currently only supports virtual data center connections with HCI6.0.0R5, HCI 6.3.0, and later versions for automatic destination VM creation. For previous versions of HCI, please use the "**bare metal restore**" boot medium method to construct the destination machine.

3.4.5.2 Steps

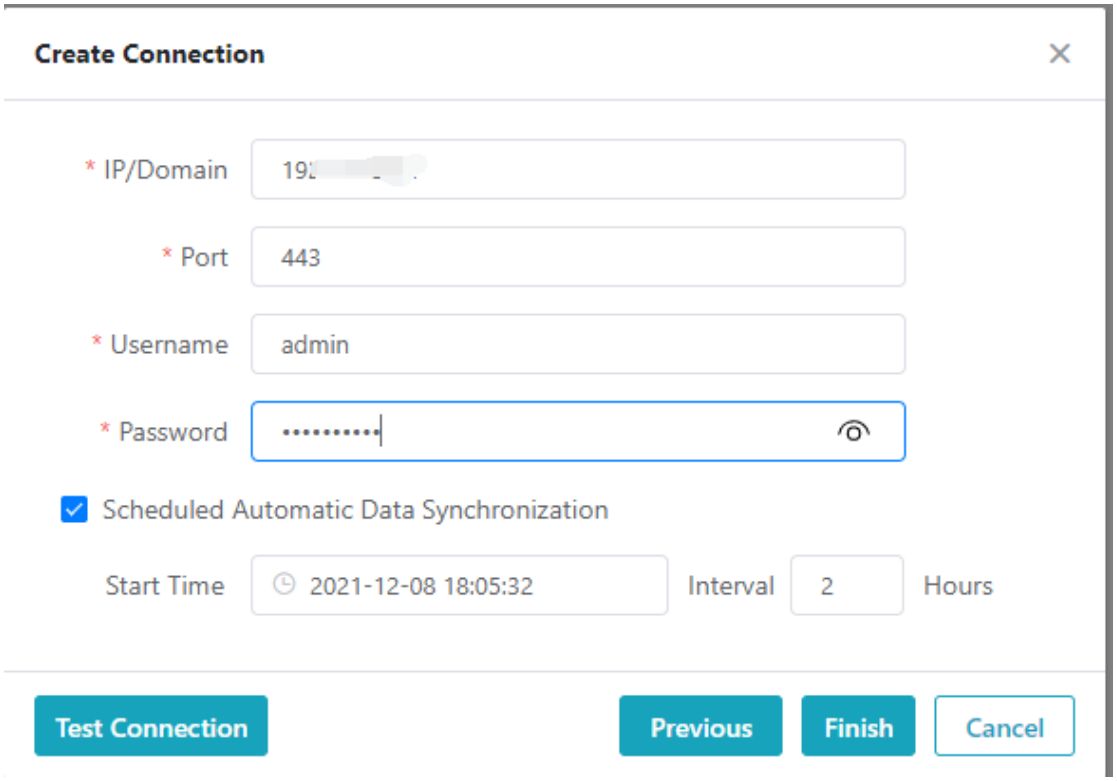
Step 1. Login to the SCMP management console with the newly created user account. Navigate to **Connections** and click the **+** button on the right side of **Virtual Data Centers**.



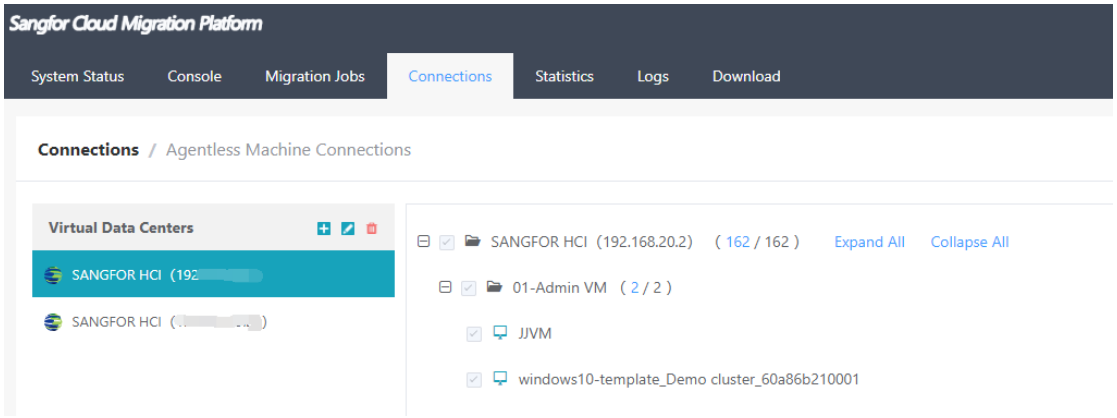
Step 2. Select the SANGFOR HCI for Platform and the corresponding version.



Step 3. In the **Create Connection** windows, enter the cluster IP address/Domain, Port, Username, and Password of the SANGFOR HCI. The **Scheduled Automatic Data Synchronization** will sync the HCI virtual machine group list periodically.

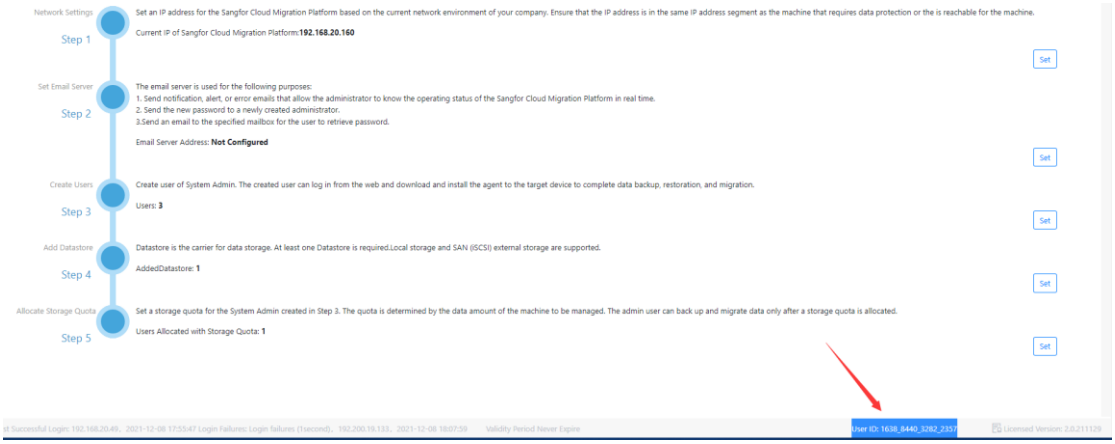


Step 4. Click **Test Connection** to verify the connection to the HCI. Click **Finish** to add the virtual data centers after the connection test is successful.



3.5 Licensing

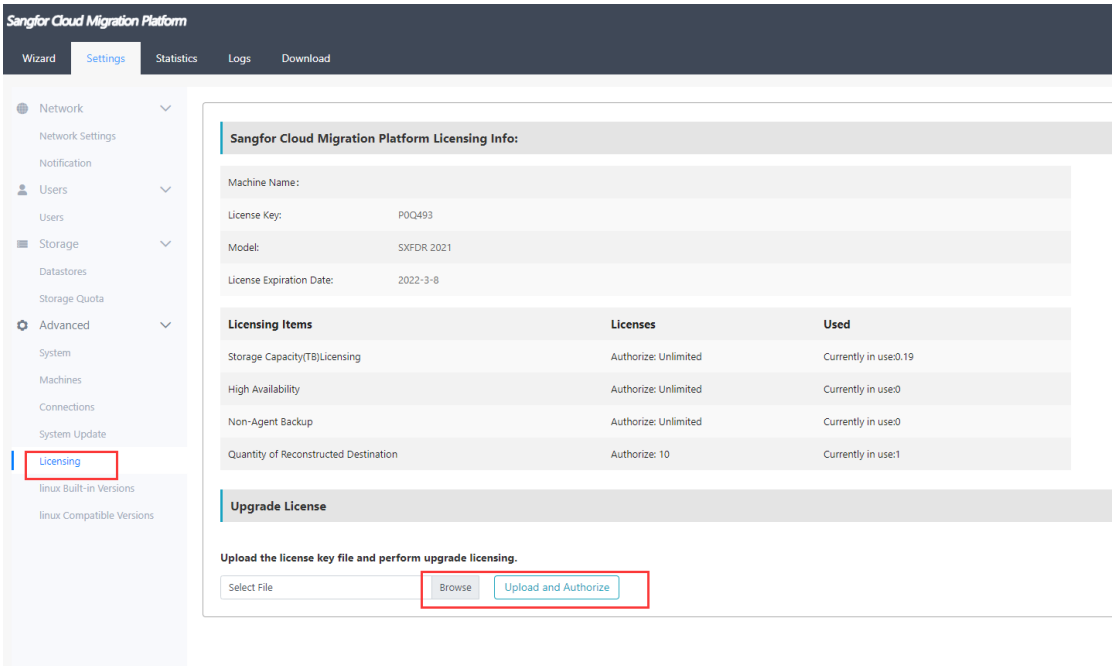
1. Login to the SCMP management console with admin and search for **User ID** at the bottom of the homepage.



2. Send the user ID and the authorized Key ID of Sangfor HCI to Sangfor Technical Support to obtain the licensing file. After obtaining the licensing file, navigate to **Settings** > **Licensing** and upload the licensing file to the platform. The licensing will be successful after uploading the licensing file.

NOTE

1. For virtual key licensing, you are only required to provide the user ID for licensing.
2. Full user IDs must be provided during the authorization file application, including underscores. For example, the user ID in step 1 is 1638_8440_3282_2357.

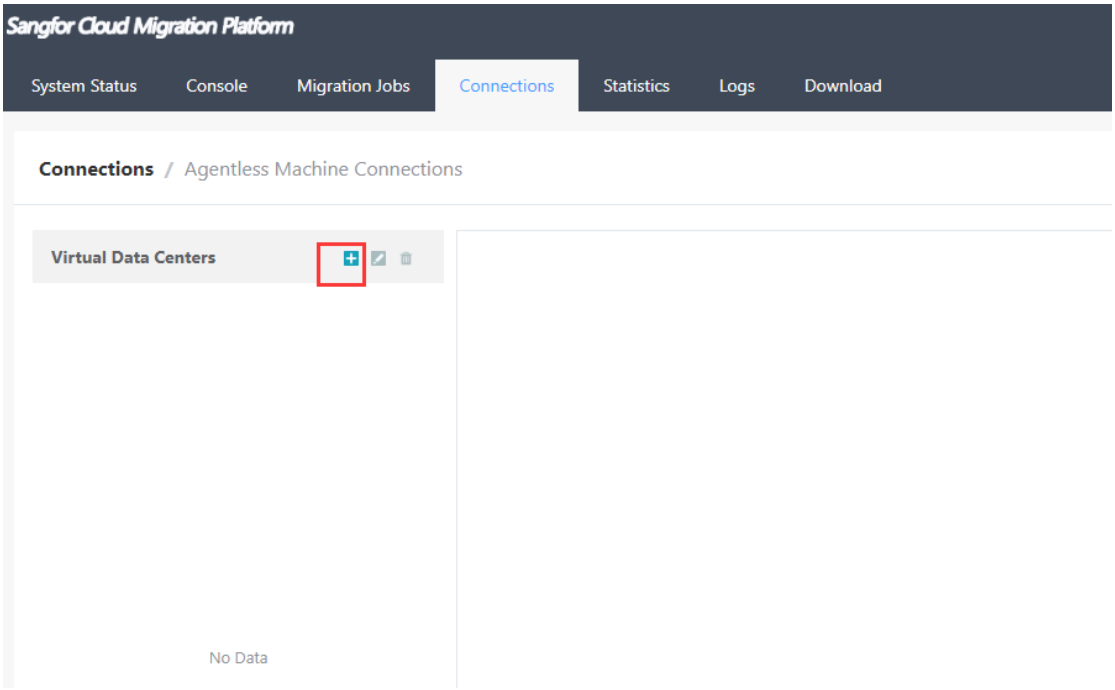


4 Migration Preparation

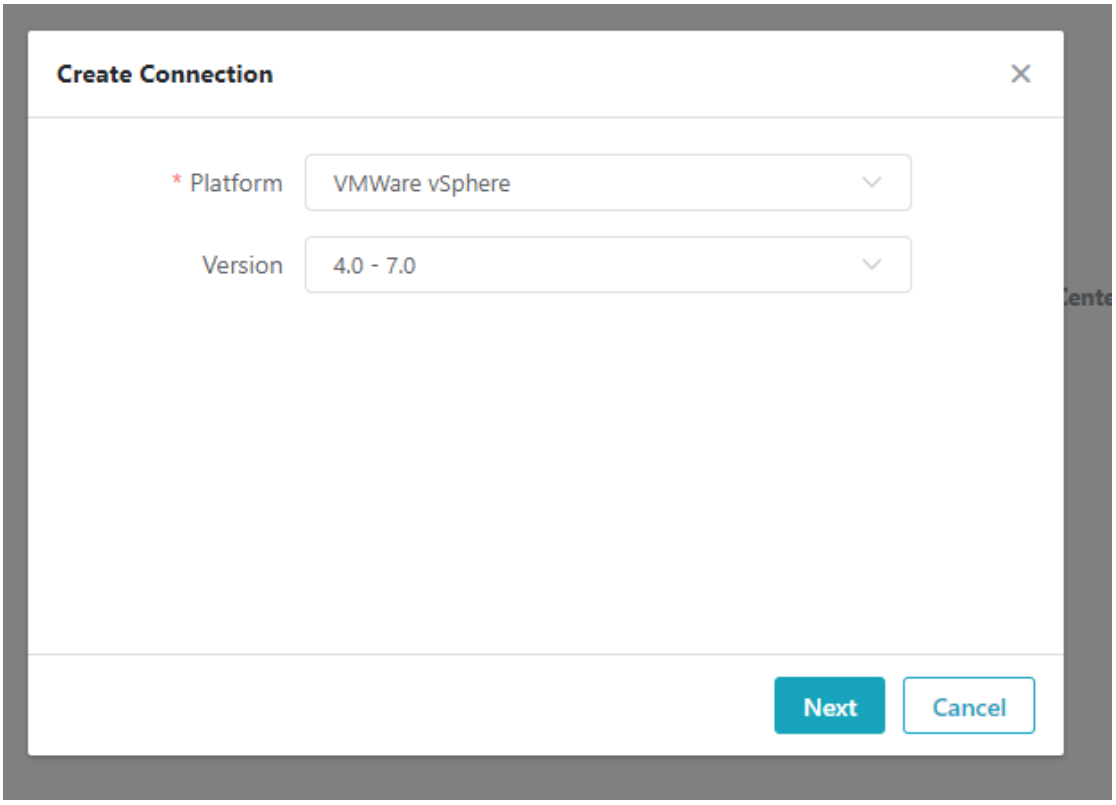
4.1 Migration Source Preparation

4.1.1 Preparation for VMware Platform Migration (Agentless)

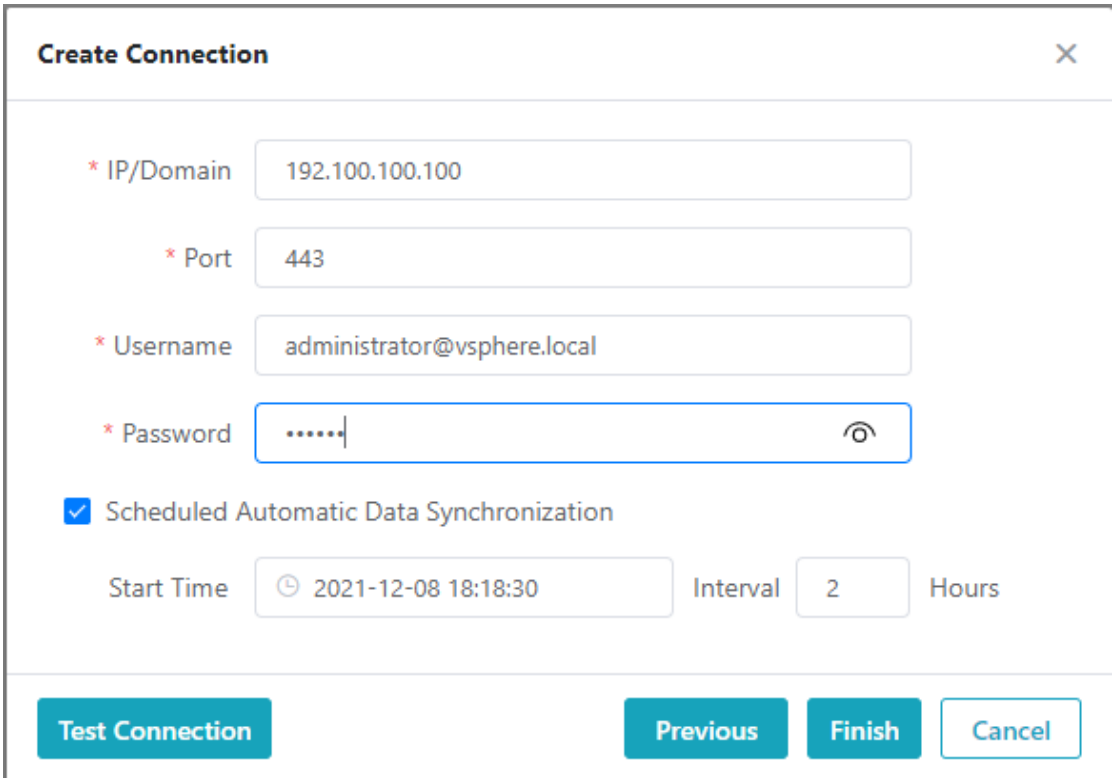
Step 1. Login to the SCMP management console with the newly created user account. Navigate to [**Connections**] and click the "**+**" next to the [**Virtual Data Centers**].



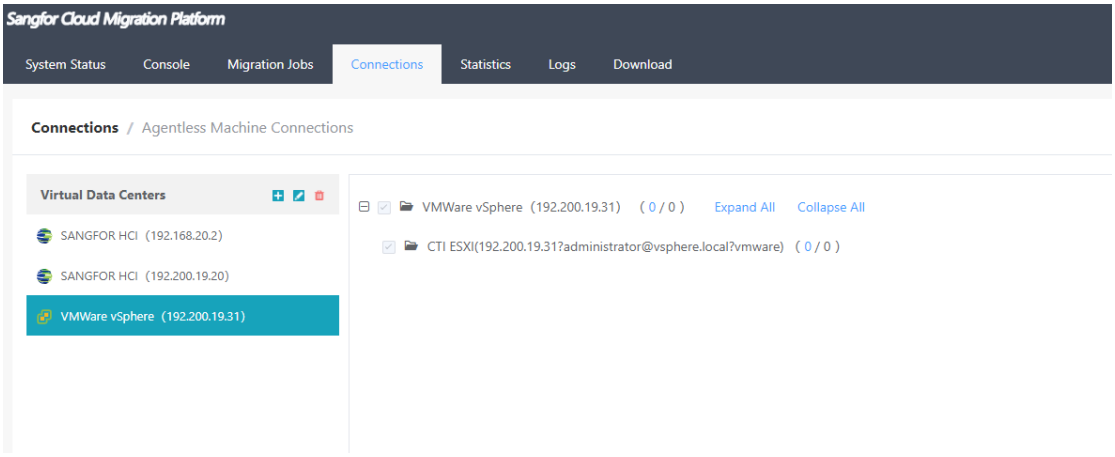
Step 2. Select the "**VMware vSphere**" platform and the corresponding version.



Step 3. Enter the vCenter or ESXi IP address/domain name, Port, Username, and Password information. Configure the "**Scheduled Automatic Data Synchronization**" option for periodic VM data synchronization.



Step 4. Click [**Test Connection**] to verify the connection to the HCI. Click [**Finish**] to add the virtual data centers after the connection test is successful.



4.1.2 Preparation for Windows System Migration

4.1.2.1 Turn Off Firewall and Anti-virus Software

System migration needs to turn off the operating system firewall and the anti-virus software. If anti-virus software is installed on the source site, data reading and writing on the source side may be protected, resulting in the installation failing. It is recommended to turn off the anti-virus software during migration.

If the firewall is unable to be turned off, you need to configure the firewall to allow the required ports to pass through.

4.1.2.2 Install the Migration Agent

Function Description

Install the migration agent at the source machine for communication. The SCMP will complete the information collection of the operating system and issue migration instructions through the agent.

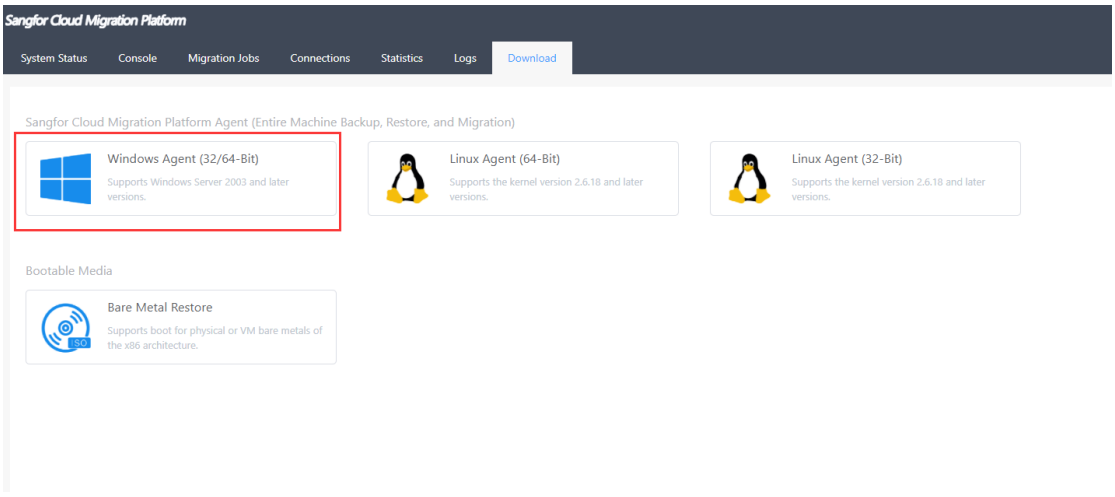
4.1.2.2.1 Precautions

1. Make sure the computer is able to run normally and the running memory is greater than 2G.

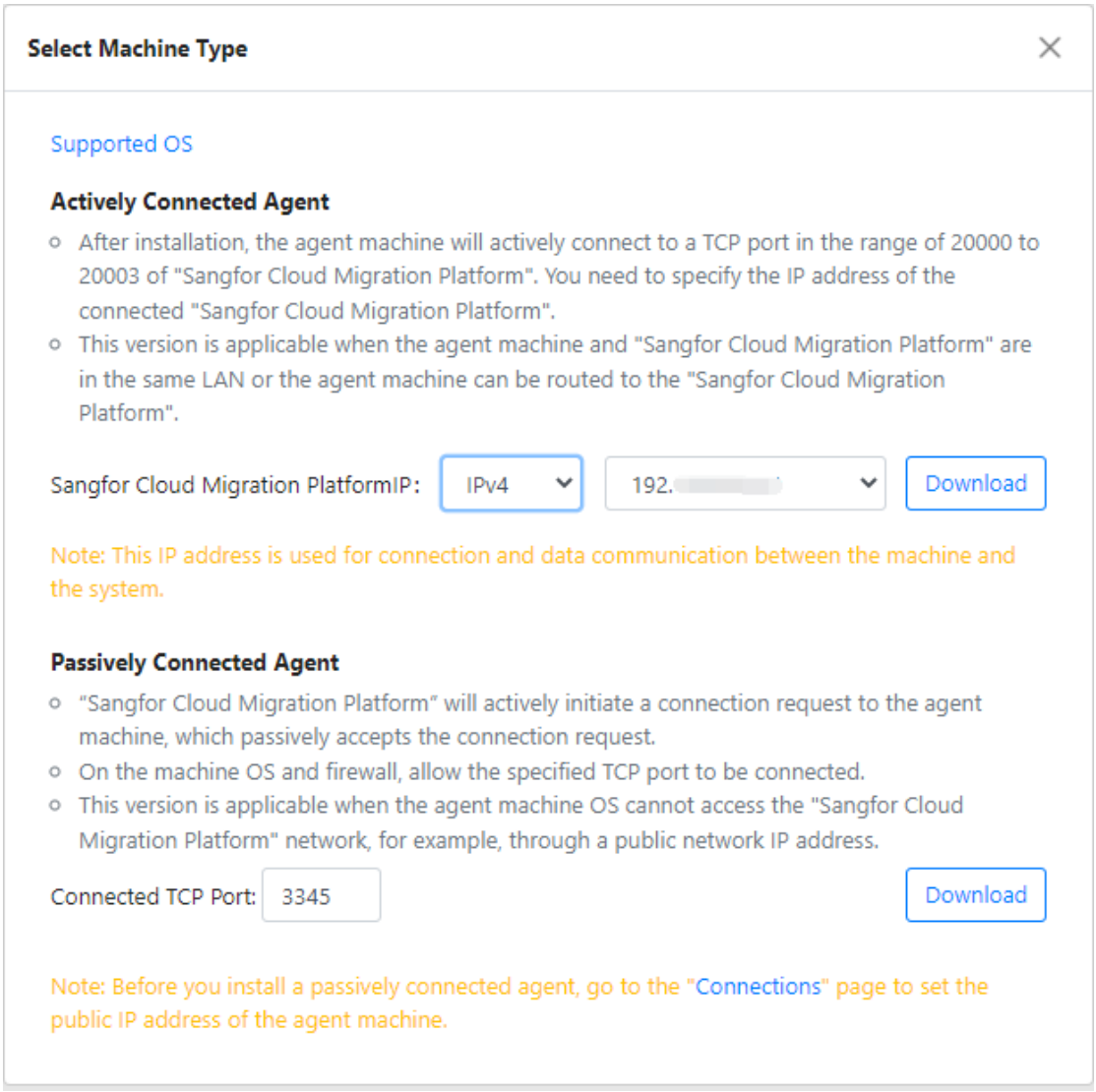
2. Ensure the selected source system is in the list of operating systems supported by the SCMP. For details, please refer to the **SCMPCompatibilityList-20211214**.
3. The MD5 value of the downloaded migration agent must be the same as the MD5 value displayed on the SCMP.
4. The agent is only available when login as a system administrator. The downloaded agent corresponds to the system administrator, where the agent downloaded through the system administrator account can only be issued migration/backup tasks by the respective administrator.
5. Ensure that the source machine can access the SCMP.
6. There are two types of agents in SCMP: **Actively Connected Agent** and **Passively Connected Agent**. When using **Actively Connected Agent**, the agent will initiate the connection from the source machine to the SCMP. For **Passively Connected Agent**, the agent will passively accept the connection initialization from the SCMP instead.

4.1.2.2.2 Steps

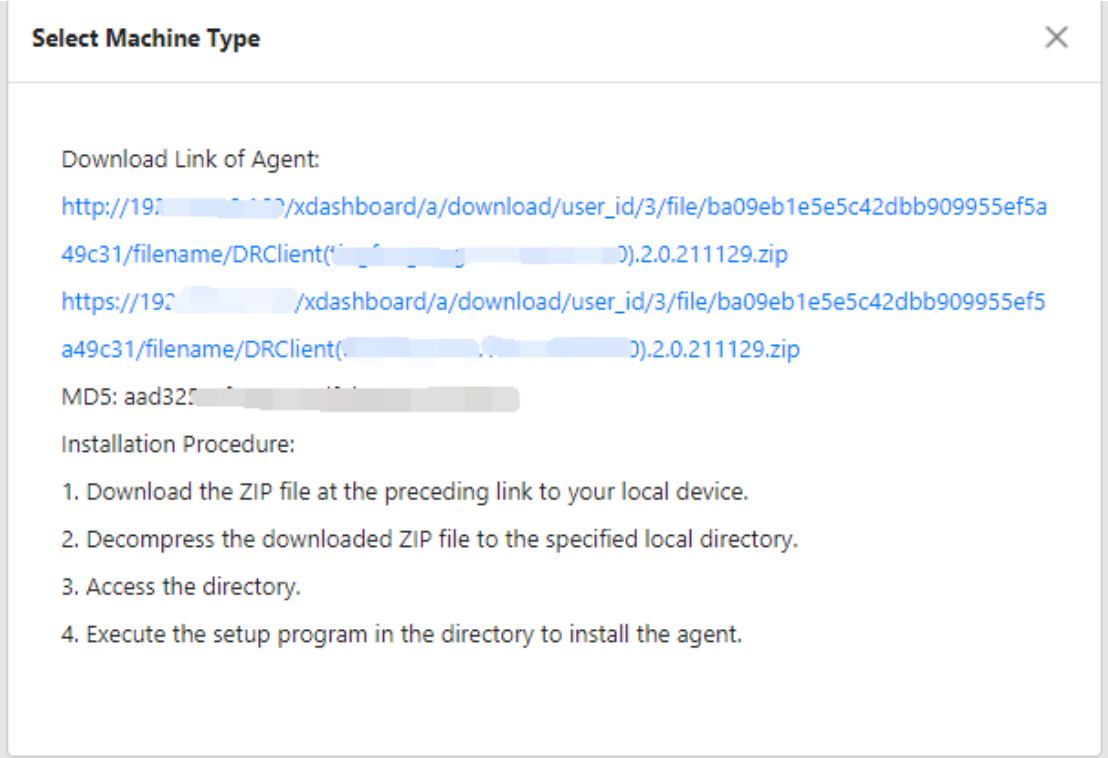
Step 1. Login to the SCMP with the newly created system administrator on the source Windows machine. Navigate to **Download** and click **Windows Agent(32/64-Bit)** to download.



Step 2. Select agent type. When the source system is in the NAT environment and unable to reach SCMP directly, select **Passively Connected Agent** for SCMP to initiate the connection to the source system.

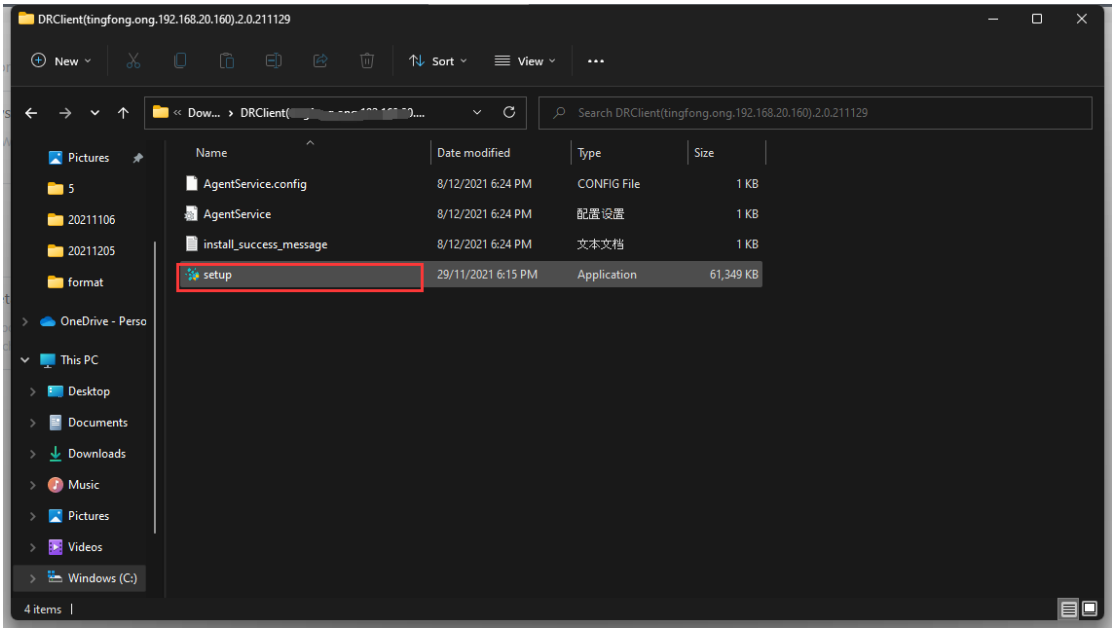


Step 3. Click on the download link to start the agent download.

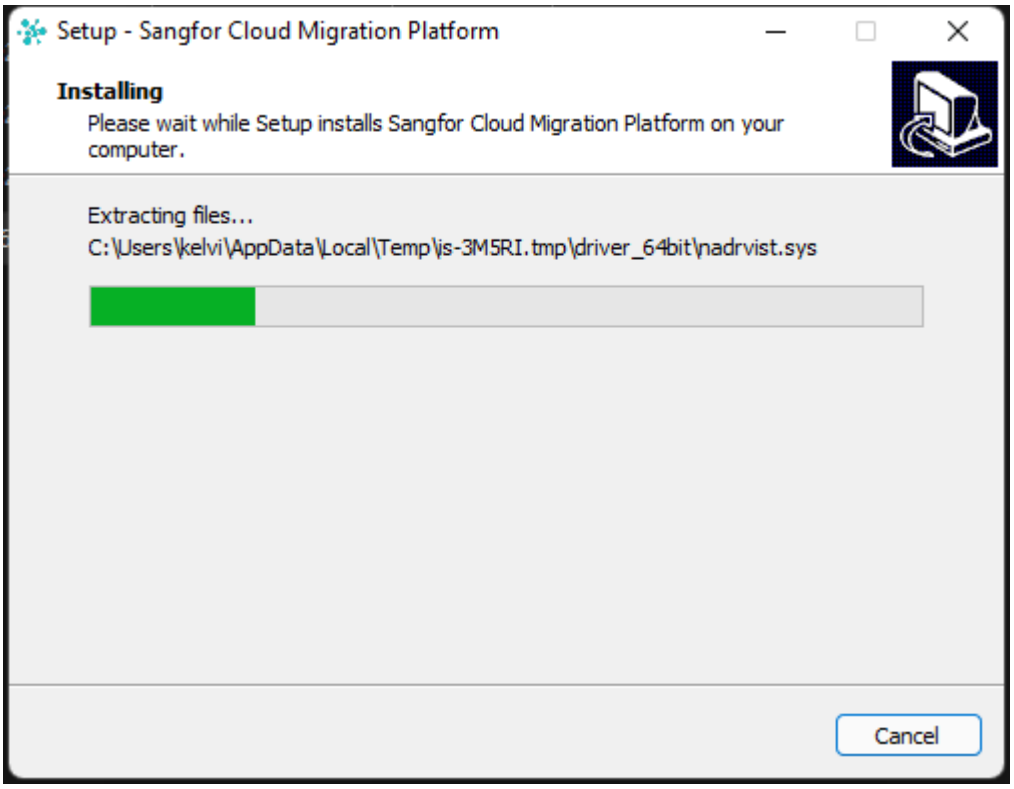


Step 4. After the download is complete, verify the MD5 value.

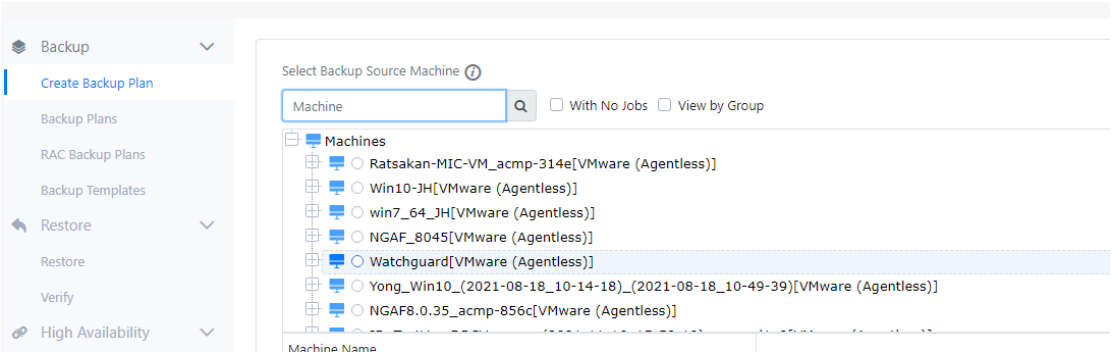
Step 5. Unzip it to the local folder, and install the application by double-clicking on the **setup** file.



Step 6. After the installation is completed, SCMP IP will then appear on the screen.



Step 7. The detailed information of this agent will be displayed in the SCMP console after login as the system administrator where the agent corresponded.



Step 8. The installation is complete.

4.1.3 Preparing for Linux System Migration

4.1.3.1 Turn Off The Firewall

The commands line for turning off the firewall in different Linux versions is as follows:

- SUSE series: **rcSuSEfirewall2 stop**.
- Ubuntu series: **ufw disable**.

- Red Hat\CentOS series: **service iptables stop** or **systemctl stop firewalld**.

4.1.3.2 Install The Migration Agent

Function Description

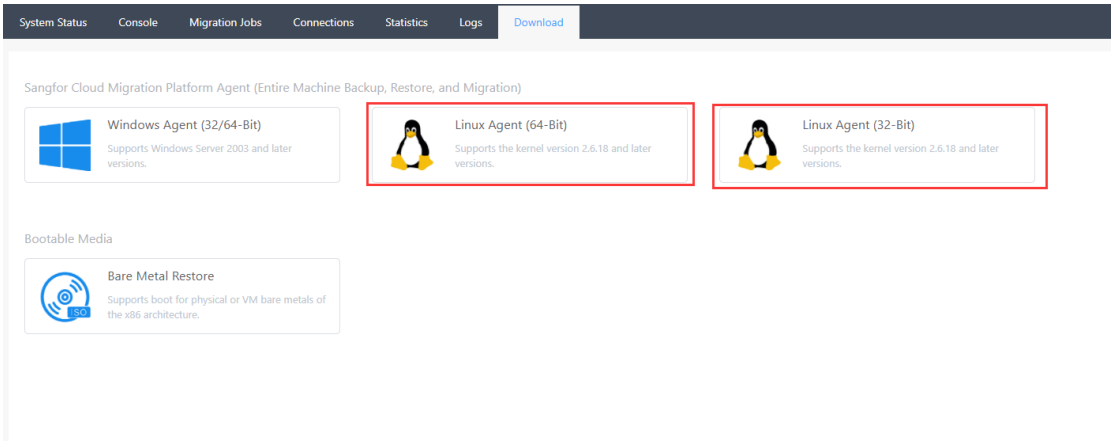
Install the migration agent at the source machine for communication. The SCMP will complete the information collection of the operating system and issue migration instructions through the agent.

4.1.3.2.1 Precautions

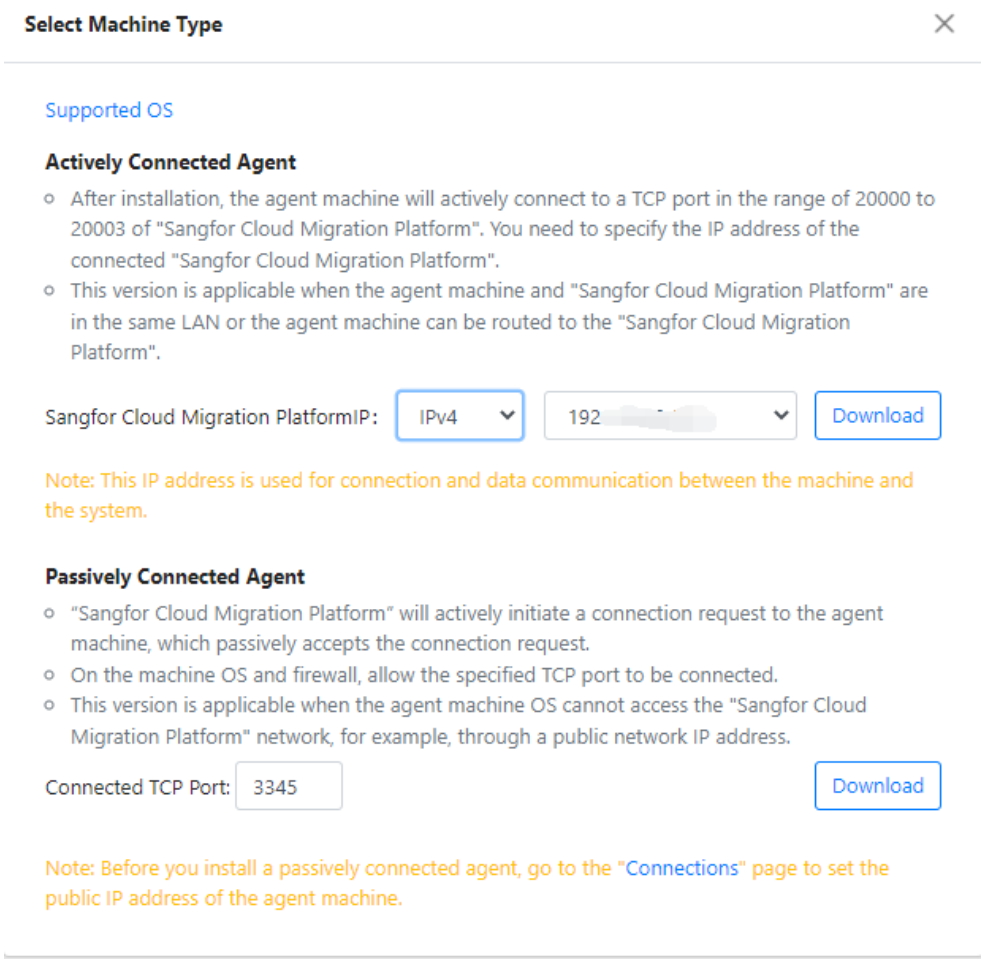
1. Make sure the computer is able to run normally and the running memory is greater than 2G.
2. Ensure the selected source system is in the list of operating systems supported by the SCMP. For details, please refer to the **SCMPCompatibilityList-20211214**.
3. The MD5 value of the downloaded migration agent must be the same as the MD5 value displayed on the SCMP.
4. The agent is only available when login as a system administrator. The downloaded agent corresponds to the system administrator, where the agent downloaded through the system administrator account can only be issued migration/backup tasks by the respective administrator.
5. Ensure that the source machine can access the SCMP.
6. There are two types of agents in SCMP: **Actively Connected Agent** and **Passively Connected Agent**. When using **Actively Connected Agent**, the agent will initiate the connection from the source machine to the SCMP. For **Passively Connected Agent**, SCMP will initiate the connection to the agent, and the source machine needs to allow the corresponding port in the firewall.
7. When using the **wget** command to access the HTTPS download link, it is required to add **--no-check-certificate** in the command. Otherwise, the execution will fail with a certification not trusted error.

4.1.3.2.2 Steps

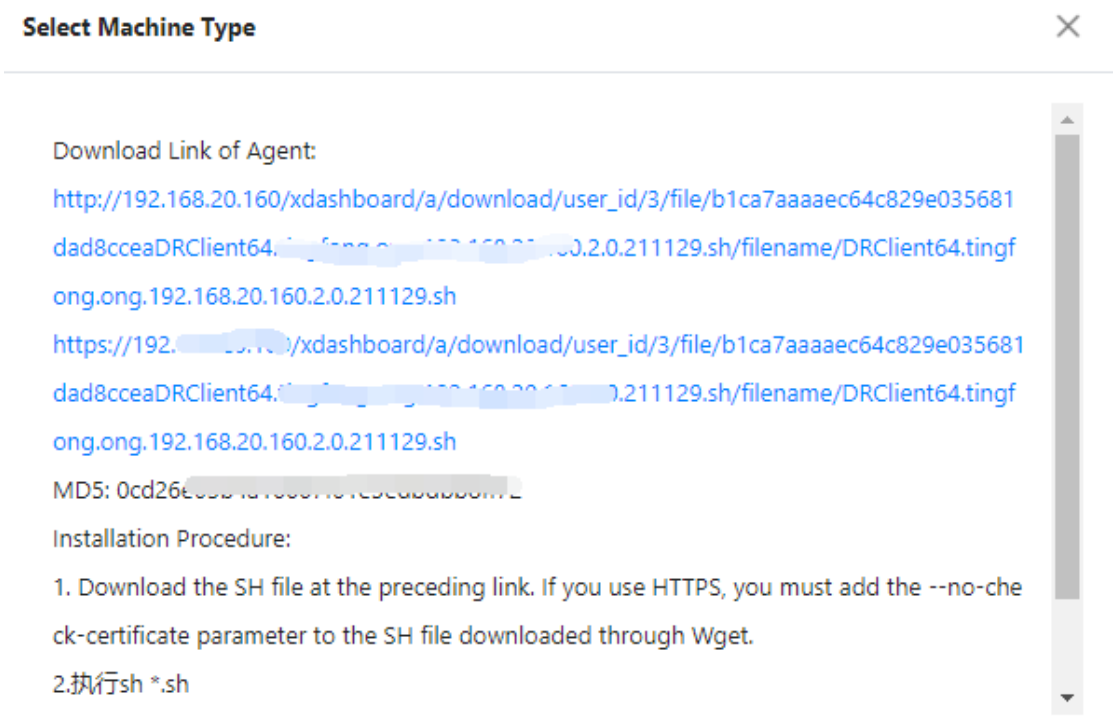
Step 1. Login to the SCMP with the newly created system administrator on any Windows system. Navigate to the **Download** page, and click **Linux Agent** to download. Select 64-bit or 32-bit based on the source machine.



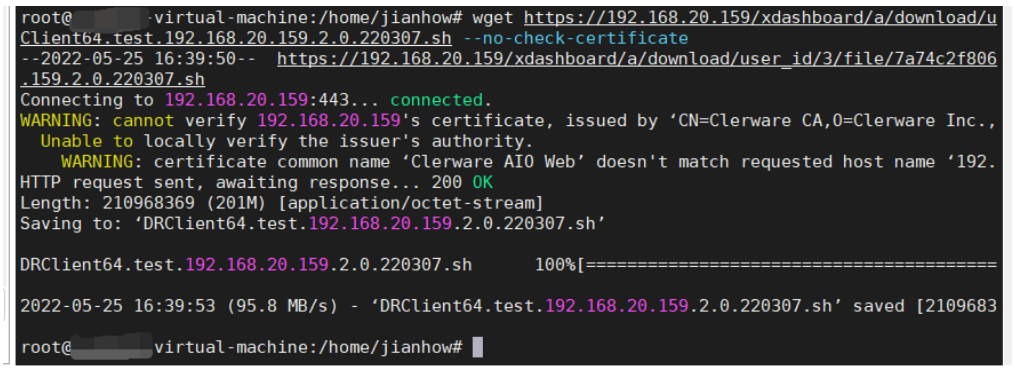
Step 2. Select agent type. If the source system can directly access the address of the SCMP, select **Actively Connected Agent**. When the source system is in the NAT environment and unable to reach SCMP directly, select **Passively Connected Agent** for SCMP to initiate the connection to the source system.



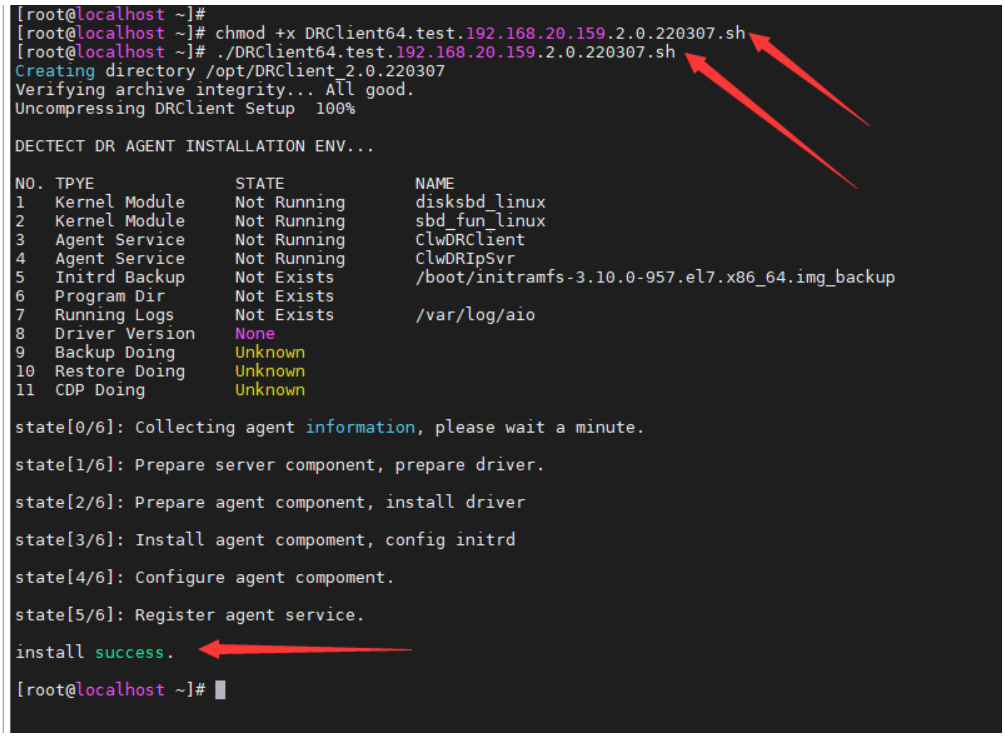
Step 3. Click **Download,** and the download link will appear.



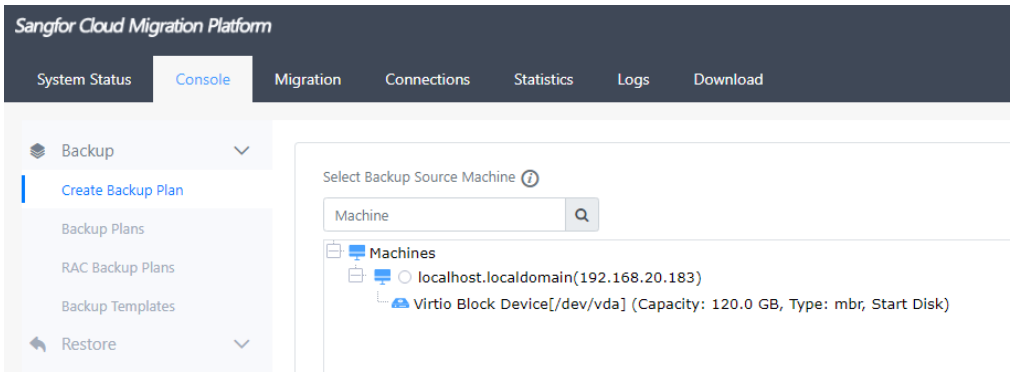
Step 4. Select one of the links, then copy and paste it into the ssh of the source Linux machine and use the **wget** command to download. If using the HTTPS download link, it is required to add the **--no-check-certificate** parameter.



Step 5. After the download is complete, add execution permissions to the installation script and execute the installation after verifying the MD5 value. (The uninstallation steps are the same).



Step 6. The detailed information of this agent will be displayed in the SCMP console after login as the system administrator where the agent corresponded.



Step 7. The installation is complete.

4.2 Preparation For Destination Machine

Function Description

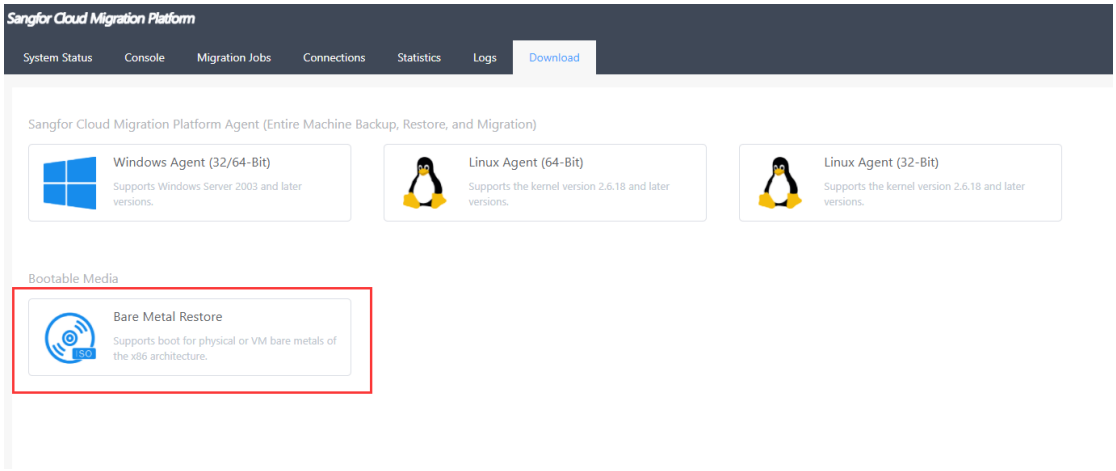
When using the HA backup/backup migration mode or the destination HCI platform is below version 6.0.0 R5, it is required to create a destination VM manually in HCI. This VM will boot from the bare metal restore boot medium and be configured with the corresponding IP address to connect to the SCMP.

4.2.1 Precautions

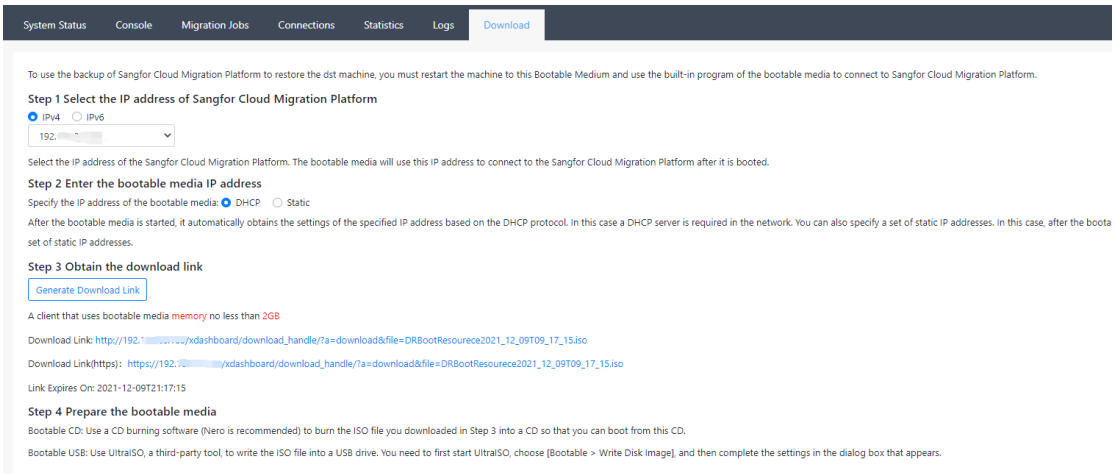
1. The IP address of the bare metal restore boot medium is specified when downloading the image, and this IP is required to be able to access the SCMP in the destination network.
2. The number of hard disks of the destination machine must not be less than the number of hard disks of the source machine, and the capacity of each hard disk of the destination machine must not be less than the source machine.
3. The memory of the destination VM boot from bare metal restores boot medium must not be less than 2GB.
4. It is forbidden to adjust the **Boot Order** for the VM under **Edit** > **Advanced** when booting using the bare metal restore boot medium. Just keep the disk as the first boot option.

4.2.2 Steps

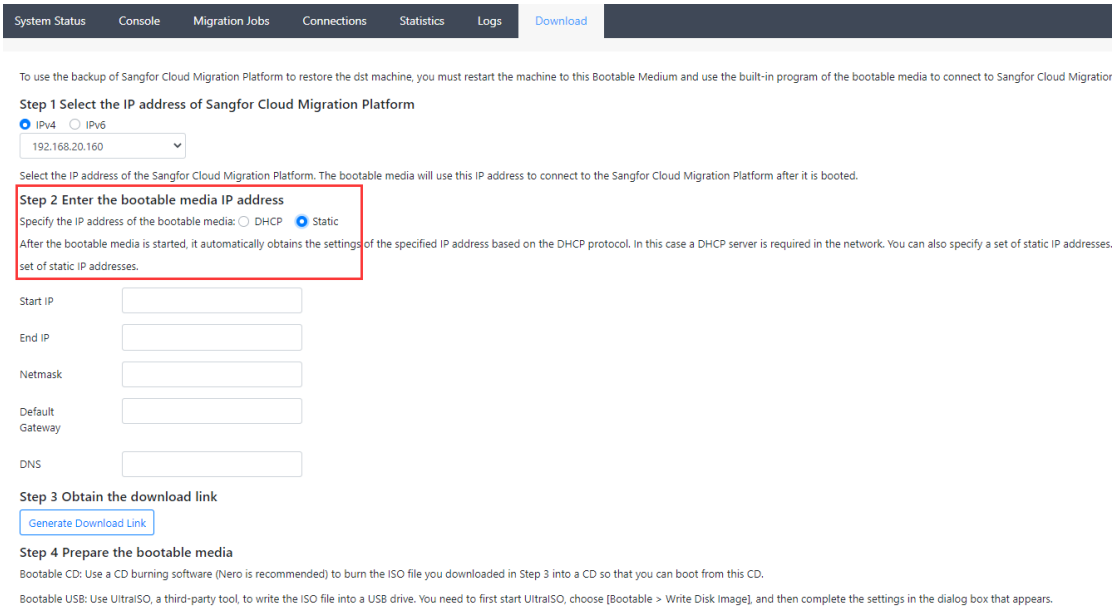
Step 1. Login to SCMP with the system administrator account. Navigate to the **Download** and download the **Bare Metal Restore** ISO.



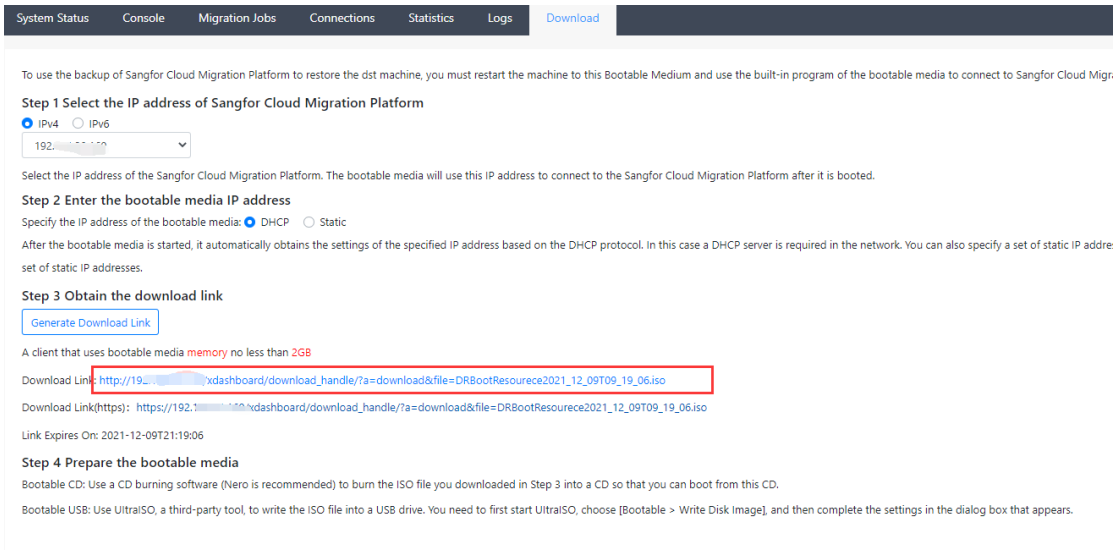
Step 2. By default, the IP address configuration will be using DHCP. As long as the DHCP pool has been specified in the network, manually configuring the temporary IP is unnecessary.



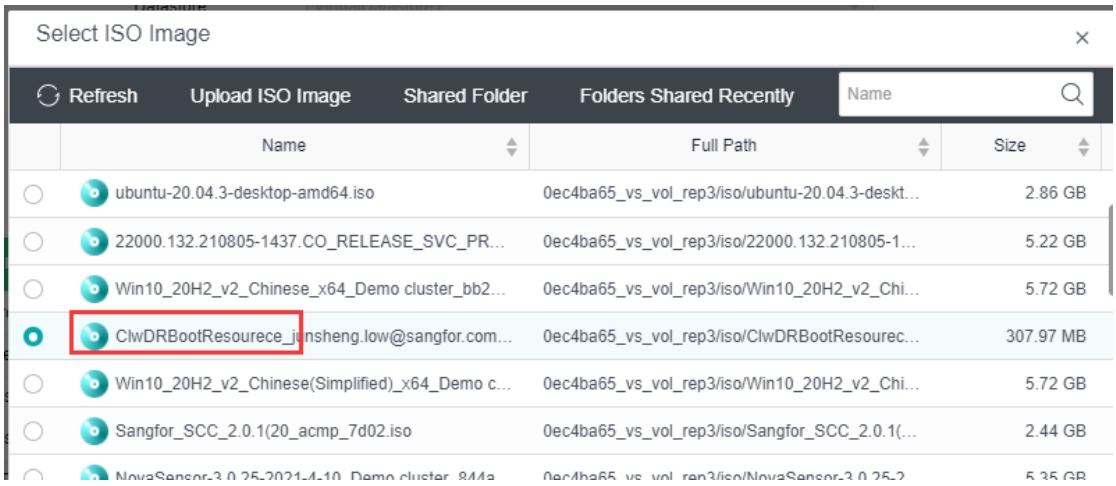
Step 3. Other than DCHP, static IP is also supported to be configured for the bare metal restore medium.



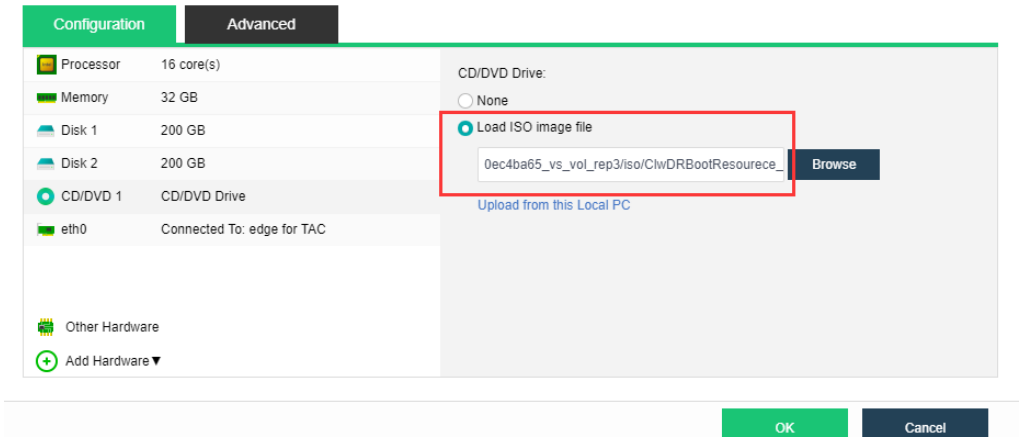
Step 4. Click **Generate Download Link** to get the download link of the bare metal restores iso file corresponding to the system admin.



Step 5. Upload the downloaded ISO image to the Sangfor HCI platform.



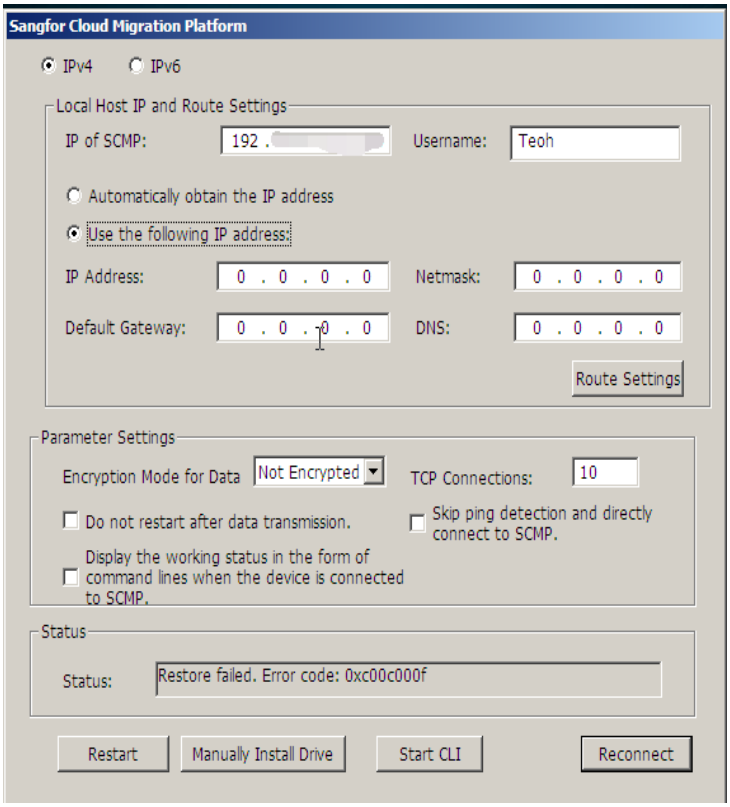
Step 6. When creating a new VM, load the ISO image uploaded in the previous step.



Step 7. Start the virtual machine and boot into the bare metal restore ISO.

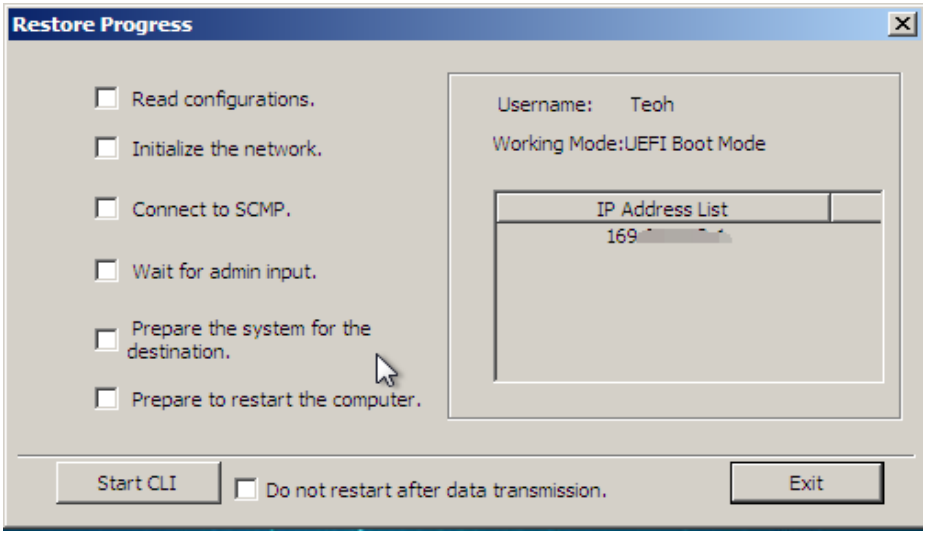
Step 8. Enter the network configuration interface and configure the IP information for the bare metal restore. It is required that the configured IP address be connected to the SCMP. This IP is only used for data migration and will be erased after the migration is completed and restored to the source system's IP address. Manual IP configuration can be avoided if DHCP/Static IP has been configured for the bare metal restore when downloading the files.

- **IP of SCMP**: the IP address of the SCMP server.
- **Username**: The system admin for migration (When the username is filled in wrongly will lead to connection failure). By default, it is filled automatically.



Step 9. If stuck in the **initialize the network** step during the restore progress, the address configured in the previous step cannot be connected to the SCMP. The **Start CLI** function can be used to perform a ping test or select **Exit** to reconfigure the IP address.

Step 10. The establishment of the bare metal restores success when the restore progress reaches the **Wait for admin input** phase. In this phase, it will be waiting for the migration instruction issued by SCMP.



5 Migration Guidance

5.1 Migration Method

5.1.1 Point-to-point Migration (Agentless)

Migration Instructions

The point-to-point migration (agentless) mode is that the migration platform uses the VMware VADP interface to obtain data and migrates the data to the HCI destination machine through SCMP. After the data migration is completed, it supports automatic compatibility processing (injecting performance optimization tools). In this way, there is no need to back up the source system.

Applicable Scenario

1. The source platform is the VMware platform, and the version of the VMware platform is in the **SCMPCompatibilityList-20211214**.
2. The agentless scenario only applies to virtual machines that use ordinary virtual disks. It is not supported for the virtual machine using the disk, which is unable to obtain data block changes through CBT, such as independent disks and RDM disks.
3. The source virtual machine does not need to install the migration agent, which reduces the migration workload.
4. There may have abnormalities in the CBT interface of the VMware platform. If the interface is abnormal, agent-based migration is required.

5.1.2 Point-to-point Migration (Agent-based)

Migration Instructions

The point-to-point migration(agent-based) mode uses the migration function to transfer the source machine to the destination machine by directly transmitting the source machine's data to the destination machine. In this way, there is no need to back up the source system. While the source machine's data is transmitted to the Sangfor HCI platform, the HCI platform starts the destination virtual machine to receive the migrated data.

Applicable Scenario

1. The migration time is relatively controllable, and the data transmission can be started as early as possible. The final data synchronization and switching actions will be performed after full data transmission is completed and the scheduled business downtime.
2. The operating system switching time for the point-to-point migration method is less than 10 minutes, and the specific interruption time is related to the business service startup time.
3. Point-to-point migration eliminates the need to back up the source host's data to the SCMP, which reduces the storage requirements of the SCMP. Data does not need to be transferred to the destination through the migration platform, which reduces the overall data migration time.

5.1.3 HA Backup Migration

Migration Instructions

HA backup migration is to use the function of CDP backup by continuously backing up the source machine's data to the SCMP and then synchronizing it to the destination virtual machine. In this way, data from the source machine will be synchronized to the destination machine in real-time through CDP, which minimizes migration and switching time.

Applicable Scenario

1. HA backup migration will save the source machine's data in the SCMP through CDP backup, which requires high storage requirements for the SCMP.
2. Before the business switching, the destination virtual machine is in the operating system loading state, reducing the switching time caused by the migration. The switch time is around 1 minute, while the specific business interruption time is related to the business service startup time.

5.1.4 Backup Migration

Migration Instructions

The backup recovery mode uses the backup function to back up the source machine's data to the SCMP and then restore the system to the destination

virtual machine through the backup file saved in the SCMP. Compared with point-to-point migration and HA backup migration, longer business downtime is required.

Applicable Scenario

This method is mainly used in scenarios where the data at the source machine is extremely large along with small bandwidth to the destination, which the data transmission time is unacceptable. Perform a full backup on the SCMP, which is deployed on the source side physical server, which has high bandwidth, then move it to the destination to perform incremental backup, then recover to complete the migration.

For scenarios where the SCMP needs to be relocated to the destination server room, it is not supported to roll back source machine back to the backup point after the migration is completed. Use carefully before proceeding.

5.2 Point-to-point Migration

Function Description

Point-to-point migration refers to migrating the entire source machine directly to the destination virtual machine through the migration agent.

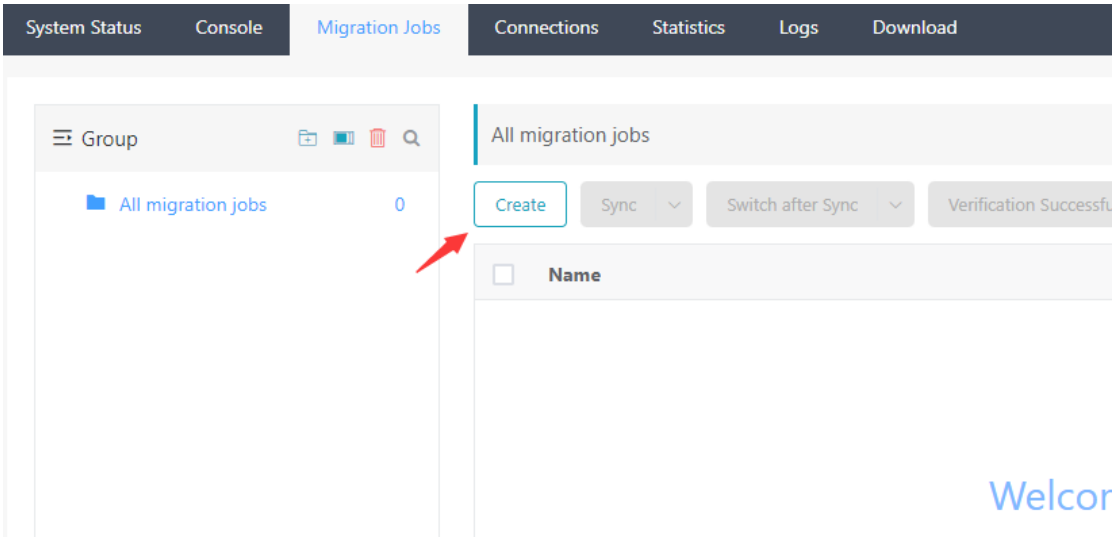
5.2.1 Precautions

1. In this migration method, since the data is not retained on the SCMP, verification can only be performed on the destination machine after the migration is completed.
2. When migrating from the source machine, the disk will configure as dynamic provisioning by default. If the data is greater than 8T and exceeds the size limit of the dynamic provisioning disk, it will automatically change to thin provisioning.

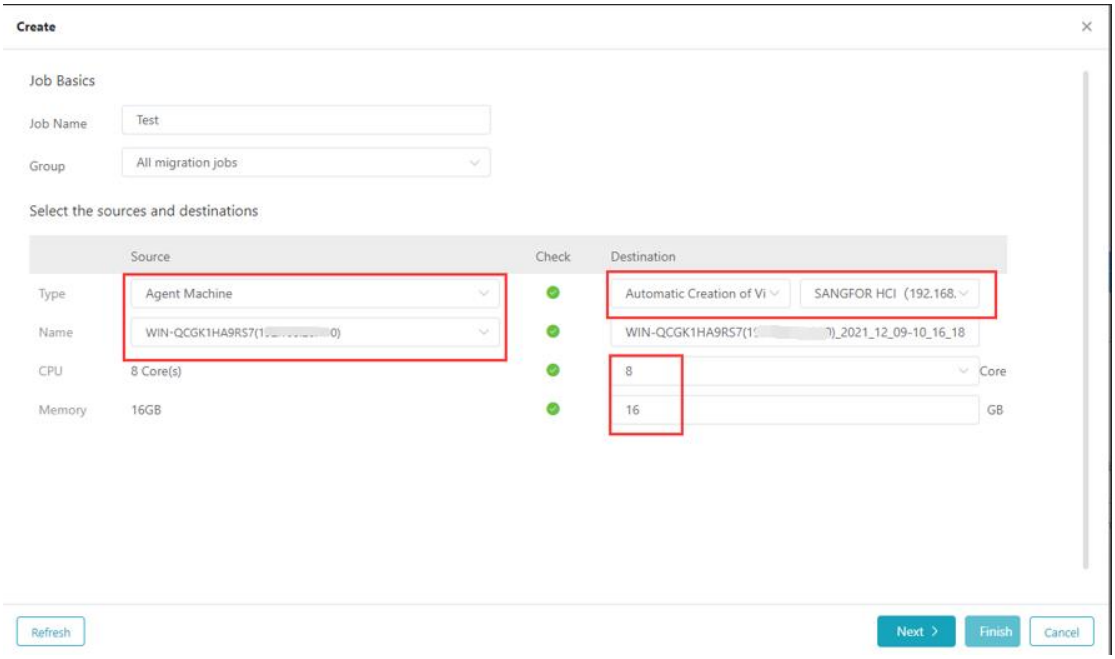
3. When performing business switching, only stop the source machine business service and do not shut down the source operating system.
4. It does not support migrating data from one disk on the source side to multiple disks on the destination side.
5. It supports external storage migration with mounted partitions and does not support the migration of raw disks without file system partitions.
6. File storage mounted on the source machine is not supported for migration.
7. The installation of the source machine migration client and preparation of the destination machine must be completed before the migration can be carried out.

5.2.2 Steps

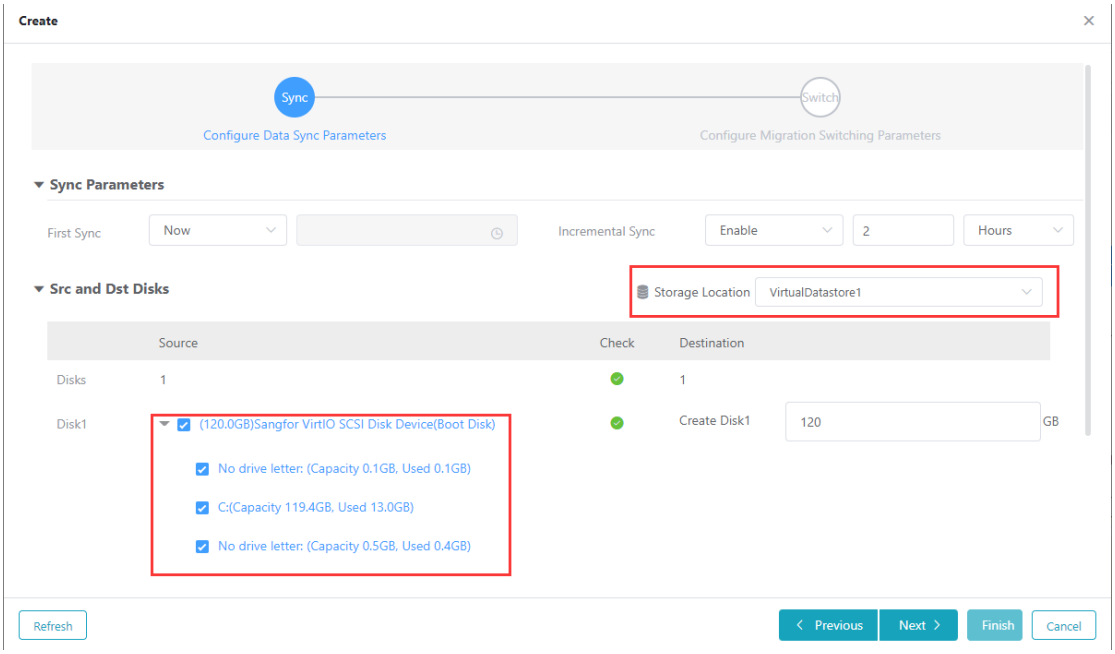
Step 1. Log in to the SCMP with the system admin account, navigate to **Migration** and click **Create**.



Step 2. Configure the basic information of the migration, select the **Agent Machine** or **Agentless Machine** for the Source and select the virtual machine to be migrated. For the destination machine, select **Automatic Creation of Virtualization Data Center** when the supported HCI has been added to **Virtualization Data Center**. Otherwise, select **Agent Machine** for VM booted with bare metal restore medium.

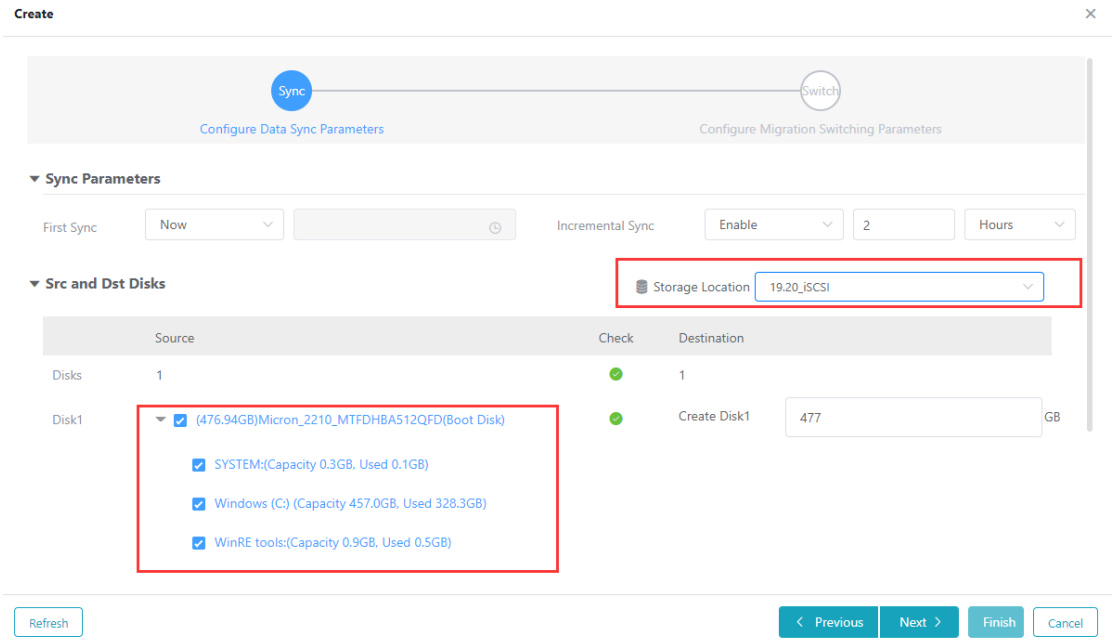


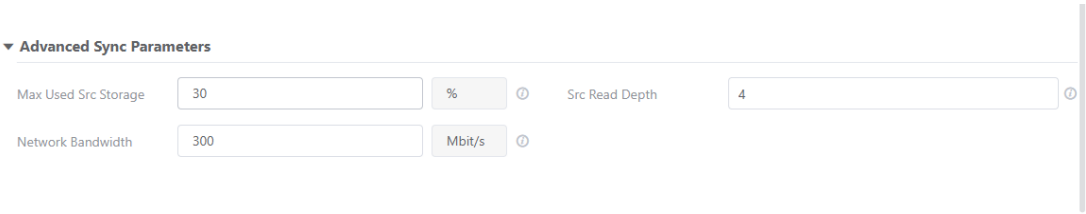
Step 3. Click **Next** to proceed with the disk information, and select the **Storage location** information of the destination HCI environment. It is required that the number of hard disks of the destination machine must not be less than the number of hard disks of the source machine, and the capacity of each hard disk of the destination machine must not be less than the source machine.



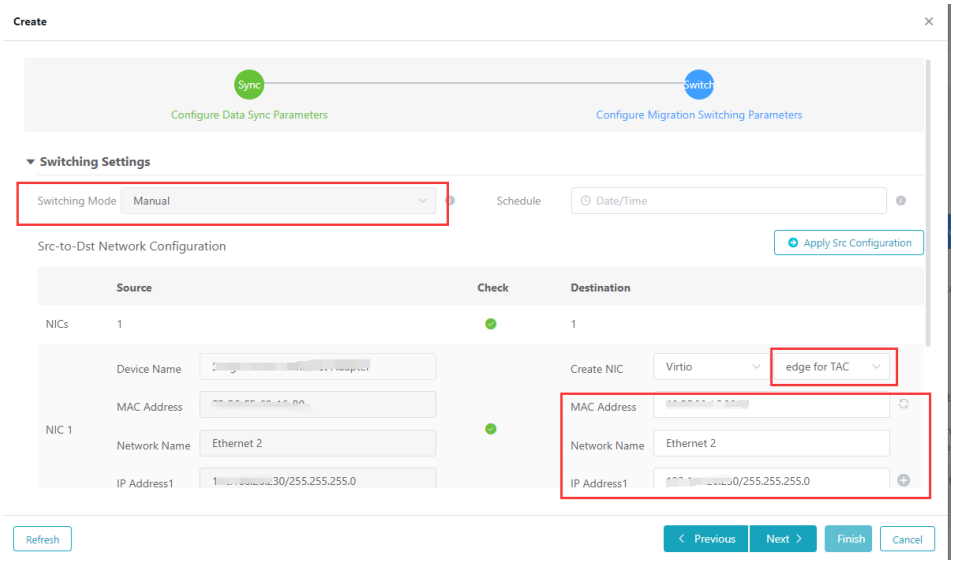
Step 4. Click **Advanced Sync Parameters** to configure the **Max Used Src Storage**, **Network Bandwidth**, and **Src Read Depth** for the migration task.

These parameters come with the default value, where you can change the configuration accordingly.



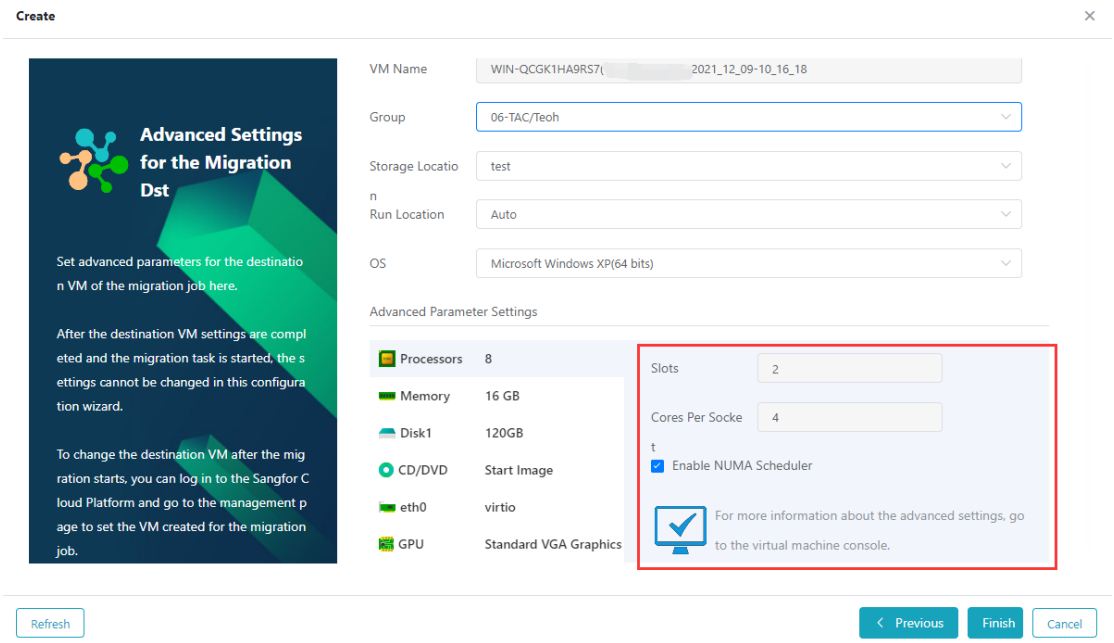


Step 5. Click **Next** to configure network configuration for migration: Currently only supports **manual** switching for migration. If the network information needs to be modified while migrating, fill in the destination machine IP configuration, as shown below.

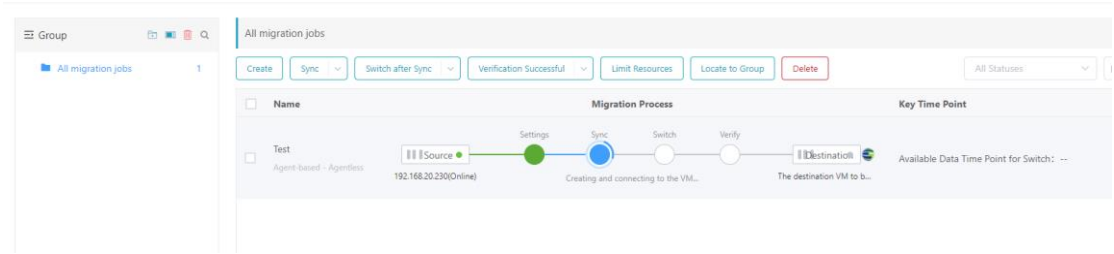


Step 6. In the above figure, an alarm appears in the DNS position because the DNS of the destination machine is configured with one line more than that of the source machine, which can be deleted manually or retained.

Step 7. Click **Next** to preview the configuration of the destination virtual machine. Some VM configurations are editable, including Group, Processors, Memory, Disk, CD/DVD, NIC, and GPU.

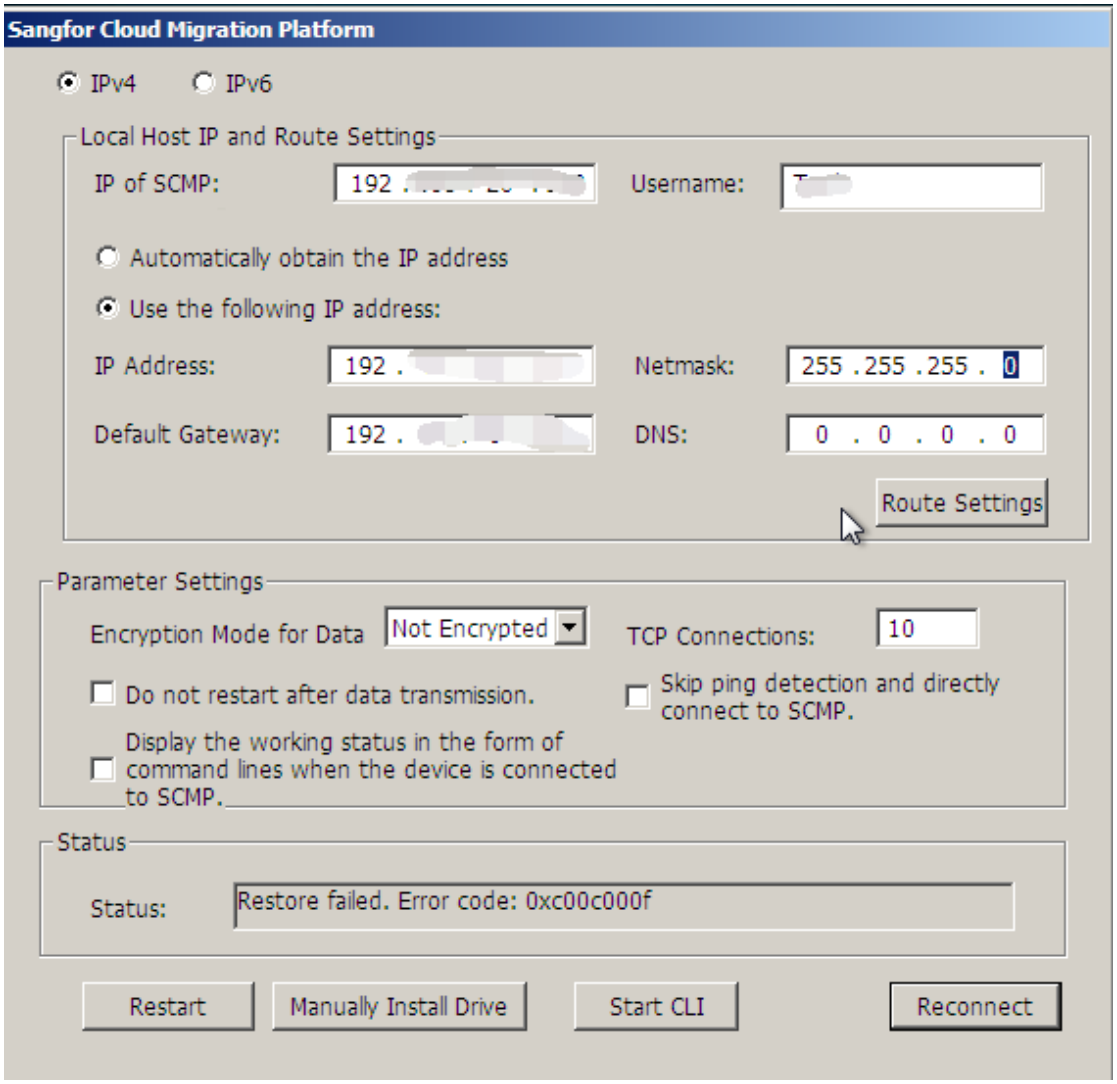


Step 8. Click **Finish** to save the configuration, and the migration task will start automatically. The process of this migration task can be traced under **All Migration Jobs**. The synchronization completion time will be calculated after the configuration check is automatically completed.

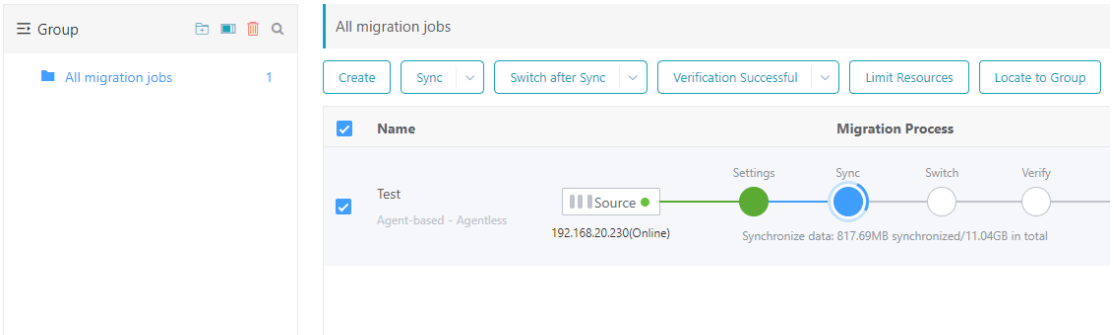


Step 9. Navigate to the destination machine console to check the status. If it shows that the bare metal restores ISO obtains the address from DHCP, you need to manually configure the IP address that can access the migration platform (and cannot conflict with the business machine address). The configuration is completed before you can continue. Perform the migration.

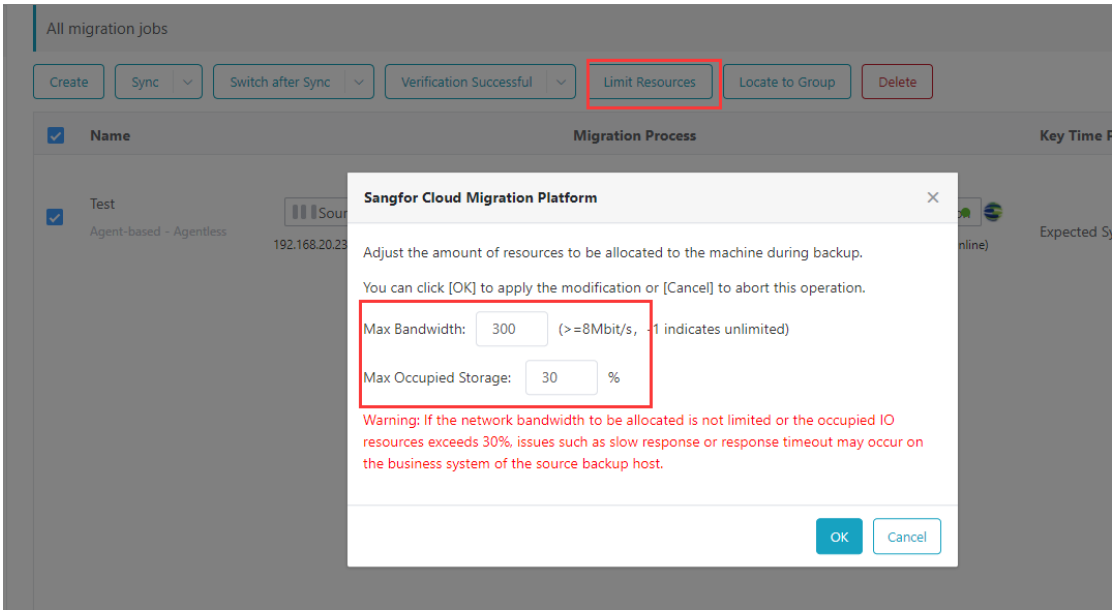
Manual configuration can be avoided if a destination cluster is configured with DHCP or uses a static IP.



Step 10. The configuration is complete, and the data transmission action is started. If the synchronization times out, click the down arrow of the **sync** to **restart complete synchronization**.

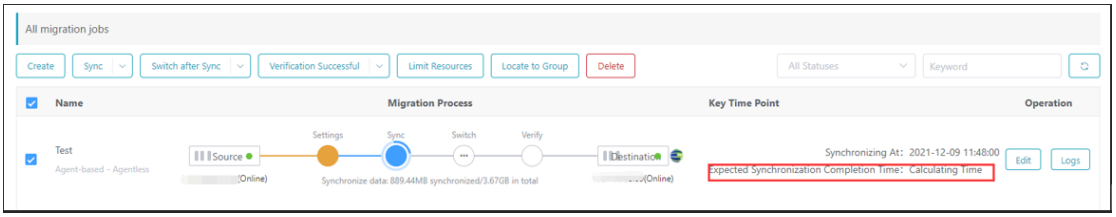


Step 11. During the data synchronization process, click **allocated resources** to configure or modify the migration QoS.

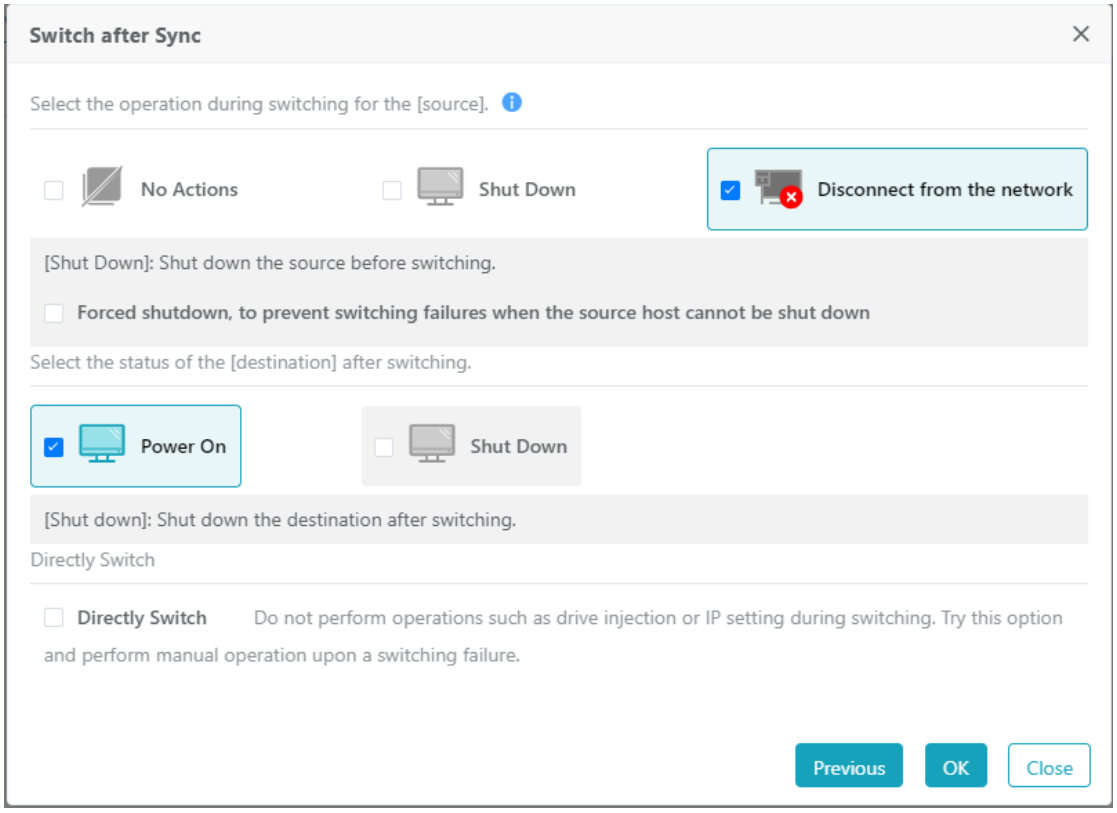


Step 12. To shorten the downtime, after waiting for the first full data to be completed and before the time allowed for downtime, click the button to perform an incremental synchronization.

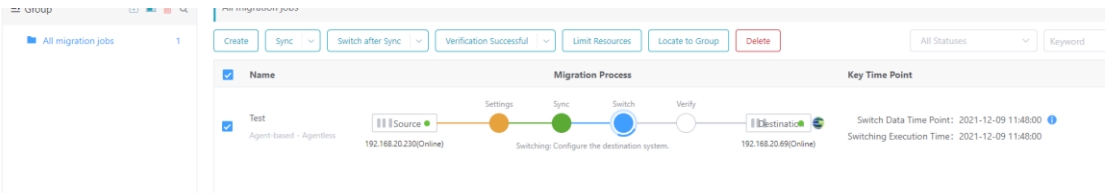
Step 13. Within the time when the business is allowed to be interrupted, stop (do not shut down the source) the business(service), and then click [**switch after sync**] to enter the switch option UI.



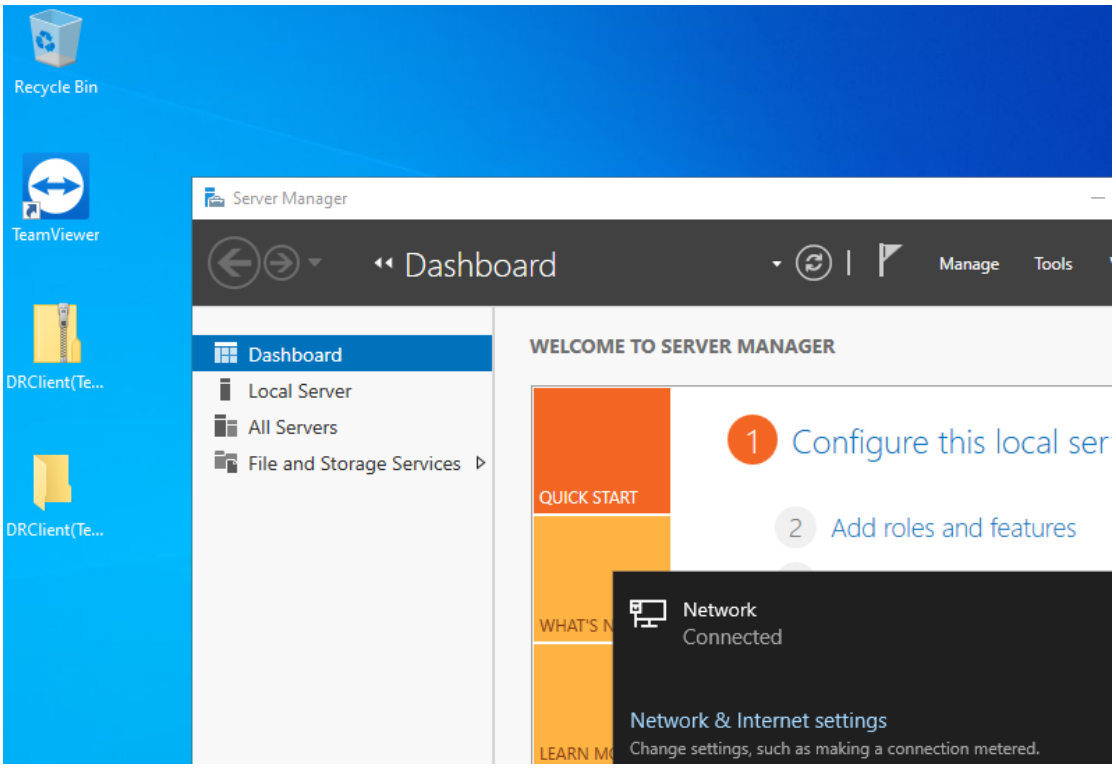
Step 14. Enter the switch option UI and select the operation when switching. Point-to-point migration scenarios recommend the user perform a disconnection operation on the source end and automatically turn on the destination end virtual machine after the switch (as shown in the figure).



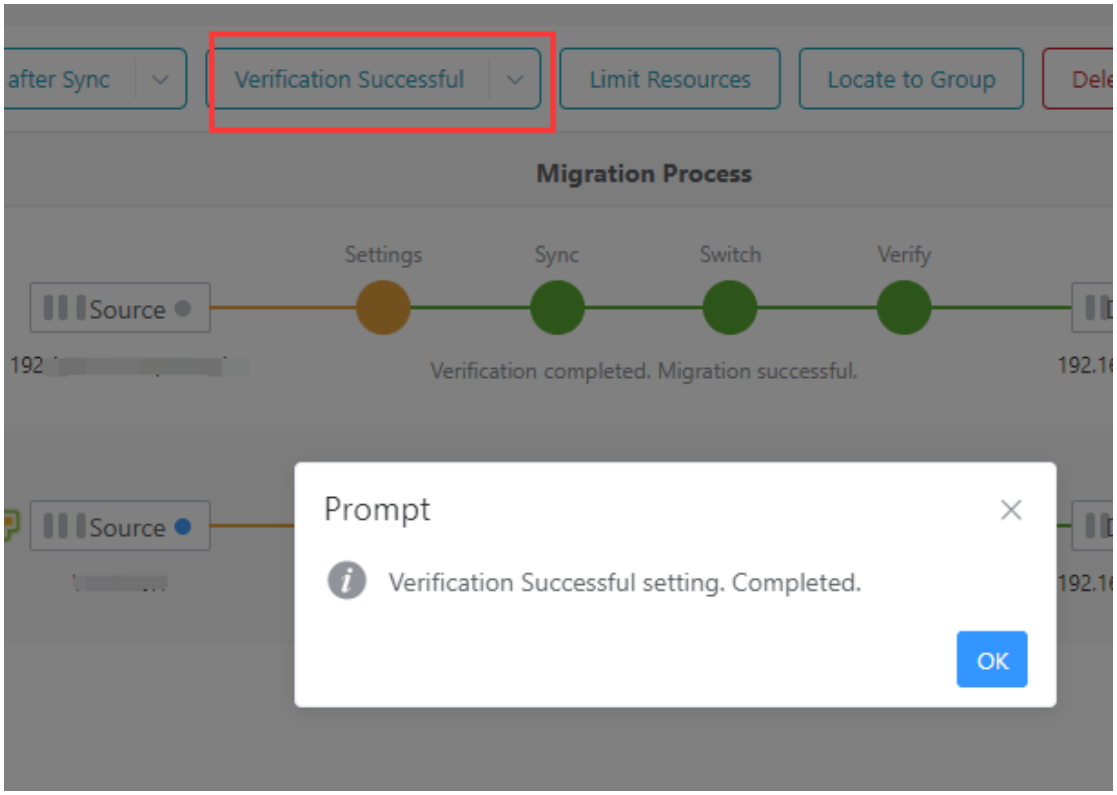
Step 15. Click **OK** to initiate the switching action.



Step 16. After the switch is completed, enter the verification state, enter the destination machine console at this time, and wait for the restart to enter the operating system.



Step 17. After the handover is completed, confirm that the source end network is disconnected and enter the destination end for business verification. If the verification is abnormal, perform abnormal troubleshooting or roll back migration actions, shut down the destination virtual machine, and connect to the source machine to resume business. If the verification is normal, enter the migration management interface and click. If the operating system of the source machine is a Linux system and the boot mode is UEFI boot, it may start abnormally after migration. To solve it, you can refer to the fault case **UEFI Linux virtual machine cannot enter the system**.



Step 18. The migration is complete.

5.3 HA Backup Migration

5.3.1 CDP Backup Plan

Function Description

HA backup migration means that the source data is continuously transmitted to the destination machine through the cloud migration platform through the CDP backup method. The business interruption time is reduced through high-frequency transmission. When the source is running normally, the destination machine enters the state of booting and loading the OS. When the source and destination are switched in the final stage of the migration, the destination machine will use the business IP for quick startup. It is usually used in scenarios where migration interruption requirements are short.

5.3.1.1 Precautions

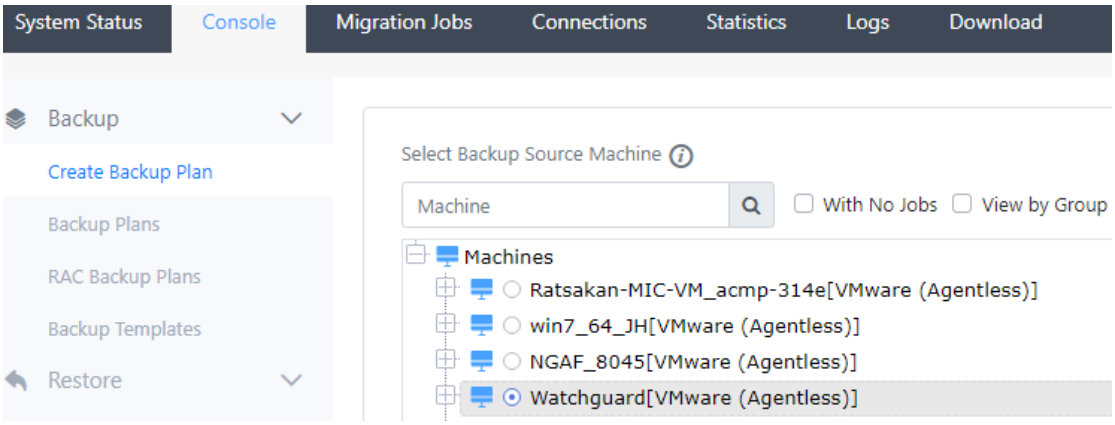
1. The disk will configure as dynamically allocated by default when migrating from the source. If the amount of data exceeds 8T and exceeds the size

limit of the dynamically allocated disk, you need to manually enter the destination side to modify the disk type to thin provisioning.

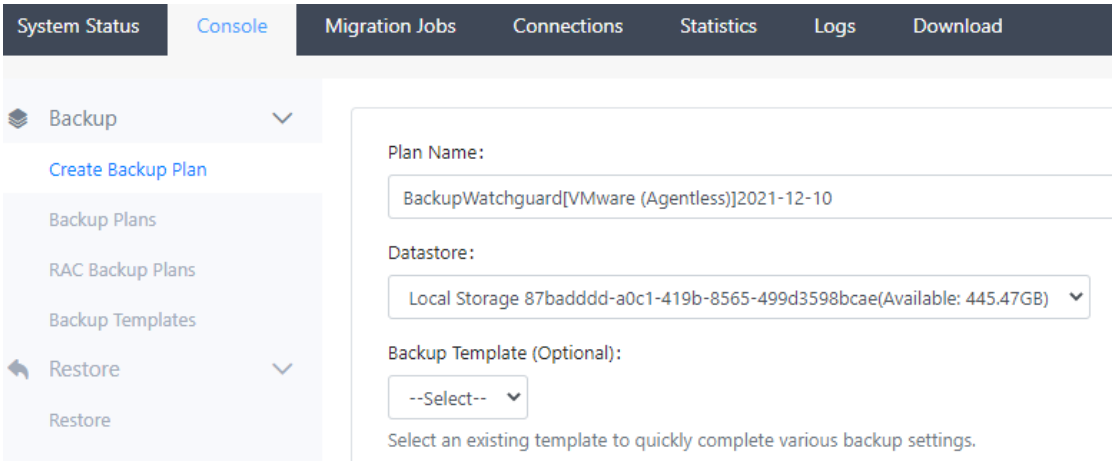
2. It does not support migrating data from one disk on the source side to multiple disks on the destination side.
3. It supports external storage migration with mounted partitions and does not support the migration of bare dictionaries without file system partitions.
4. File storage mounted on the source host is not supported for migration.
5. The source end must complete the migration client installation, and the destination end must complete the preparation of the destination machine before the migration can proceed.

5.3.1.2 Steps

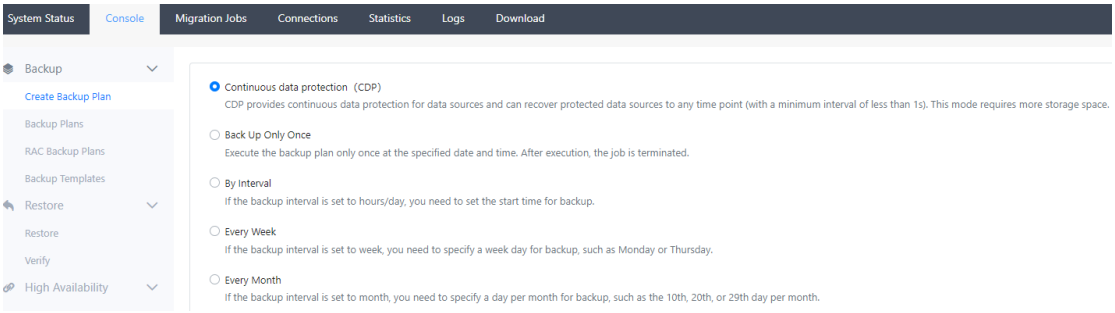
Step 1. Use the system administrator to log in to the SCMP, navigate to **Console > Create Backup Plan** UI, select the source to be migrated (the client plug-in has been installed), and click **Next.**



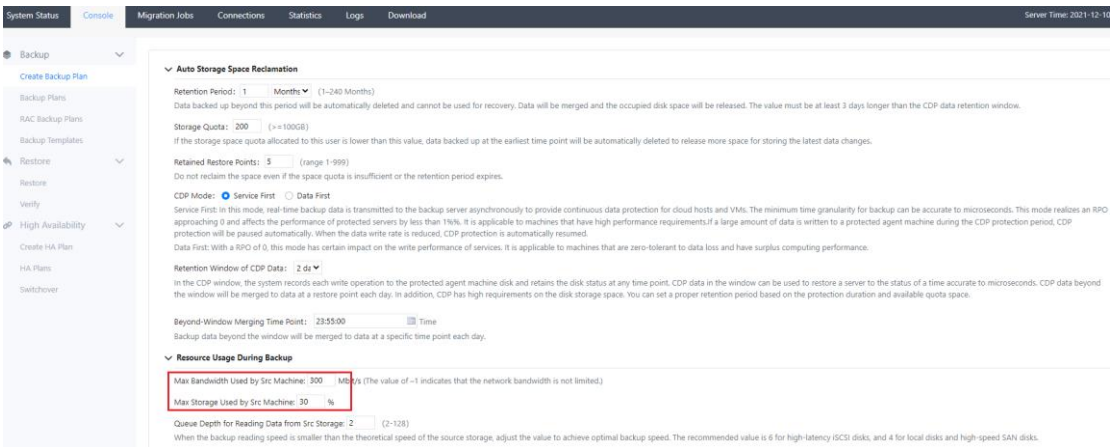
Step 2. Fill in the name of the plan and select the backup destination storage. The backup strategy can leave it blank for the time being. Click **Next** to configure the backup strategy.



Step 3. Select the backup strategy, select **Continuous Data Protection(CDP)** for proxy backup migration, and click **Next**.

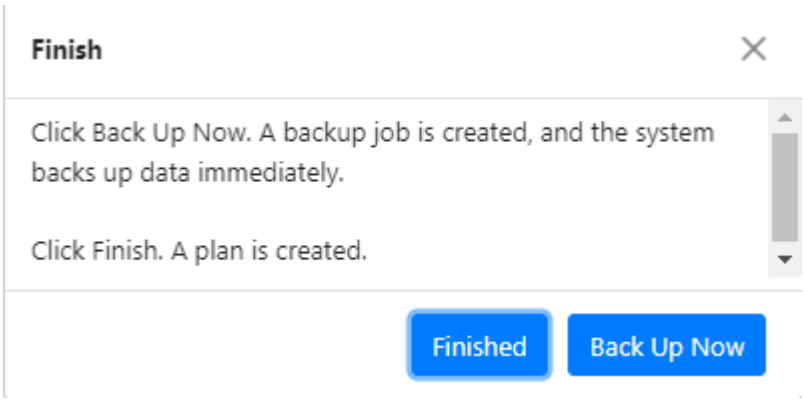


Step 4. Configure the backup details. Here, the backup rate is limited by default. If the rate is not required, modify the **Resource usage during Backup** to **-1** and **100**. Click **Next Step**.

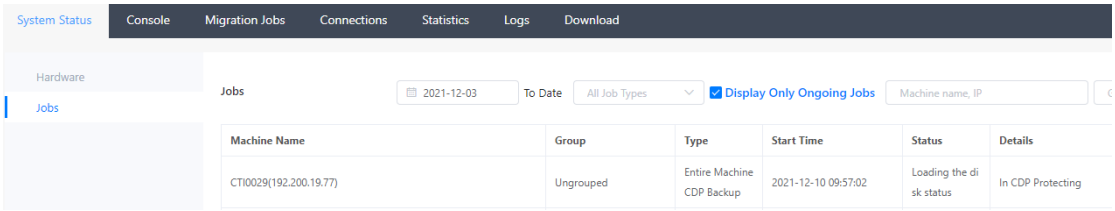


Step 5. Configure **Backup Execution Script** this interface does not need to be configured. Just skip it.

Step 6. Enter the last step to confirm the information, and click **Finished** or **Back Up Now** to start the first backup.



Step 7. Enter **System Status > Jobs** to see the progress and status of the backup.



Step 8. Wait for the backup to complete.

5.3.2 HA Backup Plan

Function Description

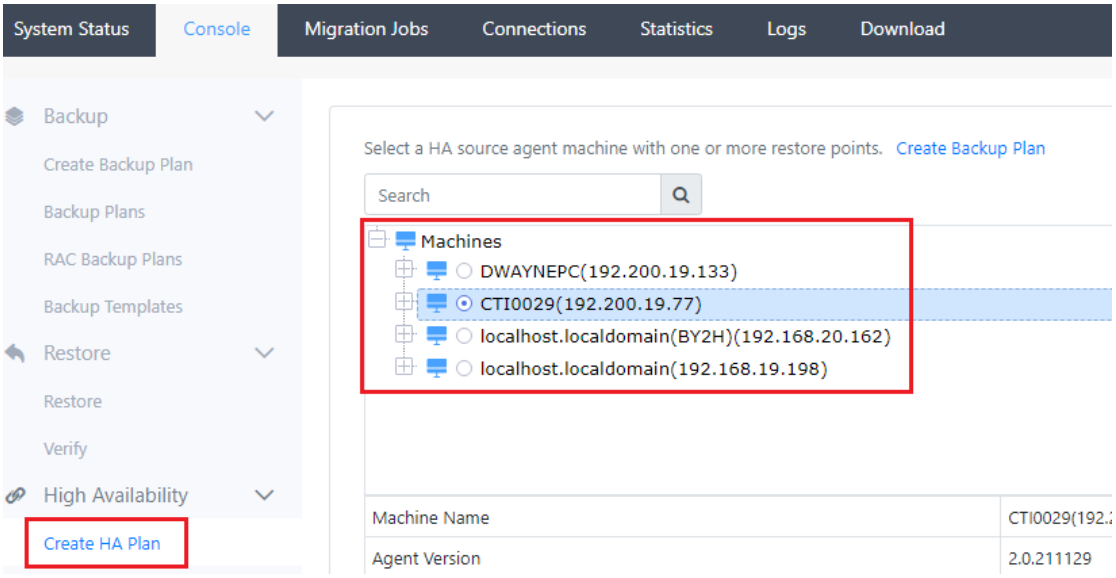
Guide to restore the backup data to the destination machine through HA backup.

5.3.2.1 Precautions

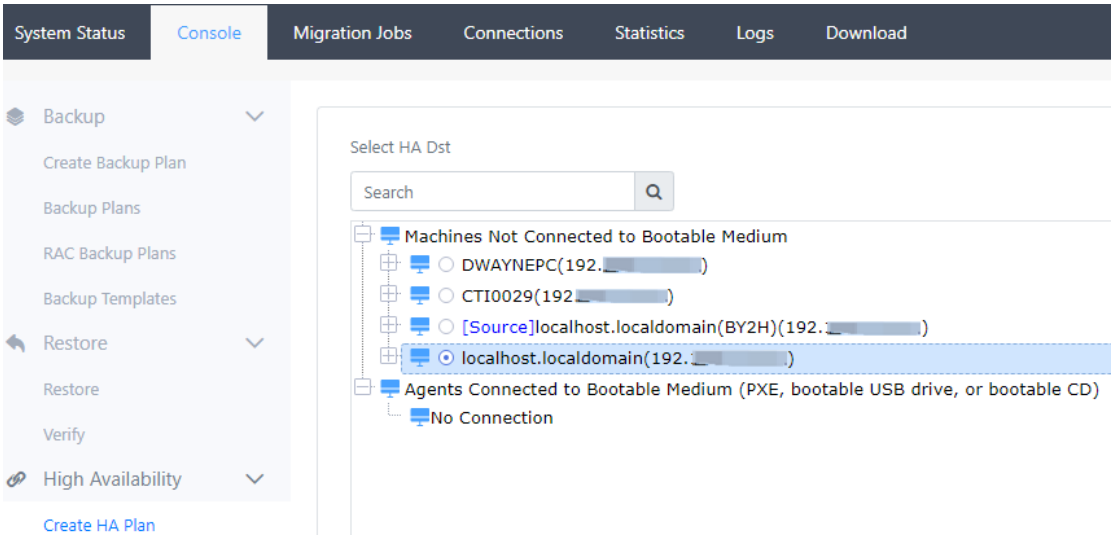
1. Complete the **CDP Backup Plan** chapter. After the CDP plan is completed for a certain point in time, the HA backup plan can be carried out.
2. The HA backup migration method only supports the destination end that uses the bare metal restore ISO to start.
3. The connection of the source system cannot be disconnected or closed during the HA backup migration. If the source and destination IP are the same, the **drift IP** function must be used. Otherwise, the IP will conflict after the migration is completed. However, this method will modify the source IP after migration, so please choose carefully.

5.3.2.2 Steps

Step 1. Enter the **Console > Create HA Plan** interface, select the HA backup client, and click **Next**.

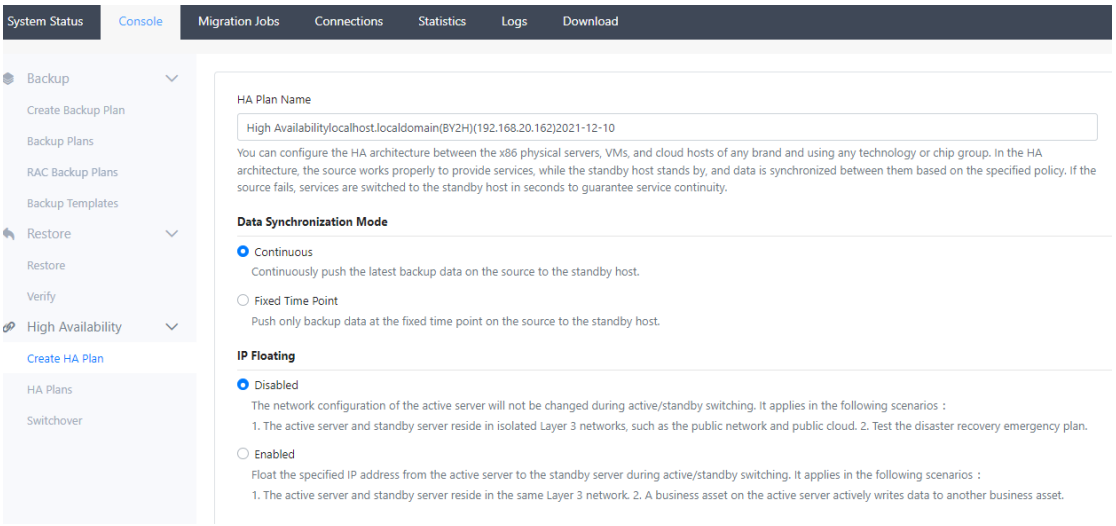


Step 2. Select the HA backup destination machine and click **Next**.

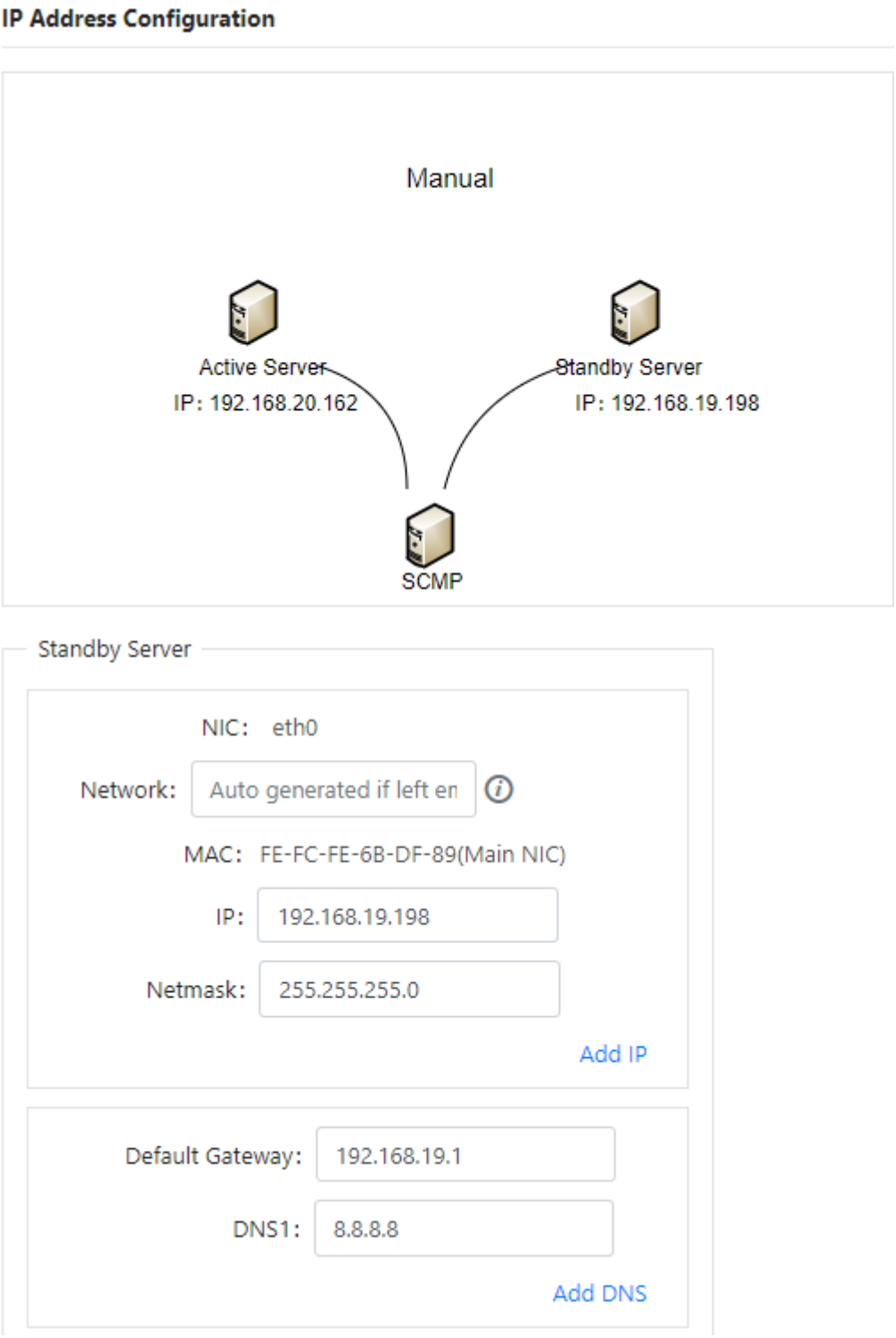


Step 3. Configure the HA backup plan. Here you can choose to **enable** the IP drift function according to your needs. Steps 4 and 6 introduce its configuration guidelines.

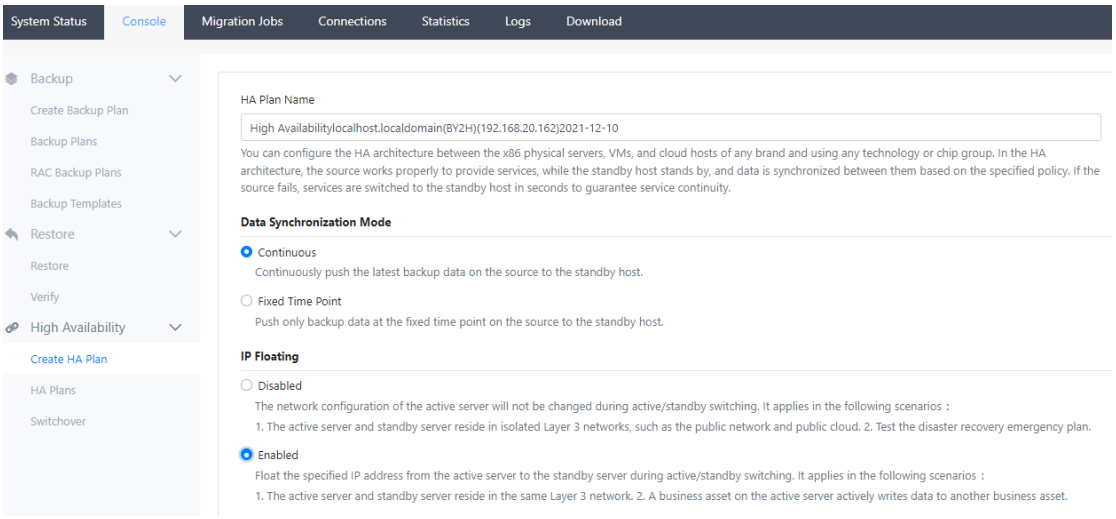
Step 4. When the source and destination IPs are different (change the IP address while migrating), select **disable** the IP drift function.



Step 5. Configure the HA backup network, and configure the IP for the destination machine. The default is to use the IP of the startup tool here to modify the IP of the destination server according to the migration requirements.



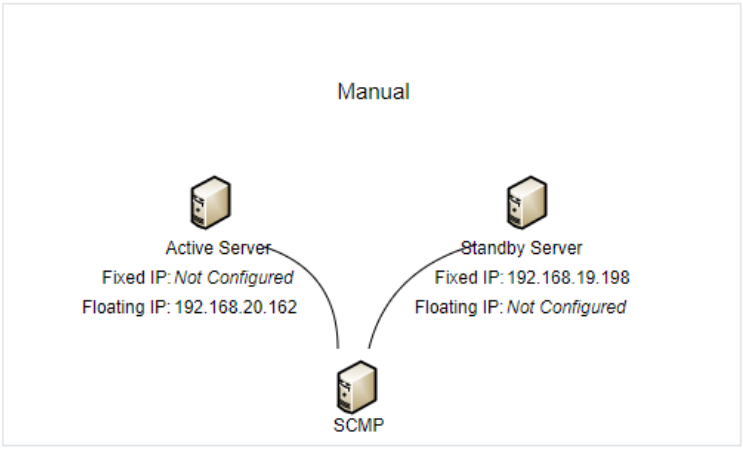
Step 6. When the source and destination IPs are the same (the migration does not change the IP address), the IP drift function must be **enabled**.



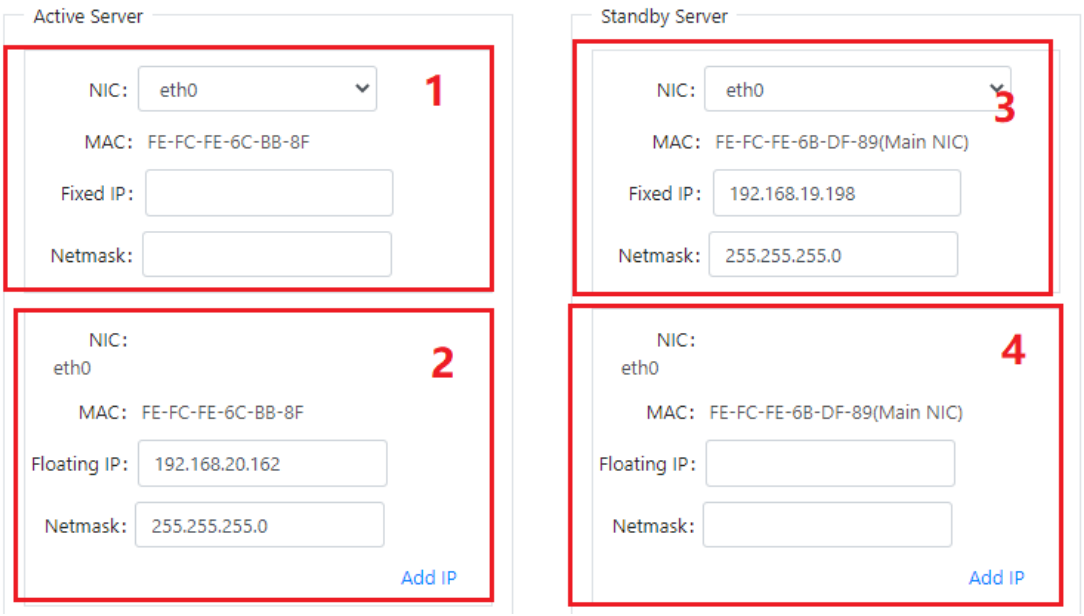
Step 7. Configure the HA backup network, the role and usage of each IP in the following figure:

- The inherent IP of the source can not be empty. This IP is configured on the source NIC after the HA backup switch is completed.
- Source drifting IP is the source service IP. This IP will drift to the destination end after the HA backup switch is completed.
- The inherent IP of the destination is the IP of the startup medium. This IP will be deleted after the HA backup switch is completed.
- The drifting IP of the destination end is consistent with the drifting IP of the source end. This IP is the destination IP after the handover.

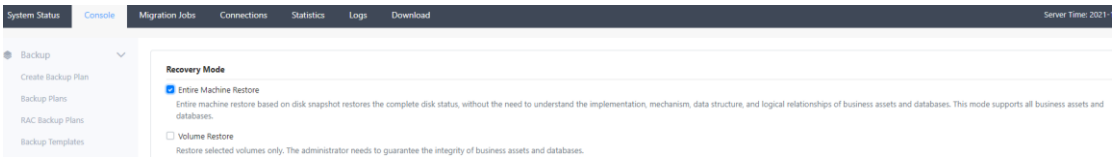
IP Address Configuration



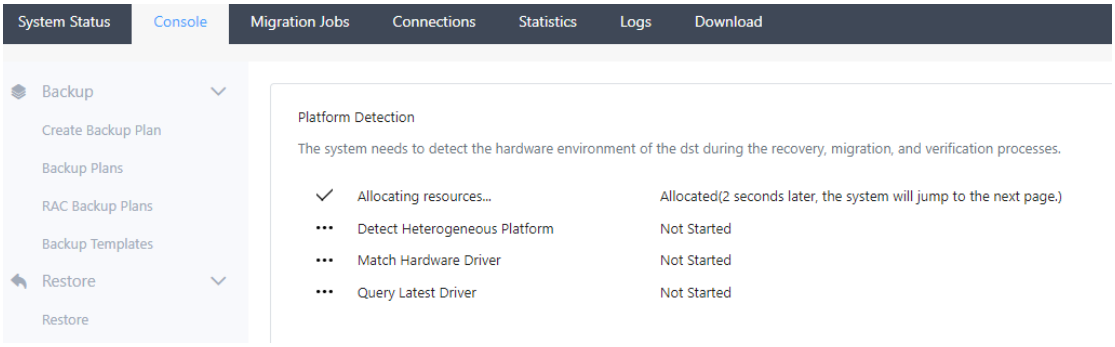
A fixed IP address is used exclusively by a server, so it cannot float between servers. A floating IP address can float from the active server to the standby server during active/standby switching.
During the execution of a HA job, services enter the quiesce state after the active server is shut down or restarted. After the active server in quiesce state is started, the fixed IP address is enabled and floating IP address is disabled. The system must connect to Sangfor Cloud Migration Platform for witnessing. Only after the backup appliance confirms that the floating IP address is not occupied by the standby server, the floating IP address will be enabled on the active server, and the active server exits the quiesce state.



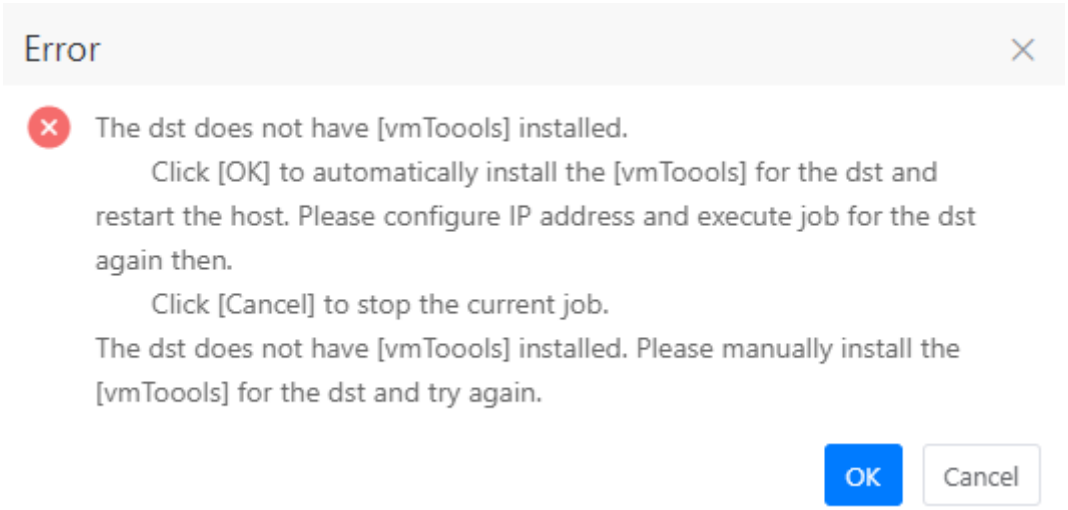
Step 8. Select **Entire Machine Restore** as the recovery mode.



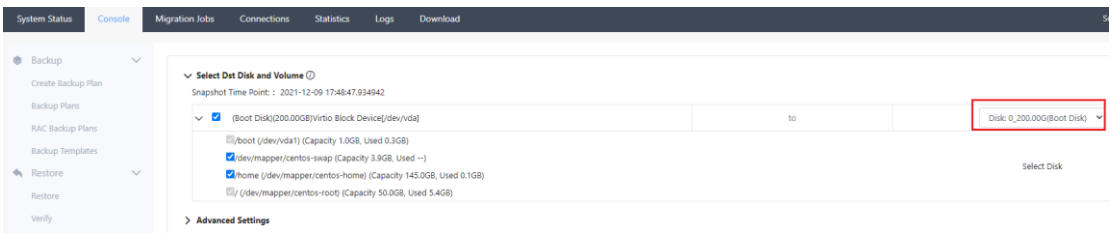
Step 9. Check whether resources, drivers, tools, etc., meet the migration conditions.



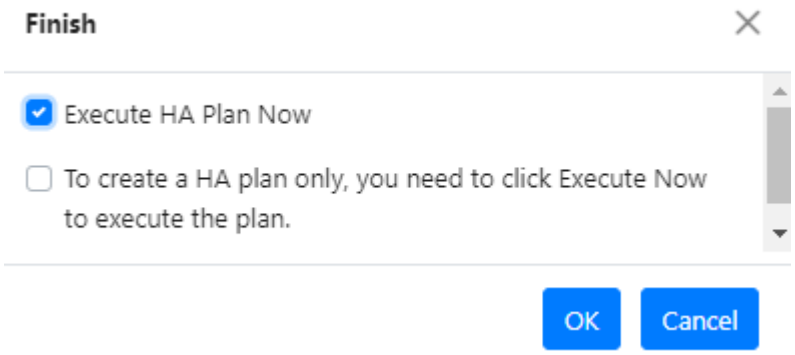
Step 10. If this bare metal restore boot medium is used for the first time, it will report an error "**The dst does not have** [**vmTools**] **installed**". Click **Restart Bare Metal Restore** and install the vmTools. This action does not affect the source side business and only restarts the bare metal restore boot medium. After restarting, enter the bare metal restore boot medium to reconfigure the IP connection to the server and reconfigure the HA backup plan according to the above steps. If no such error is reported, skip this step.



Step 11. Confirm the restored disk and partition information. The number of hard disks of the destination machine must not be less than the number of hard disks of the source machine, and the capacity of each hard disk of the destination machine must not be less than the hard disk capacity of the source machine.

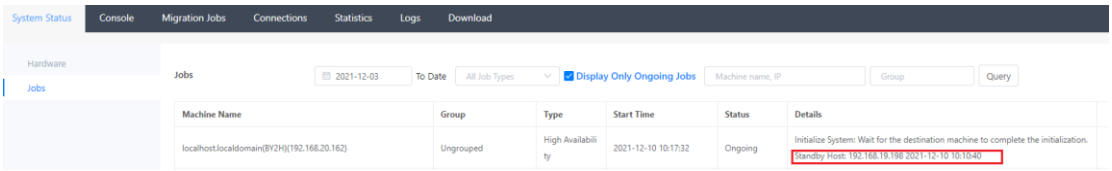


Step 12. Business stop and start scripts are uploaded according to the customer's business needs. If there is no such requirement, skip it directly. Click **Finish**.



Step 13. You can see the process and status of the HA backup in the **System Status > Jobs** interface. In the beginning, the hardware configuration of the destination client was prepared.

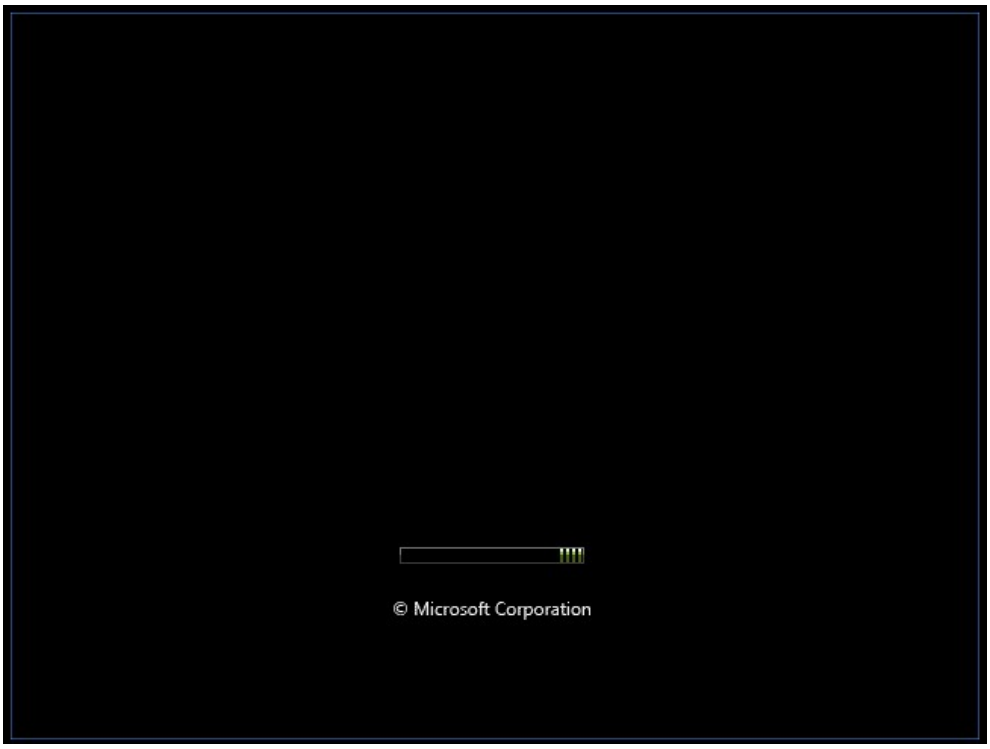
Step 14. After the hardware configuration of the destination client is ready, start to synchronize data.



Step 15. After the data synchronization reaches 100%, the destination machine enters the state of booting and loading OS (as shown in the figure below), waiting for the HA backup switch.

- The Linux operating system loads the OS status interface, as shown in the figure below.

- The Windows operating system loads the OS status interface, as shown in the figure below.



Step 16. The HA backup plan is completed.

5.3.3 HA backup switch

Function Description

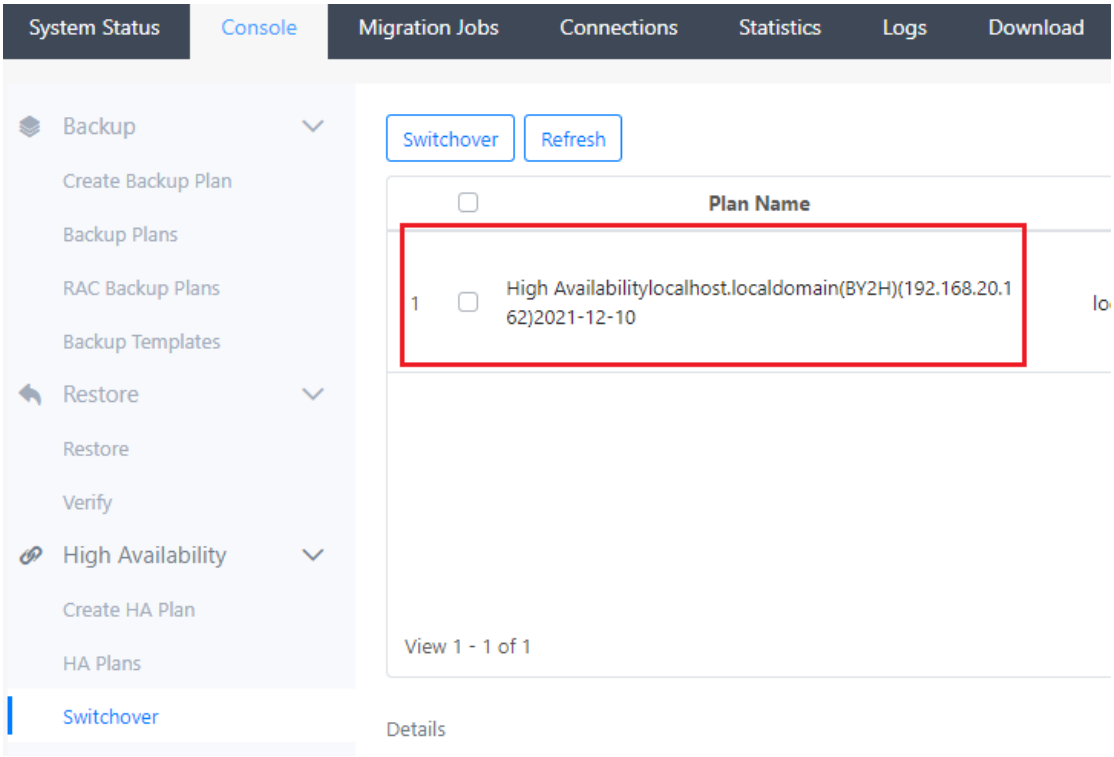
After the HA backup plan is completed, close the source business service and switch to the destination machine within the time allowed for business interruption.

5.3.3.1 Precautions

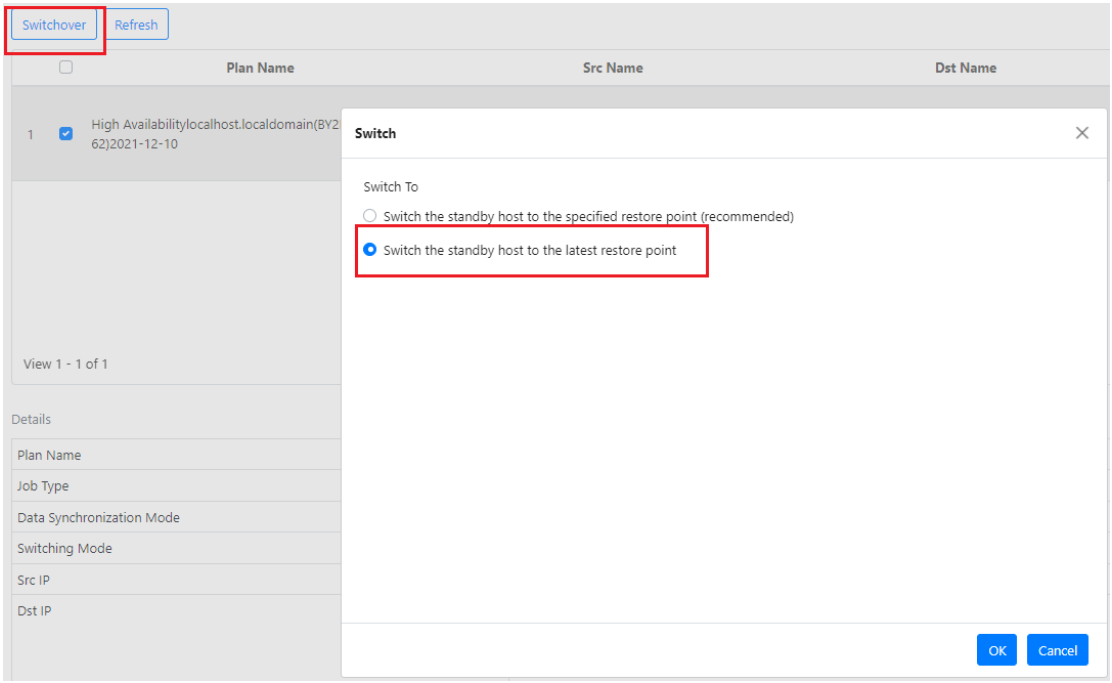
1. The switch can only be performed after the HA backup plan is completed.
2. When performing business switching, stop the source-end business service and do not shut down the source-end operating system.

5.3.3.2 Steps

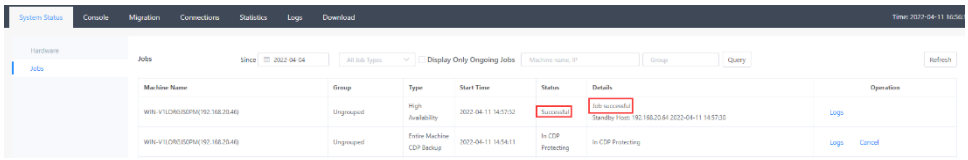
Step 1. Enter the **Console > Switchover** interface, select the HA backup plan, and click **Next**.



Step 2. Click **Switchover** and select **Switch the standby host to the latest restore point**.



Step 3. You can see **Successful** status for the HA task.



Step 4. Enter the destination machine to check the status of the destination machine and verify whether the business is normal. If the operating system of the source machine is a Linux system and the boot mode is UEFI boot, it may start abnormally after migration. To solve it, you can refer to the fault case **UEFI Linux virtual machine cannot enter the system**. If the verification is abnormal, perform the abnormal problem investigation or roll back the migration action, shut down the destination virtual machine, and enable the source machine to resume services.

Step 5. The migration is complete.

5.4 Backup Migration

Function Description

Backup migration refers to backing up the source data to the Sangfor cloud migration platform and transferring it to the destination machine. There are currently two ways of backup migration: **the proxy mode using client plug-ins** and **the proxy-free mode without plug-ins**.

The proxy mode installs a client plug-in on the source machine to back up data to the Sangfor Cloud Migration Platform and then migrates the data to the destination machine by restoring the backup. It is mainly used in the scenario of physical machine migration.

5.4.1 First Full Backup

Function Description

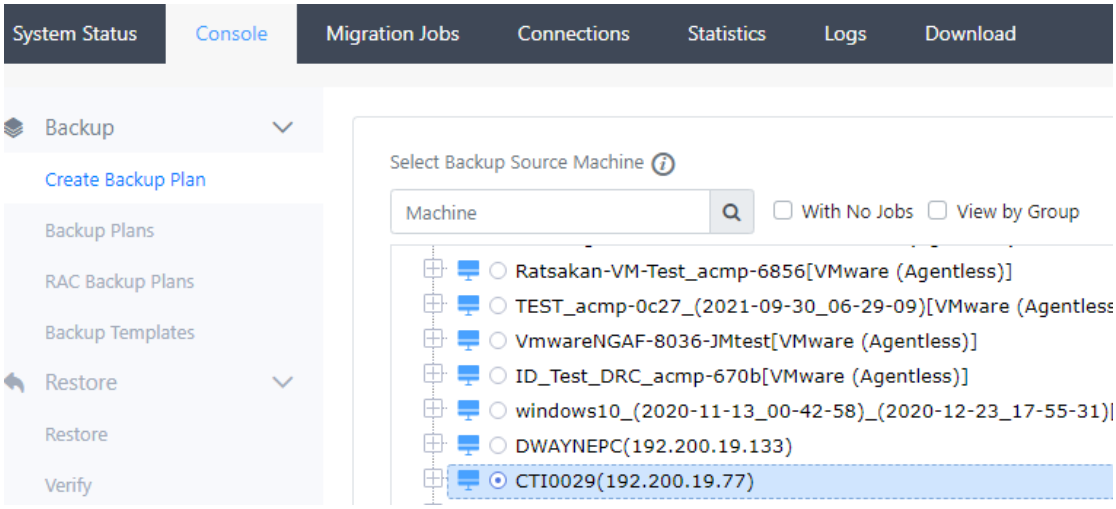
Guide to back up the source data to the Sangfor Cloud Migration Platform through the agent plugin.

5.4.1.1 Precautions

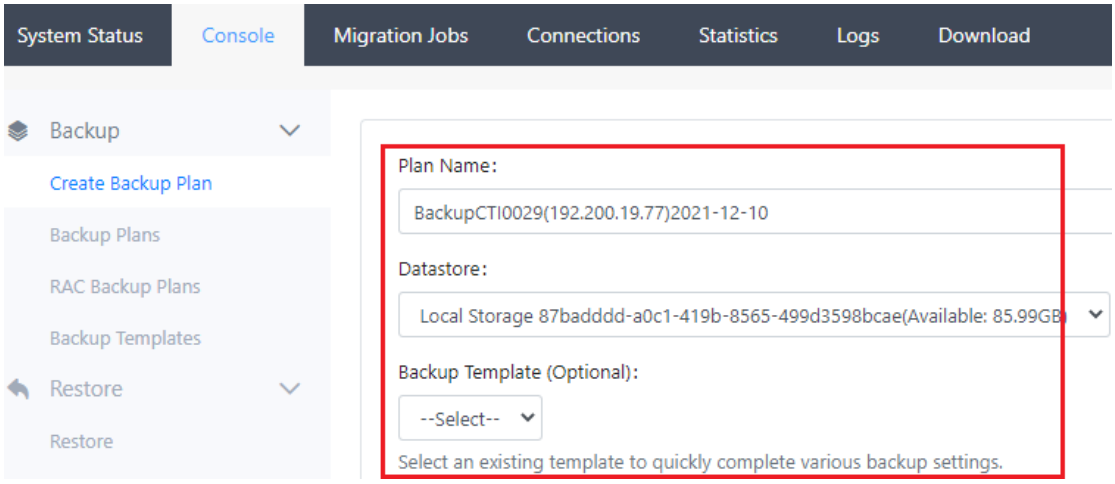
1. The disk will configure as dynamically allocated by default when migrating from the source. If the amount of data exceeds 8T and exceeds the size limit of the dynamically allocated disk, you need to manually enter the destination side to modify the disk type to thin provisioning.
2. It does not support migrating data from one disk on the source side to multiple disks on the destination side.
3. It supports external storage migration with mounted partitions and does not support the migration of bare dictionaries without file system partitions.
4. File storage mounted on the source host is not supported for migration.
5. The source plug-in installation and destination machine preparation must be completed before migration.

5.4.1.2 Steps

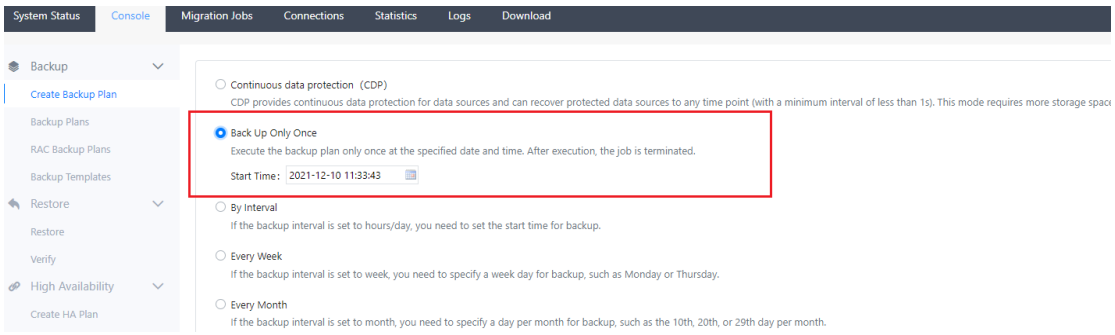
Step 1. Use the system administrator to log in to the migration platform, and in the **Console > Create Backup Plan** interface, select the source to be migrated (the client plug-in has been installed) and click **Next**.



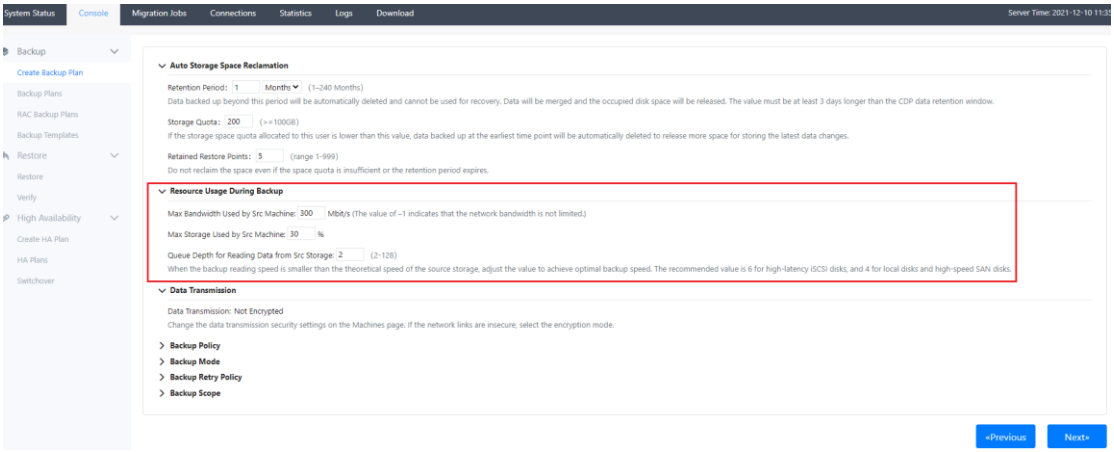
Step 2. Fill in the name of the plan and select the backup destination storage. The backup strategy can leave it blank for the time being. Click **Next** to configure the backup strategy.



Step 3. Select the backup strategy. The proxy backup migration usually selects **Back Up Only Once**, click **Next**.

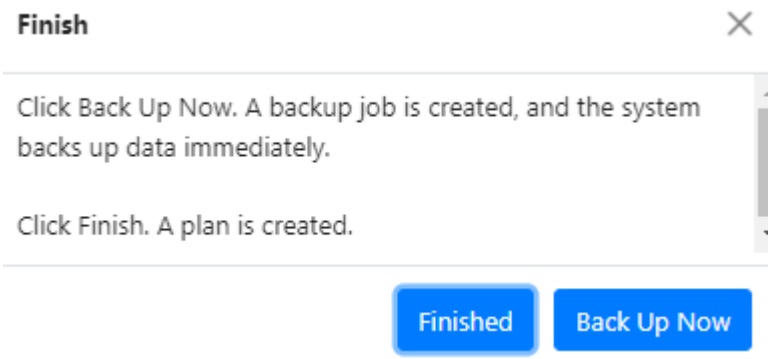


Step 4. Configure the backup details. Here, the backup rate is limited by default. If the rate is not required, modify the **Resource Usage During Backup** to **-1** and **100**. Click **Next**.

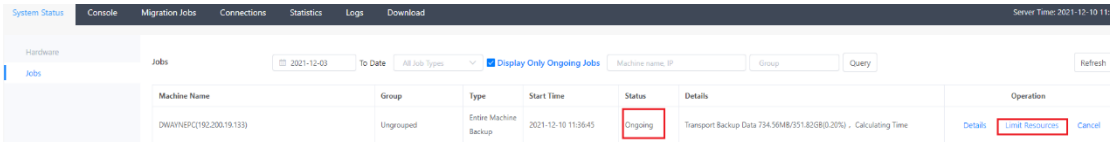


Step 5. Skip the **Backup Execution Script**.

Step 6. Enter the last step to confirm the information, click **Finished** or **Back Up Now** to start the first backup.



Step 7. Enter **System Status > Jobs** to see the progress of the backup, and click **Limit Resources** to limit the speed of this backup task again.



Step 8. Wait for the backup to complete.

5.4.2 Supplement and Migration

Function Description

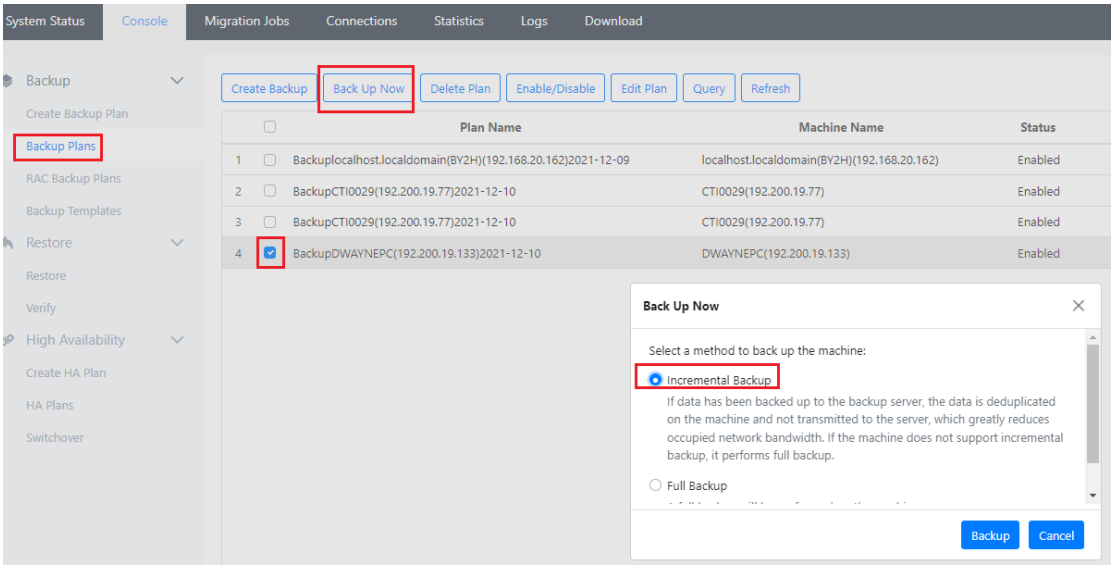
Guide the migration of backup data to the destination machine through recovery.

5.4.2.1 Precautions

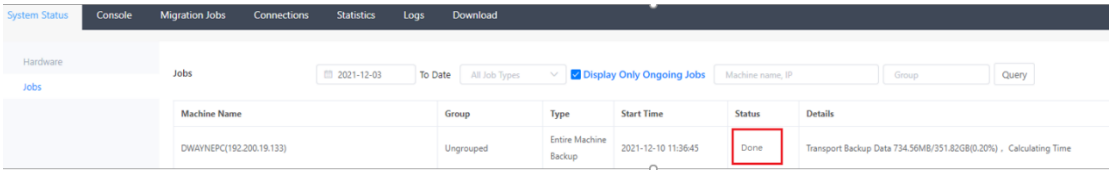
1. Complete the operations in the **First Full Backup** chapter.
2. When the business is allowed to be interrupted, stop the business (close the service and do not shut down the source system), and carry out the supplementary and recovery actions.

5.4.2.2 Steps

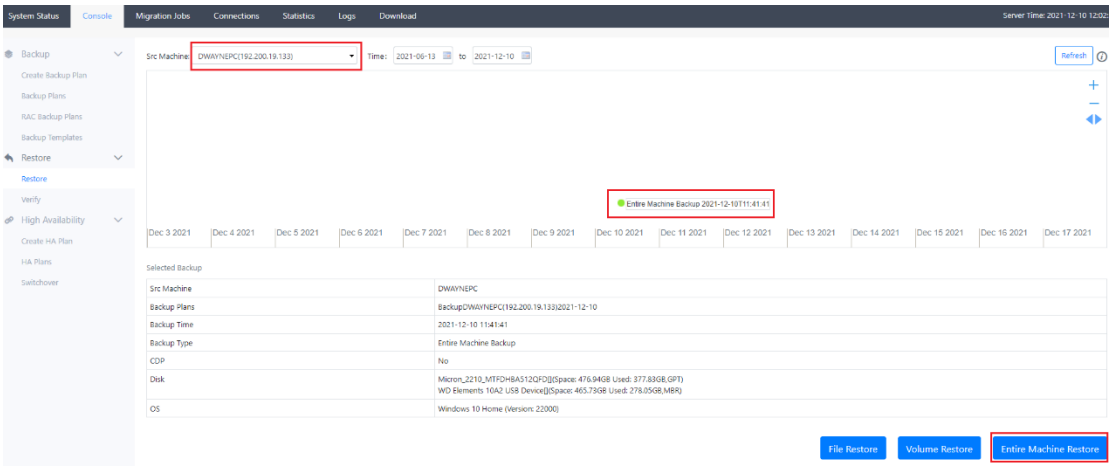
Step 1. After the first full amount of data is completed, stop the business(close the service, do not close the source system) within the period when the business is allowed to be interrupted. Enter the **Console > Backup Plans** interface, find the backup task, and click **Incremental Backup**.



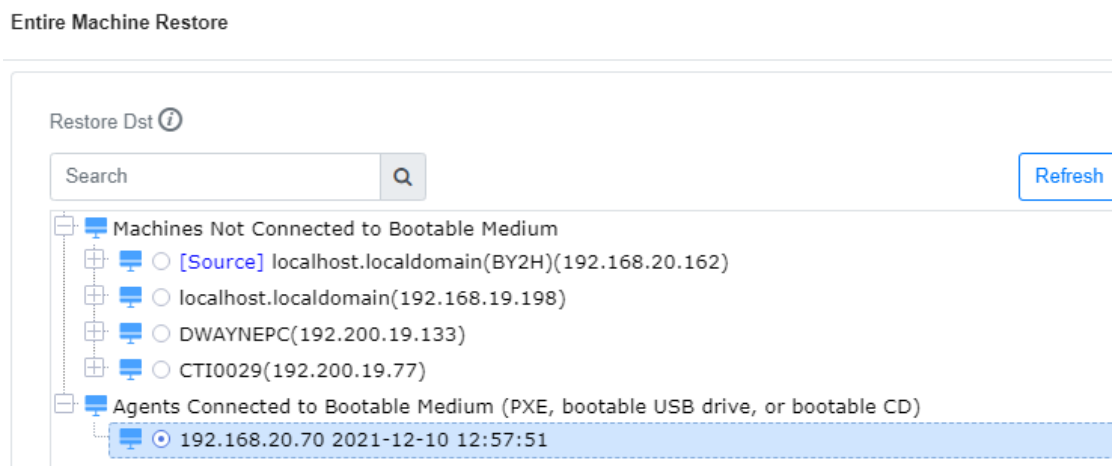
Step 2. Enter the **System Status > Jobs** interface and check the status of the incremental backup task.



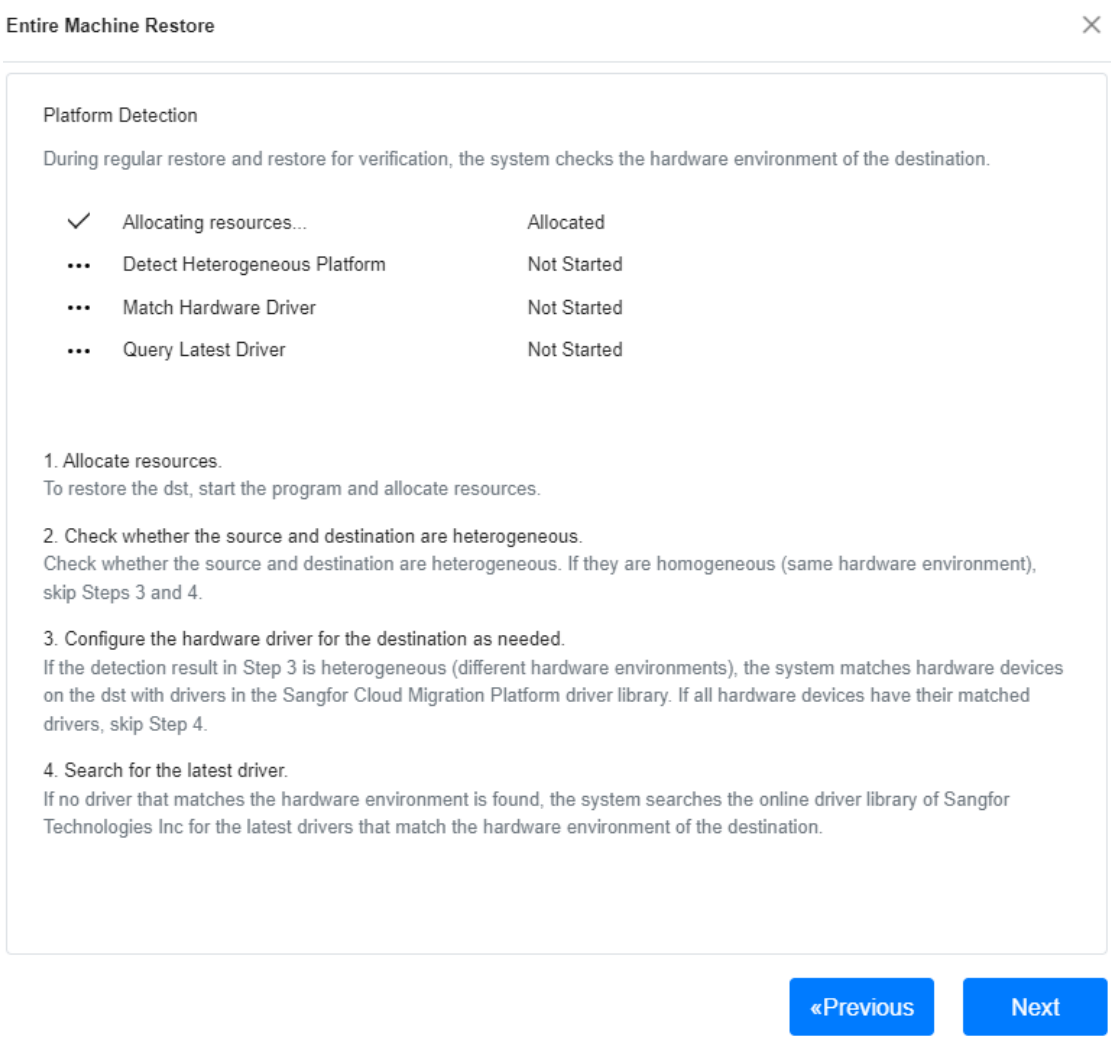
Step 3. Enter the **Console > Restore** interface, select the **Src Machine** to be migrated, select the latest backup point, and click **Entire Machine Restore**.



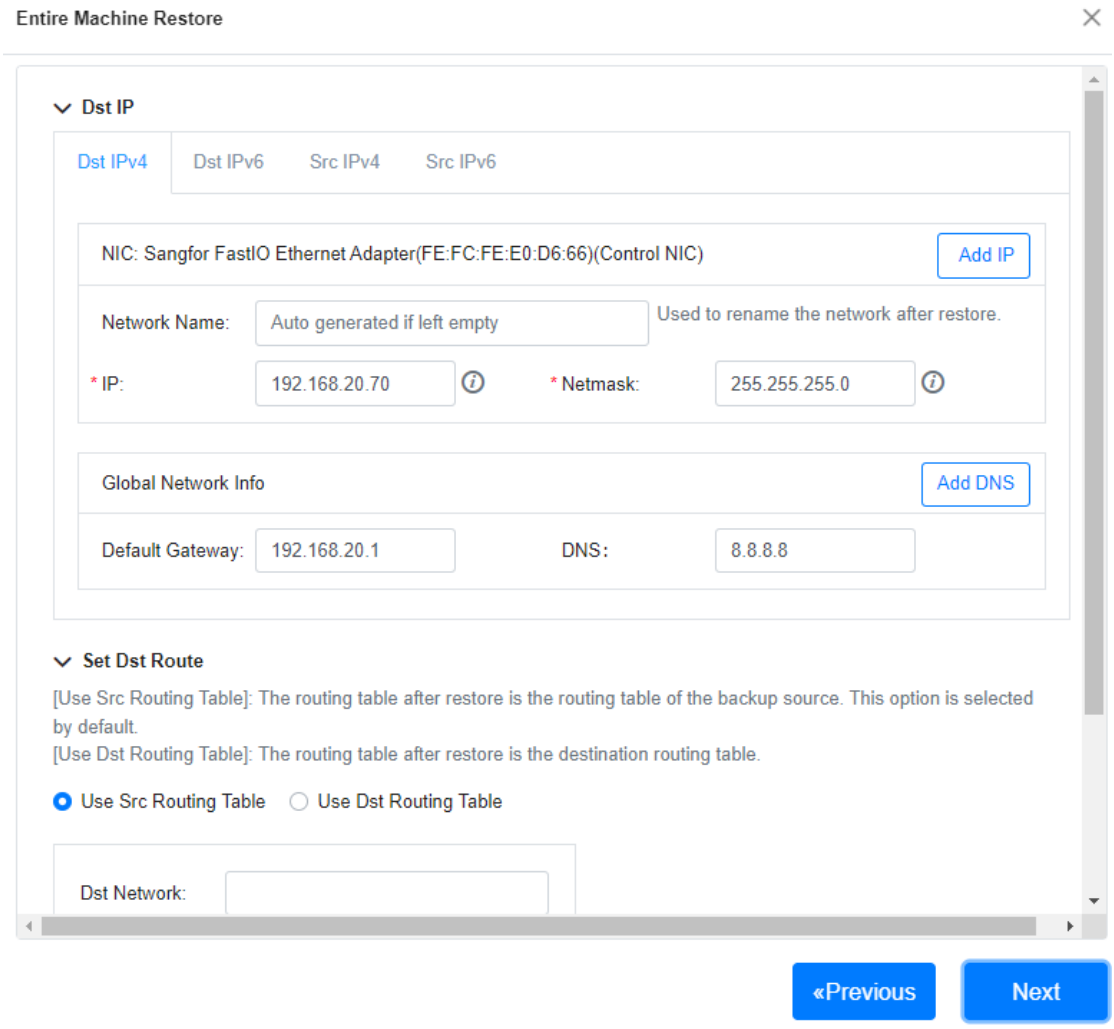
Step 4. To restore the destination, select the prepared destination machine and click **Next**.



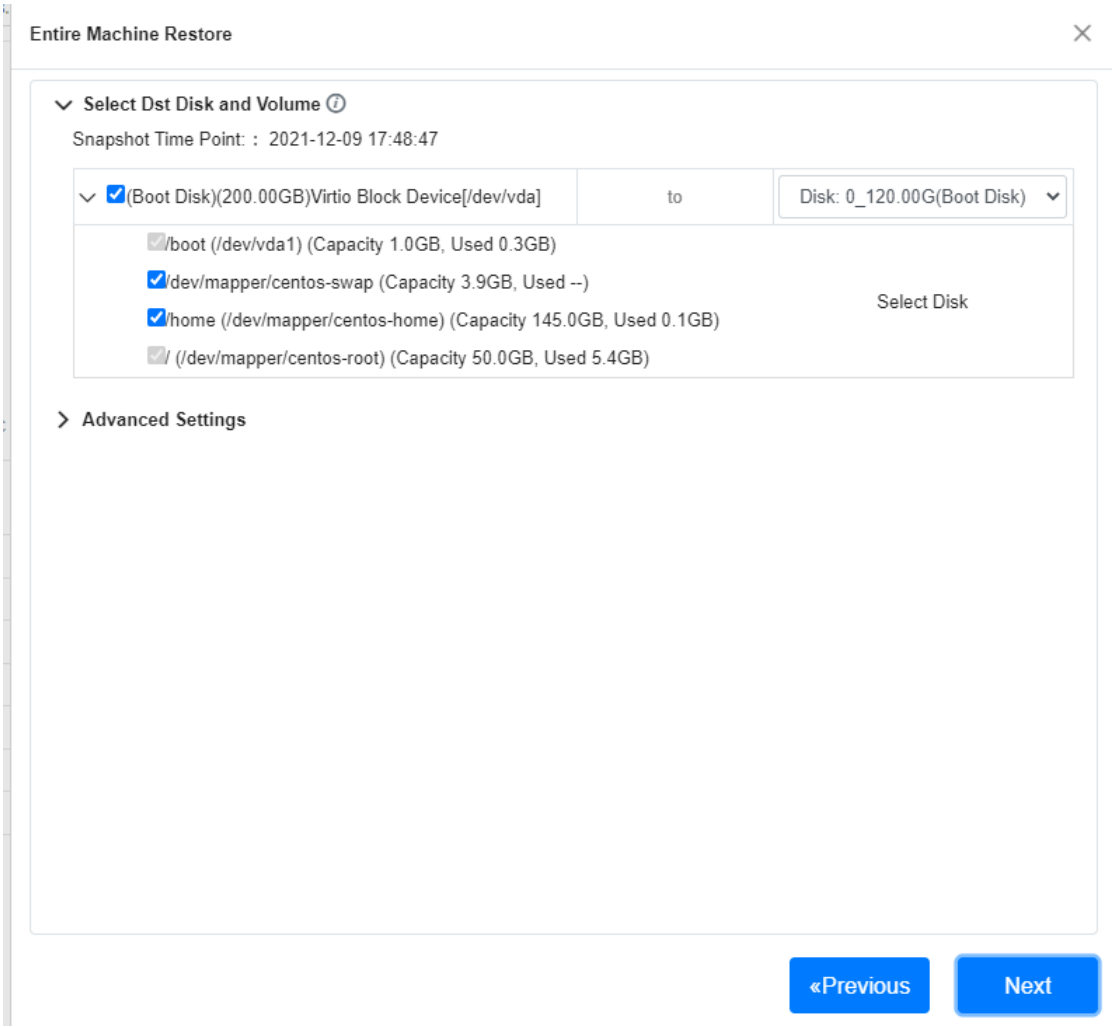
Step 5. Check whether resources, drivers, tools, etc., meet the migration conditions.



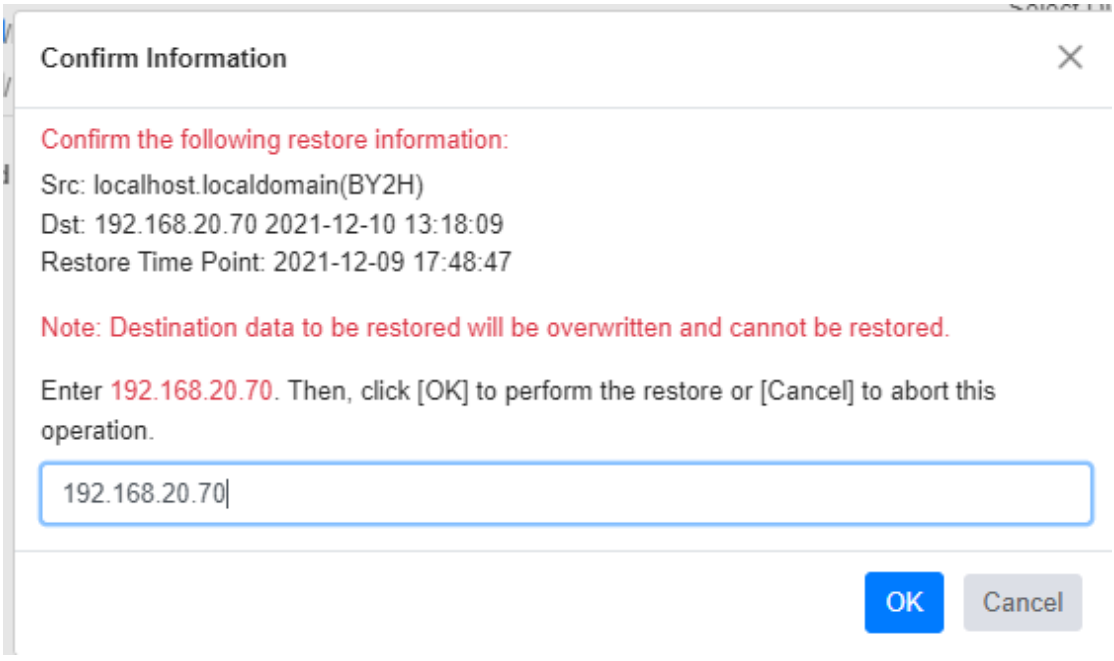
Step 6. After the checking is completed, it will automatically proceed to the next step, configure the migrated network information, including the IP address and gateway, etc. If not configured, the operating system will default to the IP address of the bare metal restore boot medium after recovery. Click **Next**.



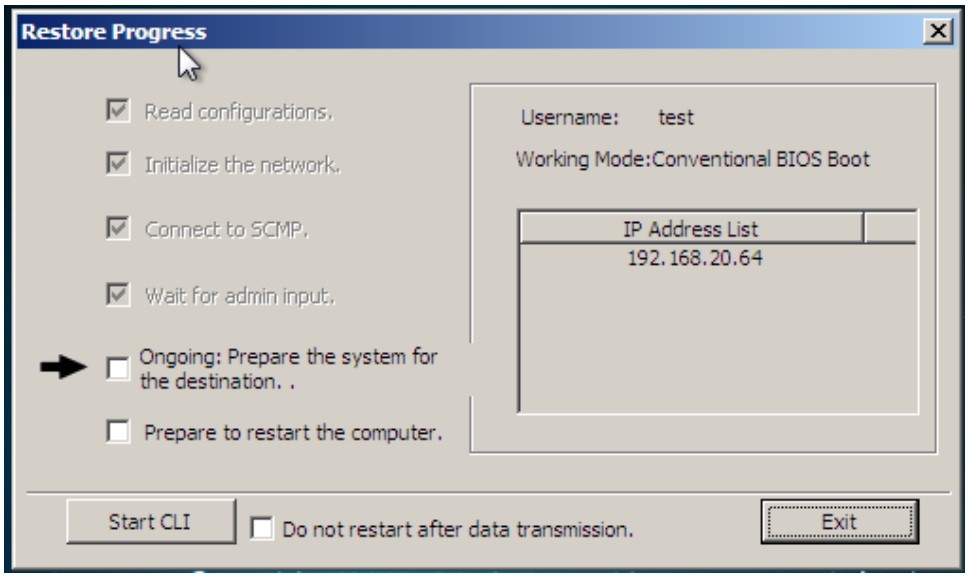
Step 7. Confirm the restored disk and partition information. The number of hard disks of the destination machine must not be less than the number of hard disks of the source machine, and the capacity of each hard disk of the destination machine must not be less than the hard disk capacity of the source machine.



Step 8. Enter the IP address to start the migration.



Step 9. Enter the destination machine console to view the status, and it displays **Ongoing: Prepare the system for the destination...**



Step 10. After the migration is completed, the destination machine will restart automatically and boot into the operating system. The migration process and status can be tracked under **System Status** > **Jobs**.

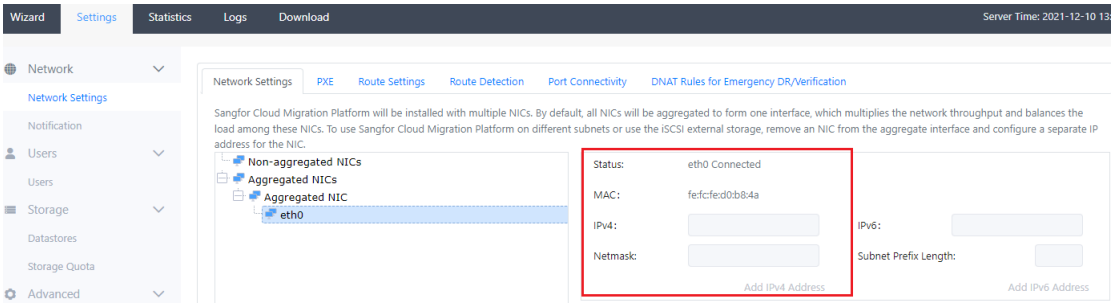
Step 11. After the migration is completed, enter the destination machine for production verification. If the operating system of the source machine is a Linux system and the boot mode is UEFI boot, it may start abnormally after migration. To solve it, you can refer to the fault case **UEFI Linux virtual machine cannot enter the system**.

6 Platform Operation and Maintenance

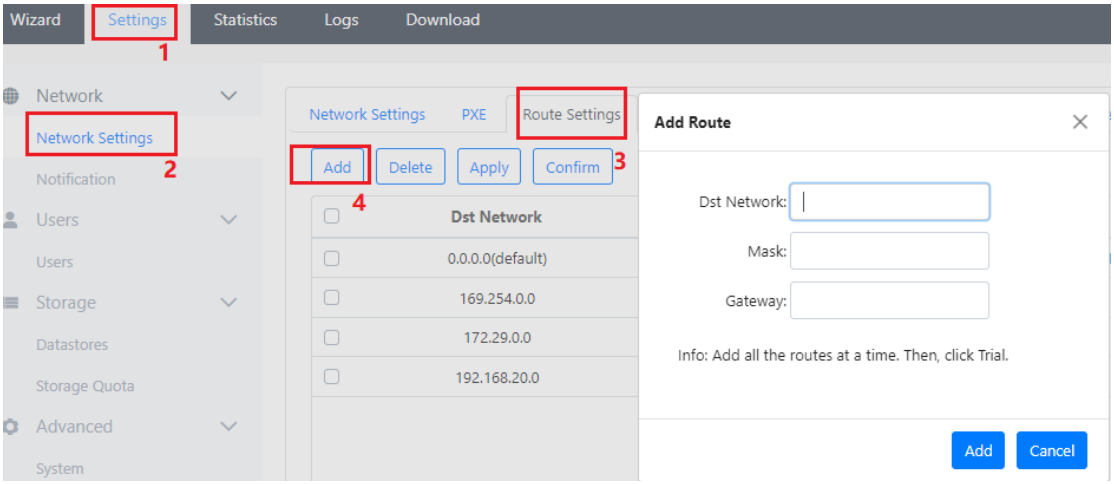
6.1 Network Management

6.1.1 Network Port Settings

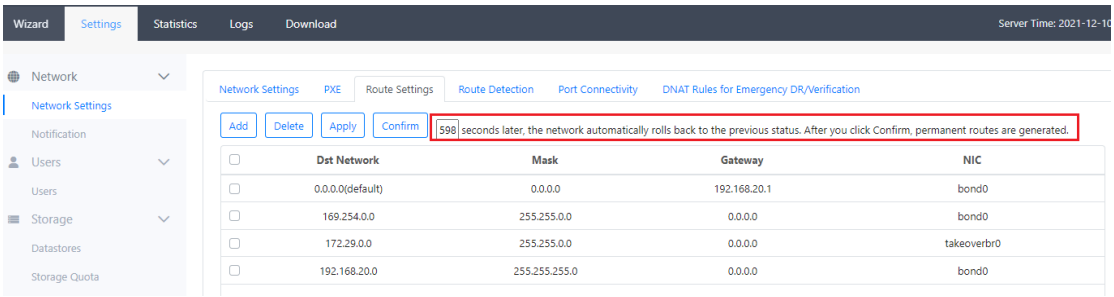
Step 1. Log in as the admin user and navigate to **Settings** > **Network Settings** interface of the Sangfor Cloud Migration Platform to configure and check the IP.



Step 2. Navigate to **Settings** > **Network Settings** > **Route Settings**, and add a new route accordingly. If the gateway needs to be configured, fill in with all 0 as the default route.



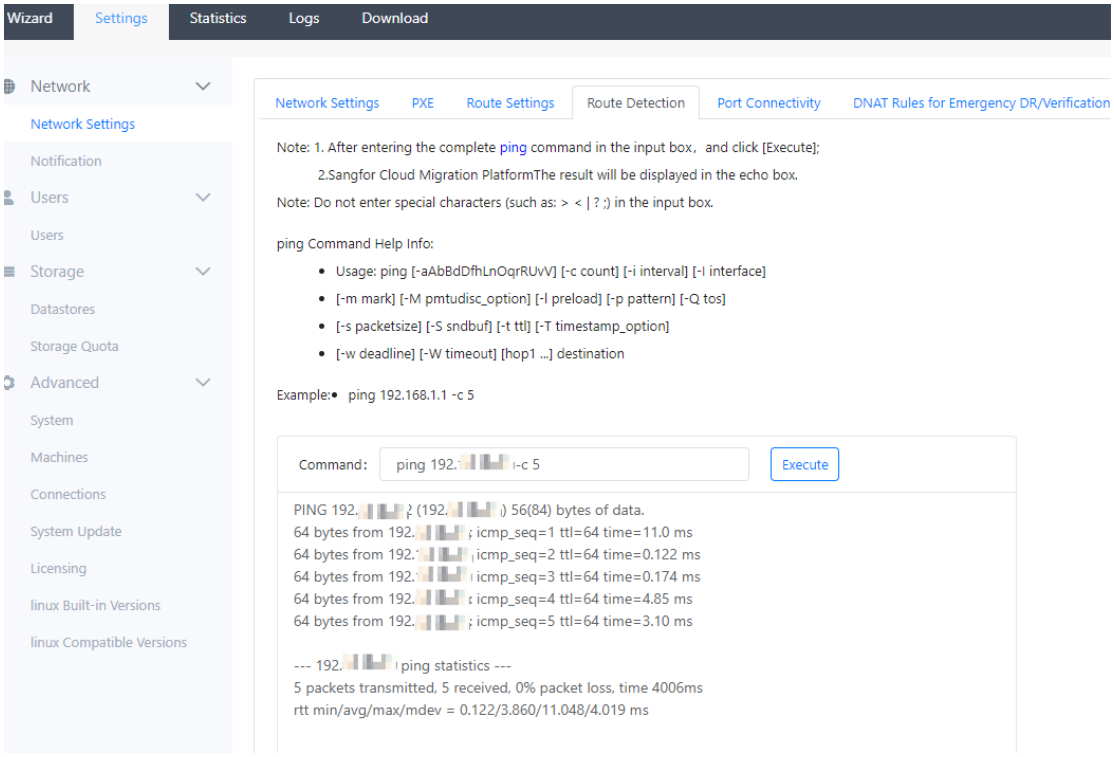
Step 3. Click the **Apply** button to perform a temporary trial on the configured routing entry. If you do not click **OK** within 10 minutes, the network will automatically roll back to the previous state. Click **Confirm** to generate a permanent route.



6.1.2 Route Detection

The route detection function is used to detect the connectivity between the Sangfor Cloud Migration Platform and the migration source host for ease of troubleshooting. Log in as the admin user, navigate to **Settings** > **Network**

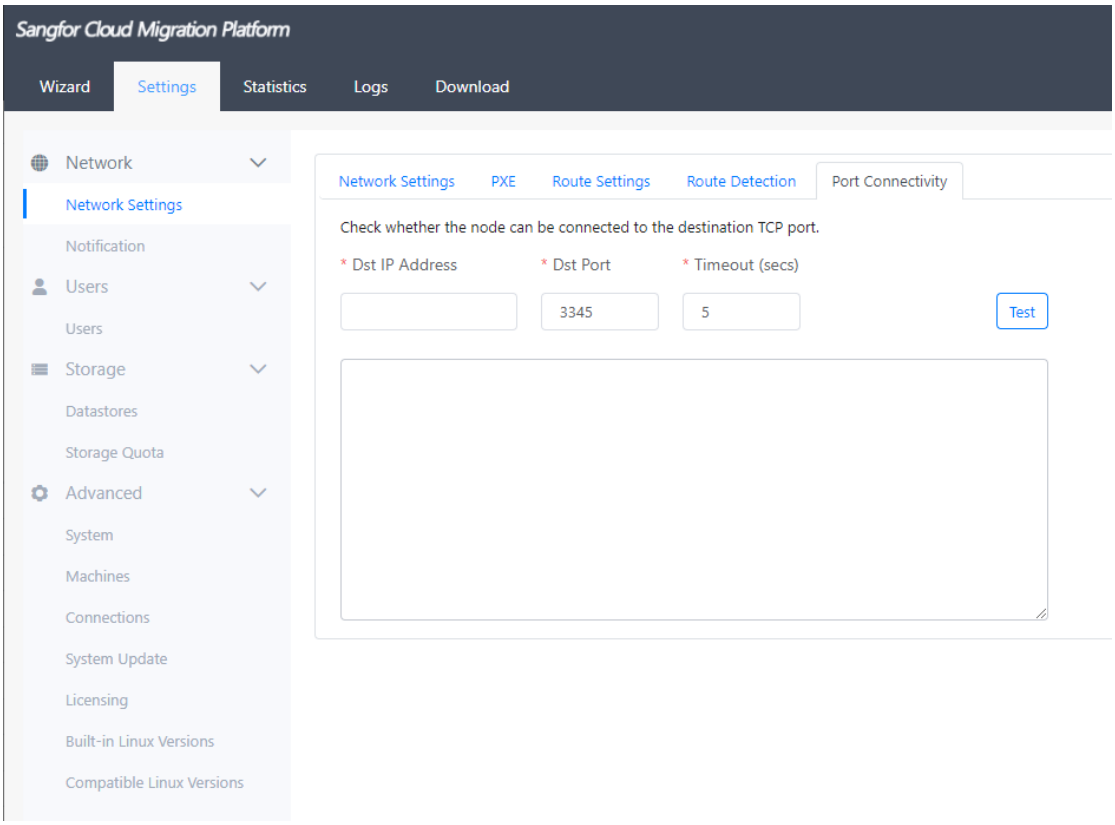
Settings > **Route Detection**, and enter the ping command in the command box to perform routing detection.



6.1.3 Port Connectivity Detection

Port connectivity detection is used to detect the port connectivity status of the Sangfor Cloud Migration Platform and the migration source host. It is mainly used for the passive connection mode of the migration client and detects whether the port of the migration client is open.

Log in as the admin user, navigate to **Settings** > **Network Settings** > **Port Connectivity** of the Sangfor Cloud Migration Platform, enter the Destination IP address, Destination Port, and timeout period, and click **Test**.

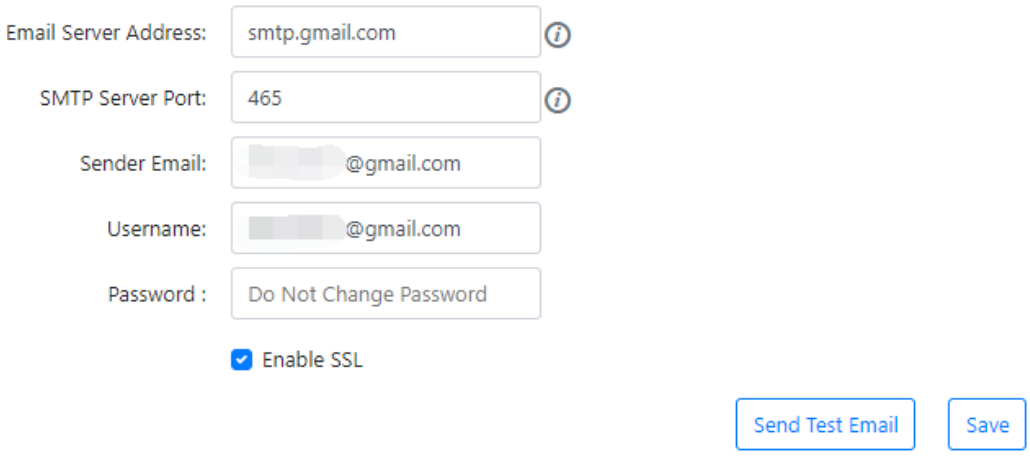


6.2 Message Notification Settings

6.2.1 Email Server

The email server can retrieve forgotten passwords and notify the execution results of various tasks, errors, and other important information to the users.

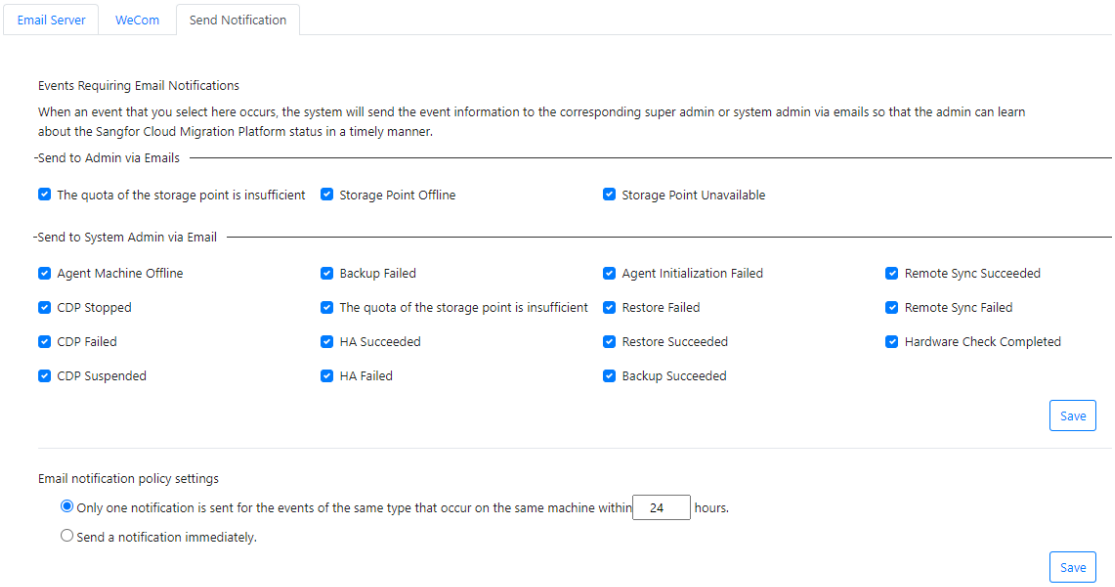
Set up the email server to ensure that it is reachable from SCMP. Verify that the **Sender's Email, Username ,Password** is valid. Click **Send Test Email** to verify the function.



- **Email Server Address: the server address of the sender email.** For example, google SMTP server **smtp.gmail.com**.
- **SMTP Server Port**: The default SMTP port is 25. Change the port according to the SMTP server.
- **Sender Email**: Fill in the email address of the sender.
- **Username**: Fill in the username of the sender email.
- **Password**: Fill in the authorization code of the sender's email.
- **Enable SSL**: If the SMTP server uses Secure Sockets Layer (SSL), enable this function accordingly.

6.2.2 Alarm Event

Select the event scope of the alarm notification. When the following events occur, the related information of this event will be sent to the relevant super/system administrator account email so that the administrator can be notified about the working status of the SCMP in time.



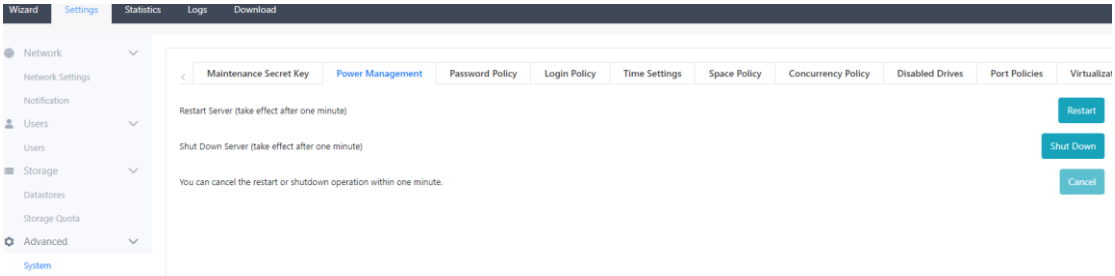
6.3 System Settings

6.3.1 Maintenance Secret Key

The background maintenance function of the node system adopts a dynamic code mechanism, and there is no fixed password account. The dynamic code comprises the device admin and the original factory codes. The original factory code changes with the password change operation of the device admin to prevent the disaster recovery system backend from being illegally logged in.

6.3.2 Power Management

Under **Settings** > **System** > **Power Management**, you can shut down or restart the Sangfor Cloud Migration Platform. Besides, the shutdown or restart operation could be canceled within one minute.



6.3.3 Password policy

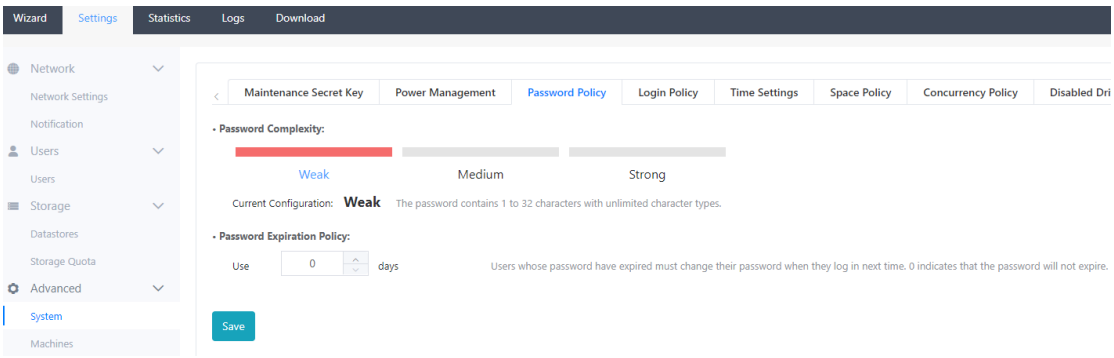
Under **Settings** > **System** > **Password Policy**, you can set the password strength and password expiration policy of the Sangfor Cloud Migration Platform.

Password Strength is divided into three levels: **weak**, **medium**, and **strong**.

- **Weak**: There is no limit to the type of password characters, and the password length is 1-32 characters.
- **Medium**: The password must consist of any three types of the following: uppercase letters, lowercase letters, digits from 0 to 9, and non-alphabetic characters such as tilde (~), exclamation point (!), at-sign (@), and pound sign (#). The password must contain 8 to 32 characters.
- **Strong**: The password must consist of uppercase letters, lowercase letters, digits from 0 to 9, and non-alphabetic characters such as tilde (~), exclamation point (!), at-sign (@), and pound sign (#). The password must contain 8 to 32 characters.

6.3.3.1 Password Expiration Policy

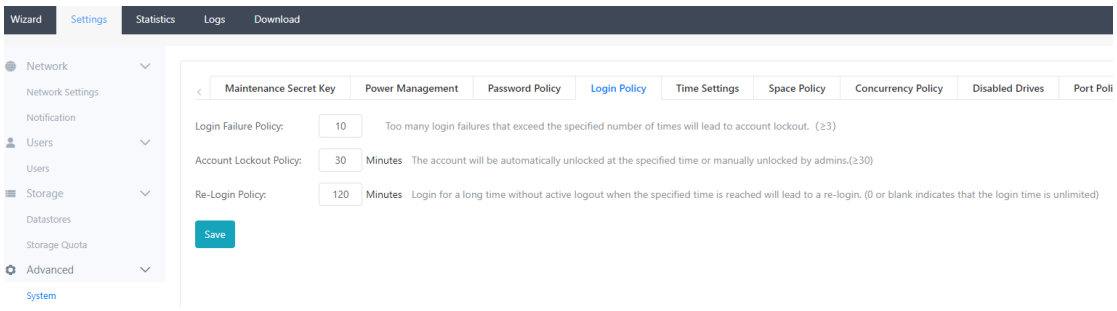
Users whose passwords have expired must change their password when they log in next time. 0 indicates that the password will not expire.



6.3.4 Login Policy

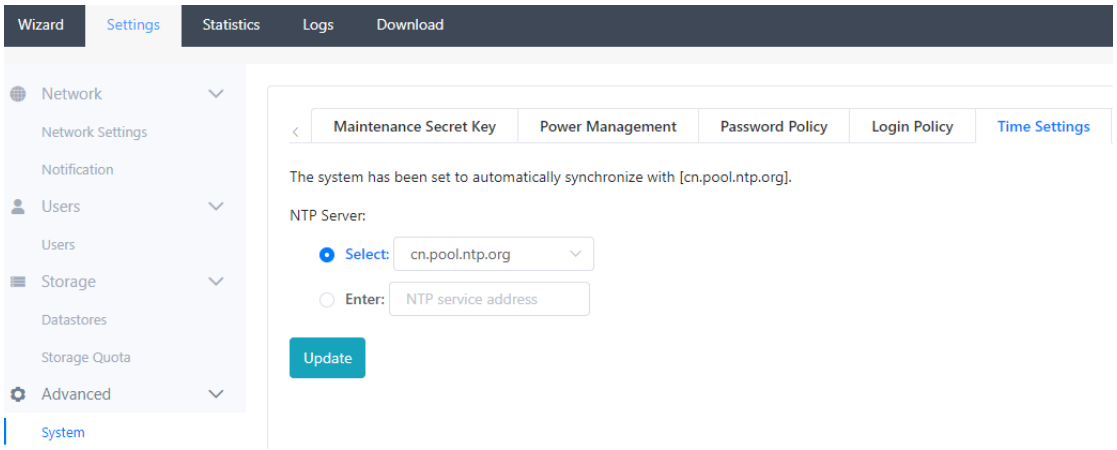
In the login policy of **Management Configuration > System Settings**, you can set the user login failure policy, account lockout policy, and re-login policy:

- **Login failure policy**: The account will be locked if the number of consecutive login failures exceeds the set times, which must be greater than or equal to 3.
- **Account Lockout Policy**: The time when a user's account is locked due to a failed login will be automatically unlocked according to the set time. You can also manually unlock it in user management. The set time must be greater than or equal to 30 minutes.
- **Re-login policy**: After logging in, if you do not actively log out after the set time, you need to log in again. (0 or empty means no limit).



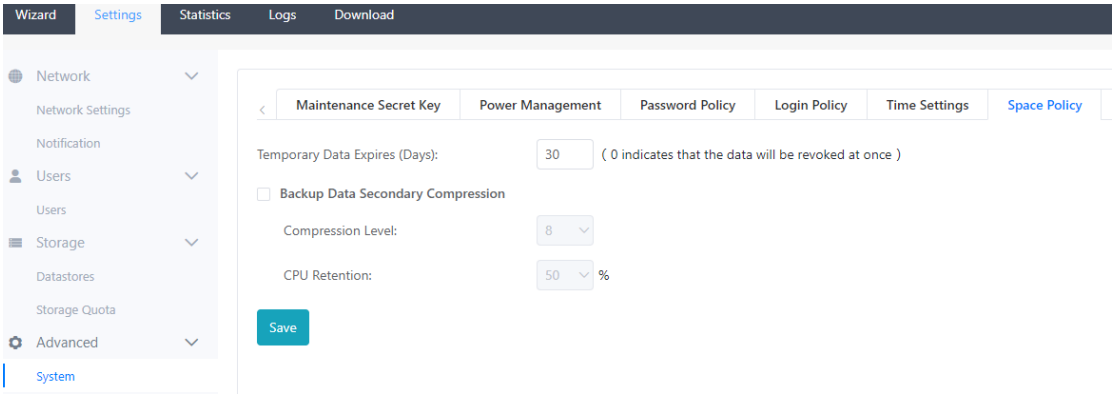
6.3.5 Time Settings

Configure the NTP server of the Sangfor Cloud Migration Platform under **Settings** > **System** > **Time Settings** for the time synchronization of the Sangfor Cloud Migration Platform. You can select the NTP server from the list or manually enter the NTP server of the intranet.



6.3.6 Space Policy

Under **Settings** > **System** > **Space Policy**, set the expiration days of temporary data and the second compression of backups. It is recommended to keep the default.



6.3.7 Port Policy

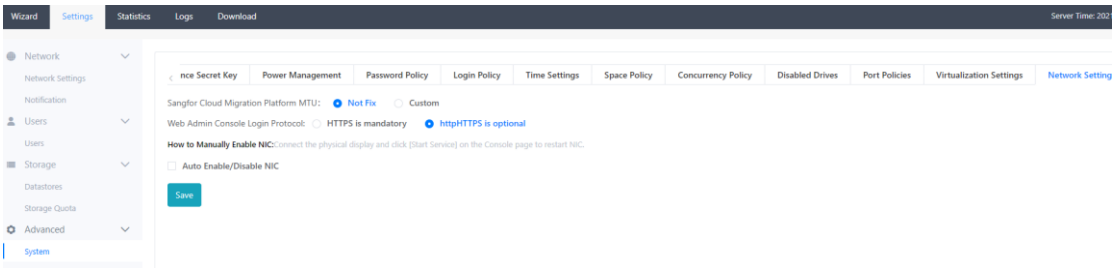
Under **Settings** > **System Settings** > **Port Policy**, configure the open ports of the SCMP.

If the WEB access port is closed and the port cannot be enabled through the WEB, connect the monitor to the server and select the **Enable WEB Service Port** function on the console interface to enable the Web access port.

Port name	The port number
SSH Port	22
Backup/Restore port	20000-20002
Web Access Port	80,8000,443
VNC port	20004, 20005
VM VNC port	6100-6611
FTP Port	21,30700-30900

6.3.8 Network Settings

Under **Settings** > **System** > **Network Settings**, set the **Sangfor Cloud Migration Platform MTU** and the **Web Admin Console Login Protocol**. It is recommended to keep the default settings.



SANGFOR