NexaVM Migrate Suite

Quick Start Guide

Version 688

Contents

1 Overview

NexaVM Migrate Suite is a hybrid cloud migration platform developed specifically for the nCSSV cloud platform and nSSV. It supports various migration scenarios, including P2V, V2V, local to local, and Cloud to Cloud, whether migrating from local to cloud or cloud to local.

This guide describes how to install NexaVM Migrate Suite and set up a migration from VMware or from another virtualization platform, including Sangfor, Nutanix, Hyper-V, Proxmox, Syneto, and OpenStack

2 Software Components

- **Management Node (Server):** Responsible for managing the entire data migration process, including lifecycle management of target endpoints, synchronization tasks, and migration cutover. For deployment convenience, the management node incorporates data gateway functionality and can directly use its image as a data gateway.
- **Data Gateway (Treker):** Performs two roles: data relay and data reception. In standard mode, it receives data from the source and transmits it to target host disks. In mounted disk mode, it acts as a receiver, simultaneously mounting multiple target disks and enabling them on-demand when the target environment is ready. This approach is ideal for scenarios where target network environments are activated only during cutover. Multiple gateways can be deployed for large-scale migrations to accelerate progress.
- **Antenna Agent (TrekerLite) for Windows/Linux:** Records IO changes on the source machine and executes synchronization and protection procedures to the target platform.
- **Target Endpoint (Target):** The destination platform for data migration, typically a virtualization or cloud platform in standard mode, a data gateway in mounted disk mode, or a BootImage target machine in PE mode.
- **Source Endpoint (Source):** The origin of data migration, which can be virtual machines or physical hosts.

3 Software Download

File	Function
win-server-2019-standard.qcow2	Windows Data Gateway, including a management console program. It contains a client and a BootImage.
linux_treker_688.mdrs.nexavm.qcow2	Linux Data Gateway, including a management console program. It contains a client and a BootImage.
BootImage_for_Linux_TrekerLite_688.qcow2	Linux base image for creating target hosts, used for system conversion by overwriting source machine data
BootImage_for_Windows_TrekerLite_688.qcow2	Windows base image for creating target hosts, used for system conversion by overwriting source machine data
Agent_for_Linux_Antenna-10.0.614.20250506.tar.gz	Agent for Linux (antenna)
Agent_for_Windows_Antenna_688.exe	Agent for windows (antenna)
LinuxConverter_685.exe	Convert Linux system, works with Windows Gateway Server

4 Network Requirements

To ensure the migration works:

Enable DHCP

Create on NexaVM a distributed port group with DHCP and limited available IP resources enabled.

Open the TCP ports

Ports	Purpose
TCP:443	Access control console and data protection process
TCP:20443	Optional to replace 443
TCP:20000	Protection and internal management
TCP:20001	Encryption management
TCP:20005	Source connection
TCP:20010	Data communication control

Network ports detailed for components

Components	TCP Port
Management Server / Treker Server	20000, 20001, 20010, 443, 20443, 3389, 50022
Source Host (Antenna Agent)	20005
Target Instance (Trekerlite)	20000, 20001, 50022
VMware (Agentless Mode)	443, 902

Registration Methods

- **RPC Connection (Active Registration):** Bidirectional connectivity between the management server and the registered resource. The registration starts from the management server.

- **HTTPS Connection (Reverse Registration):** Unidirectional connection from the host agent or Treker to the management server IP. The registration starts from the agent or Treker. Must specify the management port: 443 or 20443.

5 Architecture

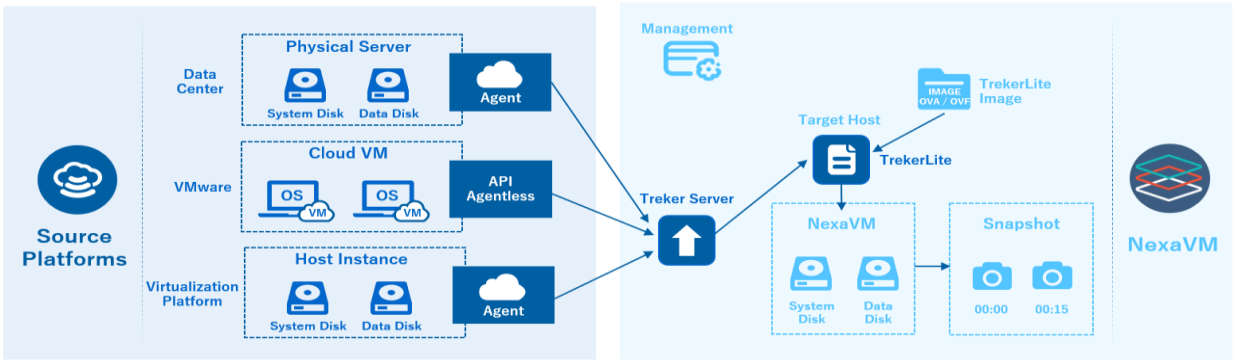
Use Cases: Online entire-machine or large-block disk migration.

Scenarios: Supports V2V and P2V with source host running Windows or Linux.

VMware Migration: Supports agentless migration via VADP replicating VMs from VMware.

Other Virtualization Platforms Migration / Physical: Agent-based; Agent tracks I/O, replicating to the target host created via TrekerLite.

Post-Migration: After the migration and cutover, the target host system will be identical to the source host system.



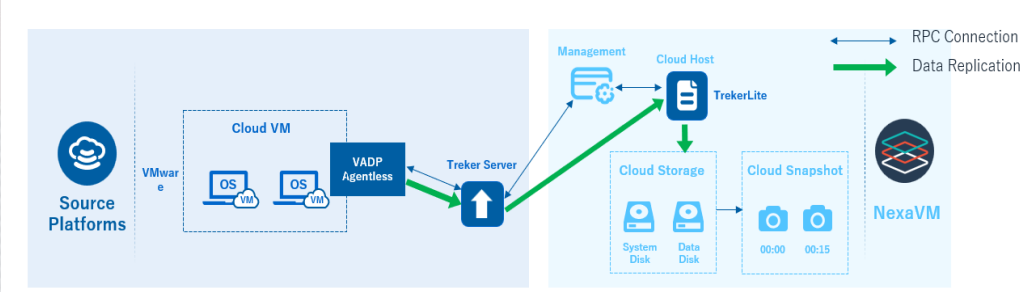
5.1 Architecture Example 1 – VMware Agentless Automated Image Mode

Scenarios & Features

Supports VMware as the source. The Treker is recommended to be deployed on the source side. Limited concurrent syncs in agentless mode, where each vCenter or ESXi can sync only one VM at a time by default. Supports multiple concurrent cutovers, suitable for projects with many migration tasks and minimal downtime. Relies on NexaVM DHCP network, and the target host must enable DHCP. If unavailable, use a DHCP network for sync and switch to a non-DHCP network at cutover.

Brief Steps

1. Install and configure the management server and Treker server.
2. Upload TrekerLite image to NexaVM (add UEFI & Legacy images separately).
3. Register NexaVM as the target cloud in the management console.
4. Register the Treker server in the management console as general-purpose server.
5. Register and add source VMware vCenter or ESXi as the target environment, associating it with the Treker.
6. Register and add VMware virtual machines as source hosts in the console.
7. Create the protection task. Once completed, a replica snapshot will be generated on the target.
8. Migration Cutover: Perform testing before executing the final migration.



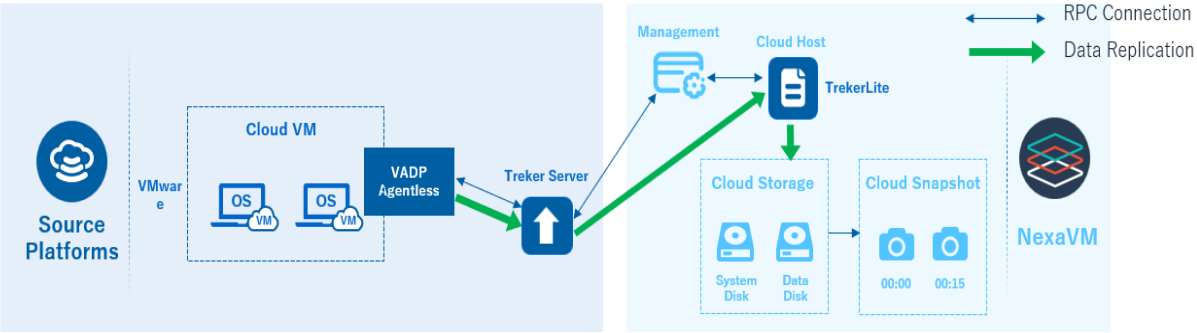
5.2 Architecture Example 2 – VMware Agentless Automated Server Mode

Scenarios & Features

Supports VMware as the source. The Treker is recommended to be deployed on the source side. Limited concurrent syncs in agentless mode, where each vCenter or ESXi can sync only one VM at a time by default. Supports multiple concurrent cutovers, suitable for projects with many migration tasks and minimal downtime. Relies on NexaVM DHCP network, and the target host must enable DHCP. If unavailable, use a DHCP network for sync and switch to a non-DHCP network at cutover.

Brief Steps

1. Install and configure the management server and Treker server.
2. Upload TrekerLite image to NexaVM (add UEFI & Legacy images separately).
3. Register NexaVM as the target cloud in the management console.
4. Register the Treker server in the management console as general-purpose server.
5. Register and add source VMware vCenter or ESXi as the target environment, associating it with the Treker.
6. Register and add VMware virtual machines as source hosts in the console.
7. Create the protection task. Once completed, a replica snapshot will be generated on the target.
8. Migration Cutover: Perform testing before executing the final migration.



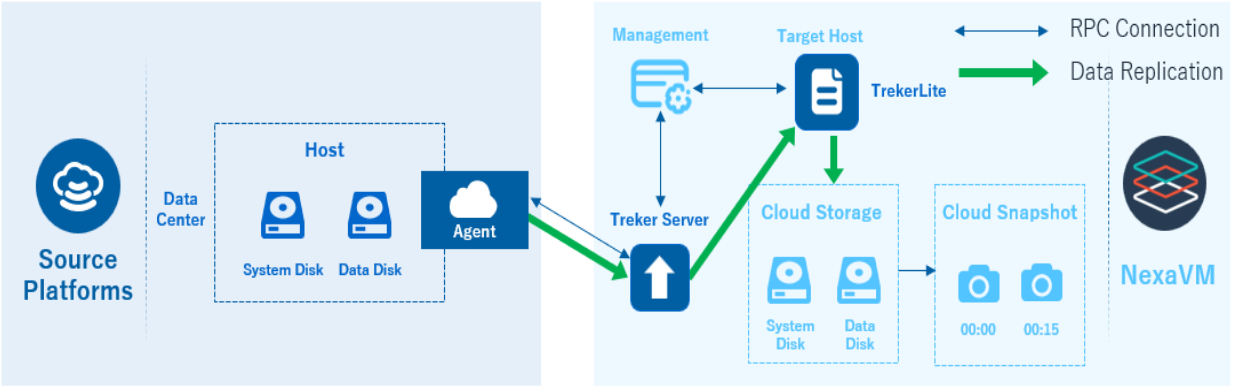
5.3 Architecture Example 3 – Agent-Based Automated Image Mode

Scenarios & Features

Supports various virtualization scenarios or P2V and requires installing a client agent on the source host. Relies on NexaVM DHCP network, and target cloud hosts must enable DHCP. If unavailable, use a DHCP network for sync and switch to a non-DHCP network at cutover. Unlimited concurrent agent-based syncs, ideal for large-scale, time-sensitive migrations. Supports multiple concurrent cutovers, suitable for projects with many migration tasks and minimal downtime.

Brief Steps

1. Install and configure the management server and Treker server.
2. Upload TrekerLite image to NexaVM (add UEFI & Legacy images separately).
3. Register NexaVM as the target cloud in the management console.
4. Register the Treker server in the management console as general-purpose server.
5. Install the client agent on the source host and register it on the management console, associating it with the Treker.
6. Create the protection task. Once completed, a replica snapshot will be generated on the target.
7. Migration Cutover: Perform testing using replica snapshot before executing the final migration cutover.



6 Server Deployment

The NexaVM Migrate server can be deployed on either Windows or Linux systems. Both versions offer the same functionalities, allowing users to choose based on their infrastructure requirements.

For deployment convenience, the management node incorporates data gateway functionality and can directly use its image as a data gateway.

6.1 Instance Requirements

Treker capacity: Each CPU core handles one concurrent migration process.

Small Scenario:

- **Management Node + Gateway Treker:** 8 cores CPU, 8GB RAM, 100GB OS disk (Windows Server 2012+ or Linux), plus 100GB data disk.

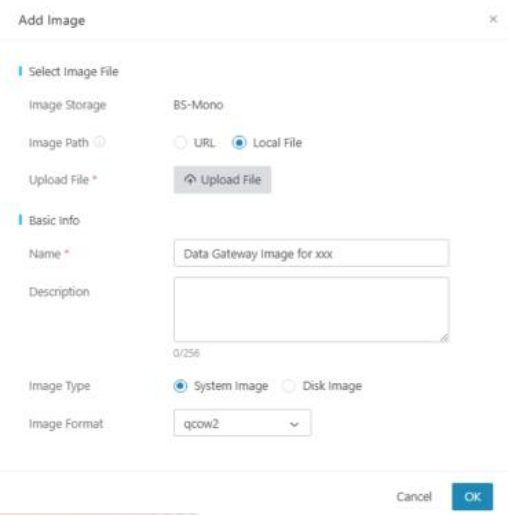
If migrating more than five hosts, it is strongly recommended to deploy the management server and Treker servers separately to avoid resource constraints. When necessary, a single server can be reused.

Recommended Specifications for Larger Deployments:

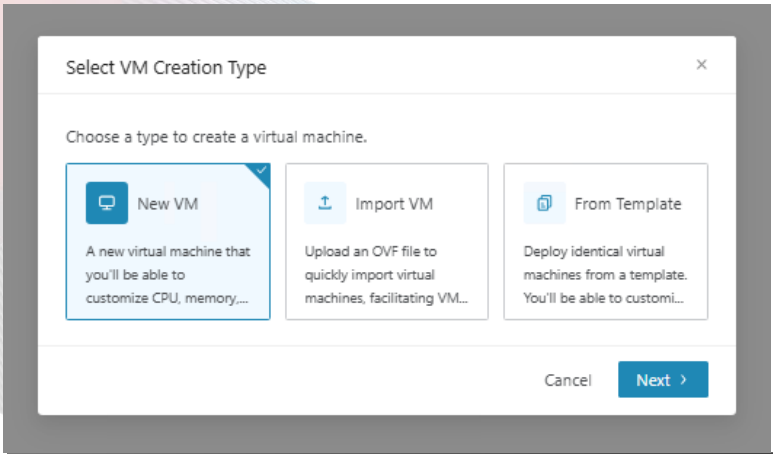
- **Management Node Server:** 4 cores CPU, 8GB RAM, 100GB OS disk (Windows Server 2012+ or Linux standard image).
- **Gateway Treker Server:** 8 cores CPU, 8GB RAM, 500GB OS disk (Windows Server 2012+ or Linux).

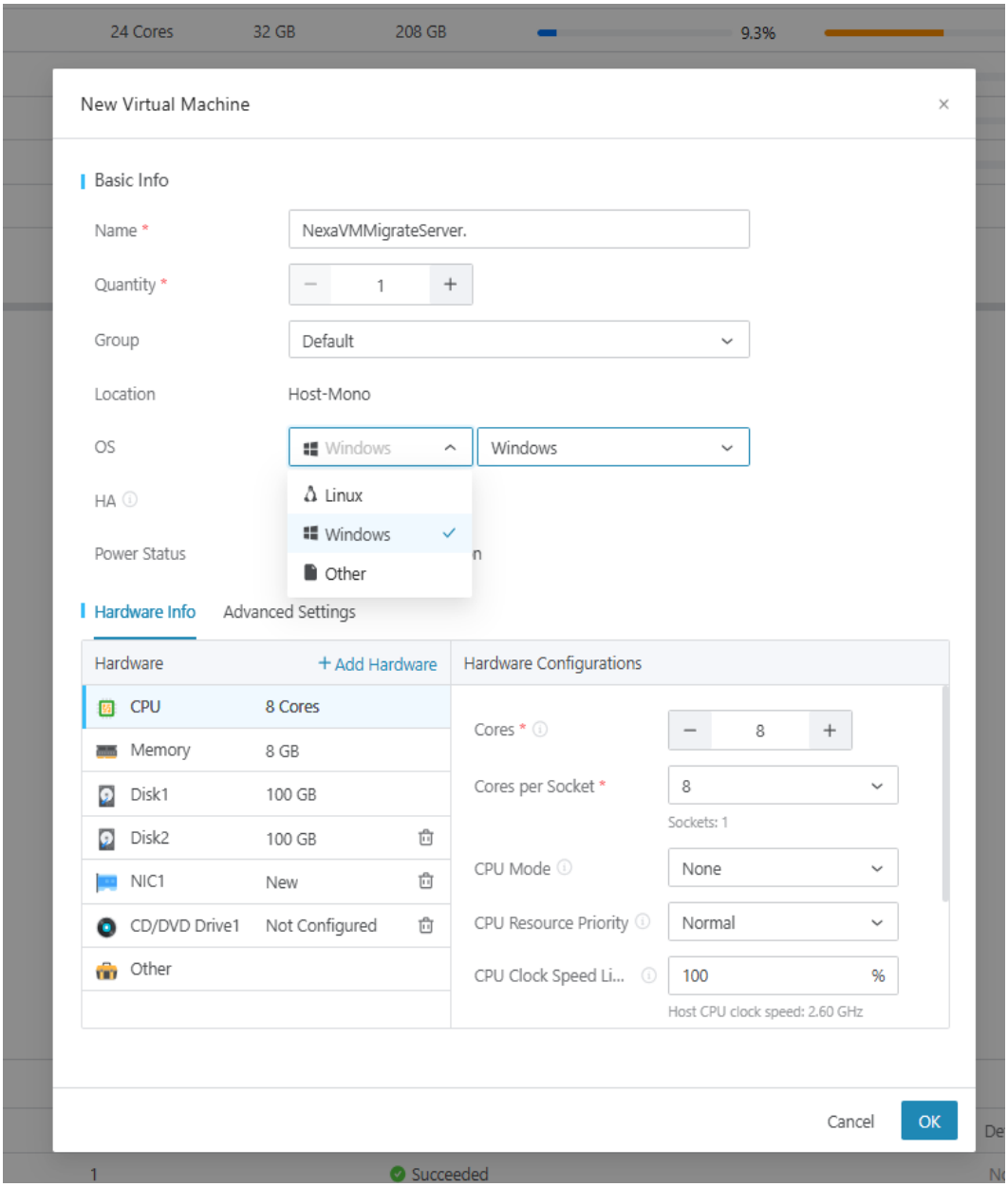
6.2 Install the Management Server on nSSV

Download the Data Gateway Image for Windows or for Linux, and import on the Image Datastore



Create the server instance using the image for the chosen operating system.

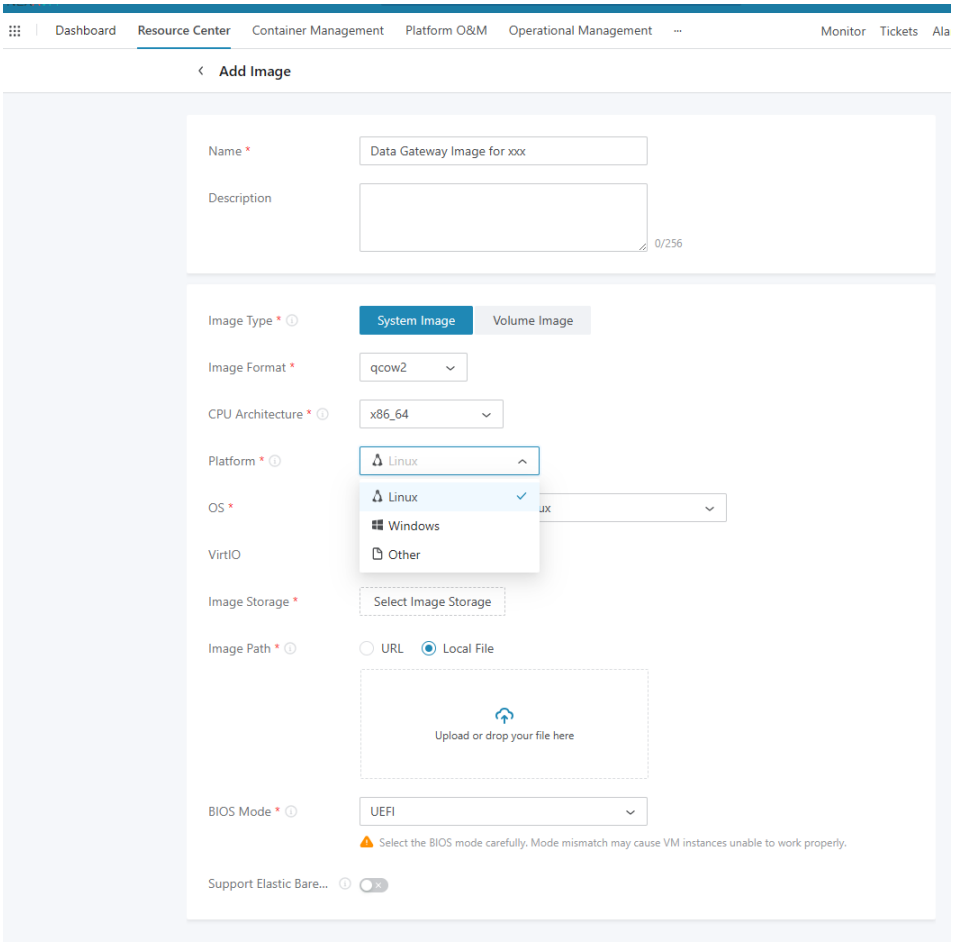




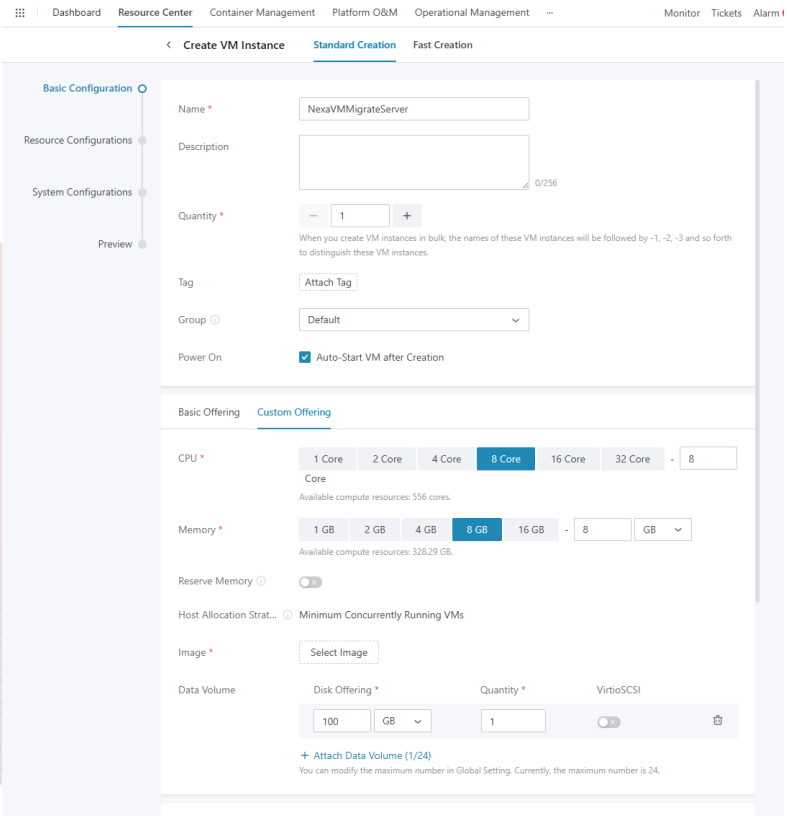
Connect the network with the DHCP previously defined.

6.3 Install the Management Server on nCSSV

Download the Data Gateway Image for Windows or Linux and import the image for the chosen operating system.



create the Server Instance



6.4 Upload Target Instance Image

The server image is required to create the target instance, which writes data to storage and performs system conversion during provisioning. It is essential for booting the target instance. Upon booting, the instance disk will be automatically configured to mirror the source, with an additional 5GB allocated for the operating system disk.

During the protection process, the appropriate boot type for the image is automatically selected.
Download the following files:

- BootImage_for_Linux_TrekerLite_xxx.qcow2
- BootImage_for_Windows_TrekerLite_xxx.qcow2

On the NexaVM nSSV or nCSSV portal, navigate to Image and click on Add Image. Upload both files to Image Storage via the NexaVM Cluster UI.

6.4.1 Linux Target Instance Image Required Parameters (RECOMMENDED METHOD):

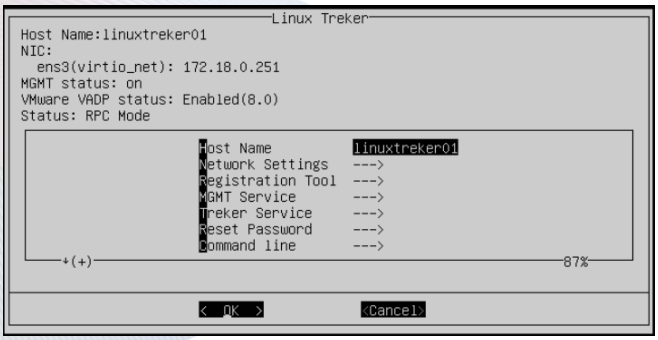
This is the **recommended approach for Linux migrations** (as opposed to the Windows method).

Image Configuration Parameters:

- **Name:** Display name of the image (e.g., MigrateServerLinux)
- **Description:** MUST enter "TrekerLiteImage"
- **Image Type:** System Image
- **Image Format:** qcow2
- **CPU Architecture:** x86_64
- **Platform:** Linux
- **OS:** Ubuntu/Ubuntu 22
- **VirtIO:** Enable
- **Backup Storage:** Select the preferred backup storage
- **Image Path:** Click Local File and upload the image
- **BIOS Mode:** Select Legacy BIOS or UEFI, depending on the source system type

Upload and Configuration Steps:

1. After entering the parameters, click **OK** to upload the image.
2. Navigate to nSSV or nCSSV and open the console of the MigrateServerLinux VM.
3. Login using the password: **admin**



4. Define the network parameters (DHCP or static IP as needed).

5. Keep the interface open—no further action is required at this stage.
6. Use the IP of one of the Gateways and continue using that to access the Migrate management console

6.4.2 Windows Target Instance Image Required Parameters:

This method is used for **Windows migrations**.

- **Image Configuration Parameters:**
- **Name:** Display name of the image (e.g., MigrateServerWindows)
- **Description:** MUST enter "TrekerLiteImage"
- **Image Type:** System Image
- **Image Format:** qcow2
- **CPU Architecture:** x86_64
- **Platform:** Windows
- **OS:** Windows/Windows Server 2012
- **VirtIO:** Enable
- **Backup Storage:** Select the preferred backup storage
- **Image Path:** Click Local File and upload the image
- **BIOS Mode:** Select Legacy BIOS or UEFI, depending on the source system type

Upload and Configuration Steps:

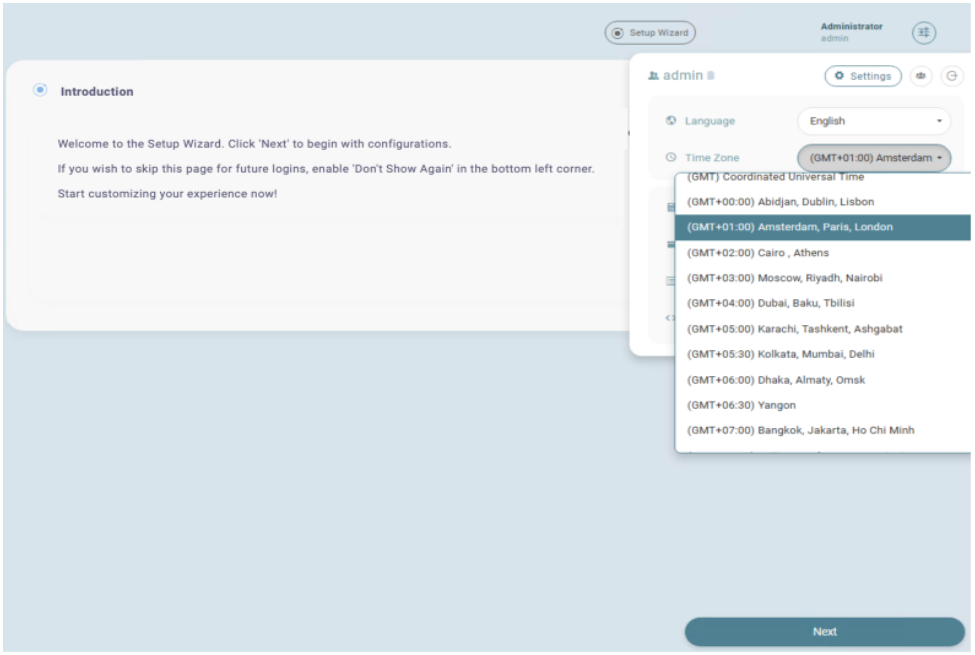
After entering the parameters, click **OK** to upload the image.

7 Login and Configure the NexaVM Migrate Server

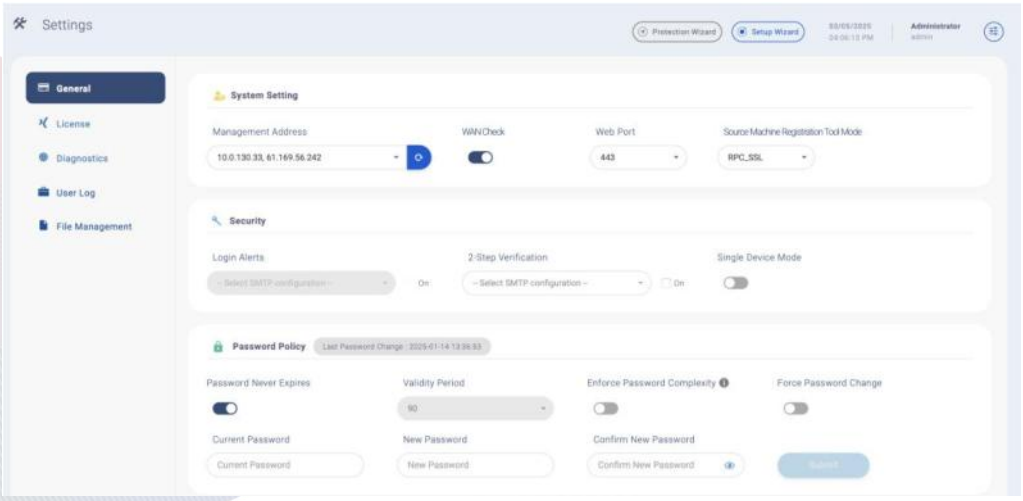
You can access the server where the management service is installed by entering the IP address or DNS name in a web browser. After logging in, the settings of the management console can be updated.

For the first login, enter the default username and password: admin/admin

1. Upon logging in, the Setup Wizard page will open, guiding you through essential configurations for the protection and provisioning processes. To prevent this page from appearing during future logins, check the “Don’t Show Again” option at the bottom left. The wizard can be accessed at any time by clicking the “Setup Wizard” icon in the top-right corner.
2. Click the settings icon in the upper right corner. During your initial login to the Management Console, begin with the basic configurations, including language, time zone, and UI display mode.



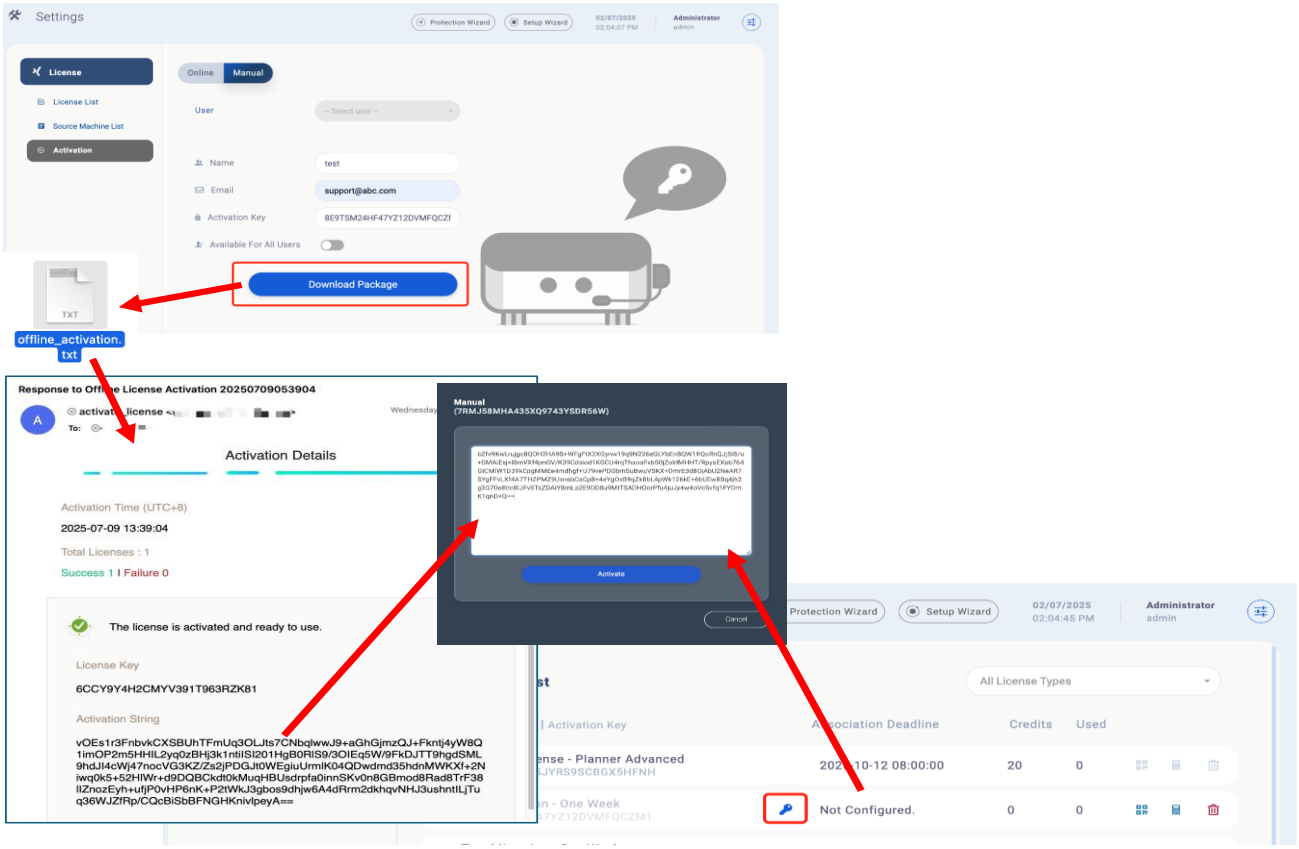
3. In the General settings, configure the "Web Port" option. The default web port is 443. However, if network security policies do not allow access to TCP:443, the TCP port can be changed to 20443. The "WAN Check" option determines whether to enable automatic scanning of the instance public IP address.



8 License Activation

Before executing any protection or provisioning process, licenses must be activated. Activating a license requires ensuring that the Management Console can access the internet and has the correct DNS settings to query the IP address of the activation server.

1. Login to the UI.
2. Select the License tab under the settings page and click on Activation.
3. Select the Manual tab under the License page and enter the license key.
4. Download the offline activation file: key_date.txt or offline_activation.txt.
5. Attach the offline activation file (.txt) to an email (multiple attachments supported) and send it to NexaVM.
6. Click the Key icon next to the license and enter the activation string.



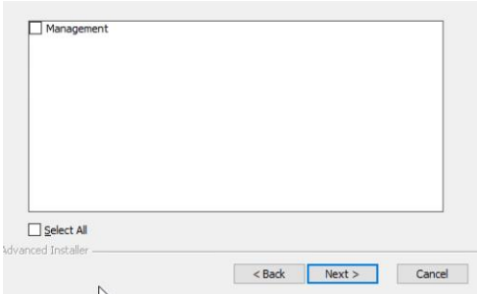
7. Once activation is successful, the manually activated license can be confirmed in the license list.

9 Source Server Deployment

The NexaVM Migrate server is designed for agentless access to VMware virtual machines. It can be deployed either as a standalone server or co-located with the management server, giving users flexibility to choose based on their specific requirements.

9.1 Source Server Installation - Windows

1. Run the server installation package TrekerInstallation_xxx.exe
2. Uncheck Management under Optional Features to Install.

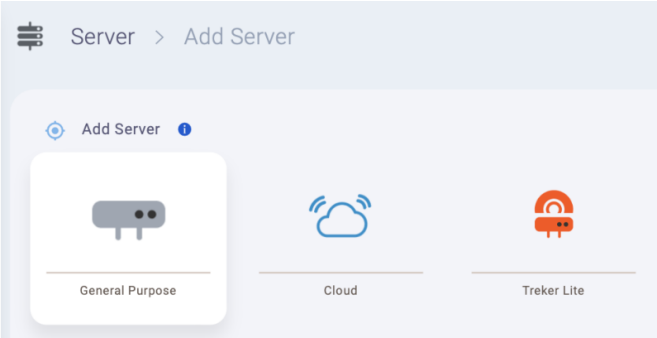


3. Specify the target folder for server installation “D:\Program Files\MDRS\Treker”
   It is recommended to install it on a non-system disk to ensure sufficient available disk space
4. Click on Install to start the installation process. Wait for approximately two minutes for the installation to complete.

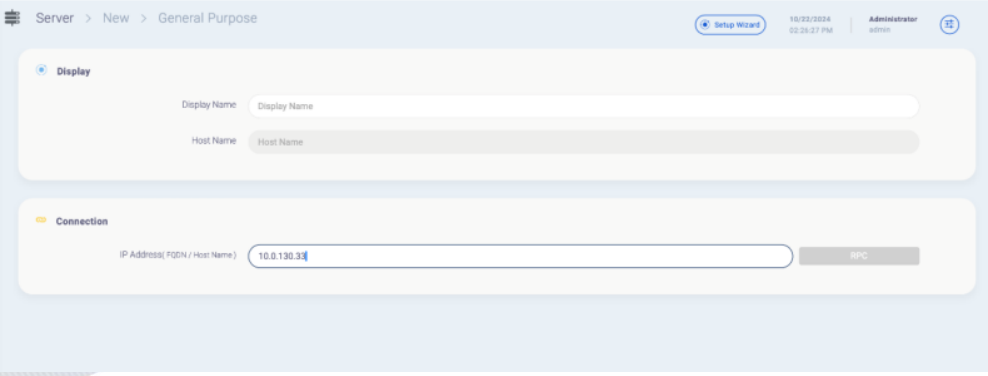
9.2 Register Source Server

The following steps outline the process of registering a proxy server in RPC mode through the Management Console.

1. Under Resources, choose Server and click to Add a new server to the console.
2. For server type, select General Purpose.



3. Enter the IP address

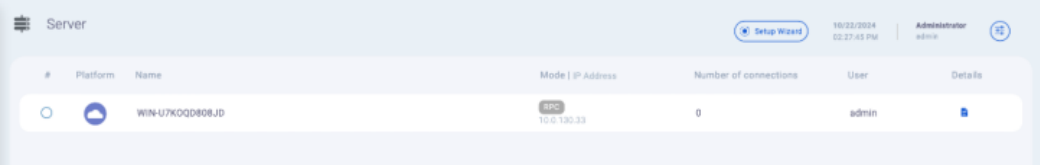


4. Click on Verify Server.

   If the IP address is unidentifiable, the browser will attempt verification for up to three minutes. If verification fails, check the following and re-enter the IP address.

   - Ensure the server service software is properly installed.
   - Verify that the server service is running.
   - Confirm that the server is accessible via the internet.
   - Check that TCP port 20001 is open.

5. Once verification is complete, update the server display name if needed, then click Submit to save

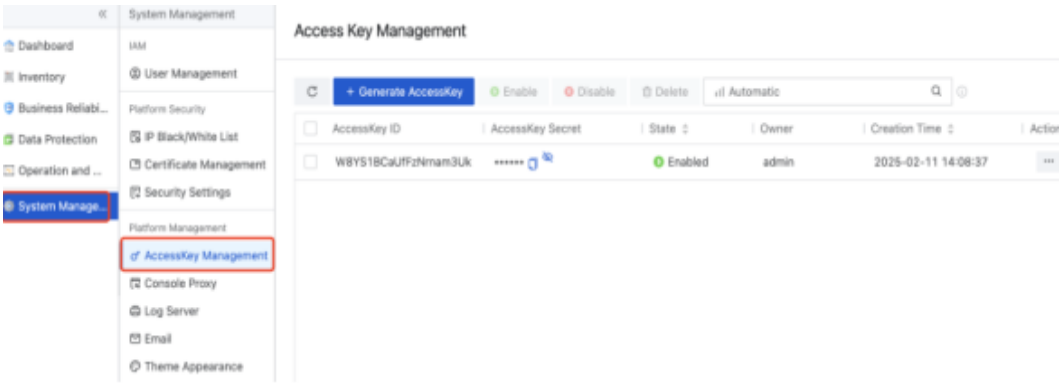


10 Register NexaVM and Cloud Source API

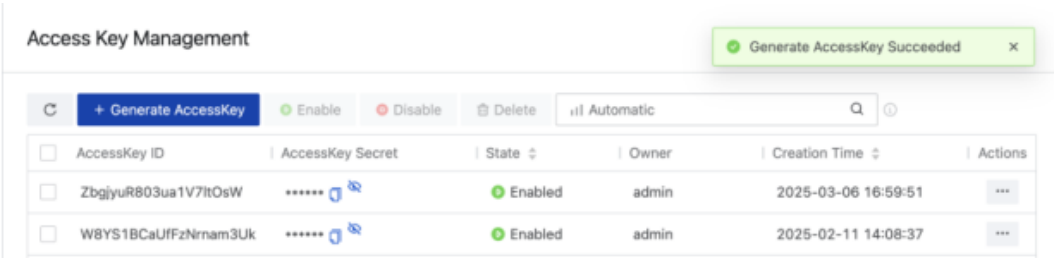
The management service integrates with cloud APIs to enable automated Provision by Disk/Snapshot and DevTest by Snapshot processes. This allows for streamlined and automated execution of protection and provision tasks. Follow the instructions below to generate an API AccessKey on nSSV or nCSSV and register VMware and NexaVM APIs.

10.1 Generate NexaVM API AccessKey on nSSV

On the NexaVM nSSV Cloud portal, click the menu icon and navigate to AccessKey Management under System Management.

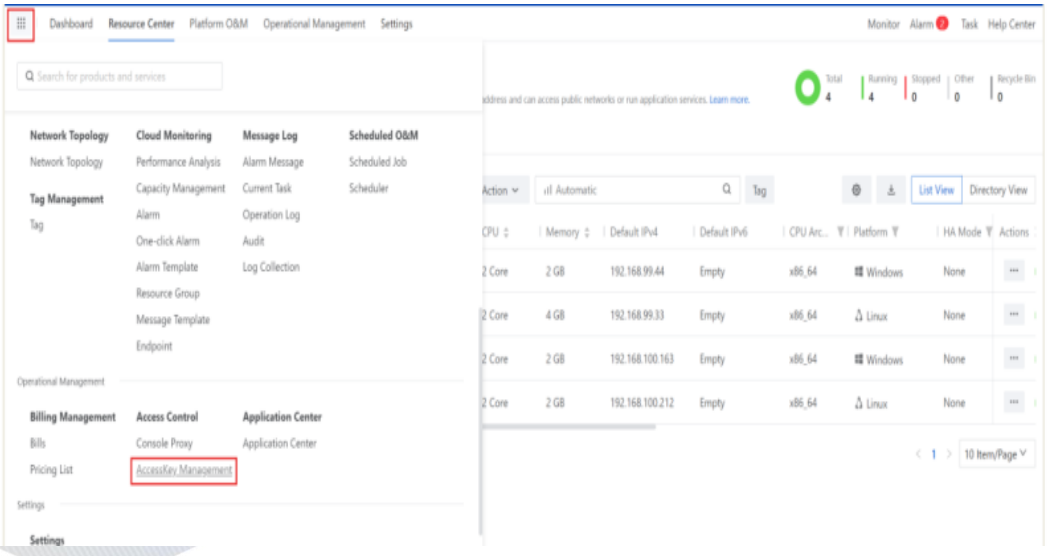


Click Generate AccessKey. The newly generated AccessKey will be displayed.

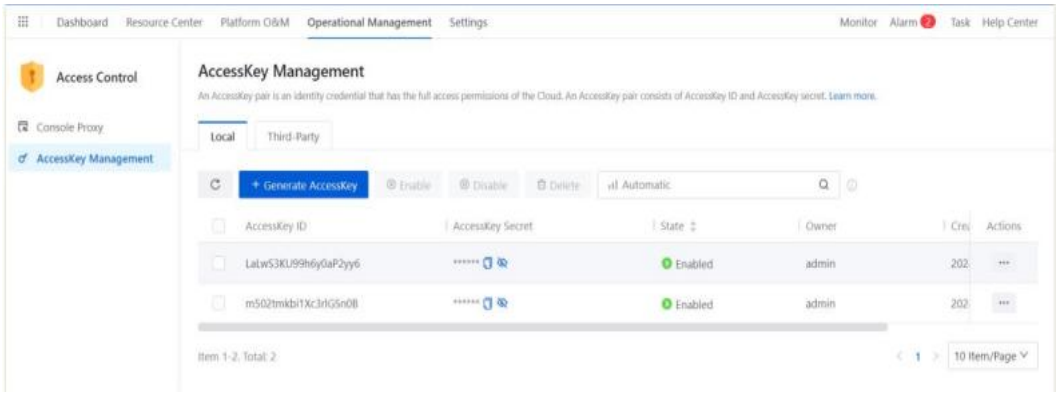


10.2 Generate NexaVM API AccessKey on nCSSV

On the nCSSV portal, click the menu icon and navigate to AccessKey Management under Operational Management

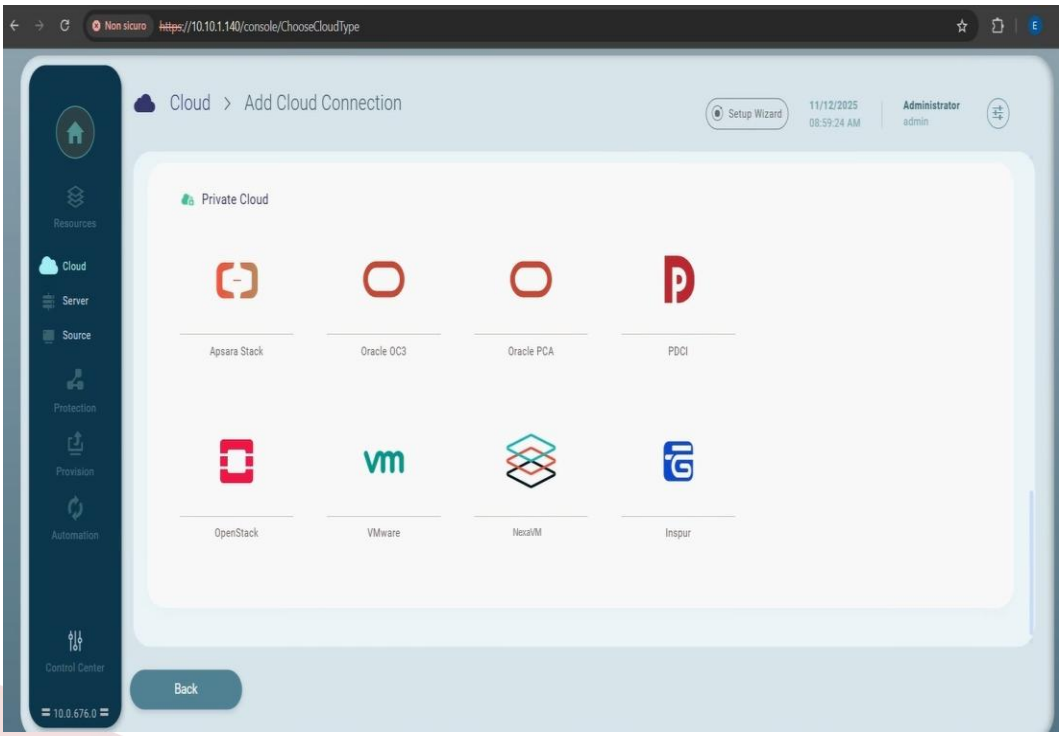


Click Generate AccessKey. The newly generated AccessKey will be displayed.



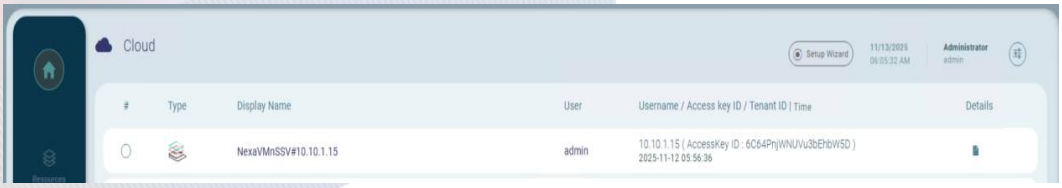
10.3 Connect the NexaVM Environment

Under the Cloud page, click Add to create a new cloud connection select NexaVM



Select Use AccessKey ID / AccessKey Secret, then enter the NexaVM IP, AccessKey ID, and AccessKey Secret. Select the Time Zone based on the actual environment of NexaVM, then click Verify Connection.

Once the verification is successful, click Submit to save the settings. The new NexaVM cloud connection will be displayed.

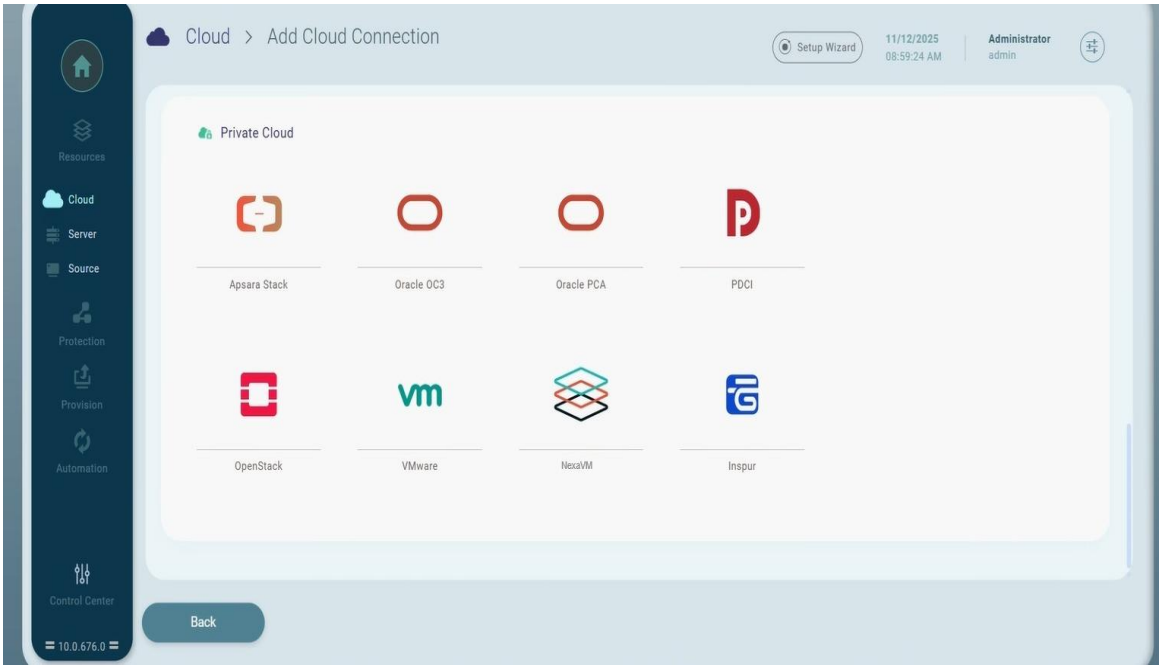


10.4 Connect VMware

Before establishing a VMware API connection, ensure the following prerequisites are met:

- Prepare a Windows Server or a Linux CentOS Server in the source VMware environment.
- If using vCenter, the server must have connectivity to both vCenter and ESXi.
- Ensure ports 902 and 443 are open for communication with vCenter and ESXi.
- Use an admin account or an account with Virtual Storage permissions and administrative access to the source virtual machines.

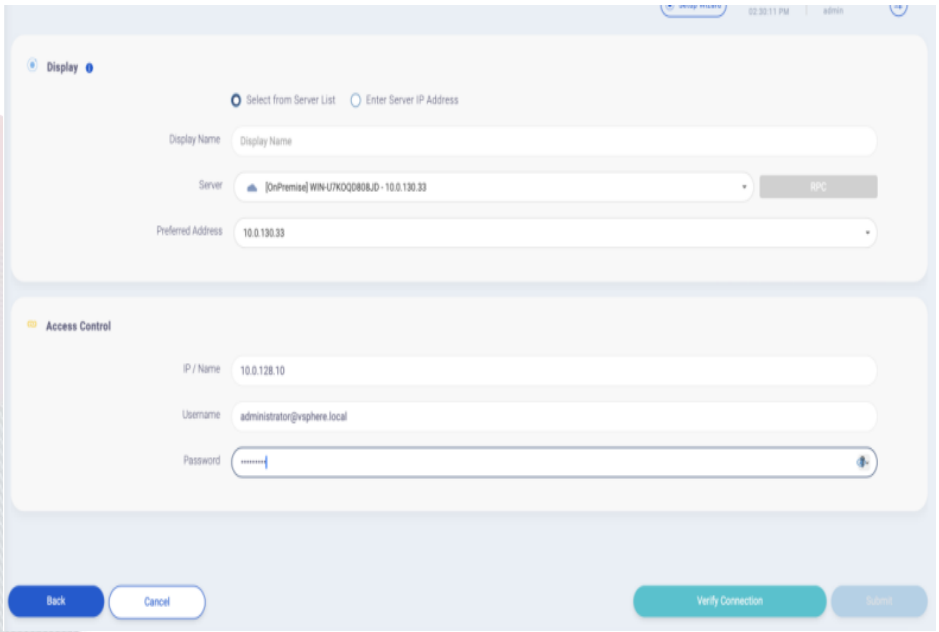
Under the Cloud page, click Add to create a new cloud connection select VMware



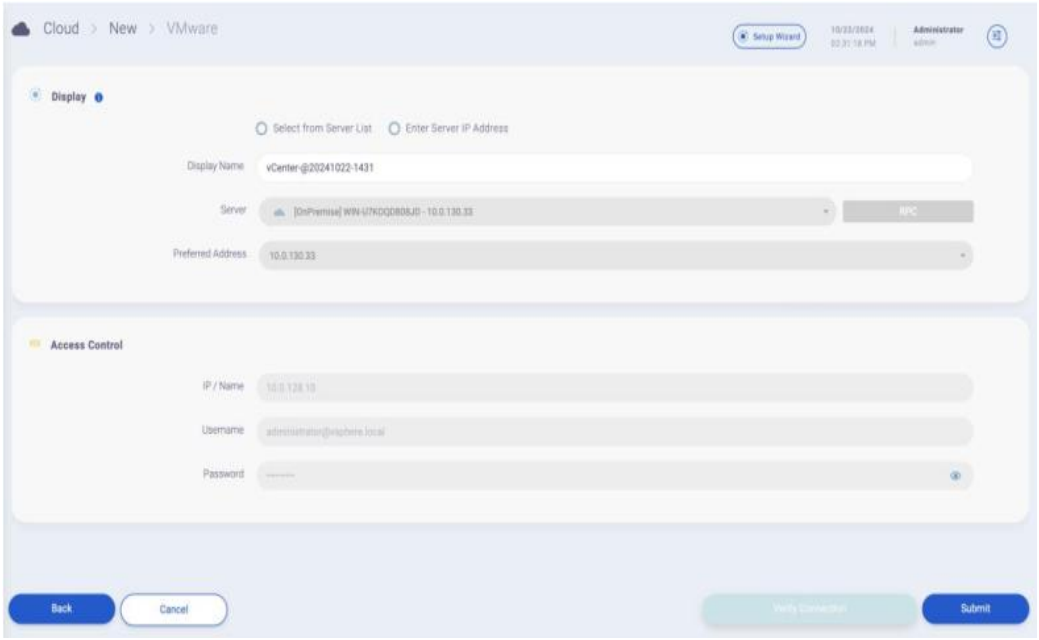
Choose one of the following methods to add a cloud connection:

Method 1: Select from Server List

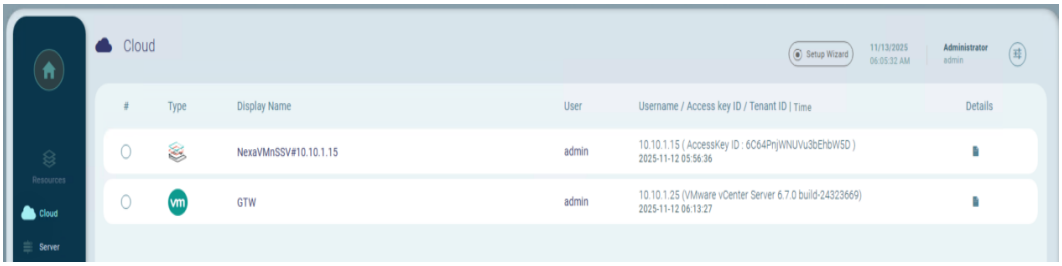
1. Select from Server List and enter the ESXi IP/Name, Username, Password, then click Verify Connection.



2. Once the verification is successful, click Submit to save the settings.

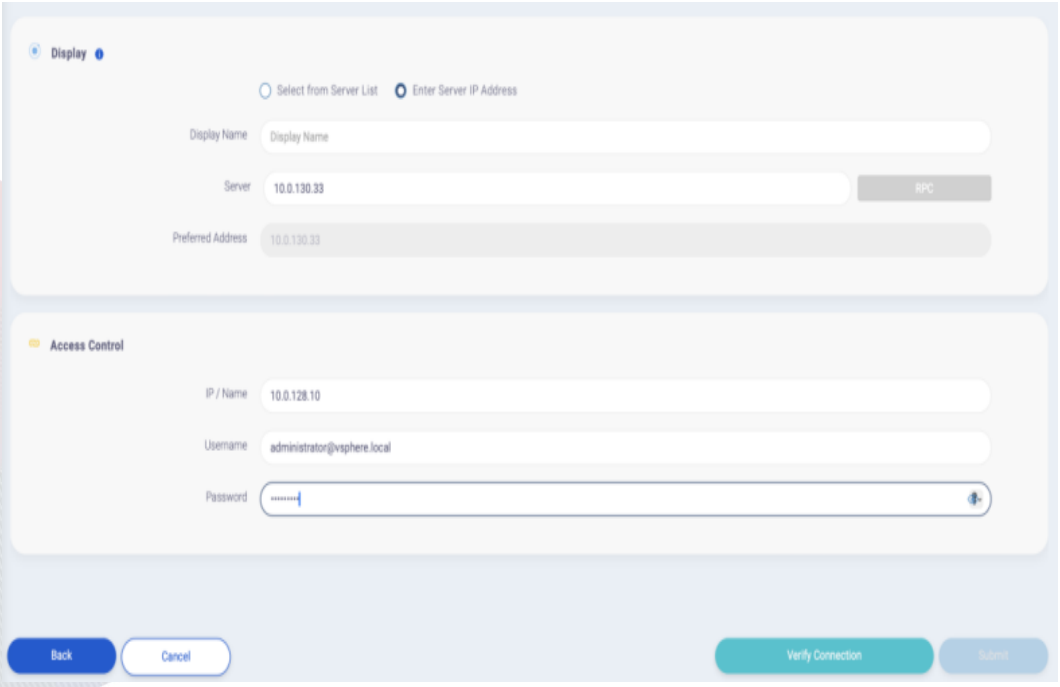


3. the new VMware cloud connection will be displayed.

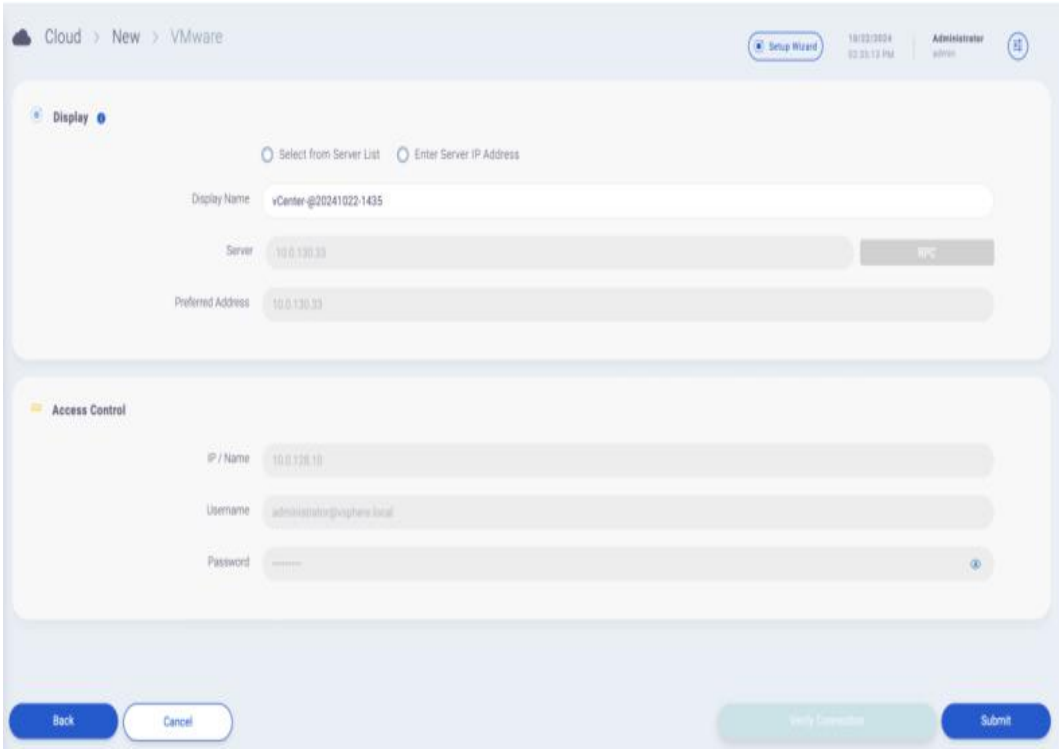


Method 2: Enter Server IP address

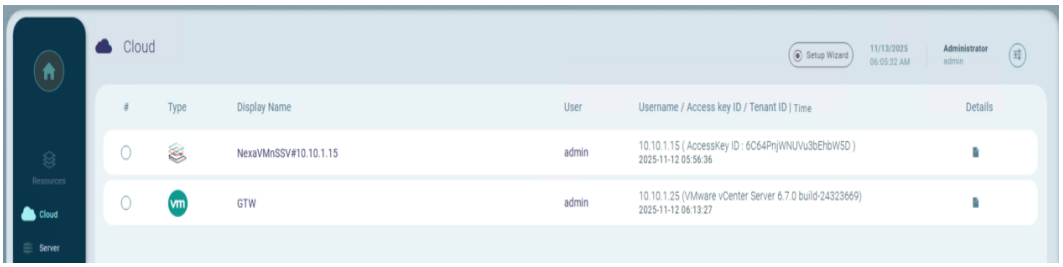
1. Choose Enter Server IP address and enter the ESXi IP/Name, Username, Password, then click Verify Connection.



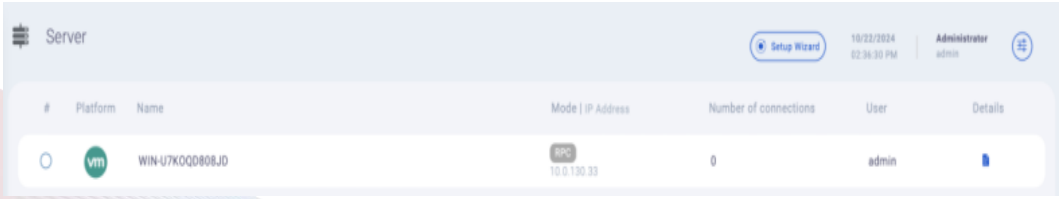
2. Once the verification is successful, click Submit to save the settings.



3. The new VMware cloud connection will be displayed.



4. Servers deployed under the registered VMware connection will be automatically added to the Management Console



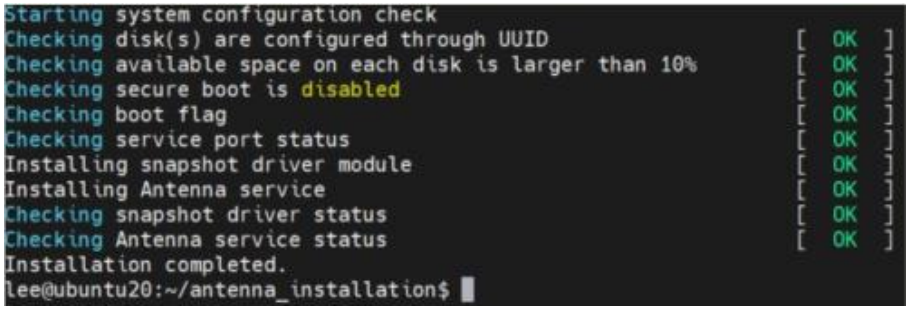
11 Source Agent Deployment

11.1 Linux Agent

The Linux agent is specifically designed for Linux systems. It is responsible for recording IO changes on the source machine and executing synchronization and protection procedures to the target platform.

1. Download the packages “Agent_for_Linux_Antenna-xxxxx.tar.gz”
2. upload on the source machine
3. extract the installation files using the command: tar-xvf Agent_for_Linux_Antenna- xxxxx.tar.gz
4. Select The installation package for the Antenna of the correct Linux kernel version (To retrieve the correct kernel version, run *uname -r*)

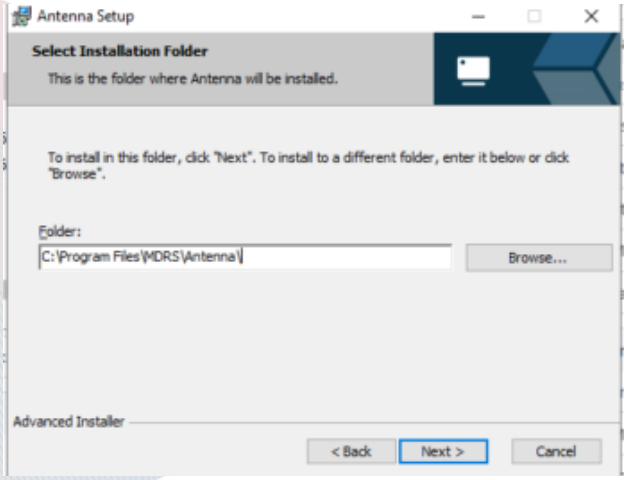
   NOTE: If there is a mismatch, open a ticket at support.nexavm.com and provide the kernel version for generating the appropriate Linux installation package.
5. Change the installation directory using the command: cd antenna_installation/
6. Execute the command to begin the installation: ./install.sh.



11.2 Windows Agent

The Windows agent can be installed on Windows servers or source platforms. Its responsibility is to record IO changes on the source machine and execute synchronization and protection procedures to the target platform.

1. Download the packages “Agent_for_Windows_Antenna_xxx.exe” .
2. upload on the source machine.
3. Run the server installation package.
4. Choose the installation folder and click Next. (The source agent only requires 50 to 100MB of hard disk space).

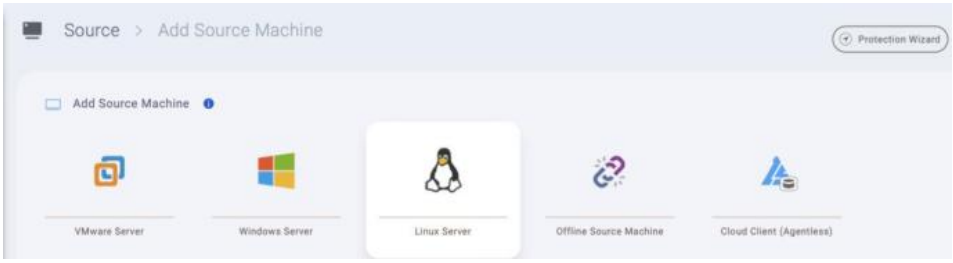


5. Click install and finish.

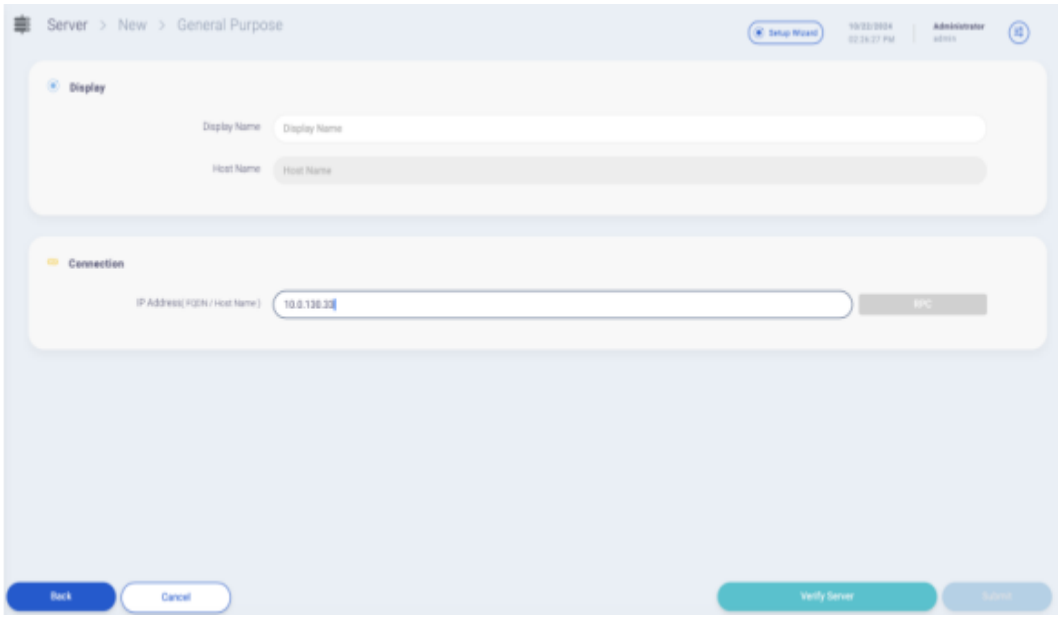
11.3 Register Linux Source Agent- RPC Mode

From the Management UI,

1. Under Resources, choose Source to add a new source machine and select Linux Server



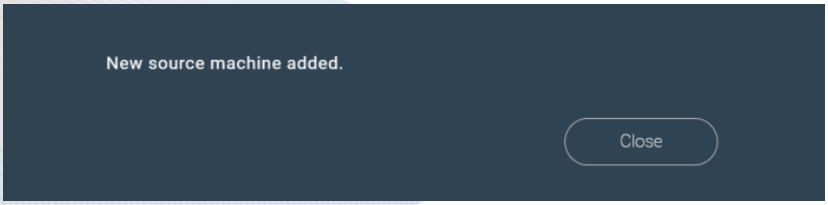
2. Enter the IP address of the server that the software is installed on and Click Test Source Machine to verify the connection.



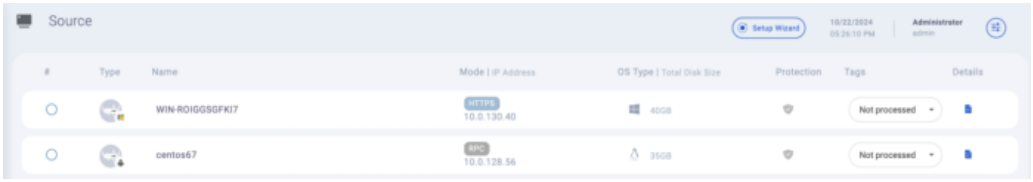
NOTE: If the verification takes longer than three minutes, please check the following:

- Ensure the source agent is correctly installed on the source machine.
- Verify that the source agent is operating normally.
- Confirm that TCP: 20005 is enabled on the source machine.
- After confirming the above, proceed to re-verify.

3. Once verified, options to modify the display name of the source machine will be enabled. Modify as needed and click Submit.



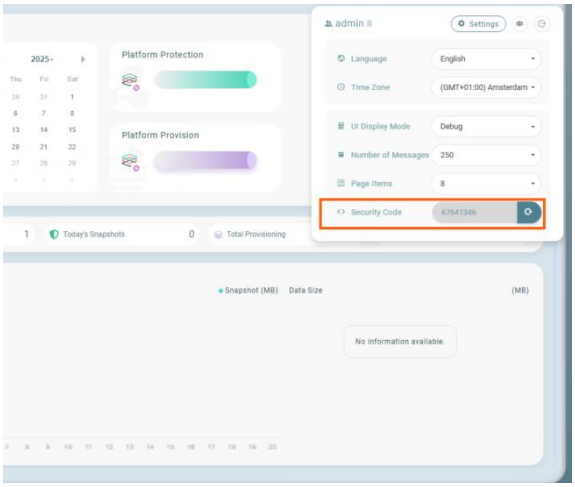
4. Once registered, the source machine will be displayed on the list.



11.4 Register Linux Source Agent - HTTPS Mode

From the Management UI,

1. Obtain the security code from the Settings page located in the top right corner of the Management Console.



2. Log in on the source machine, execute the command to run the registration:
   /usr/local/antenna/antenna-t [Console IP]-c [Security Code]
3. If the Management Console port is 20443, append ":20443" to the end of the IP address.

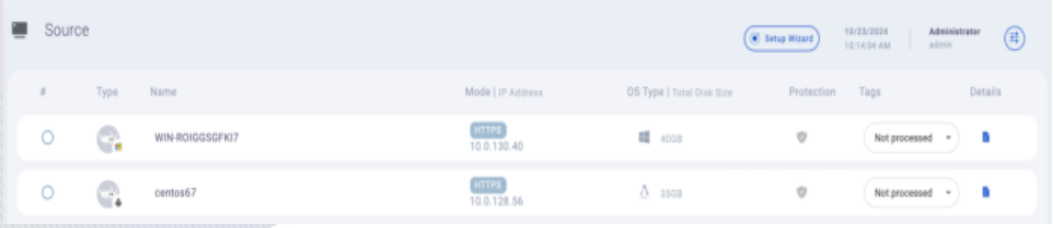
```
[root@centos67 ~]# /usr/local/antenna/antenna -t 10.0.130.33 -c 44297089
Source added. Please verify settings on management portal.
```

For example:

/usr/local/antenna/antenna-t 10.0.130.33-c 44297089

/usr/local/antenna/antenna-t 10.0.130.33:20443-c 44297089

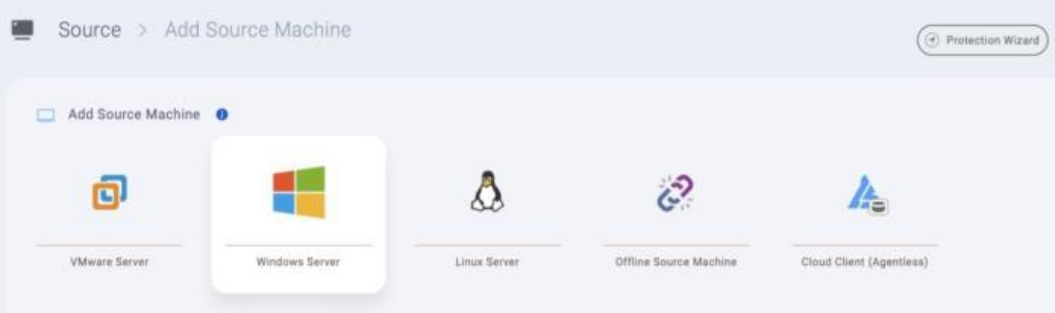
4. After registration, refresh the Source page of the Management Console to display the newly registered server



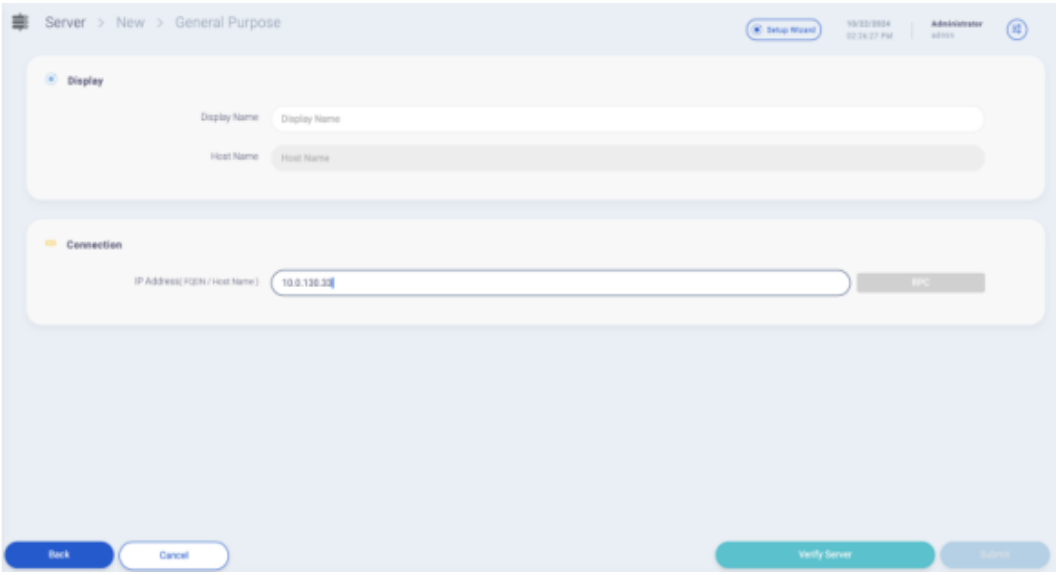
11.5 Register Windows Source Agent - RPC Mode

From the Management UI,

1. Under Resources, choose Source to add a new source machine and select Windows Server



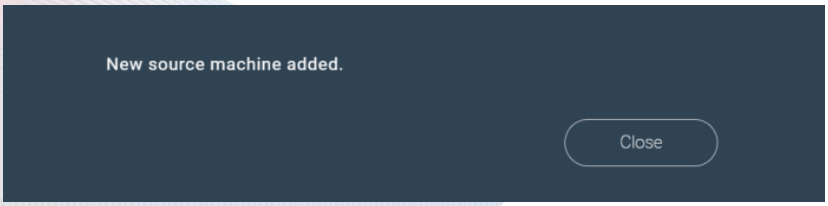
2. Enter the IP address of the server that the software is installed on and Click Test Source Machine to verify the connection.



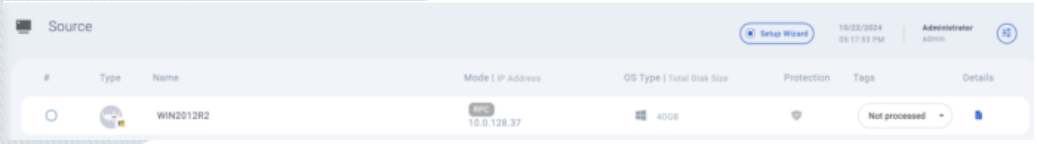
NOTE: If the verification takes longer than three minutes, please check the following:

- Ensure the source agent is correctly installed on the source machine.
- Verify that the source agent is operating normally.
- Confirm that TCP: 20005 is enabled on the source machine.
- After confirming the above, proceed to re-verify.

5. Once verified, options to modify the display name of the source machine will be enabled. Modify as needed and click Submit.



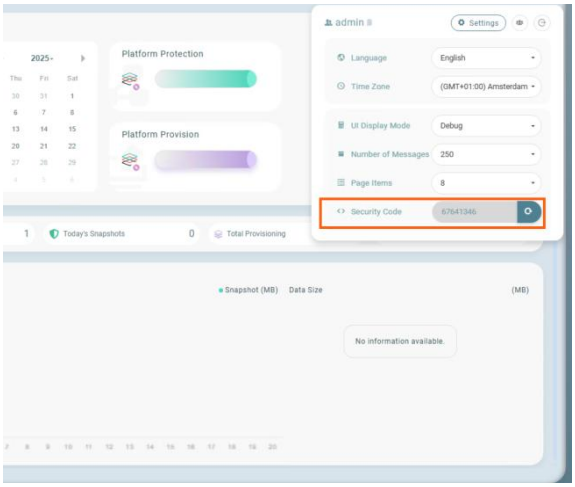
6. Once registered, the source machine will be displayed on the list.



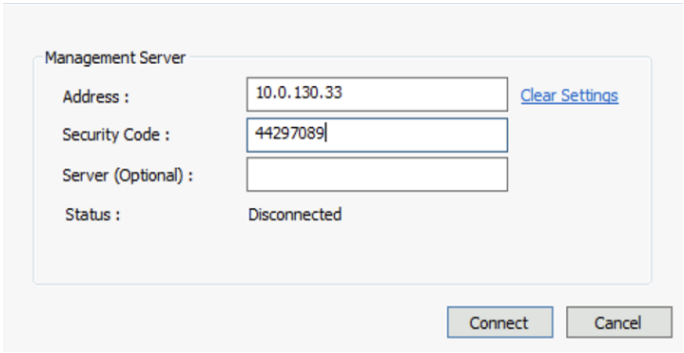
11.6 Register Windows Source Agent - HTTPS Mode

From the Management UI,

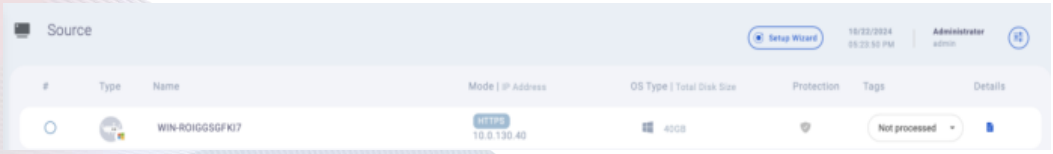
1. Obtain the security code from the Settings page located in the top right corner of the Management Console.



2. Log in on the source machine and run
   C:\Program Files\MDRS\Antenna\RegistrationTool.exe.
3. Enter the IP address of the Management Console and the security code. If the Management Console port is 20443, append ":20443" to the end of the IP address. Click Connect to add the source machine to the Management Console. The registration process should complete within 10 to 30 seconds, depending on the network speed



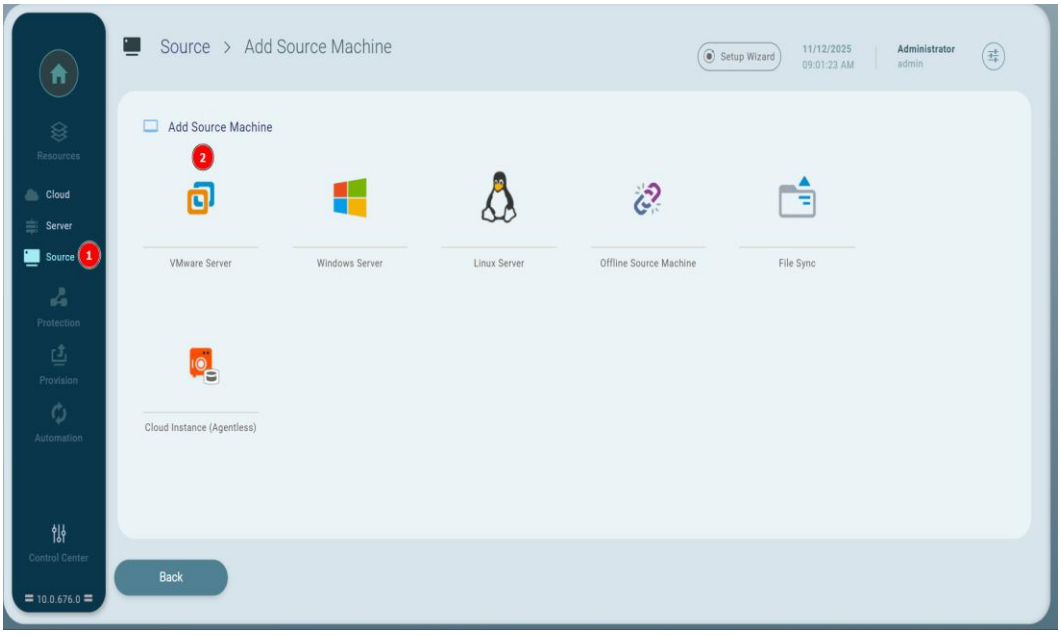
4. After registration, refresh the Source page of the Management Console to display the newly registered server



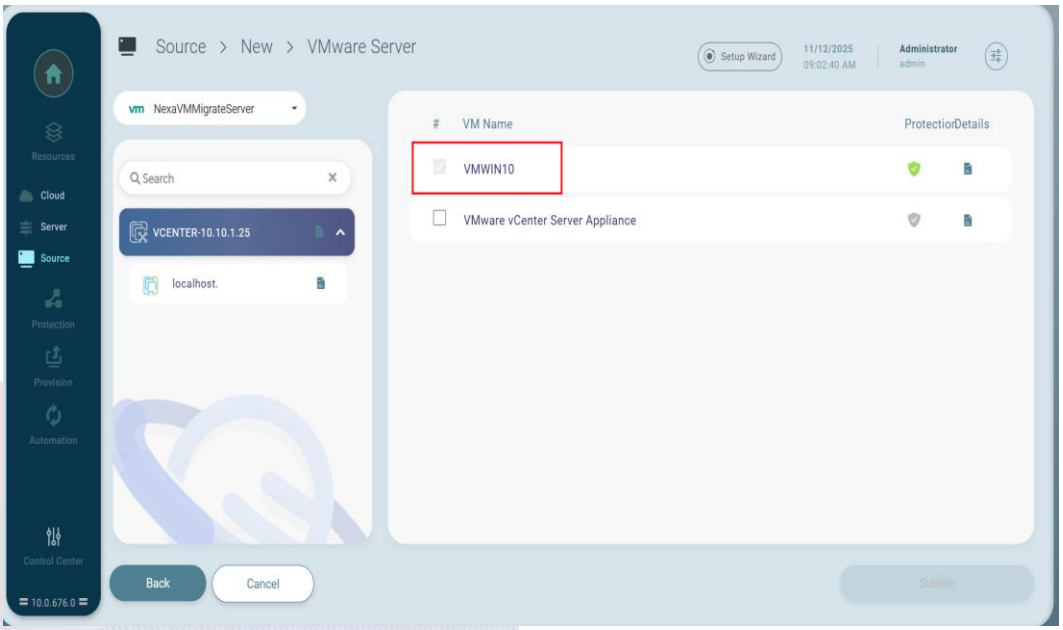
12 Register VMware Source

From the Management UI,

1. Under Resources, select Source to add a new source machine.
2. Choose VMware Server as the source machine type



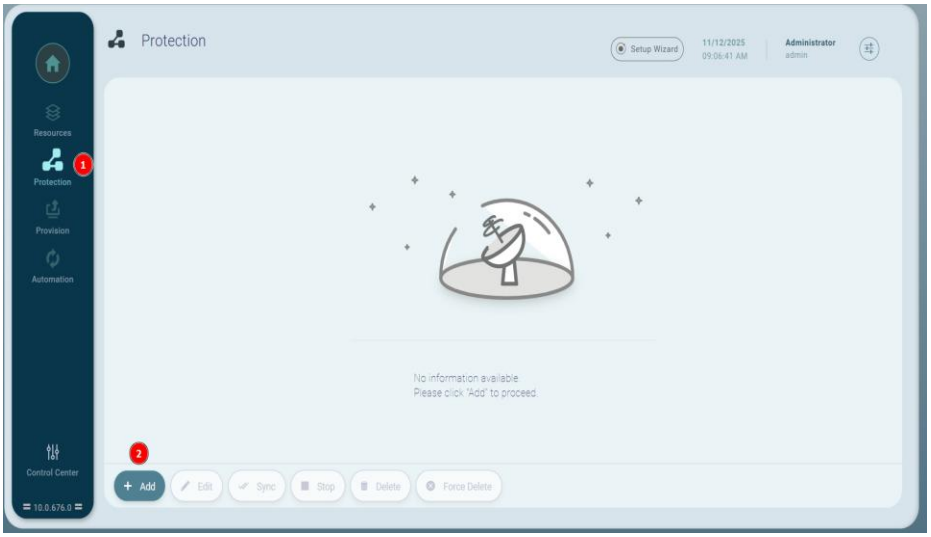
3. Choose the VMware server from the drop-down list and select the desired virtual machine and click Submit to register.



4. Once registered, the new source virtual machine will be displayed.

13 Create Protection Plan for Windows or Linux

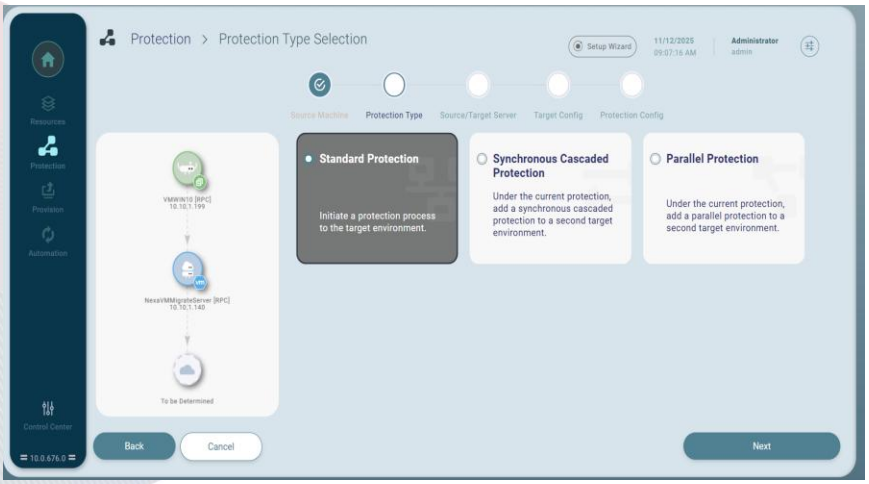
1. Within the left-hand menu, click on Protection and then Add.



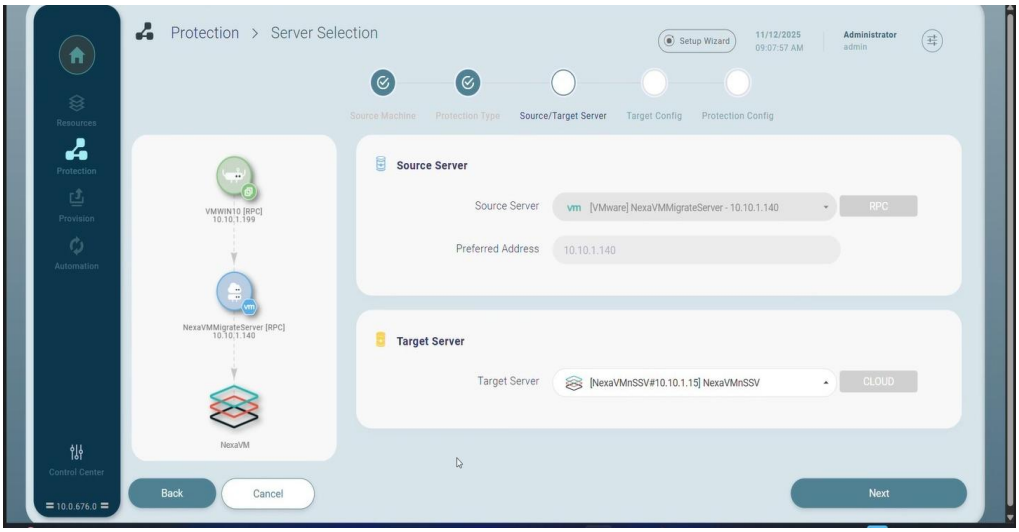
2. Select the source machine to perform protection

3. Choose the protection type: Standard Protection.

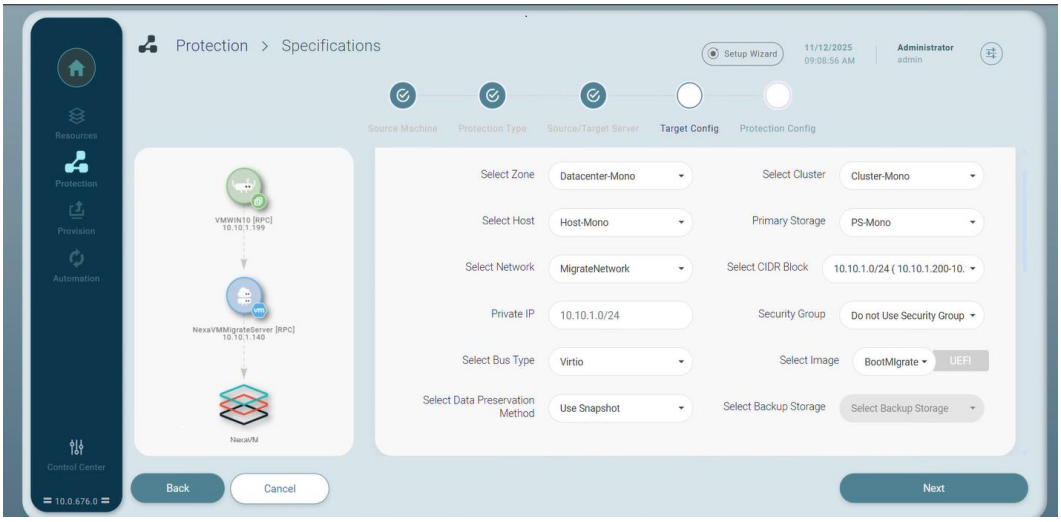
Note: This step will be automatically skipped in simple UI display mode.



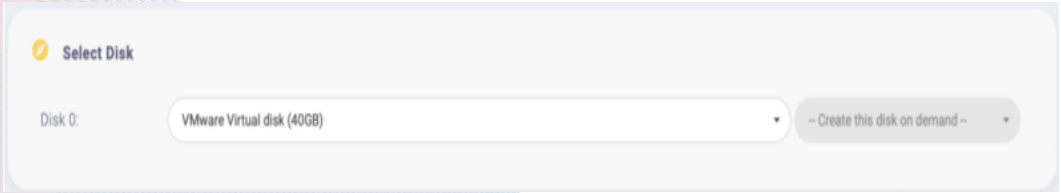
4. Define the protection route by selecting the source and target servers



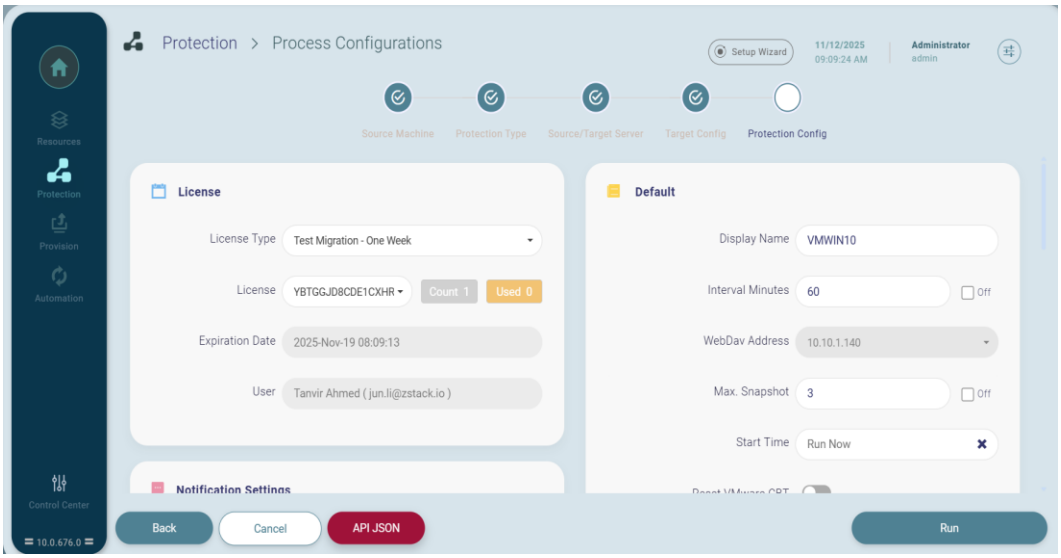
5. Select the zone, primary storage, network, image, security group, and data preservation method. Primary storage options include Ceph, NFS, and shared mount point. If Ceph is selected, snapshots will be retained up to the configured limit. Other primary storage types will retain only one snapshot. Data can be preserved as either snapshots or backups.



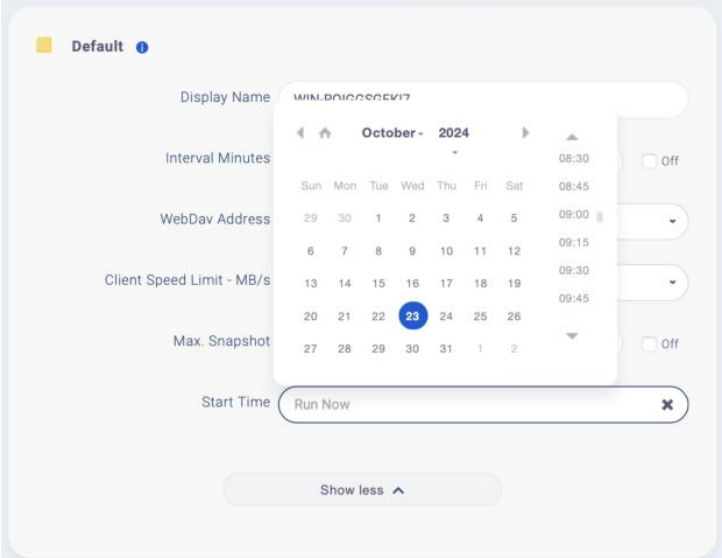
6. Choose the disks to protect and, if needed, enter pre- and/or post-scripts to customize the snapshot creation process. At least one system or data disk must be selected.



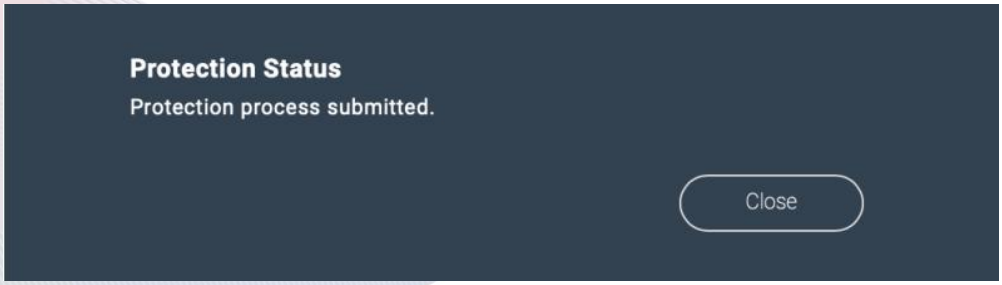
7. On the protection process configuration page, select the license to use, define protection intervals, specify the number of client snapshots to retain, and configure read/write threads.



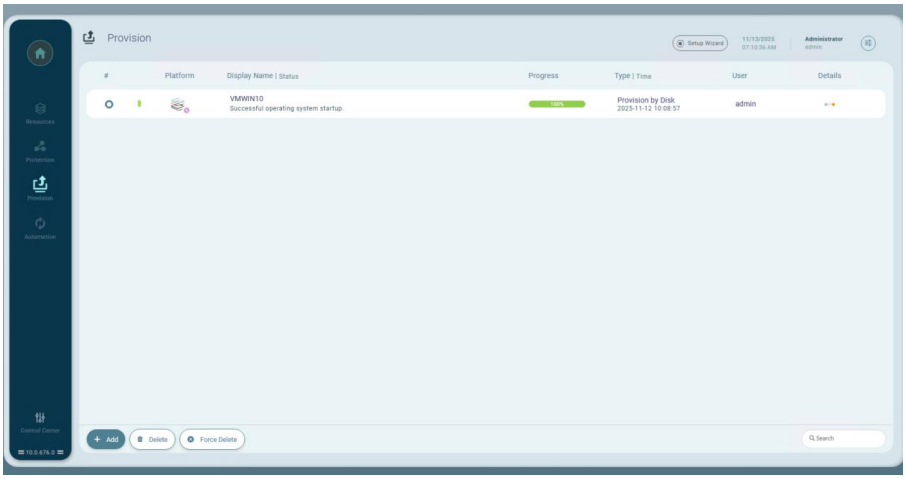
8. The protection process start time is configurable. Run Now immediately submits tasks to the source client. Alternatively, a specific date and time can be scheduled.
9. For example, if an interval of 120 minutes is set with a start time of 07:00, subsequent protection tasks will automatically run at 09:00, 11:00, and so on.



10. Once the process configurations are confirmed, click Run to execute.



11. The synchronization starts



12. After completing synchronization, the process status will display the message: "Target snapshot created" to indicate a successful protection

14 Provision Process

NexaVM Migrate Suite offers two activation modes to ensure maximum security and minimize downtime during the migration cutover.

Provision by Disk: involves directly using the latest synchronized target disk to achieve server cutover without creating new disks at the target platform. Before executing the provisioning process, the associated protection process will be disabled to prevent further synchronization writes to the target cloud disk undergoing provisioning. This method ensures a seamless transition by leveraging the most recent disk state.

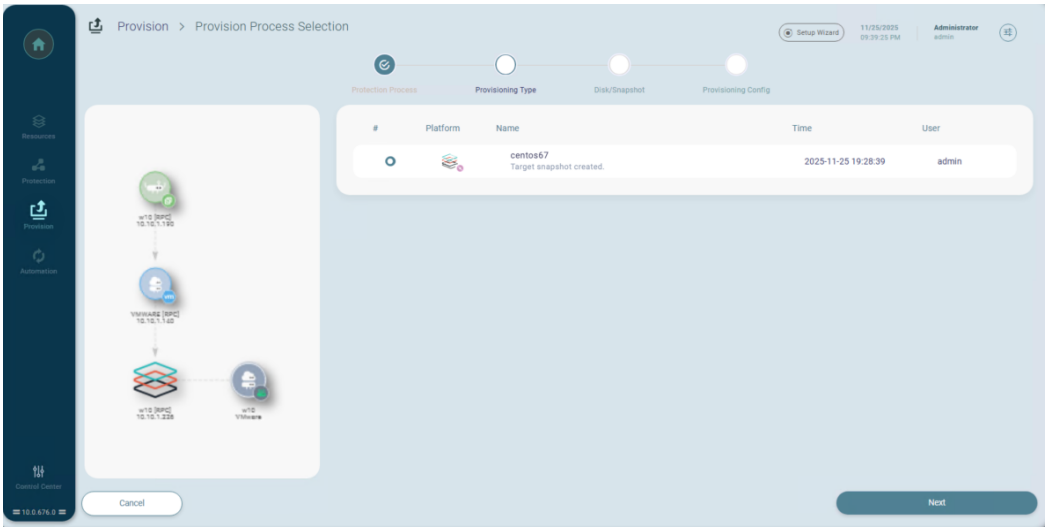
Provision by Snapshot: Allows creating test instances using a user-specified snapshot without interrupting the ongoing protection process.

DevTest by Snapshot (designed for testing and verification): enabling users to create test instances on the target platform using a user-specified snapshot. This allows users to validate the provisioning process and ensure that the provisioned instance operates as expected before executing the final cutover. This mode does not disrupt the associated protection process, allowing it to continue running while enabling an unlimited number of test executions.

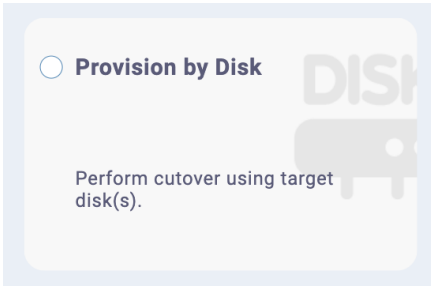
14.1 Provision by Disk

Provisioning by Disk mode utilizes the most recently synchronized disk(s) at the target to achieve cutover. To complete the provisioning process, follow the steps below:

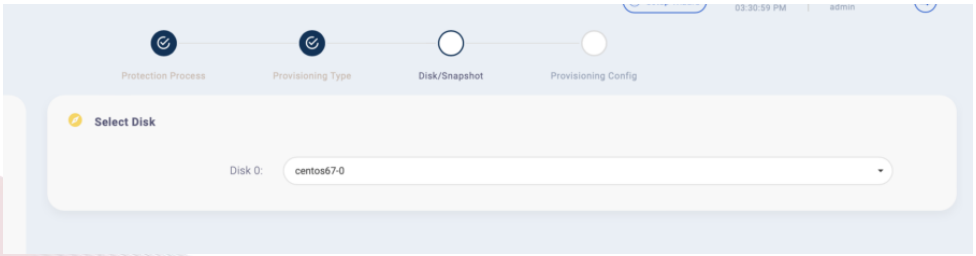
1. Within the left-hand menu, click on Provision and then Add.
2. Select the protection process for provisioning.



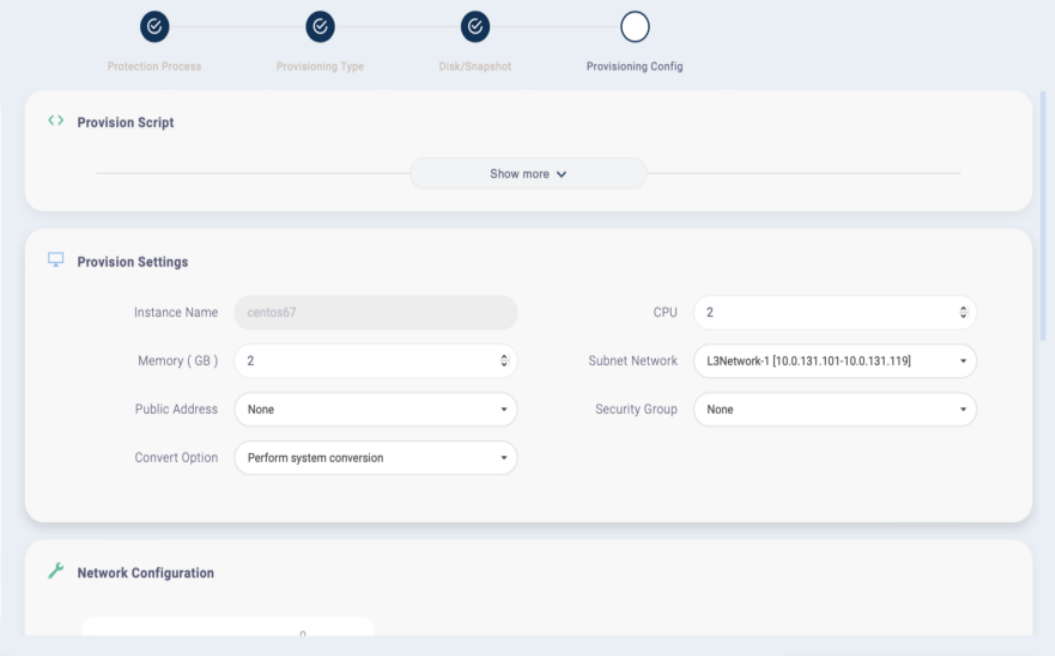
3. Select the provisioning type: Provision by Disk.



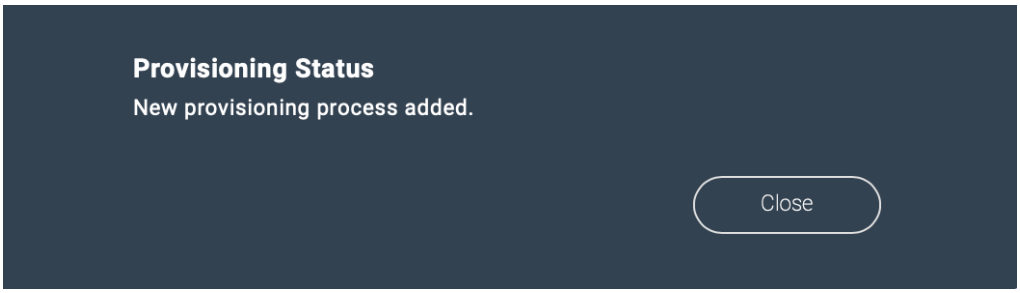
4. Choose the disk from which to provision.



5. Specify the instance type, network information, and other details for the instance to be provisioned. Then click Submit



6. After clicking Submit, the provisioning process will initiate, and the task progress will be displayed. In Provision by Disk mode, the related protection process will be interrupted to ensure synchronization consistency.



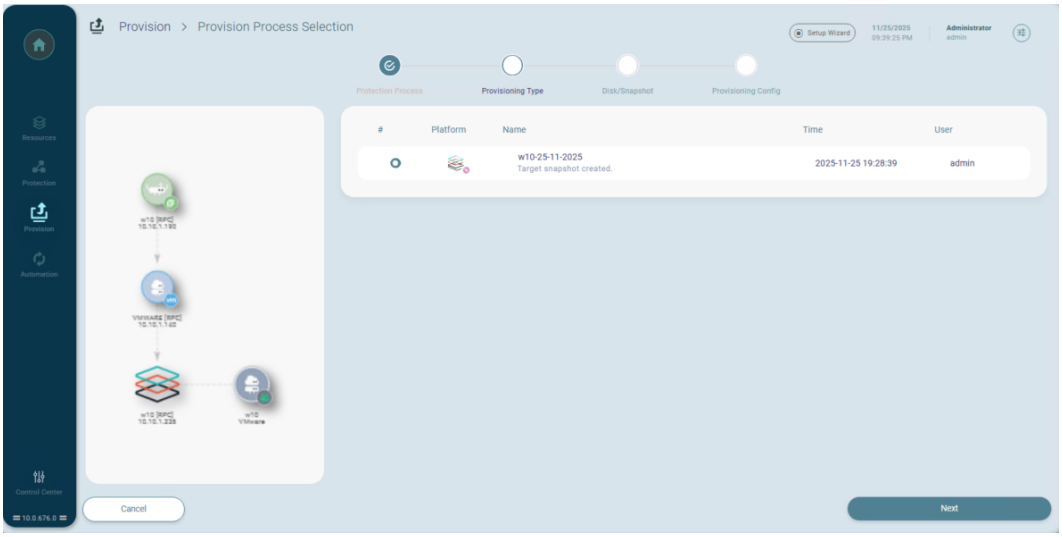
7. After completing the provisioning, the process status will display the message: "Successful operating system startup.

NOTE:

If the migration fails, try the procedure again by selecting ‘Skip system conversion’ under ‘Convert Option’.

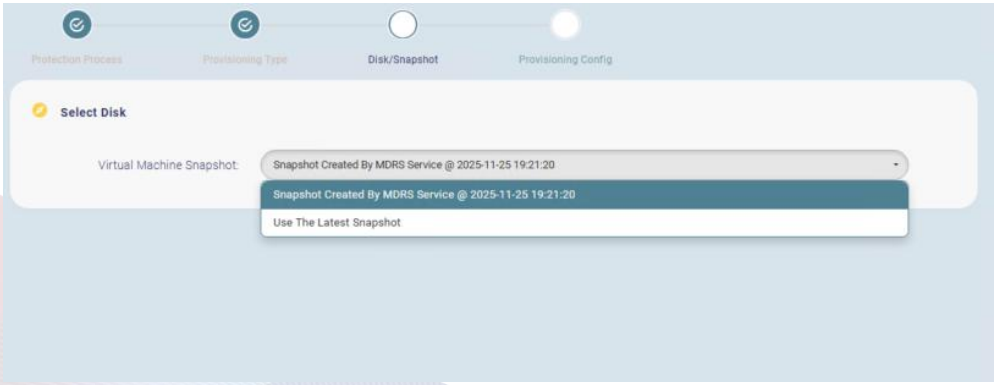
14.2 Provisioning by Snapshot / DevTest by Snapshot

1. Within the left-hand menu, click on Provision and then Add.
2. Select the protection process for provisioning.

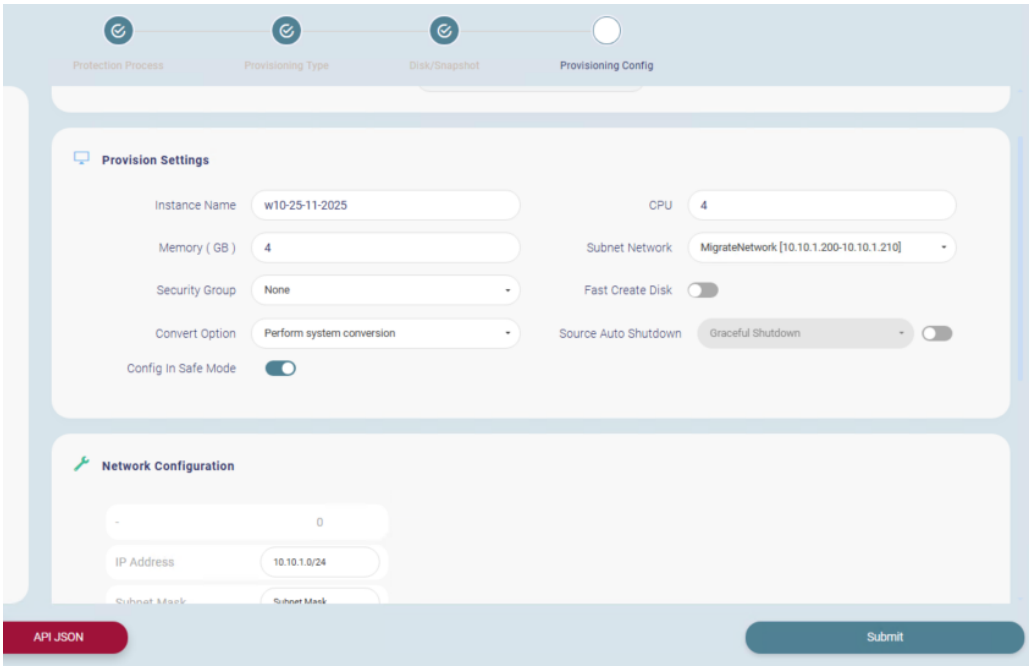


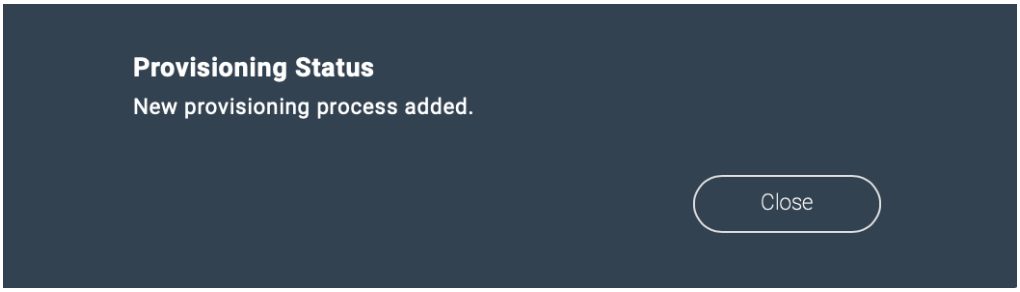
3. Select the provisioning type: Provision by Snapshot or DevTest by Snapshot if you want to create a staging environment

4. Select the disk snapshot time points from which to provision.



5. Specify the instance type, network information, and other details for the instance to be provisioned. Then click Submit.





6. Under the DevTest by Snapshot provisioning mode, the related protection process will remain unaffected and synchronize as usual. After completing the provisioning, the process status on the provision page will display the message: "Successful operating system startup."

NOTE:

If the migration fails, try the procedure again by selecting ‘Skip system conversion’ under ‘Convert Option’.

14.3 Provision Mode Summary

Architecture-Provision Mode	Scenario	Behavior	When Deleting Provision Process
Image Mode- Provision by Disk	**Final Migration Cutover** Directly boots the target system from the latest synchronized target disk.	Stops the protection process, creates a pre-provision snapshot of the target host, performs system conversion, and restarts into the operating system. Fast provisioning with no additional resource consumption.	**Left Option:** Deletes the provisioning process and rolls back the target instance to the pre-provision snapshot state, allowing re-execution. **Right Option:** Deletes both the protection and provisioning processes while retaining the target instance (optionally, clean up the target disk snapshot).
Image Mode- DevTest by Snapshot	Creates a test instance from a target snapshot for migration validation or walkthrough.	1. Selects a historical snapshot to create a test instance, performs system conversion, and starts the system. 2. Does not affect ongoing protection processes.	**Left Option:** Deletes the provisioning process and created the test instance. **Right Option:** Deletes the provisioning process but retains the created test instance.
Server Mode- Provision by Disk	**Final Migration Cutover** Creates and boots a new target instance from the latest synchronized target disk.	Stops the protection process, creates a pre-provision snapshot of the target host, provisions a new instance from the target disk, performs system conversion, and starts the system. Fast provisioning.	**Left Option:** Deletes the provisioning process and the target instance, rolls target disk back to the pre-provision snapshot state, allowing re-execution. **Right Option:** Deletes both the protection and provisioning processes but retains the target instance (optionally, clean up the target disk snapshot).
Server Mode- DevTest by Snapshot	Creates a test instance from a target snapshot for migration validation or walkthrough.	1. Selects a historical snapshot to create a test instance, performs system conversion, and starts the system. 2. Does not affect ongoing protection process.	**Left Option:** Deletes the provisioning process and the test instance. **Right Option:** Deletes the provisioning process but retains the test instance.

15 Best Practices

15.1 Architecture Summary

1. Use Chrome, Edge, or Firefox for console access.
2. Ensure NexaVM management server, NexaVM platform, and the browser have same system time to prevent login failures and synchronization errors.
3. Image mode supports multiple parallel cutovers, making it ideal for environments with DHCP, multiple concurrent migration processes, and minimal cutover downtime.
4. Server mode requires queuing for multiple cutovers, best suited for environments without DHCP, fewer concurrent processes, and more flexible cutover schedules.
5. If migrating more than 5 hosts, it is strongly recommended to deploy the management server and Treker servers separately to avoid resource constraints. When necessary, a single server can be reused.
6. Treker capacity: Each CPU core handles one concurrent migration process.
7. Recommended specifications for small scenario: Management Node plus Gateway Treker with 8 cores CPU, 8GB RAM, 100GB OS disk (Windows Server 2012+ or Linux), plus 100GB data disk.
8. Recommended specifications if migrating more than five hosts: Deploy the management server and Treker servers separately. Management Node Server with 4 cores CPU, 8GB RAM, 100GB OS disk (Windows Server 2012+ or Linux standard image). Gateway Treker Server with 8 cores CPU, 8GB RAM, 500GB OS disk (Windows Server 2012+ or Linux).
9. For optimal performance, use:
    - Windows TrekerLite for Windows source hosts
    - Linux TrekerLite for Linux source hosts
10. UEFI source hosts require UEFI TrekerLite, while BIOS source hosts require Legacy TrekerLite. To support both Windows and Linux migrations, prepare four TrekerLite types in advance.
11. For NexaVM environments requiring "Falloc disk mode", use ISO-type TrekerLite, which does not require the target system disk to be 5GB larger than the source. This mode is only available in manual operation.

15.2 Agentless Model Considerations

A standard-mode Treker is required to invoke the VMware agentless interface. It is recommended to deploy the gateway server on the source ESXi for optimal network performance.

Replication & Concurrency

1. By default, each Treker run one sync process for VMware host at a time to avoid impacting production. Additional tasks will queue.
2. If multiple virtual machines reside on different ESXi hosts, they can be synchronized concurrently.
3. Concurrency settings can be adjusted in the Treker registry (max: 3 tasks).
4. For higher concurrency, consider the agent-based model.

Compatibility & Registration

1. Treker communicates with ESXi and vCenter via VMware's VDDK.
2. Choosing between ESXi and vCenter registration: If you have more than five ESXi hosts or 100+ VMs, register each ESXi host individually. For fewer hosts or VMs, register vCenter instead.

Limitations

Agentless mode does not support the following disk types:

- RDM (Raw Device Mapping)
- Independent-Persistent & Independent-Non-Persistent disks
- SCSI bus shared disks
- Disks directly connected to virtual machines

15.3 Agent Considerations

Windows Installation Considerations

1. Installing Agent proxy on Windows Server 2008 may require a Microsoft KB update, which needs a restart. It is recommended to install the update to enable KB-supported drivers and incremental synchronization. Without it, contact support for a driver-less agent package, which supports only differential synchronization.
2. Before installation, check and complete all pending Windows updates and restart.

Linux Installation Considerations

1. When installing the Agent client on a Linux source host, the system will check for environmental compatibility. Pay attention to the following:
    - **Filesystem Free Space:** Ensure at least 10% free space per filesystem shown through **df** command. If not, modify the snapshot configuration file to reduce the ratio below 10.
    - **ext3 Filesystem:** Recommended to adjust the snapshot ratio in the configuration file to below 10.
    - **Port 20005 availability:** If occupied, install with **./install.sh disable-listen**.
    - Once completed, register the client using HTTPS reverse registration.
2. Kernel Consistency Check: Ensure the current running kernel matches the next boot kernel to avoid migration failure. Compare outputs of the following commands:
        - **uname-r** *# Check the current running kernel version*
        - **cat /boot/grub2/grubenv** *# Check the next boot kernel version*

15.4 Migration Plan

1. **Pre-Implementation Check:** Verify the source host system version and kernel for compatibility. Refer to the NexaVM Hive Community: go to ***Download -> Manuals -> Migrate - Hybrid Cloud Migration Platform*** and consult the "OS Compatibility list of NexaVM Migration Tool 688.pdf".
2. **Snapshot Before Installation:** Take a snapshot of the production machine before installing the agent to enable rollback if needed.
3. **Monitor Daily Sync:** Address incremental sync errors early to prevent last-minute issues affecting migration cutover.
4. **Final Sync Before Cutover:** Stop the source business, manually initiate the last incremental sync, upon completion proceed with cutover.
5. **Post-Migration Steps**
    - Restart the target machine after provisioning and verify stability.
    - Take a snapshot of the target disk for temporary retention.
    - If rollback is unnecessary, uninstall agent to prevent future troubleshooting confusion.
6. **Task Cleanup:** To remove completed migration processes, delete ONLY from the “Provision” page while retaining the target machine. DO NOT clear processes from the "Protection" page to avoid accidental deletion.