SANGFOR

HCI

User Manual

Version 6.2.0

Change Log

Date	Change Description
January 18 2021	Edited the user manual of HCI6.2.0

Contents

Preface

About This Manual

Chapter 1 Installing & Initializing Sangfor HCI Software

Chapter 2 Initial Login to Sangfor HCI Console

Chapter 3 Case Study

This manual is for SANGFOR HCI 6.0.1 official version. There are some differences in configurations for different versions. For details, refer to the corresponding chapter.

Document Conventions

This manual uses the following typographical conventions for special terms and instructions:

Convention	Meaning	Example
boldface	Page title, parameter, button, key press, other highlighted keyword or item	Page/tab name example: Navigate to **Storage** to enter the **Storage** configuration page. Parameter example: **IP Address:** Specifies the IP address that you want to reserve for certain computer. Button example: Click the **OK** button to save the settings. Key press example: Press **Log In** to enter the administrator console of the Sangfor HCI platform. Highlighted keyword/item example: The username and password are **Admin** by default.
italics	Directory, URL	Enter the following address in the IE address bar: *http://10.254.254.254:1000*

>	Multilevel menu and submenu	Navigate to **Storage > iSCSI Virtual Disks** to create iSCSI virtual disk.
" "	Prompt	The browser may pop up prompt to ask you to confirm the current operation.

Symbol Conventions

This manual also adopts the following symbols to indicate the parts which need special attention to be paid during the operation:

Convention	Meaning	Description
	Caution	Indicates actions that could cause setting error, loss of data or damage to the device
	Warning	Indicates actions that could cause injury to human body
	Note	Indicates helpful suggestion or supplementary information

Technical Support

For technical support, please contact us through the following:

E-mail: tech.support@sangfor.com

Tel: 60 12711 7129 (7511)

Website: www.sangfor.com

Acknowledgments

Thanks for using our product and user manual. If you have any suggestions on our products, please provide us feedback by phone or e-mail. Your suggestion will be much appreciated.

Chapter 1 Installing & Initializing Sangfor HCI Software

Sangfor HCI software provides an Enterprise-class cloud management platform which integrates resources, such as compute, networking and storage, etc. It is often defined according to requirements of business system and can help to build data center and deploy business system more easily. It combines compute, networking and storage capabilities onto industry-standard x86 servers by using virtualization technologies. All the resources are aggregated into a resource pool on node basis that is easy to scale out.

Sangfor HCI is a suit of software which is installed on a physical server, and used to virtualize servers and resources of physical server (CPU/memory/storage, etc), and to provide guest operating systems with complete hardware system functions and independent operating environment, which are called virtual machines.

This section introduces the installation of Sangor HCI software and requirements for hardware. After the software is installed properly, you also need to configure it, and do debugging.

aSV refers to management software or operating system of Sangfor HCI, if not otherwise specified.

1.1Hardware Requirements

Before installation, a number of physical servers are needed. Performance of virtual machines is determined by that of server's CPU, memory, and storage. The better the server's performance, the better virtual machine's user experience will be.

Additionally, there are some requirements for the physical server on which you want to install the Sangfor HCI software.

The server's CPU must support Intel Intel Virtualization Technology(VT) or AMD-V. For some servers, it is required to enable VT-x in BIOS.

Memory of the server must be greater than 16GB.

Free disk space of the server must be greater than or equal to 60GB. To run virtual machines, data disk is also required. You can use external iSCSI or FC storage, or build virtual storage by

configuring SSD and HDD.

The server must have at least 4 NICs.

1.2 Installing Sangfor HCI Software

Install ISO file of the brand-new Sangfor HCI operating system on a third-party server.

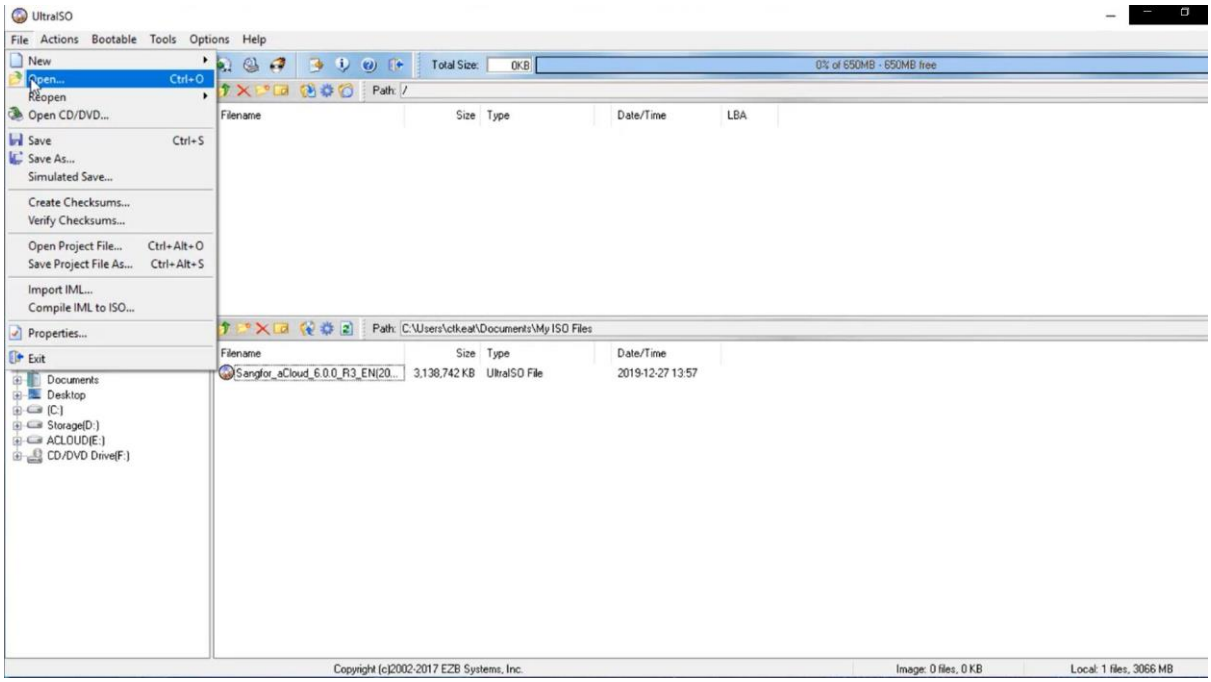
1.2.1 Writing Image File to USB Drive

Required software: UltraISO

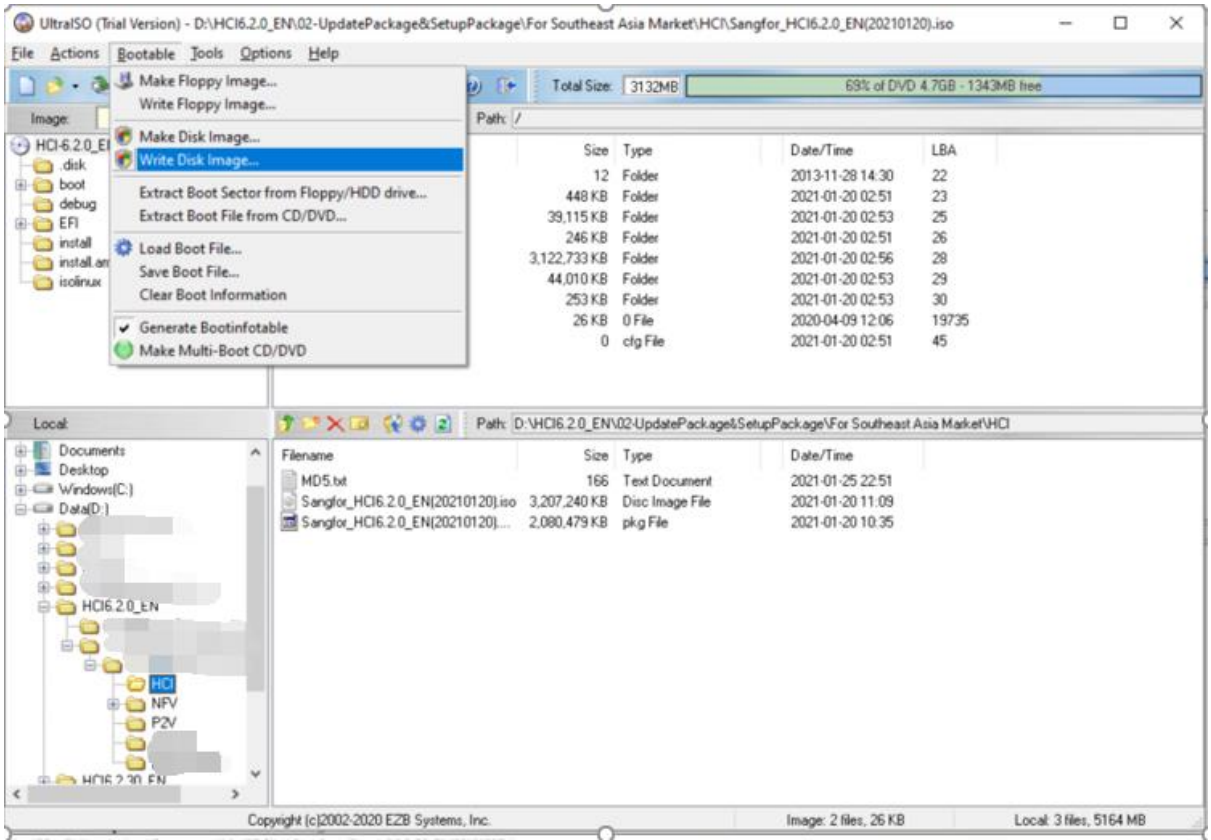
Steps: Insert a USB drive into PC, and then follow the steps below:

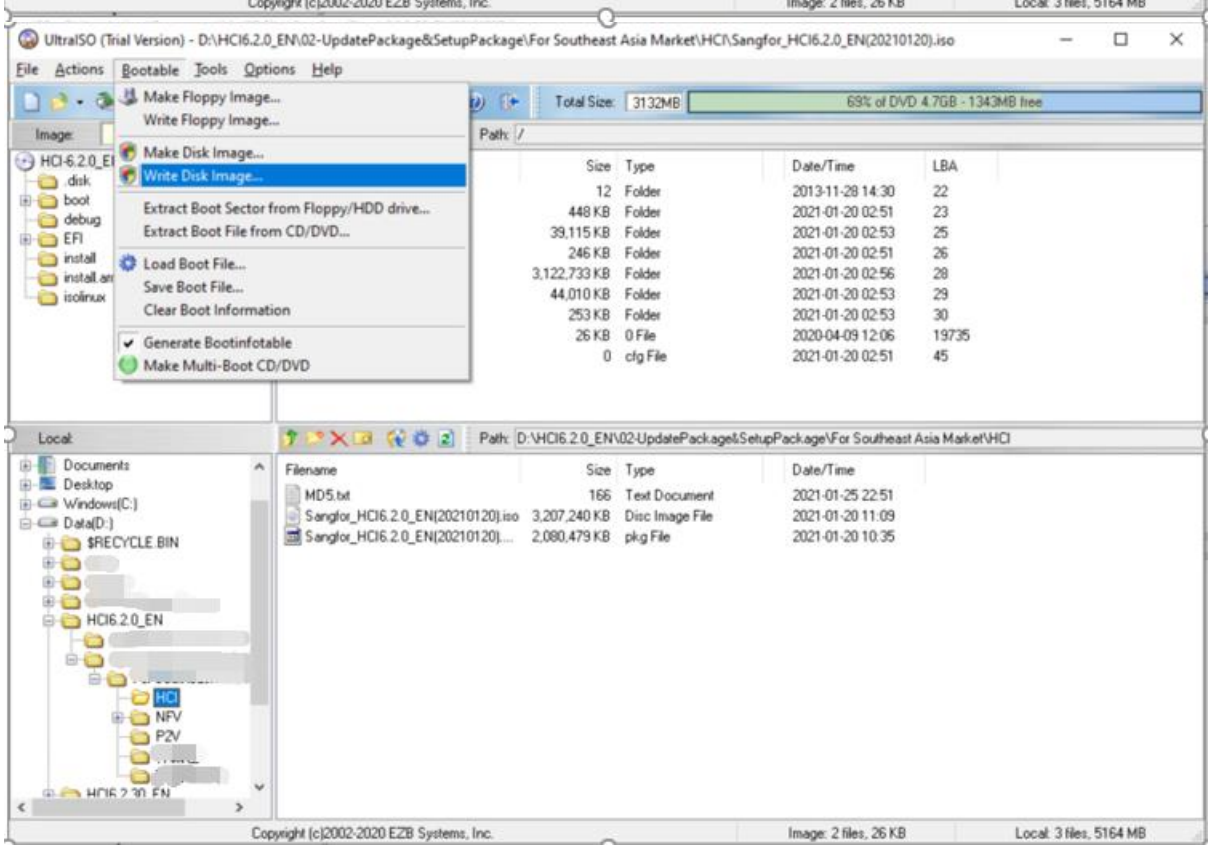
UltraISO should be the latest version; Write format of the USB drive should be USB-HDD or USB-HDD+, choose **Verify** to check whether the image file is written correctly; USB drive capacity should be greater than the size of ISO file.

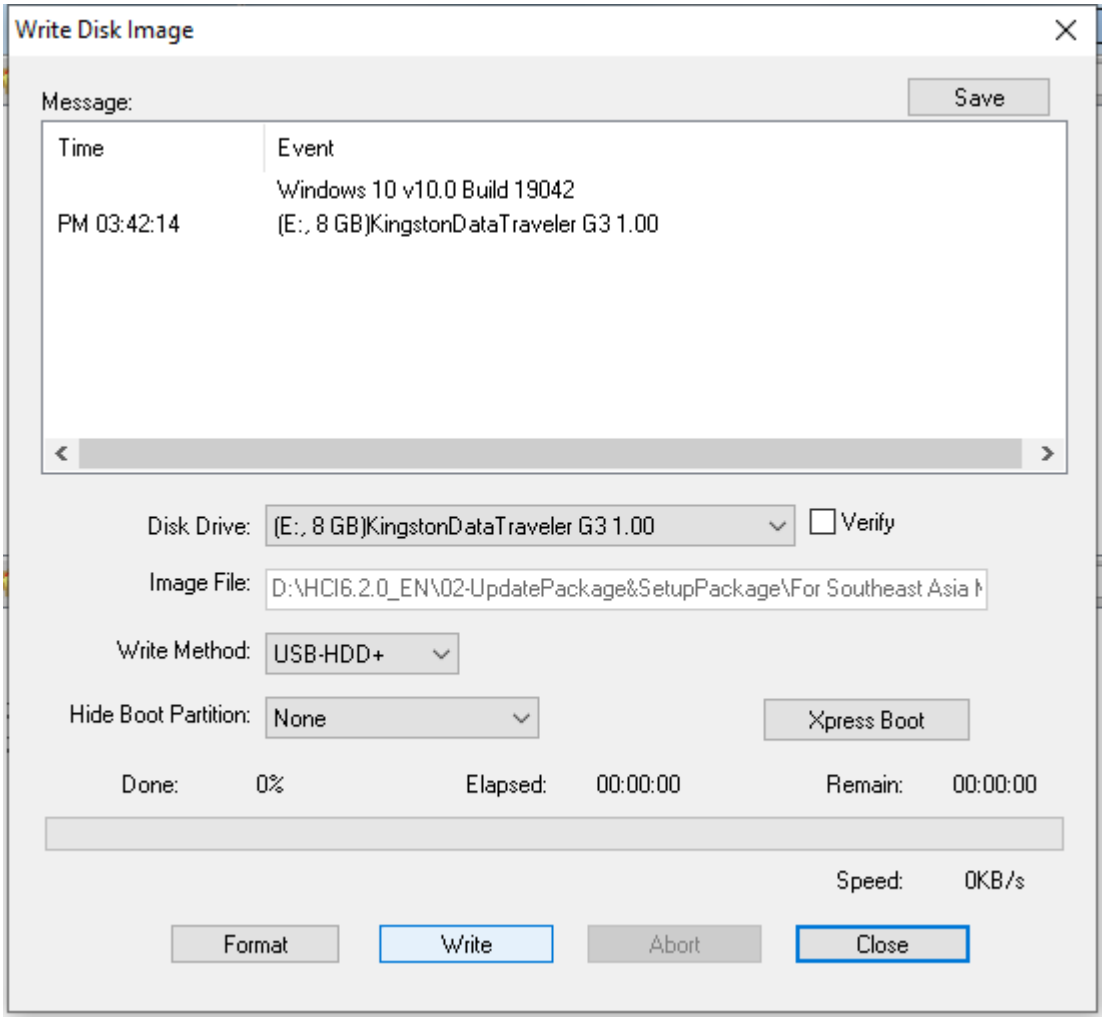
1. Launch UltraISO.
2. Select **File > Open** and load ISO file of Sangfor HCI software from local disk.



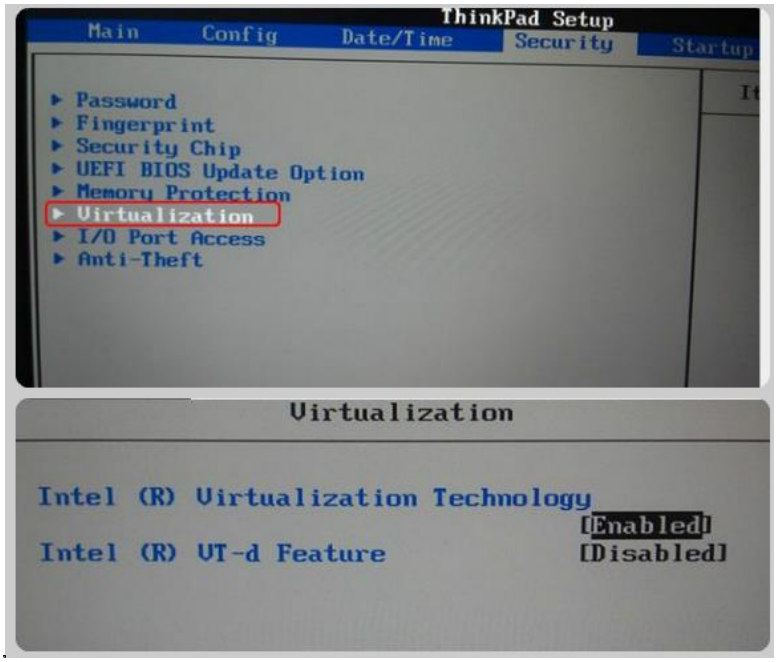
3. Select **Bootable > Write Disk Image** and choose the USB drive into which you want to write the image file. Then, click on **Write** button and keep others settings unchanged. You can remove the USB drive after the image file is written to the USB drive.


UltraISO (Trial Version) - D:\HCI6.2.0_EN\02-UpdatePackage&SetupPackage\For Southeast Asia Market\HCI\Sangfor_HCI6.2.0_EN(20210120).iso
File Actions Bootable Tools Options Help
Make Floppy Image...
Write Floppy Image...
Make Disk Image...
Write Disk Image...
Extract Boot Sector from Floppy/HDD drive...
Extract Boot File from CD/DVD...
Load Boot File...
Save Boot File...
Clear Boot Information
Generate Bootinfotable
Make Multi-Boot CD/DVD
Total Size: 3132MB
69% of DVD 4.7GB - 1343MB free
Path: /
Size Type Date/Time LBA
12 Folder 2013-11-28 14:30 22
448 KB Folder 2021-01-20 02:51 23
39,115 KB Folder 2021-01-20 02:53 25
246 KB Folder 2021-01-20 02:51 26
3,122,733 KB Folder 2021-01-20 02:56 28
44,010 KB Folder 2021-01-20 02:53 29
253 KB Folder 2021-01-20 02:53 30
26 KB 0 File 2020-04-09 12:06 19735
0 cfg File 2021-01-20 02:51 45
Path: D:\HCI6.2.0_EN\02-UpdatePackage&SetupPackage\For Southeast Asia Market\HCI
Filename Size Type Date/Time
MD5.txt 166 Text Document 2021-01-25 22:51
Sangfor_HCI6.2.0_EN(20210120).iso 3,207,240 KB Disc Image File 2021-01-20 11:09
Sangfor_HCI6.2.0_EN(20210120).... 2,080,479 KB pkg File 2021-01-20 10:35
Copyright (c)2002-2020 EZB Systems, Inc.
Image: 2 files, 26 KB
Local: 3 files, 5164 MB


UltraISO (Trial Version) - D:\HCI6.2.0_EN\02-UpdatePackage&SetupPackage\For Southeast Asia Market\HCI\Sangfor_HCI6.2.0_EN(20210120).iso
File Actions Bootable Tools Options Help
Make Floppy Image...
Write Floppy Image...
Make Disk Image...
Write Disk Image...
Extract Boot Sector from Floppy/HDD drive...
Extract Boot File from CD/DVD...
Load Boot File...
Save Boot File...
Clear Boot Information
Generate Bootinfotable
Make Multi-Boot CD/DVD
Total Size: 3132MB
69% of DVD 4.7GB - 1343MB free
Path: /
Size Type Date/Time LBA
12 Folder 2013-11-28 14:30 22
448 KB Folder 2021-01-20 02:51 23
39,115 KB Folder 2021-01-20 02:53 25
246 KB Folder 2021-01-20 02:51 26
3,122,733 KB Folder 2021-01-20 02:56 28
44,010 KB Folder 2021-01-20 02:53 29
253 KB Folder 2021-01-20 02:53 30
26 KB 0 File 2020-04-09 12:06 19735
0 cfg File 2021-01-20 02:51 45
Path: D:\HCI6.2.0_EN\02-UpdatePackage&SetupPackage\For Southeast Asia Market\HCI
Filename Size Type Date/Time
MD5.txt 166 Text Document 2021-01-25 22:51
Sangfor_HCI6.2.0_EN(20210120).iso 3,207,240 KB Disc Image File 2021-01-20 11:09
Sangfor_HCI6.2.0_EN(20210120).... 2,080,479 KB pkg File 2021-01-20 10:35
Copyright (c)2002-2020 EZB Systems, Inc.
Image: 2 files, 26 KB
Local: 3 files, 5164 MB

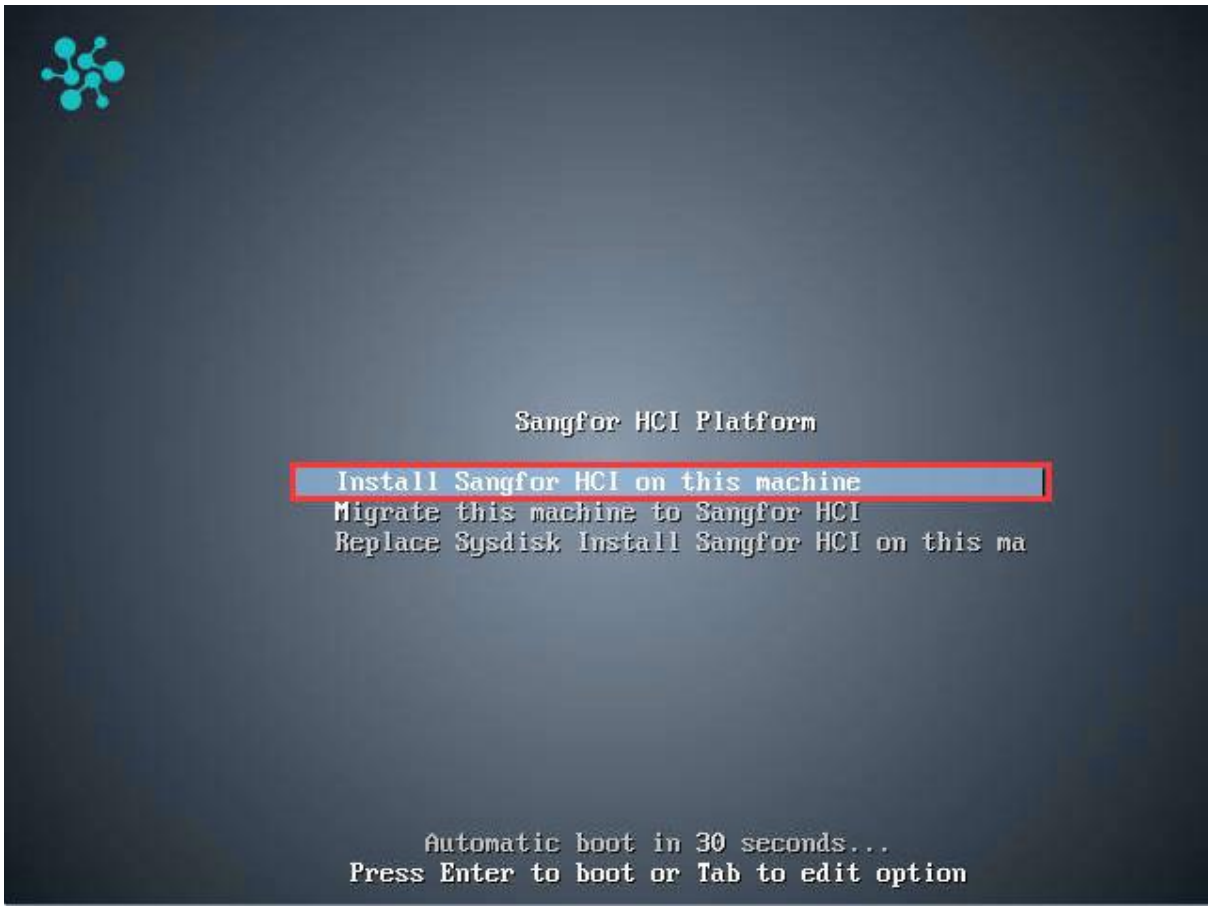


4. Enable **Virtualization Technology** in BIOS, as shown below (Note: BIOS settings vary from computer to computer).


ThinkPad Setup
Main
Config
Date/Time
Security
Startup
Password
Fingerprint
Security Chip
UEFI BIOS Update Option
Memory Protection
Virtualization
I/O Port Access
Anti-Theft
Virtualization
Intel (R) Virtualization Technology
[Enabled]
Intel (R) VT-d Feature
[Disabled]

1.2.2 Installation of Sangfor HCI Manager

Insert the USB drive into a server, and set the USB drive as the first boot device priority in BIOS settings. Reboot the computer and system enters the following page. Select **Install Sangfor HCI on this machine,** and then press **ENTER** to enter installation page.

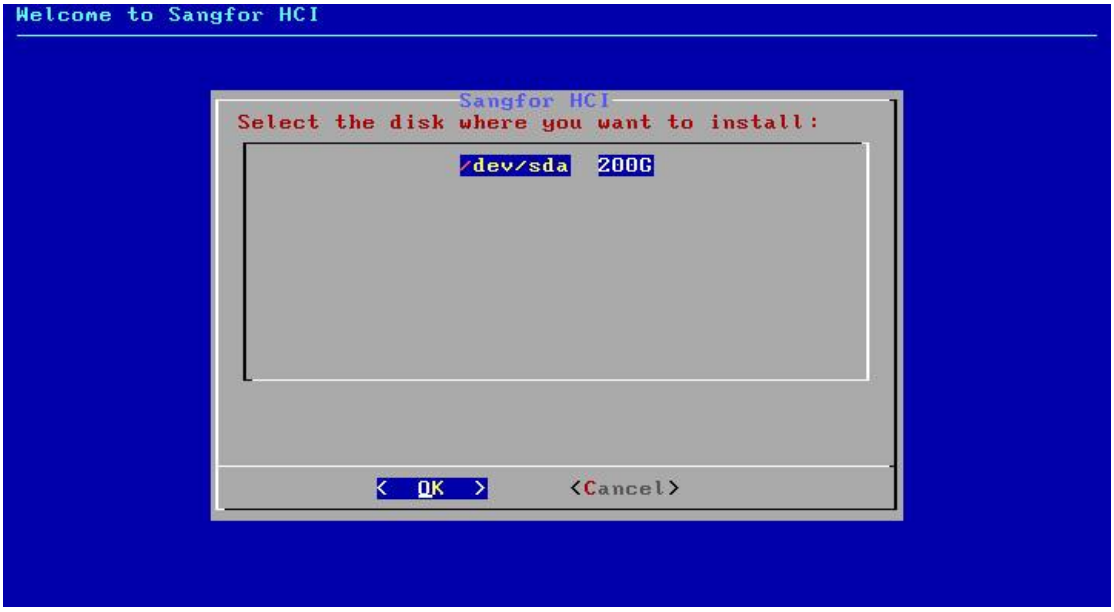


Select **SANGFOR HCI Installer** to begin installation.

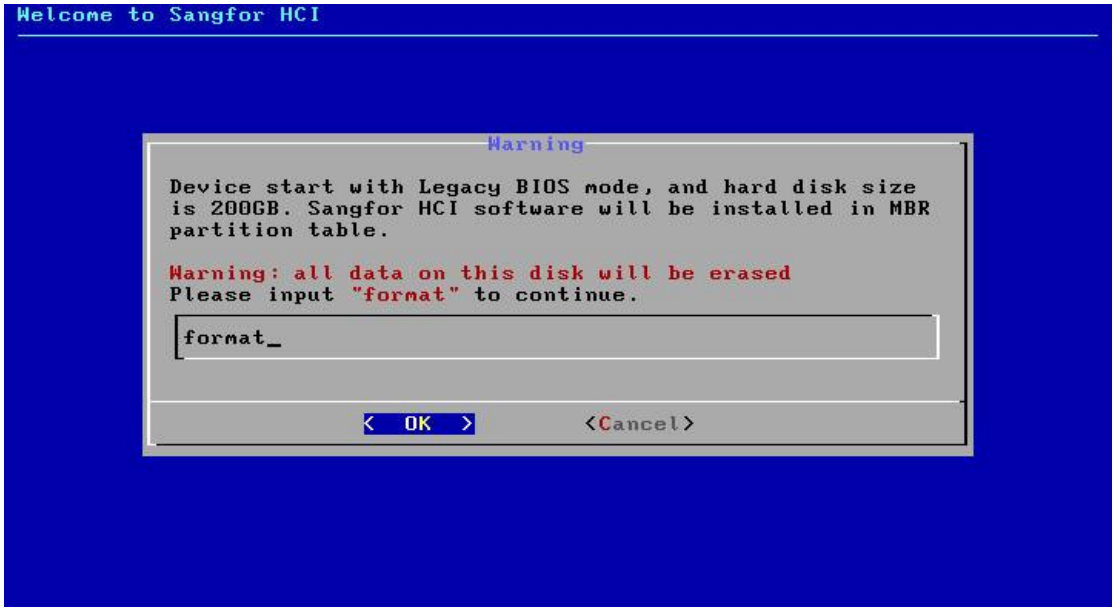
For versions earlier than Sangfor HCI5.0, only 64-bit Intel CPU processor is supported. Starting from Sangfor HCI5.0 and later versions, AMD processor is also supported.

Select a disk where you want to install Sangfor HCI software and then select **OK**. If there is only one disk, you can select **OK** directly.

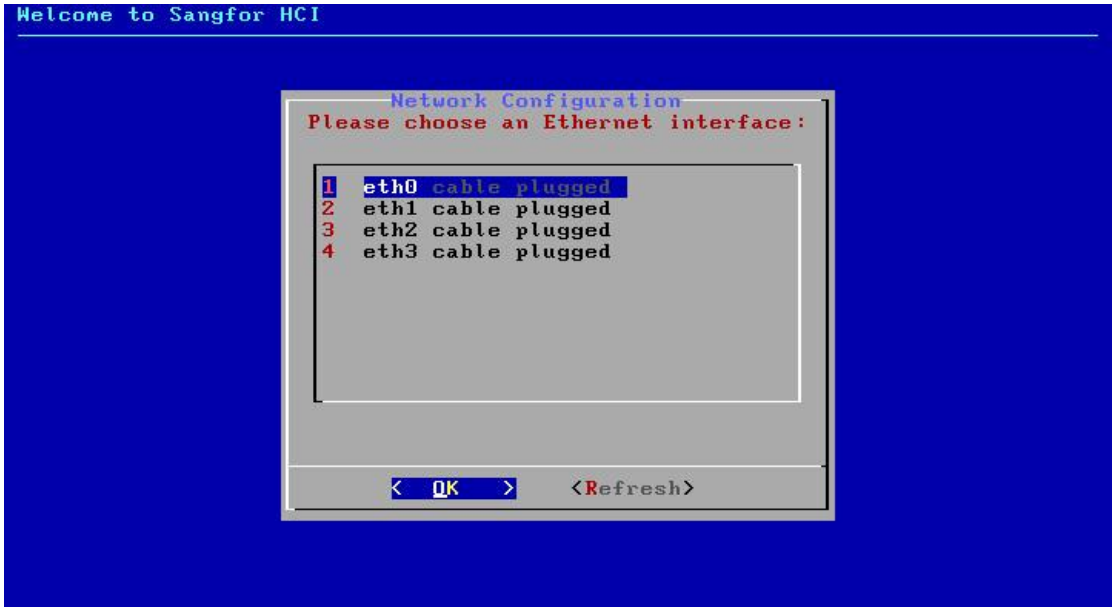
Capacity of the selected disk must be greater than 60GB. If it is greater than 2TB, it is better to use UEFI mode for installation.



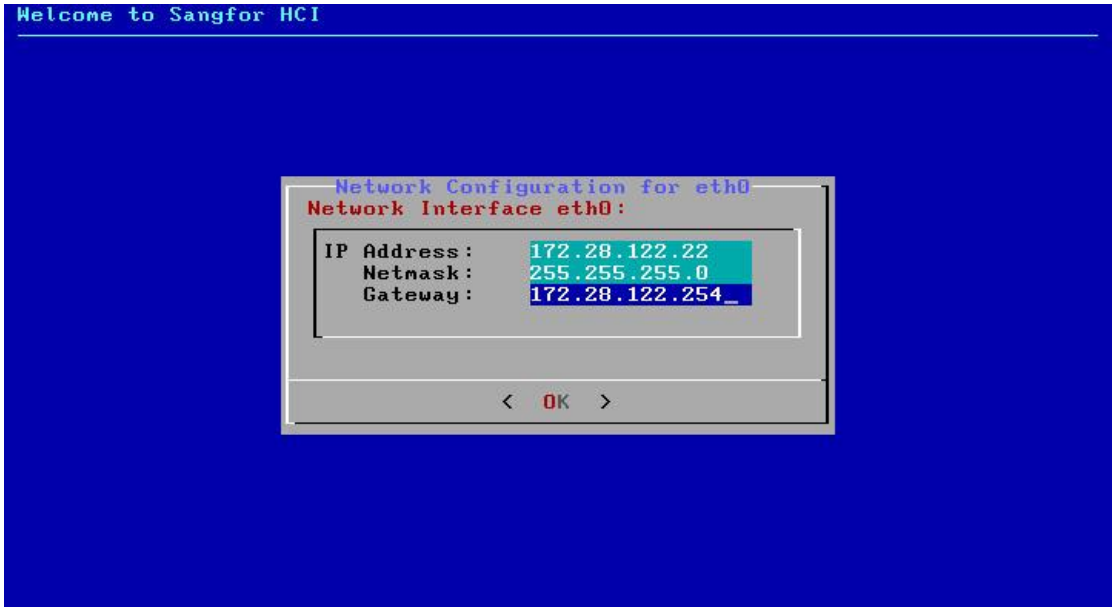
After the disk is selected, you will be prompted to format the disk. Enter "format" to confirm formatting disk, and select **OK** to continue installation. After you select **OK**, the **Disk Speed Tester** page will appear. To test disk speed, select **Yes**. To skip this step, select **No**.



After installing the Sangfor HCI software, you will be prompted to select an Ethernet interface and configure IP address for that interface.



If you skip the step of configuring Ethernet interface, etho interface will be chosen and assigned with the IP address 10.250.0.7, and gateway will be set to 255.255.255.0 by default. If there are more than one servers having Sangfor HCI software installed but their NICs are not configured, a same default IP address will be assigned to those NICs, resulting in IP address conflict.

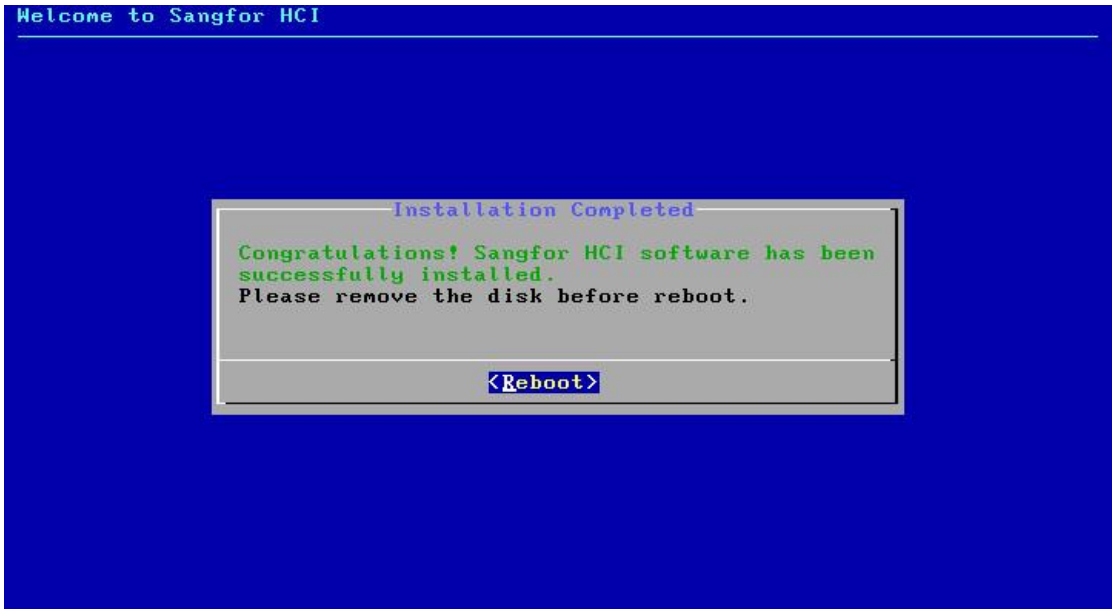


Select an Ethernet interface and set IP address, netmask and gateway address, then click **OK**.

Default gateway can only be set for one NIC. IP addresses configured for the selected interface and gateway should be on a same network segment, otherwise error may occur.

After the selected interface is configured, you will be asked whether to continue to configure another interface. Select **Yes** to return to network configuration page. or select **No** to finish the installation

After the installation completes, remove the USB drive and then select **Reboot** to restart the server.



Administrator can log into Web admin console of Sangfor HCI platform by entering https://IP address into browser address bar(that IP address is the IP address of the Ethernet interface selected on the network configuration page).

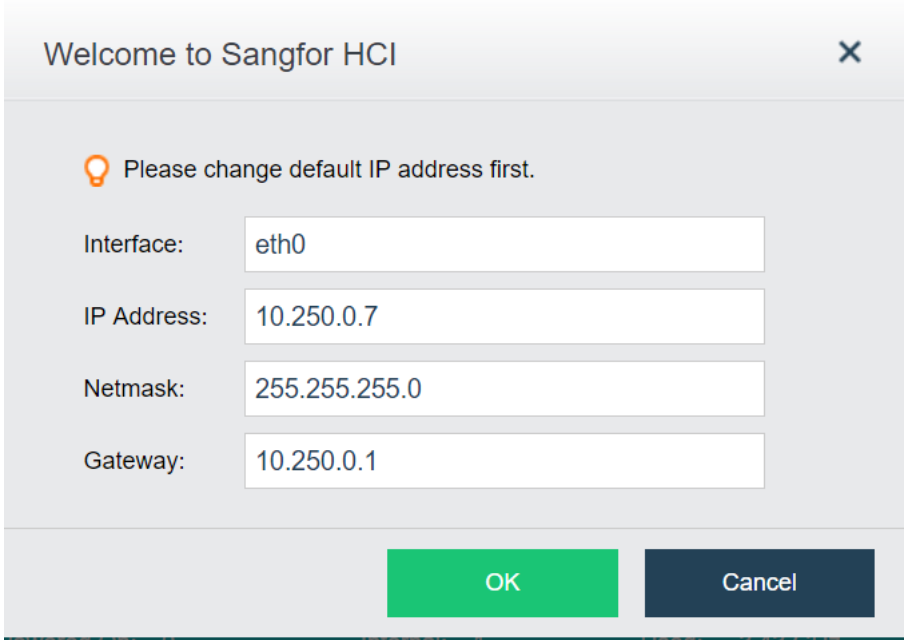
Web admin console of Sangfor HCI platform can only be accessed through the following browsers: Chrome, Firefox, IE11, IE10.

1.2.3 Initializing Sangfor aServer

Sangfor aServer has been pre-installed Sangfor HCI operating system and configured with a management interface(etho, default IP address:10.250.0.7/24). To access Web admin console of Sangfor HCI platform on a PC, first configure the PC with an IP address on a same network segment with that management interface and connect it to the etho interface on the aServer. Then open your browser and enter https://10.250.0.7/ into address bar to log in to Sangfor HCI platform console.

Default username and password are **admin**. Administrator will be prompted to change default password upon first login. If the default password has not been changed for one month, administrator will be forced to change it.

Upon first login, administrator will be prompted to modify default IP address of management interface, as shown below. If there are multiple aServers deployed in network, default IP address of management interface on each aServer needs to be modified, and addresses of management interfaces must be on a same network segment.



1.3Initializing Sangfor HCI Platform

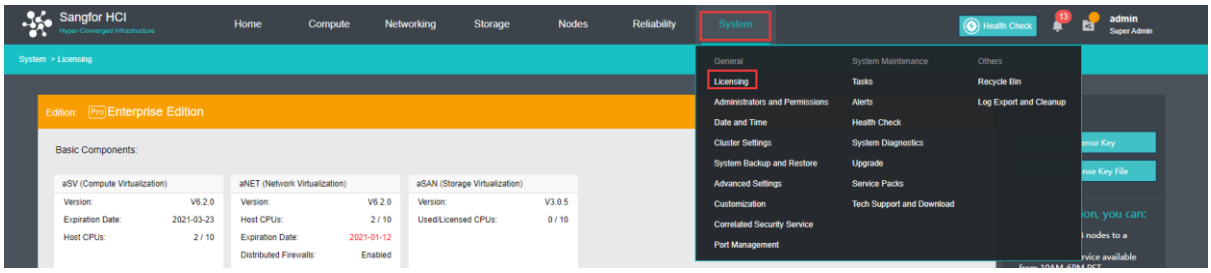
When you log into Web admin console of Sangfor HCI platform for the first time, a wizard will pop up to guide you through initialization of Sangfor HCI platform. To initialize Sangfor HCI platform, follow the instructions in the wizard.

1.3.1 Configuring Cluster

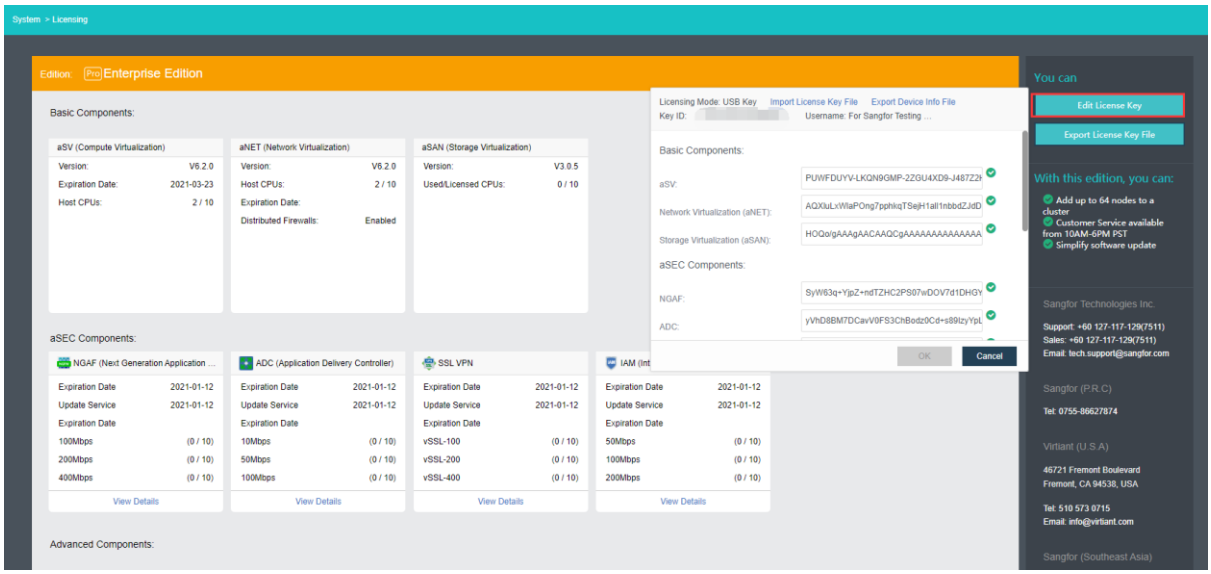
On Sangfor HCI platform, a cluster can be created by adding multiple nodes in order to manage resources centrally. To create a cluster, you need to add hosts into that cluster.

1.3.1.1 Authorization

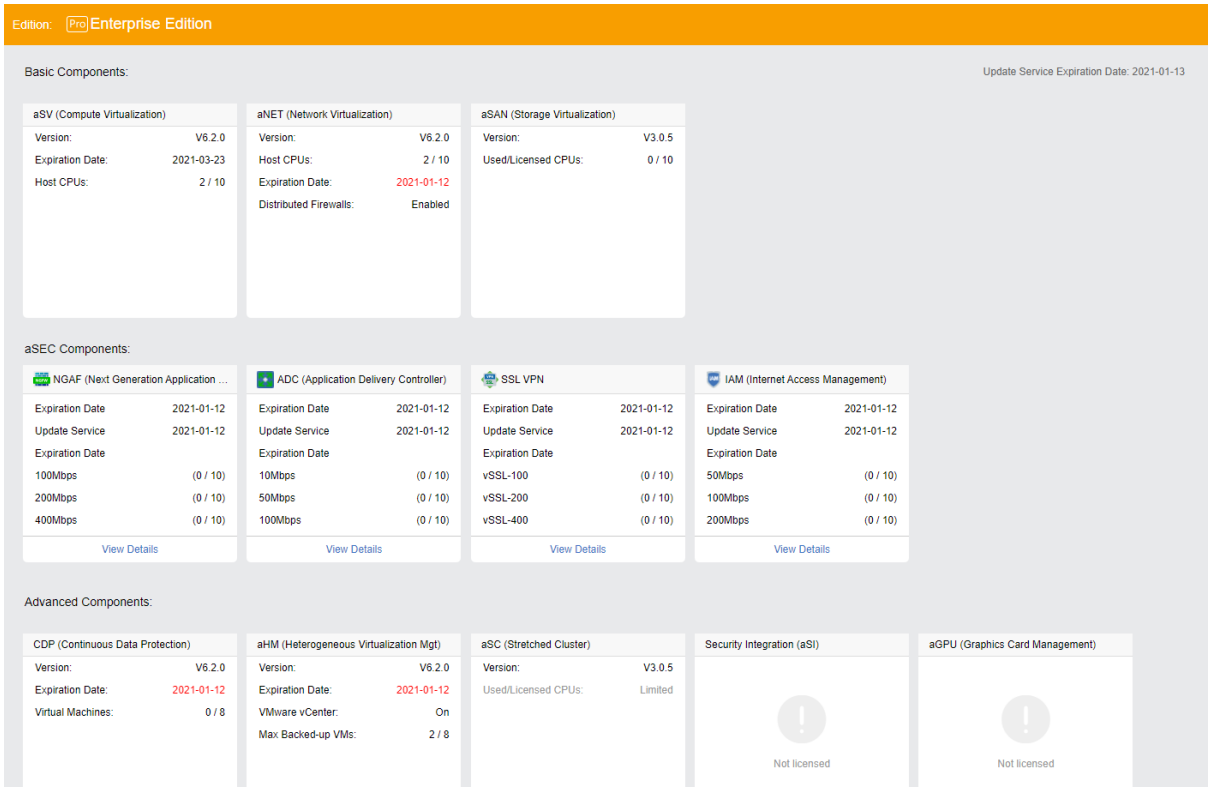
Insert a USB key containing license key information into the cluster controller, and then go to **System > General > Licensing**, as shown below:



To input license key, click **Edit License Key** > **Import License Key File**.

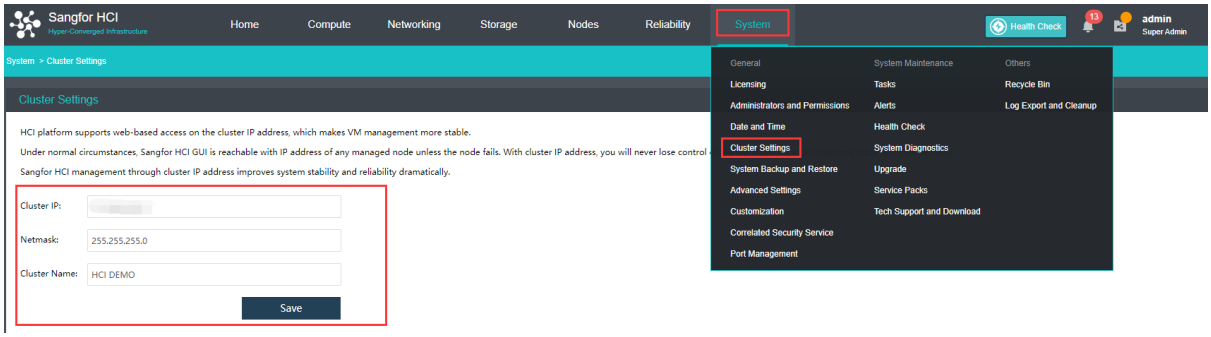


After clicking **OK,** you can check the license information on the left panel to determine whether the license key is activated successfully, as shown below:



1.3.1.2 Configuring Cluster IP Address

You can access Sangfor HCI GUI to manage virtual machines through cluster IP address in case one node fails. To configure cluster IP address, go to **System > Cluster Settings**.

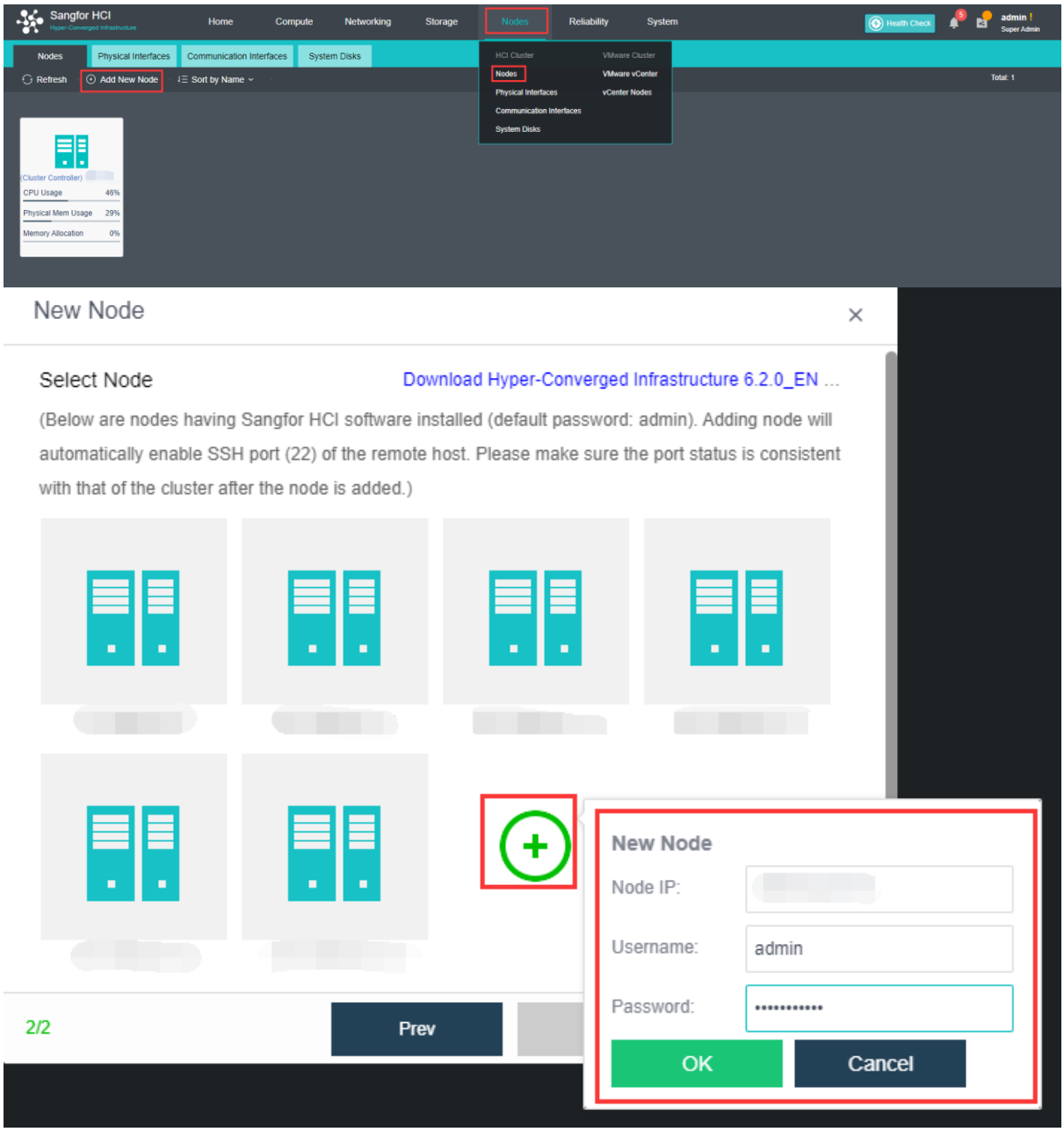


Note that cluster IP address and host NIC address cannot be the same, or else, it will result in IP address conflict.

1.3.1.3 Adding Node

In **Nodes,** you can add node to a cluster by clicking **Add Node**.

On the following page, select a node that you want to add to cluster and input the corresponding username and password. Once a node is chosen, node icon turns green, which indicates that node can be added to the cluster.



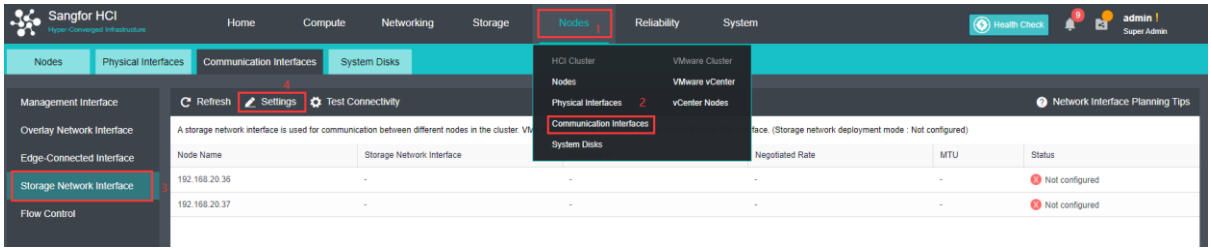
1.3.2 Initializing Virtual Storage

1.3.2.1 Configuring Storage Network Interfaces

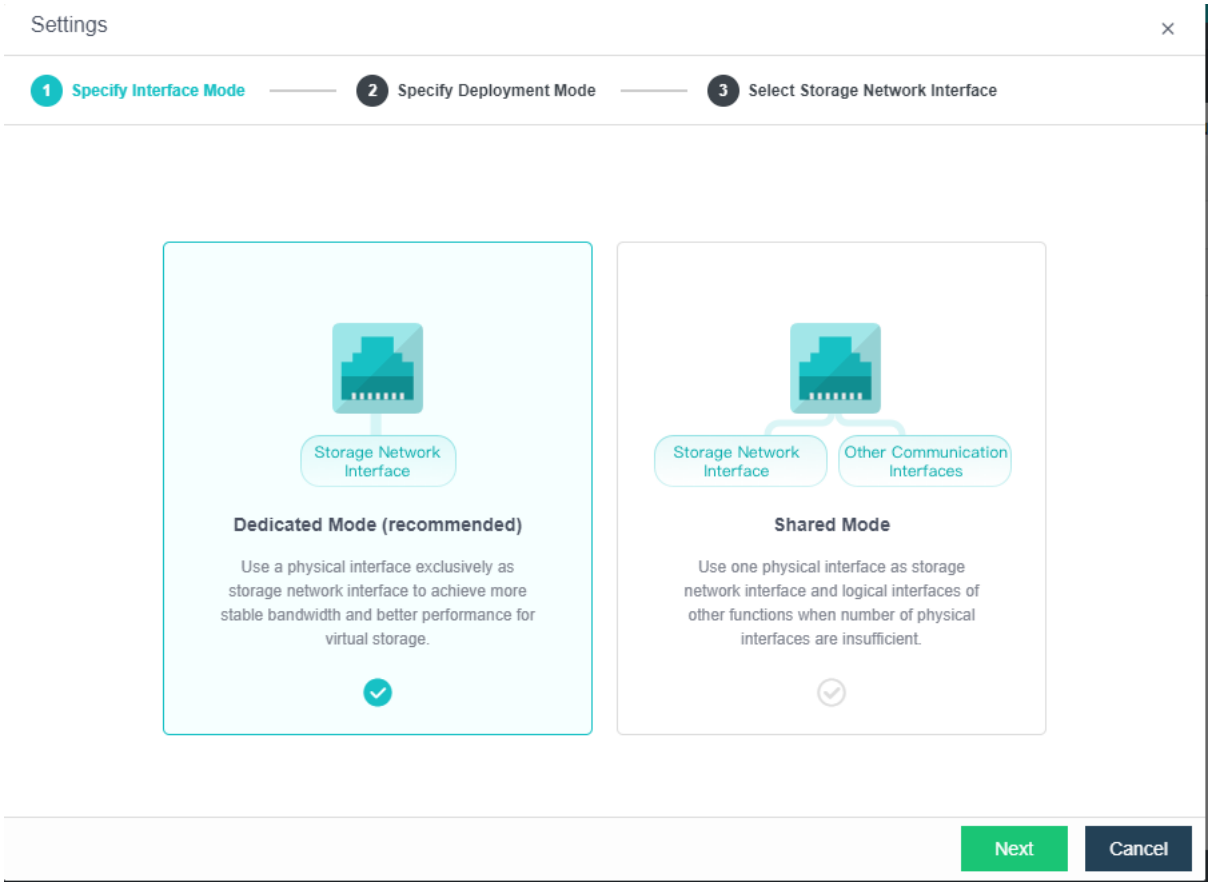
Go to **Storage** and click **Settings** on the dialog that pops up to configure storage deployment mode.

By default, etho is used as management interface and communication interface to synchronize configurations on Sangfor HCI platform. Storage network interface is used to synchronize file data on virtual storage. It is better to use separate interfaces as management interface and storage network interface.

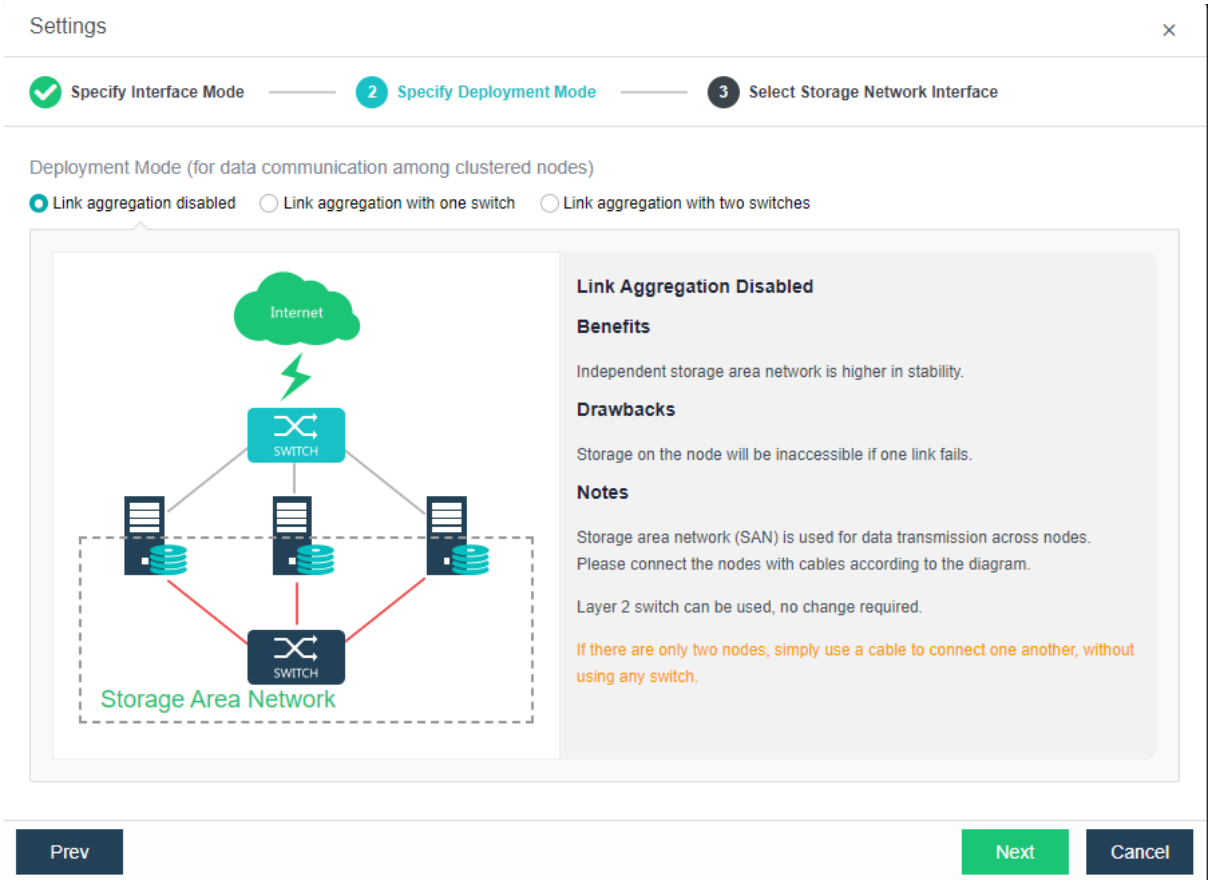
a. Navigate to **Nodes** > **Communication Interfaces** > **Storage Network Interface,** and select **Settings**.



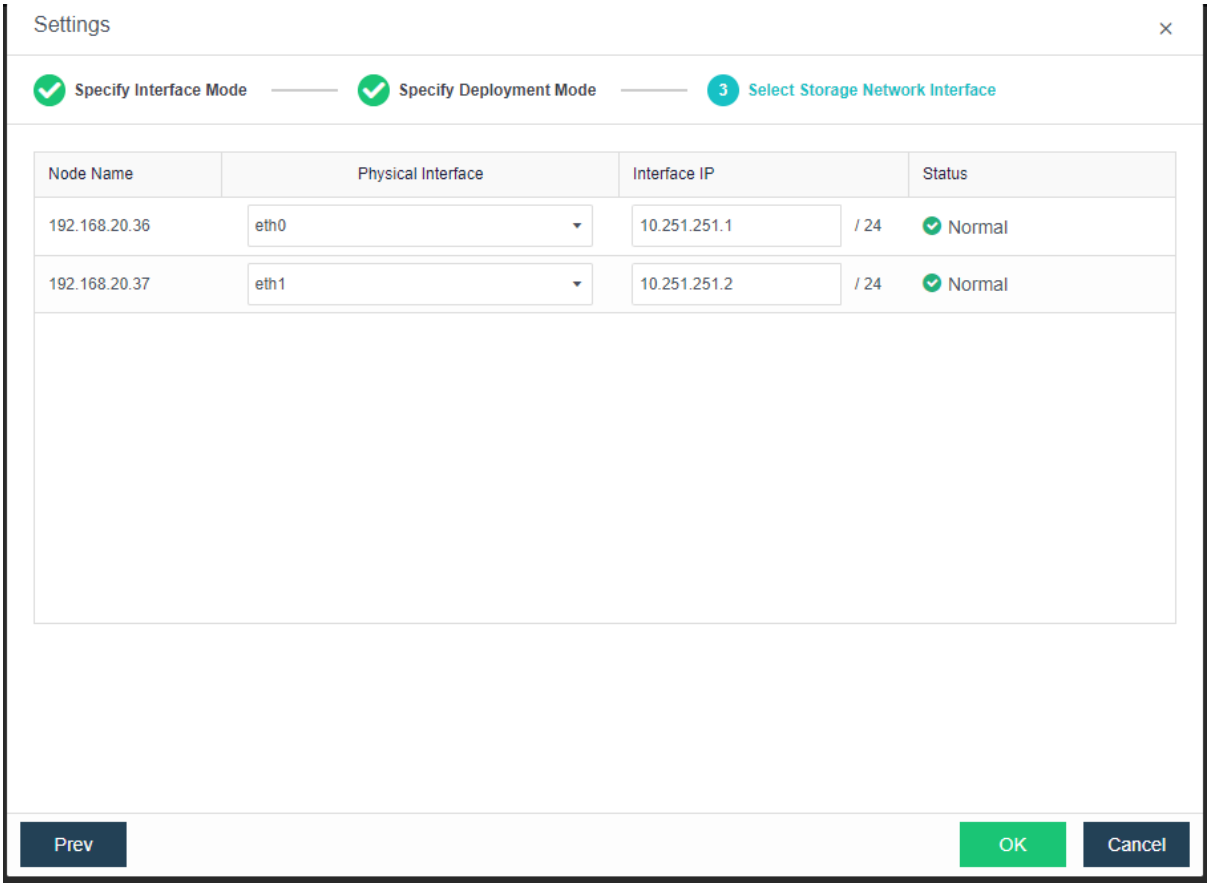
b. Specify the interface mode from dedicated mode or shared mode. In this case, dedicated mode will be used.



c. Specify the deployment mode of the storage network interface. In this case, Link aggregation disabled will be use.



d. Lastly, specify the interface used for storage network and configure the corresponding IP address for communication.

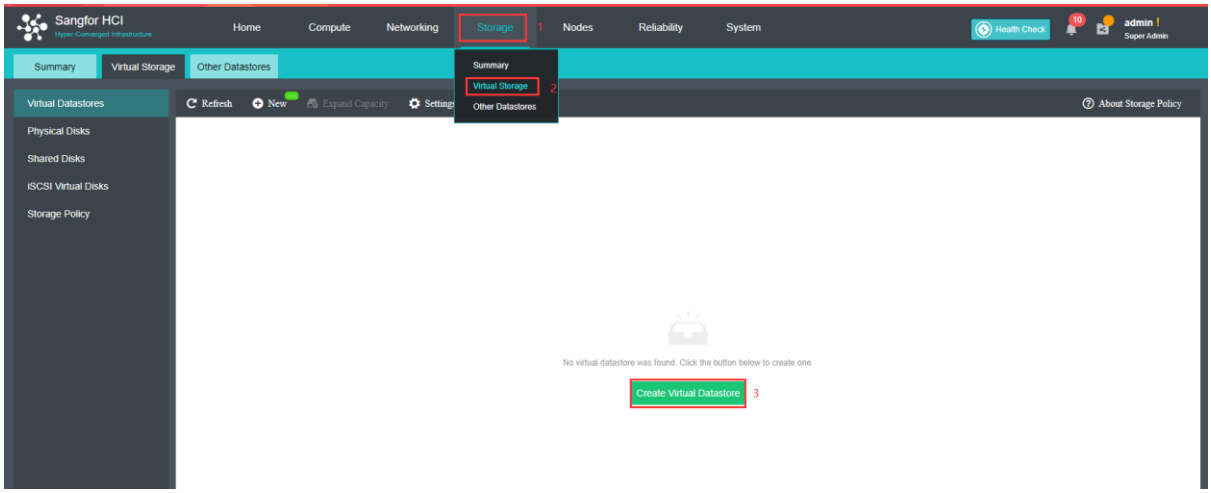


Each node communicates with another one using two physical interfaces which are connected to a same layer 2 switch. Storage network interfaces will be aggregated automatically without the need to configure link aggregation on switch. After the deployment mode is selected, you need to deploy the network according to the digram illustrating deployment architecture of storage area network, and then select storage network interface for each node and configure IP address for that interface.

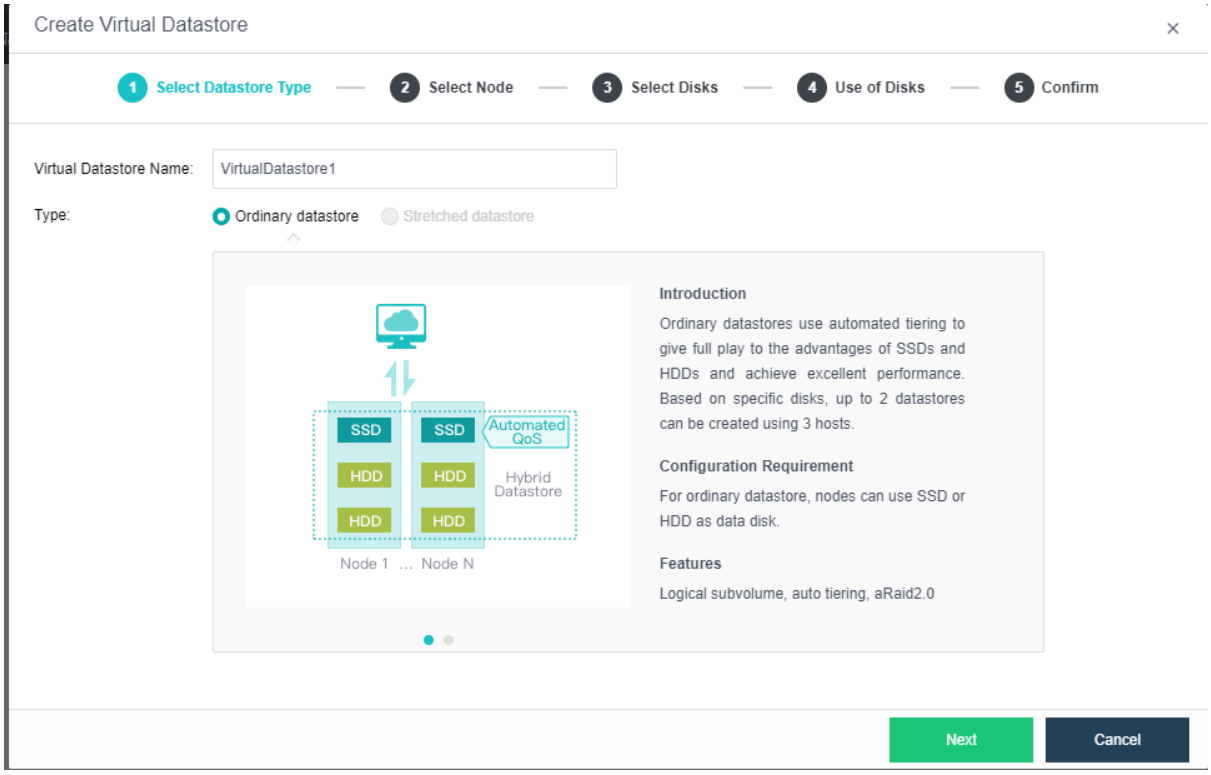
Storage area network is built after storage network interface is configured.

Configuring Datastore Type and Disks

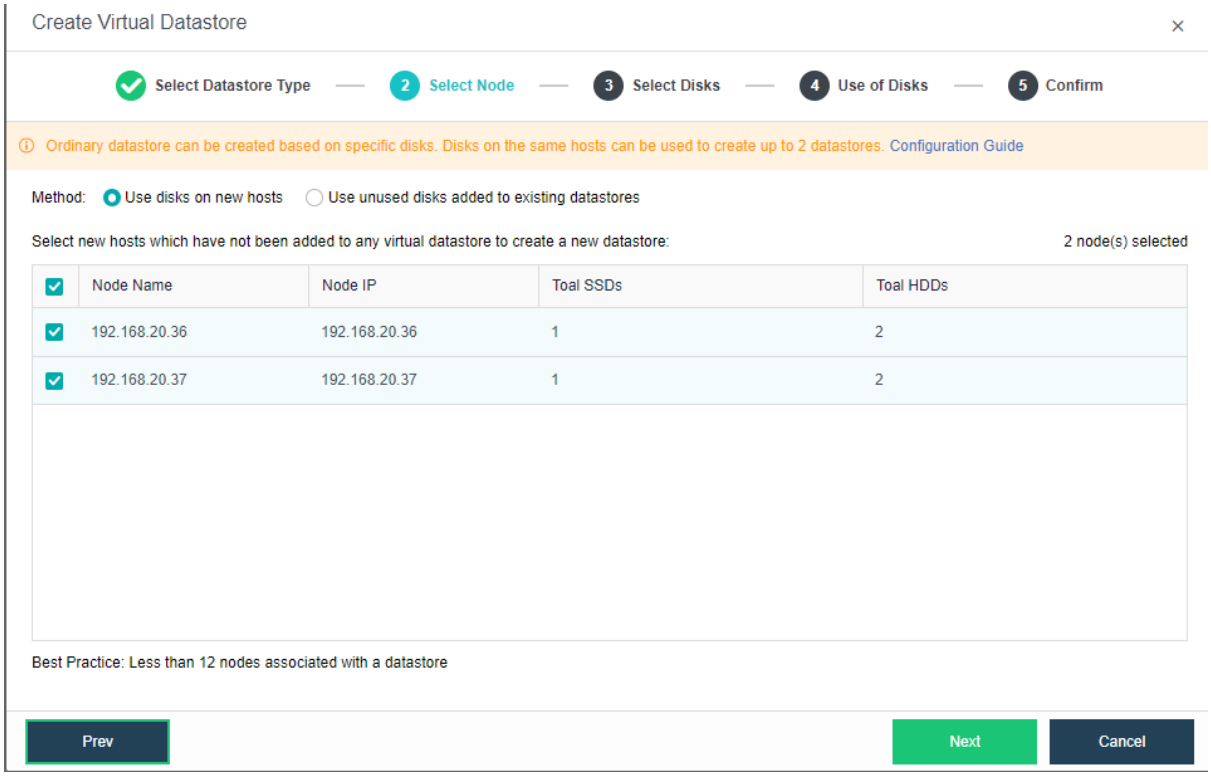
1. Navigate to Storage > Virtual Storage, select **New** or **Create Virtual Datastore**.



2. Select datastore type, in this case Ordinary datastore will be created.

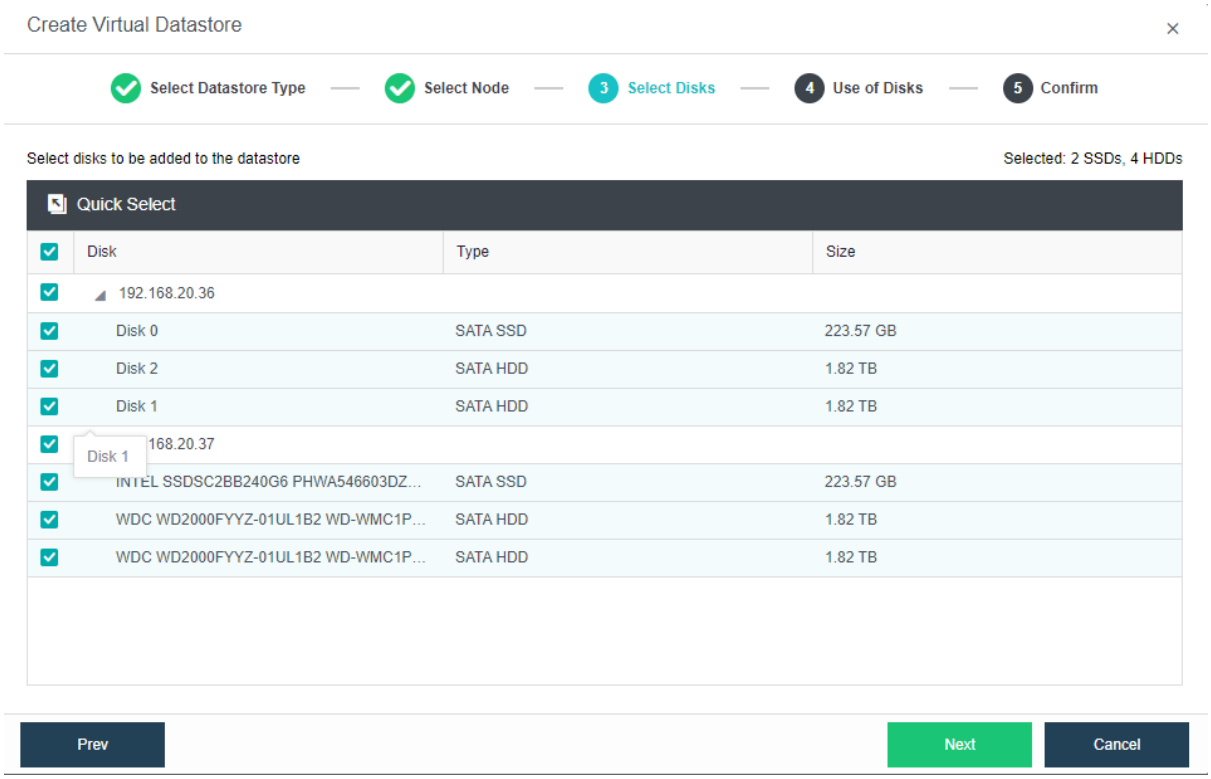


3. Select corresponding method and nodes to create virtual datastore, as currently creating very first virtual datastore, [**Use disks on new hosts**] will be use.

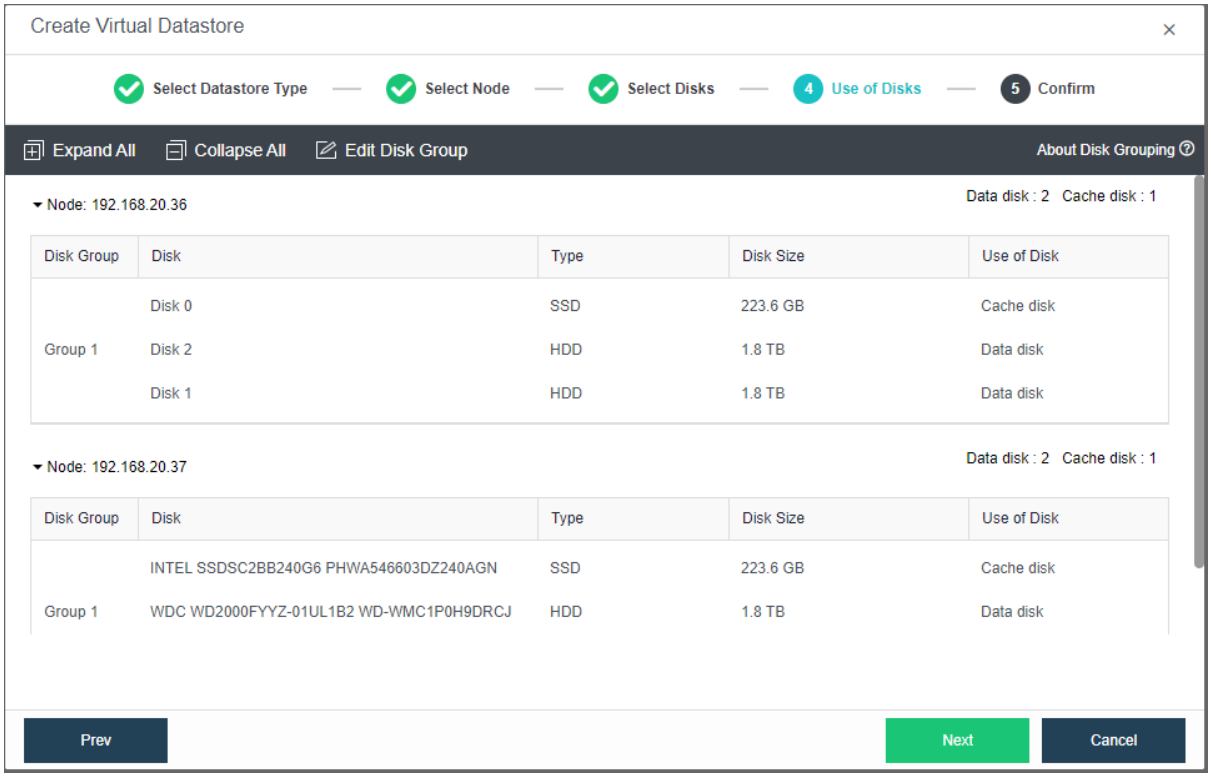


4. Select the disks will be used to create virtual datastore.

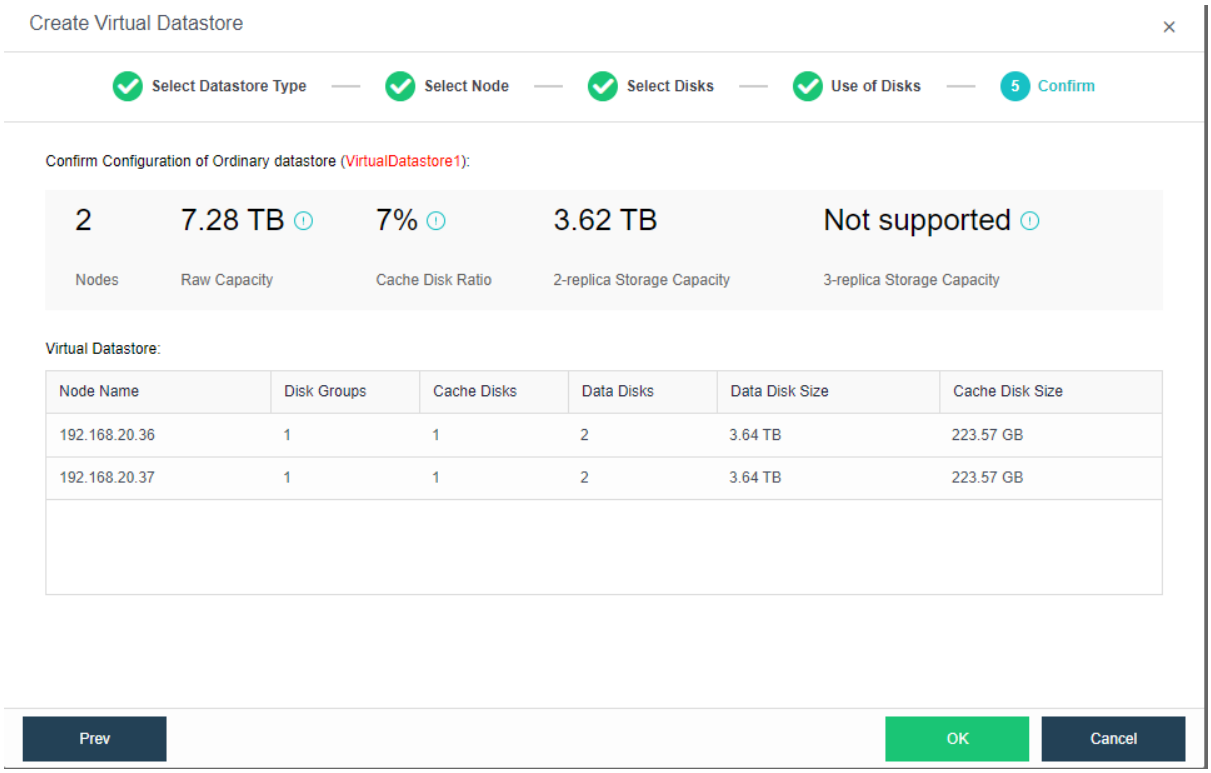
   For hybrid datastore, at least 1 SSD is required as cache disk.



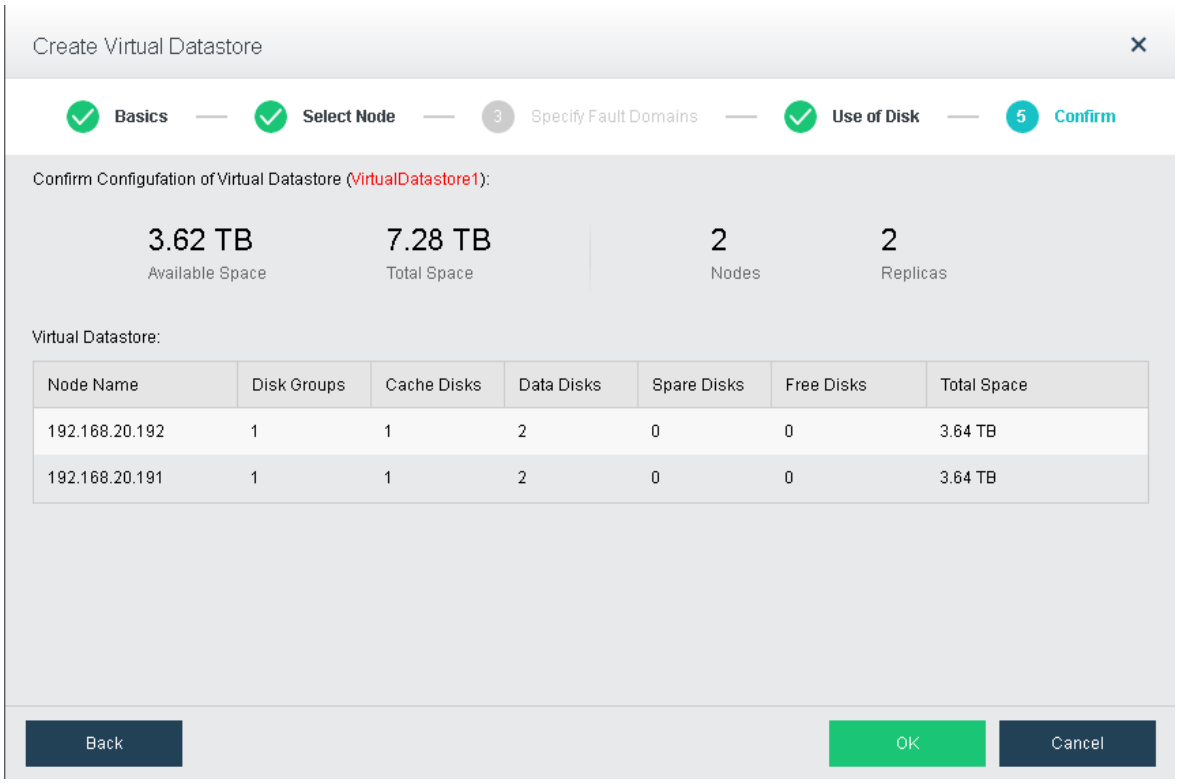
5. Specify the use of disks. By default, HCI will assign the disk automatically.



6. Confirm on the details and proceed with the virtual datastore creation.

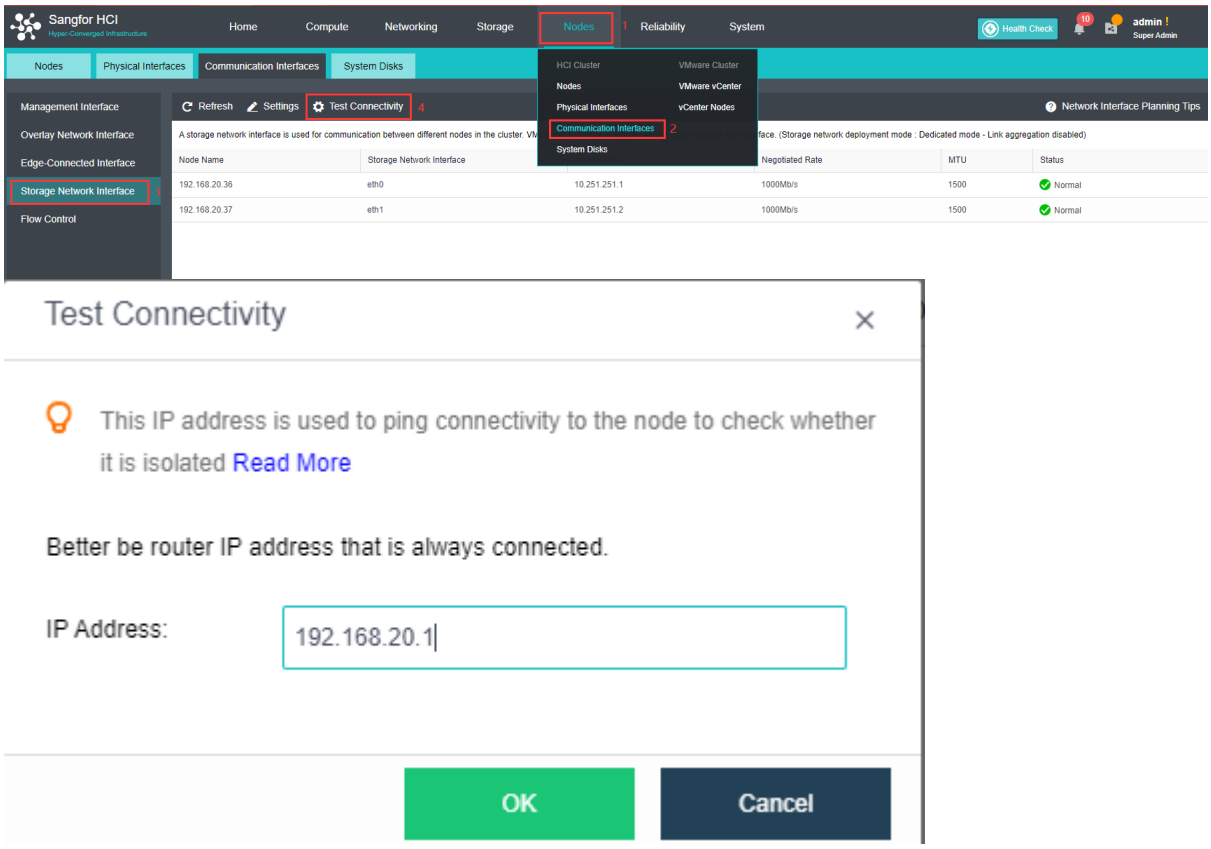


The following page displays virtual storage configurations, including available disk space, number of data copies, and total number of disks. After confirming configurations, click "OK" and input administrator account password admin, and then click Finish to begin initialization of virtual storage.



Testing Connectivity

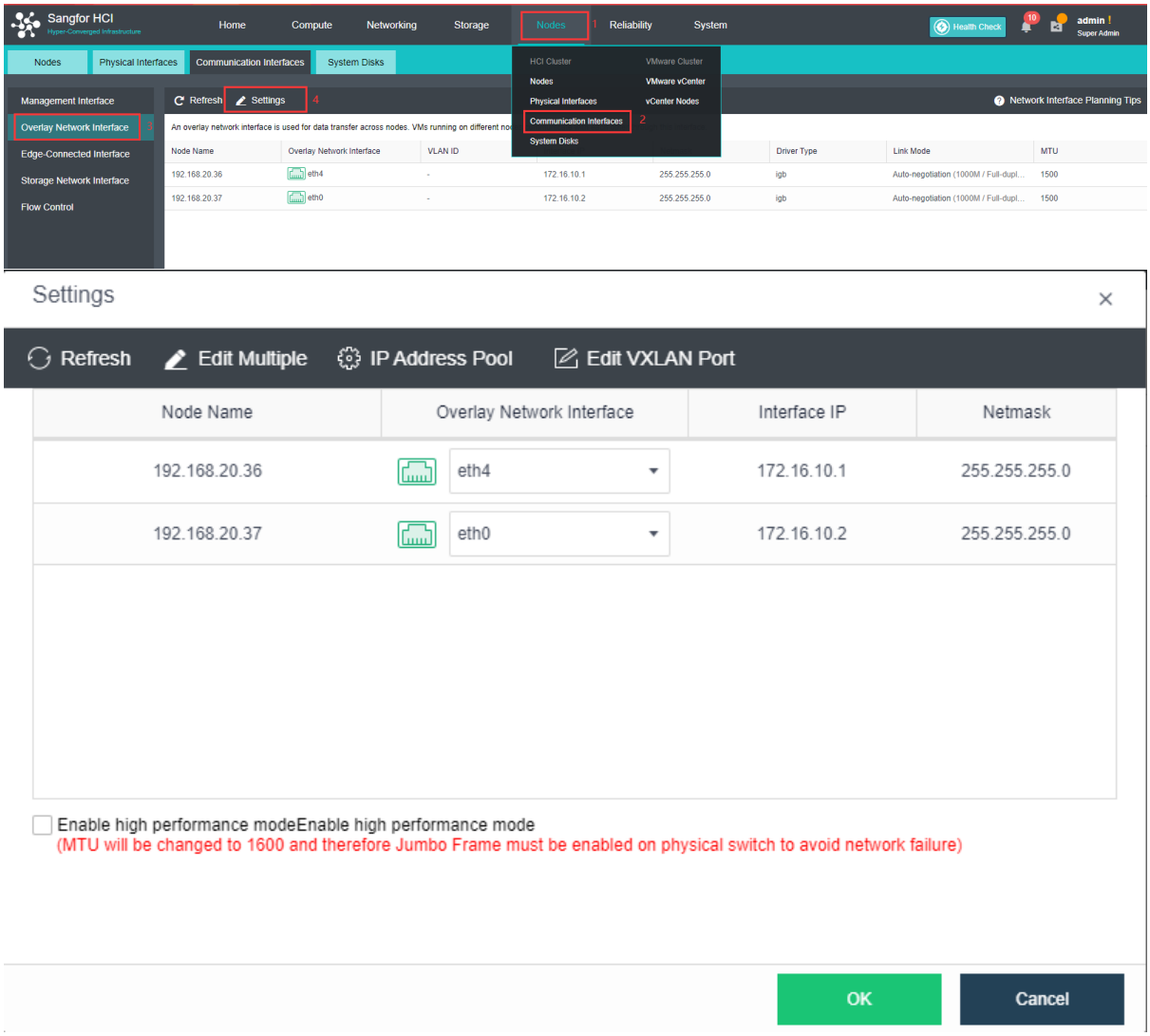
On the Virtual Storage dialog, click on Test Connectivity button to enter the following page. On that page, specify an IP address(it is often the gateway address)which should be allowed to ping, in order to check if the node is connected.



1.3.3 Configuring Overlay Network Interface

After a cluster is created, you need to configure overlay network interface for each node. Overlay network interface must be a Gigabit or 10-Gigabit interface and connected to a Gigabit or 10-Gigabit switch (If there are only two nodes, connect two overlay network interfaces directly without using any switch). To improve bandwidth and redundancy of overlay network interface, you can use an aggregate interface as a overlay network interface.

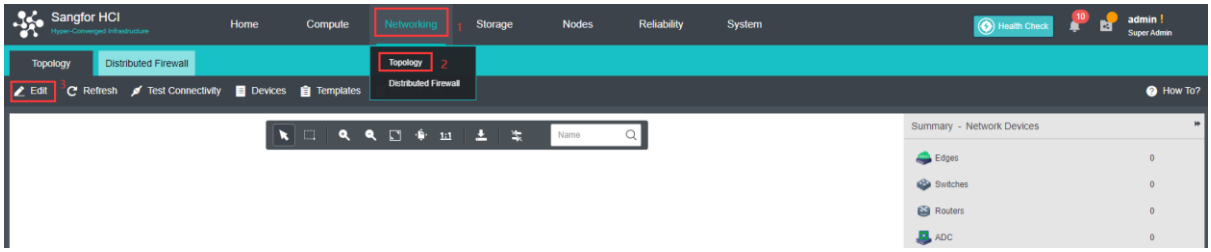
By default, management interface and overlay network interface are set to a same interface. To improve data transmission efficiency, configure the management interface and overlay network interface(VXLAN) to reside on different physical NICs. To configure overlay network interface, go to **Nodes > Communication Interface > Overlay Network Interface(vxLAN)**. Specify an overlay network interface for each node and configure a corresponding IP address and netmask.

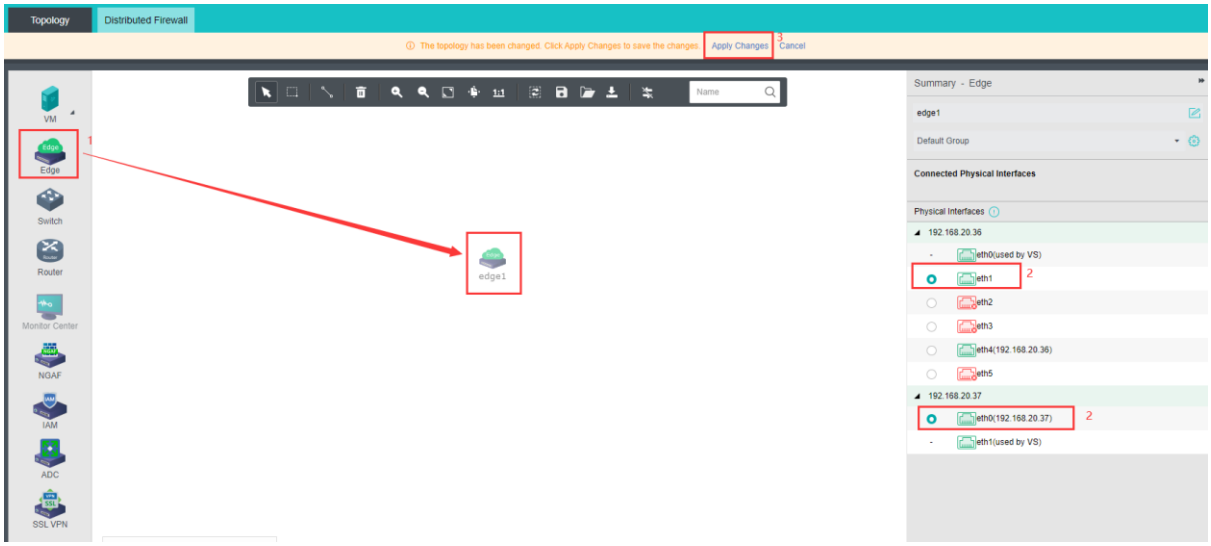


To improve data transmission efficiency, enable high performance mode. In that mode, MTU will be changed to 1600 and therefore VXLAN encapsulated data will not be fragmented when being forwarded to physical network, but Jumbo Frame must be enabled on the physical switch connected to a host installed Sangfor HCI software.

1.3.4 Configuring Edge

If multiple nodes form a cluster and provide business service as a whole, a virtual machine may run on any node, therefore, an edge should be connected to an interface on each node and that interface should be connected a same L2 physical switch, ensuring that virtual network traffic can go into physical network through any node.



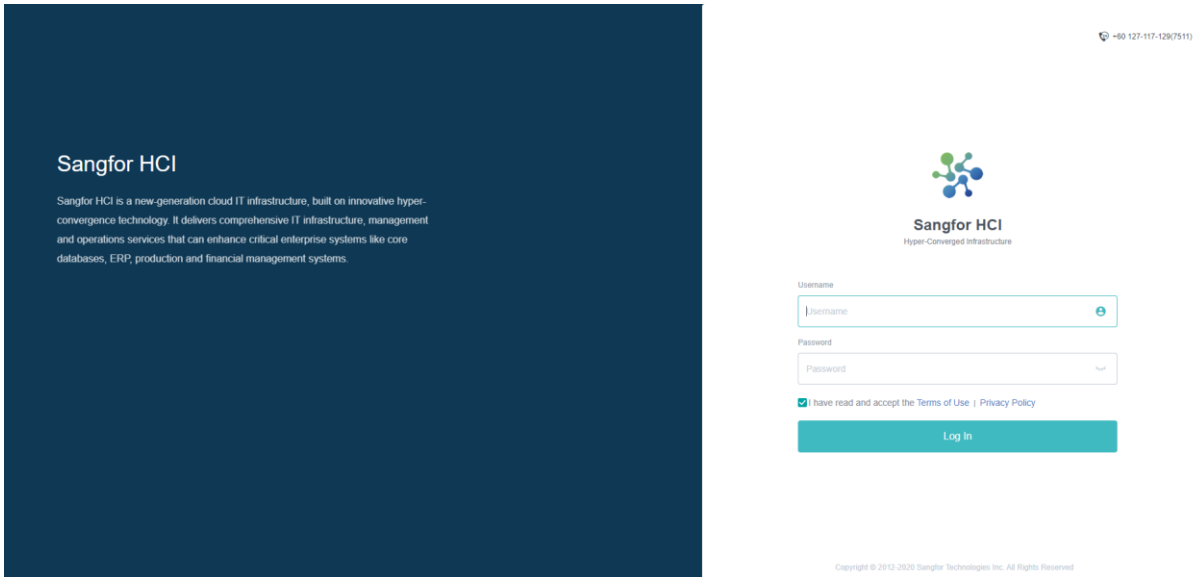


Chapter 2 Initial Login to Sangfor HCI Console

Sangfor HCI platform provides web-based administration. Administrators can access admin console of Sangfor HCI platform through its management interface address which is specified during installation of Sangfor HCI software.

If that management interface address is not specified during the installation, the default IP address(10.250.0.7) will be used. Before logging into Sangfor HCI GUI, connect a physical interface on a PC to the first interface on the host where Sangfor HCI software is installed, and then configure an IP address on that PC, which should reside on the network segment 10.250.0.x. Open browser and enter https://10.250.0.7 into the address bar to log into Sangfor HCI GUI, as shown below:

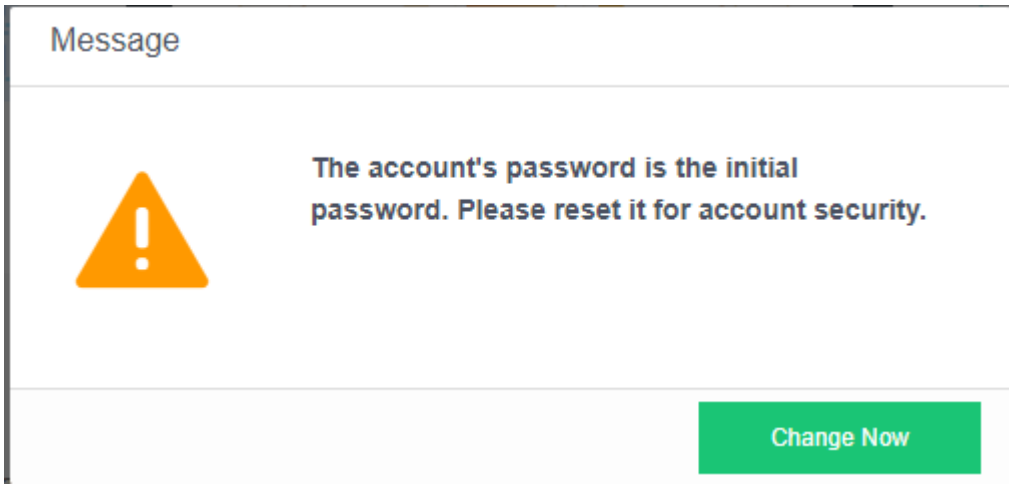
If that management interface address is specified during installation, access Sangfor HCI console through that specified IP address.



On the login page, as shown above, enter username and password, and then click **Log In**. Default username and password are **admin/admin**.

Upon successful login, the following dialog box will pop up to prompt administrator to

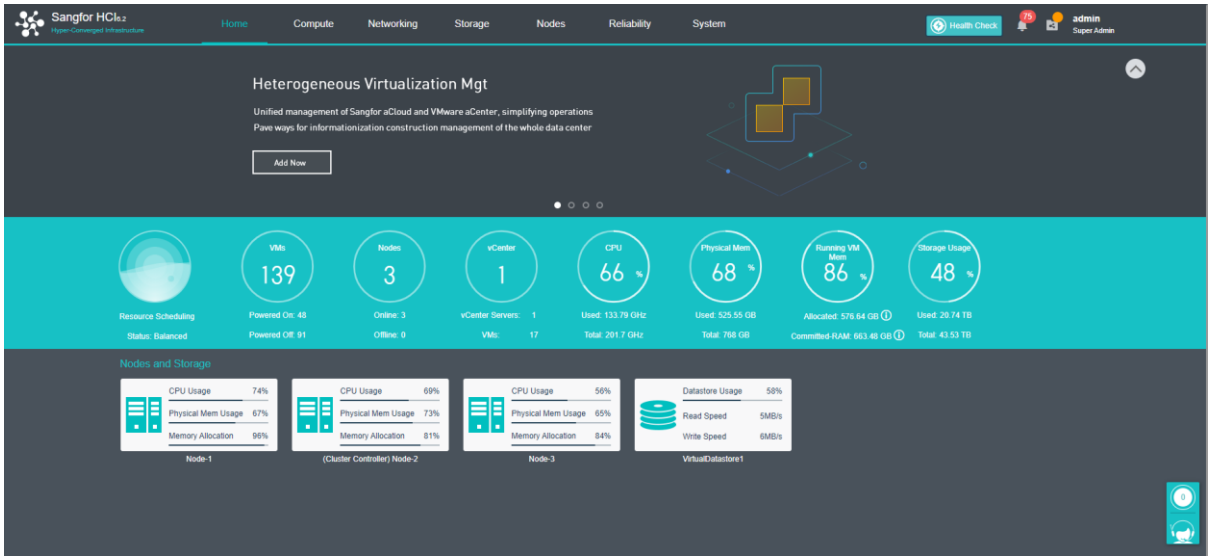
change password.



- Sangfor HCI console can be accessed with the following browsers: IE11, Firefox, Chrome, etc.
- The host installed Sangfor HCI software is taken as a clustered node by default. It can be added to other clusters, or be regarded as a cluster controller so that other nodes can be added onto its HCI platform.

Log in to Sangfor HCI Web admin console and a QR code will pop up , and you can scan the QR code to verify software edition.

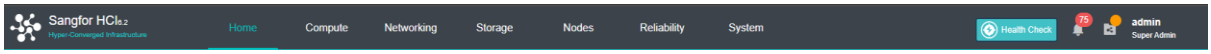
GUI of Sangfor HCI platform is shown below:



2.1 Home

2.1.1 Navigation Bar

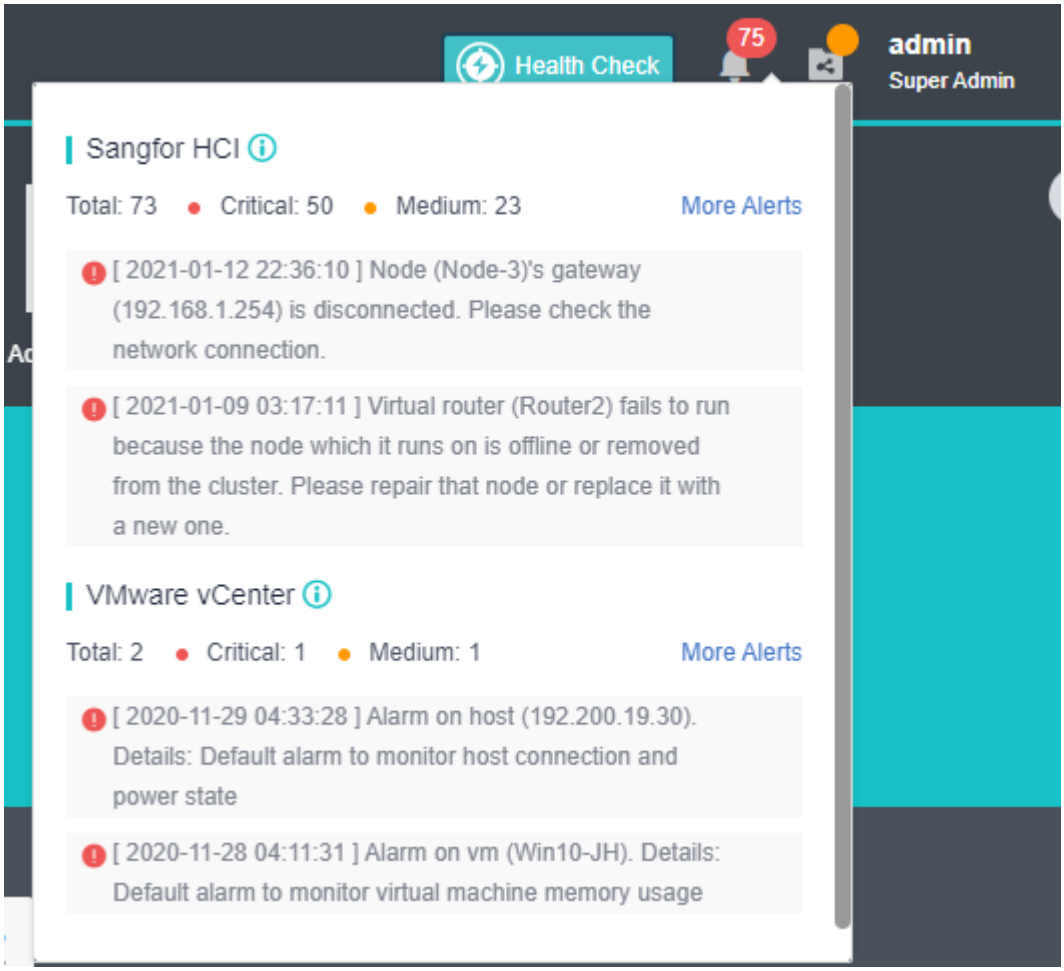
There are six modules on the navigation bar, as shown below:



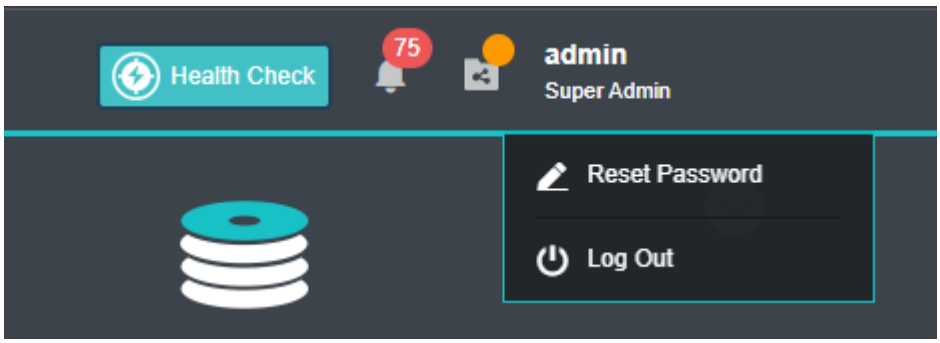
- ✓ **Home**: You can view information about nodes, virtual machines, storage, CPU usage, memory usage and storage usage.
- ✓ **Compute**: You can configure and manage virtual machines.
- ✓ **Networking**: You can configure virtual network.
- ✓ **Storage**: You can view storage status and configure virtual storage.
- ✓ **Nodes**: You can configure and manage cluster, nodes and storage.
- ✓ **Reliability**: You can configure scheduled backup, snapshot, HA, resources scheduling,VM scheduling, UPS.
- ✓ **System: It** includes **General**, **System Maintenance** and **Others**. **General** includes **Licensing, Date and Time, System Administrators and Permissions, Alarm Options, Cluster Settings, System Backup and Restore, VMware vCenter** and **VM Backup and Recovery**, etc. **System Maintenance** includes **Tech Support & Download, Logs and Alarms, Upgrade, Health Check** and **Customization, User Management, Work Orders**, etc. **Others** includes **Recycle Bin** and **HA & Resource Scheduling** etc.
- ✓ **Health Check**: It checks cluster environment to find and locate issues, and offers solutions for discovered issues.

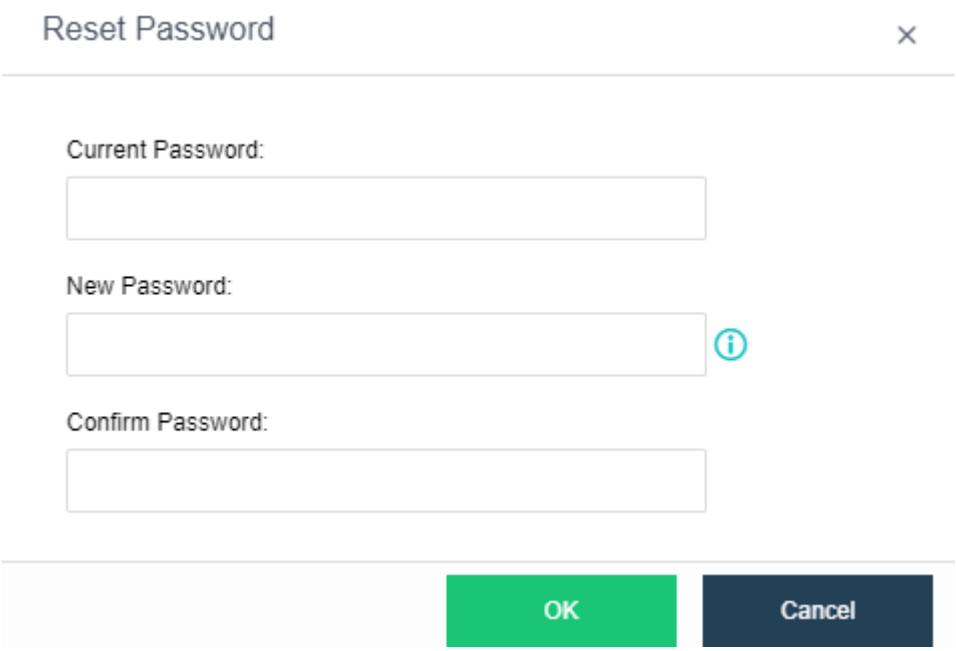
To view alarm events, click the following icon (the number on the icon indicates the number of the current alarm events) to view the latest 5 alarm events, as shown below:

The number beside the exclamation mark indicates the number of alarms. To view details of the alarms for SANGFOR HCI and VMware vCenter(if any is added), click on the exclamation mark.



To change admin password, click on the "**admin Super Admin**"located on the right top of web ui.

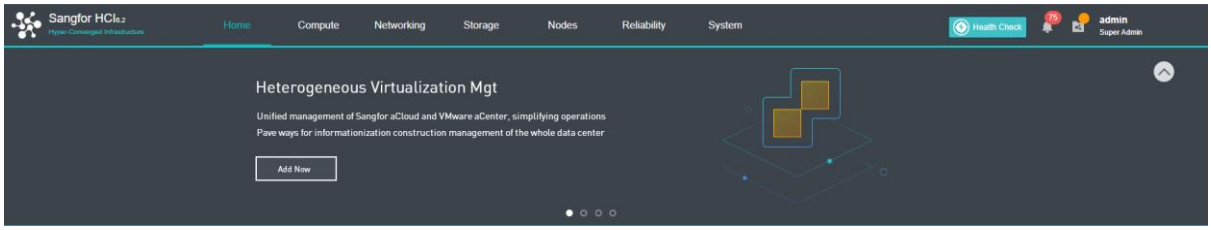


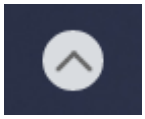


Password should contain 8-64 characters which must consist of any two of the following: upper-case characters, lower-case characters, digits and the special characters: ~`@#%&<>"',;_-^$.*+?=!:|{}()[]/\

2.1.2 Slideshow

The slideshow appears every time the administrator navigates to **Home** and later hides automatically.

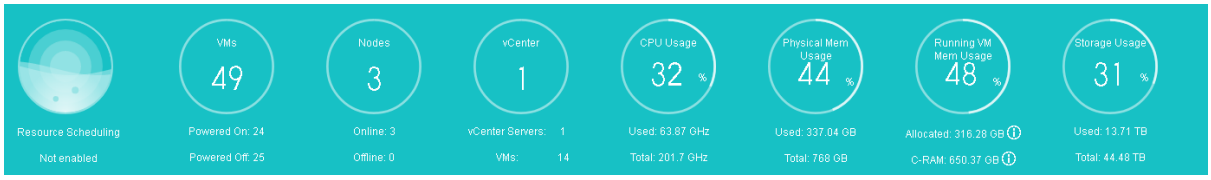


To hide the slideshow, you can click the icon  on the upper right corner.

Once the slideshow is hidden, the following buttons appear: **Create VM, Backup VM, Recover VM, Convert to VM, Add Node, Add Datastore**.

2.1.3 Viewing Resources

This section displays information about resource scheduling, nodes, VMs and storage, CPU usage, memory usage, and storage usage.



2.1.4 Viewing Nodes and Storage

A gray node icon indicates that the node is offline. A red node icon indicates the node gives alarm, while red storage icon indicates the storage is offline. Blue node icon and storage icon indicate that the node and storage operate properly.

To view node details, click on the node name to enter its **Summary** page(For details, refer to the **2.5.3.1 Node** Summary section).

To view running tasks and logs, move the cursor above the following icon at the lower right corner.

To view detailed information, click on it and the following page pops up, which lists the latest admin logs.

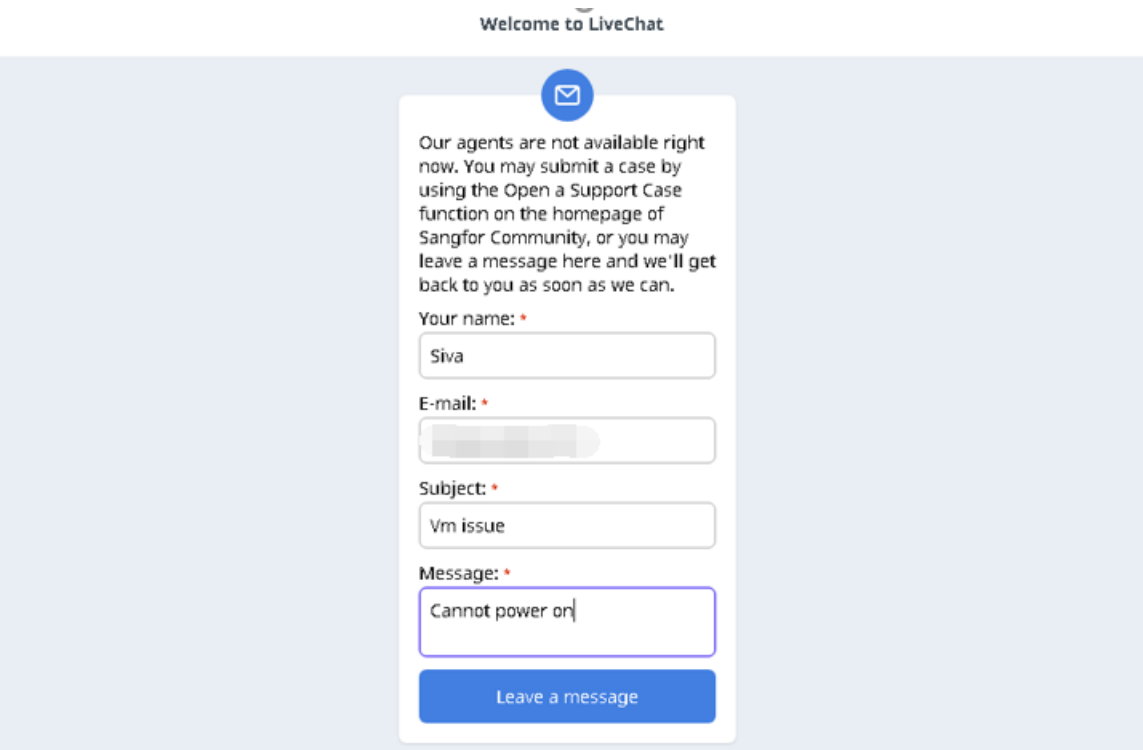
Tasks

All

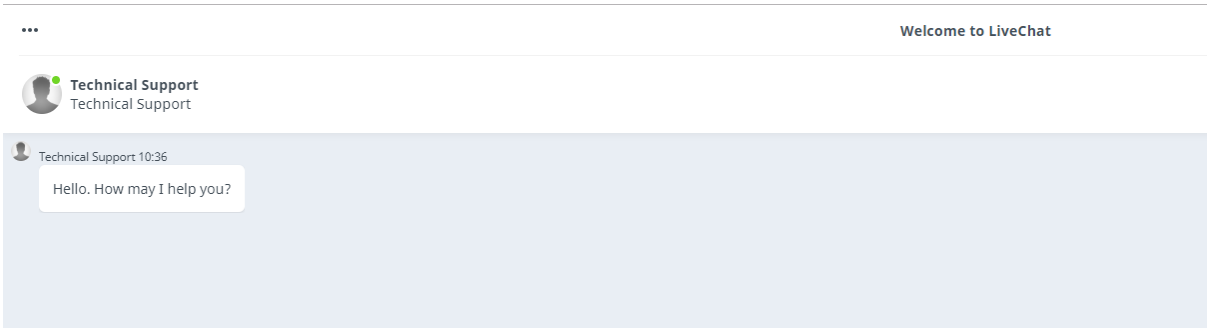
Status	Action	Object	Start Time	End Time	Admin	Operation
Completed	Power on VM	USER_acmp-c55f	2018-11-14 10:06:36	2018-11-14 10:06:36	Administrator (192.168.19.17...	View
Completed	Log in	admin	2018-11-14 09:56:27	2018-11-14 09:56:27	admin(192.168.1.213)	View
Failed	Log in	admin	2018-11-14 09:56:21	2018-11-14 09:56:21	admin(192.168.1.213)	View
Completed	Reset VM	windows7_clone...	2018-11-14 09:53:44	2018-11-14 09:54:17	Administrator (192.168.19.17...	View
Completed	Import backups	Windows server ...	2018-11-14 09:49:48	2018-11-14 09:49:53	Administrator (192.168.19.17...	View
Completed	Import backups	Windows server ...	2018-11-14 08:48:29	2018-11-14 08:48:34	Administrator (192.168.19.17...	View
Completed	Import backups	Windows server ...	2018-11-14 07:47:19	2018-11-14 07:47:24	Administrator (192.168.19.17...	View
Completed	Import backups	Windows server ...	2018-11-14 06:45:23	2018-11-14 06:45:28	Administrator (192.168.19.17...	View
Completed	Import backups	Windows server ...	2018-11-14 05:44:07	2018-11-14 05:44:11	Administrator (192.168.19.17...	View
Completed	Import backups	Windows server ...	2018-11-14 04:42:38	2018-11-14 04:42:43	Administrator (192.168.19.17...	View
Completed	Import backups	Windows server ...	2018-11-14 03:41:16	2018-11-14 03:41:21	Administrator (192.168.19.17...	View
Completed	Import backups	Windows server ...	2018-11-14 02:50:20	2018-11-14 02:50:25	Administrator (192.168.19.17...	View
Completed	Import backups	Windows server ...	2018-11-14 01:48:58	2018-11-14 01:49:03	Administrator (192.168.19.17...	View

If you have any questions about HCI, you can click on the LiveChat option at the lower right corner to do online consultation.

After clicking the online consultation option, you will be redirected to the following page to ask for your personal information.



Fill in the personal information and click Start the Chat. The page will jump to the online consultation page, then you can directly ask your question.



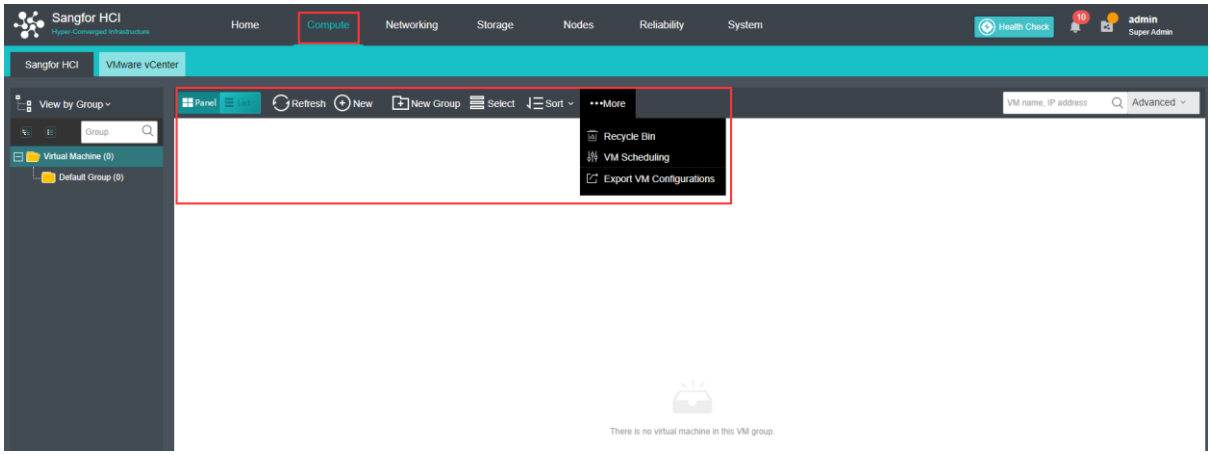
2.2 Compute

A virtual machine is an operating system simulated by specific software, running in an isolated environment. It can be installed with the operating system such as Windows, Linux, etc.

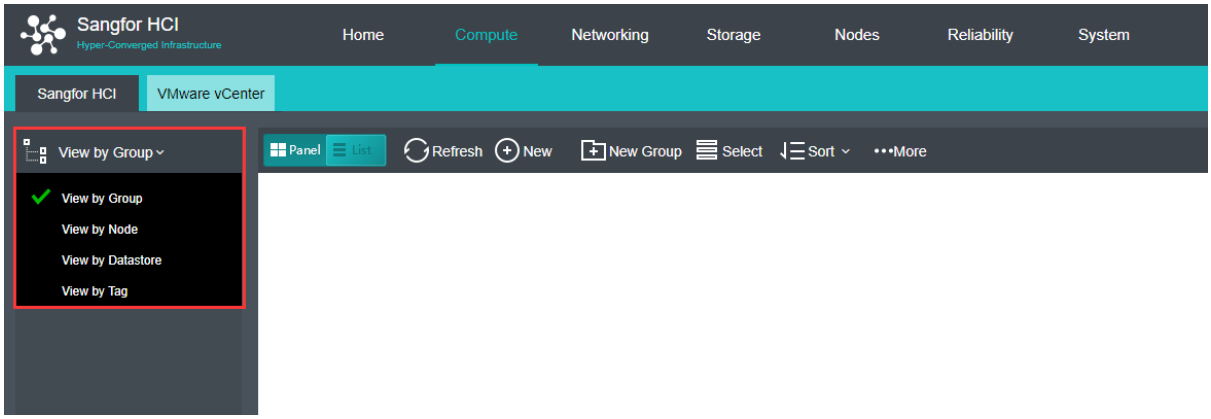
VMware vCenter can be added to and managed on Sangfor HCI platform.

2.2.1 Managing Virtual Machines on Sangfor HCI

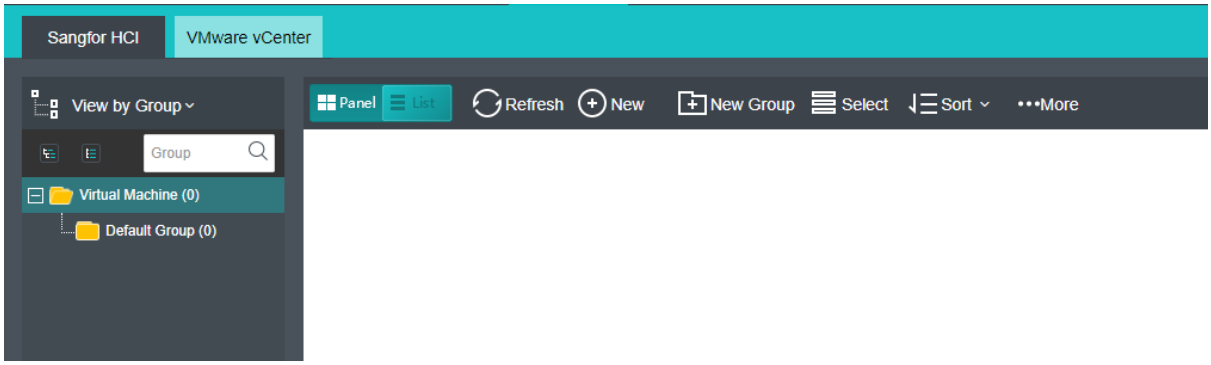
Navigate to **Compute** and you will see the following toolbar, as shown in the following figure. On the toolbar, there are the following items: **View By Group/Node/Datastore/Tag, Panel/List, Refresh, New, New Group, Select, Sort, Recycle Bin, VM scheduling, Export vm configurations and Advanced**.



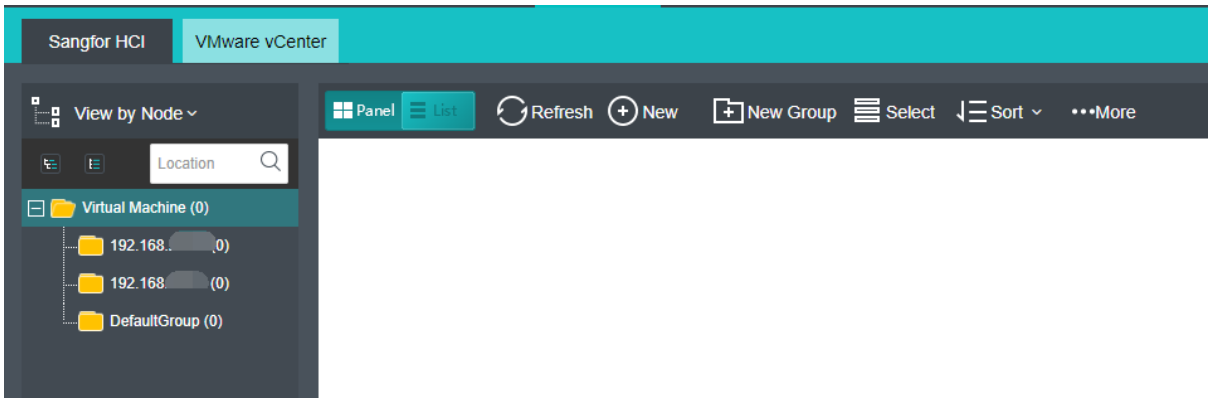
Virtual machines can be viewed by **Group, Node, Datastore** or **Tag**.



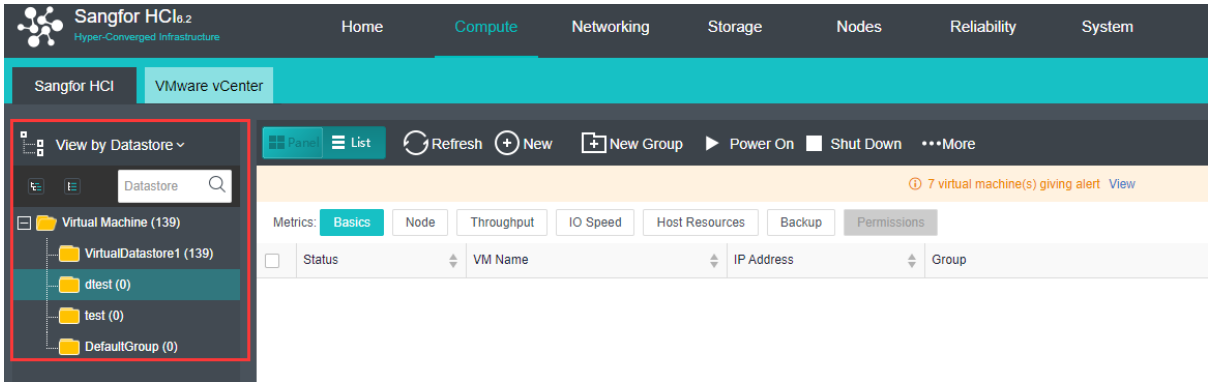
To view virtual machines by group, select **View** By **Group** in **Compute**, as shown below.



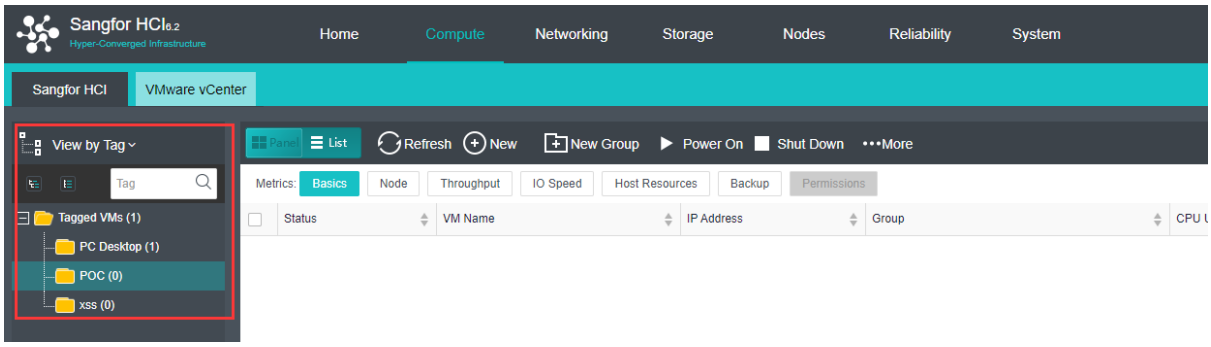
To view virtual machines by node, select **View By** Node in **Compute**, as shown below.



To view virtual machines by datastore, select **View By** Datastore in **Compute**, as shown below.

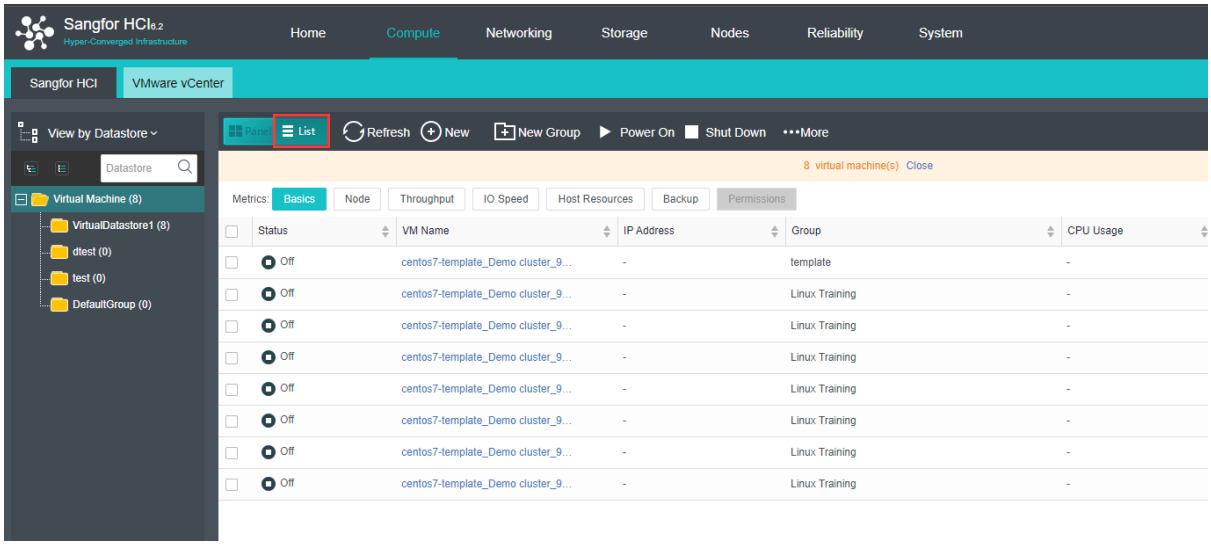


To view virtual machines by tag, select **View By Tag** in Compute, as shown below.



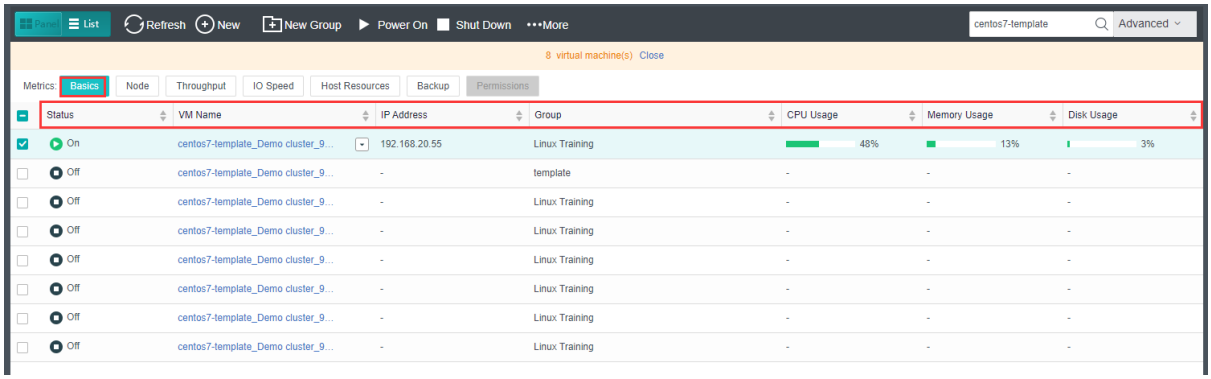
2.2.1.1 Viewing VMs by Panel or List

Virtual machines can be viewed by **Panel** or **List**. By default, virtual machines are displayed by **Panel**. To view VMs by **List,** click on **List,** as shown below:

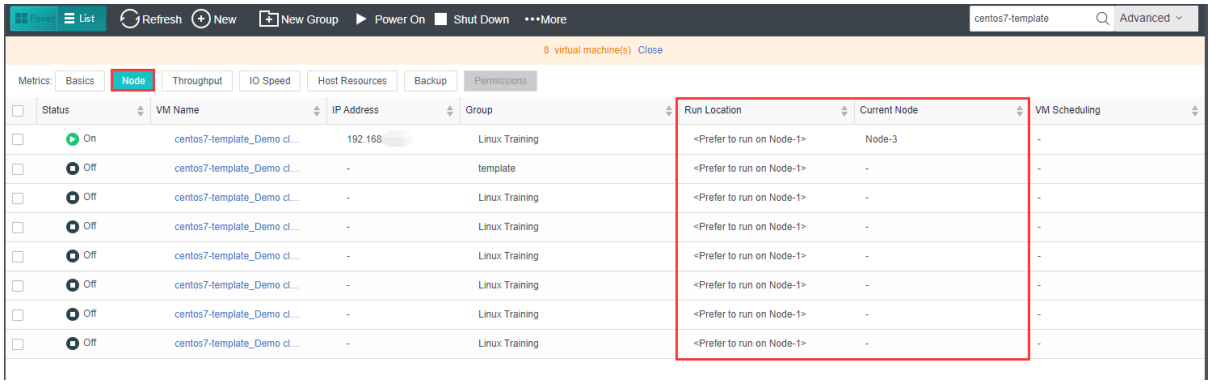


VM details are displayed, as shown below:

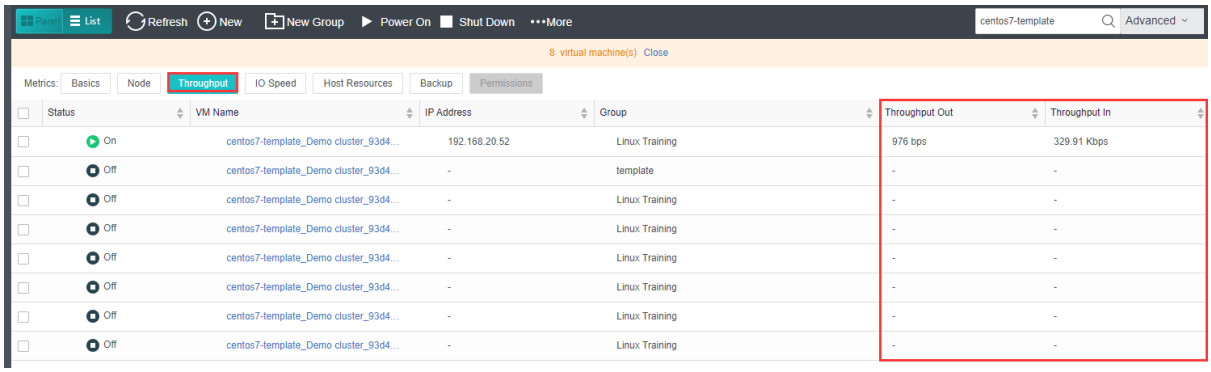
Basics: Displays basic information of virtual machines.



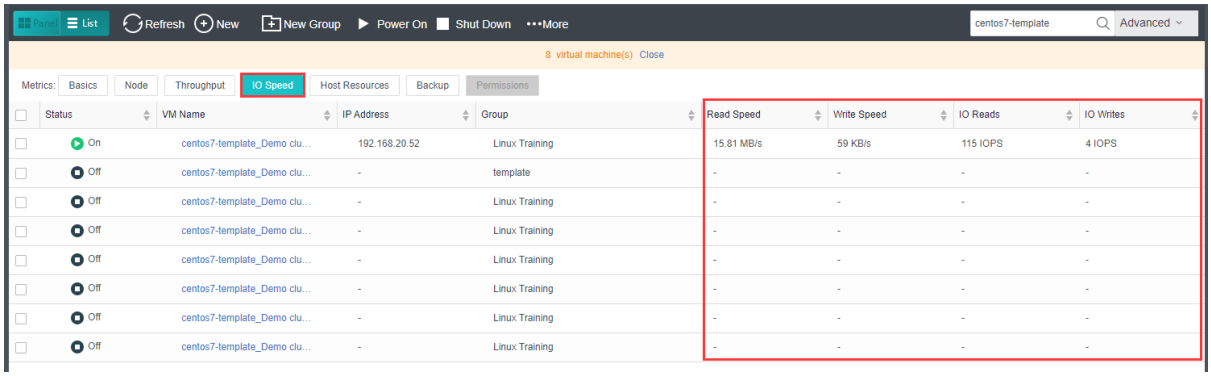
Node: Display the node where the VM is running on.



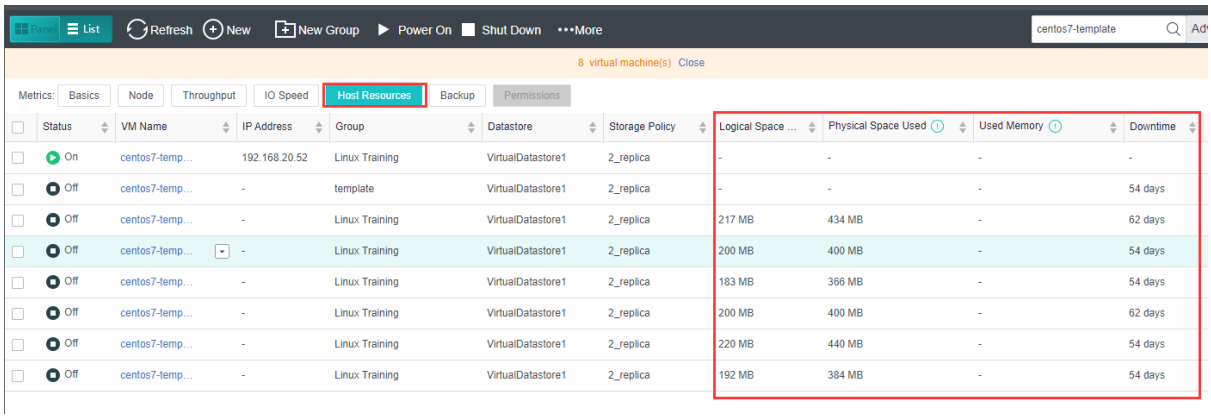
Throughput: Displays outbound and inbound speed.



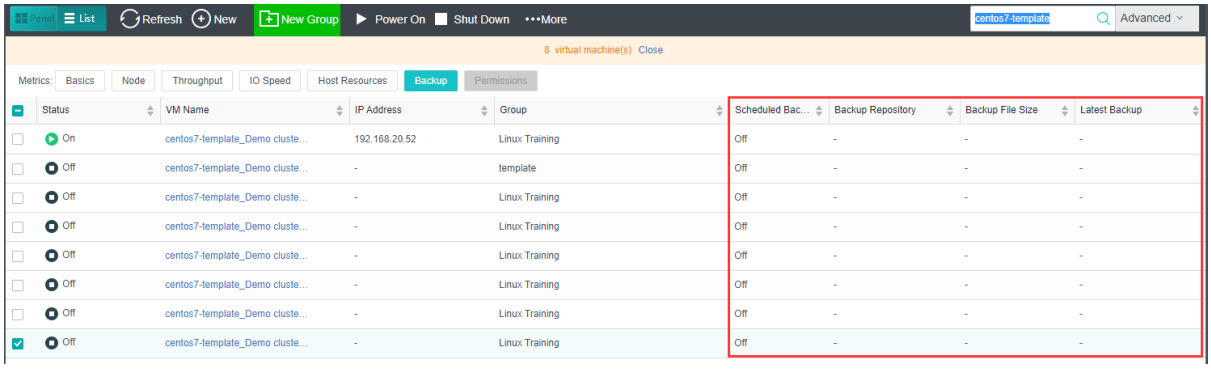
IO Speed: Displays IO speed.



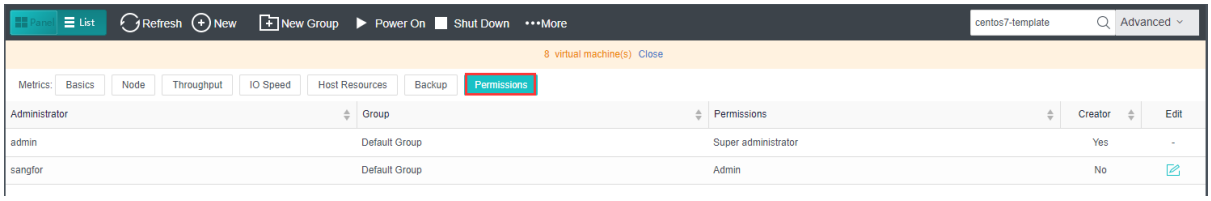
Host Resources: Displays used resources and downtime.



Backup: Displays backup information of virtual machines and backup file size.

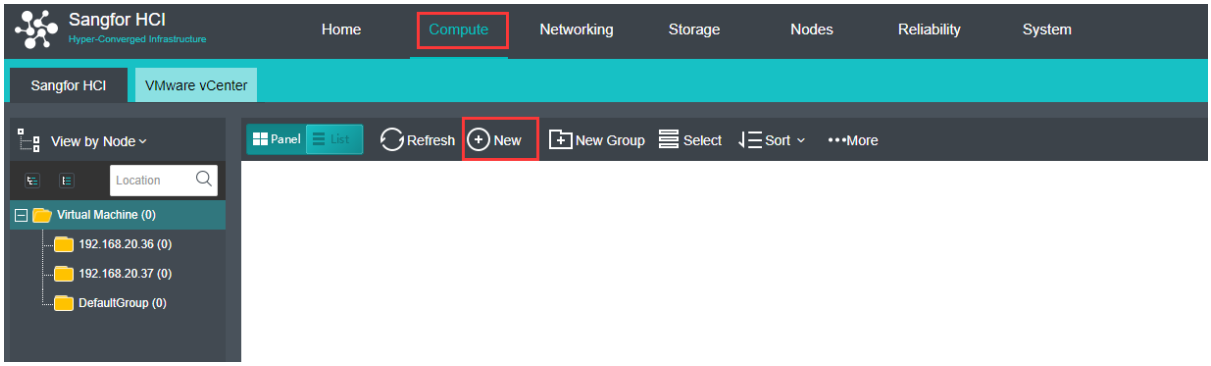


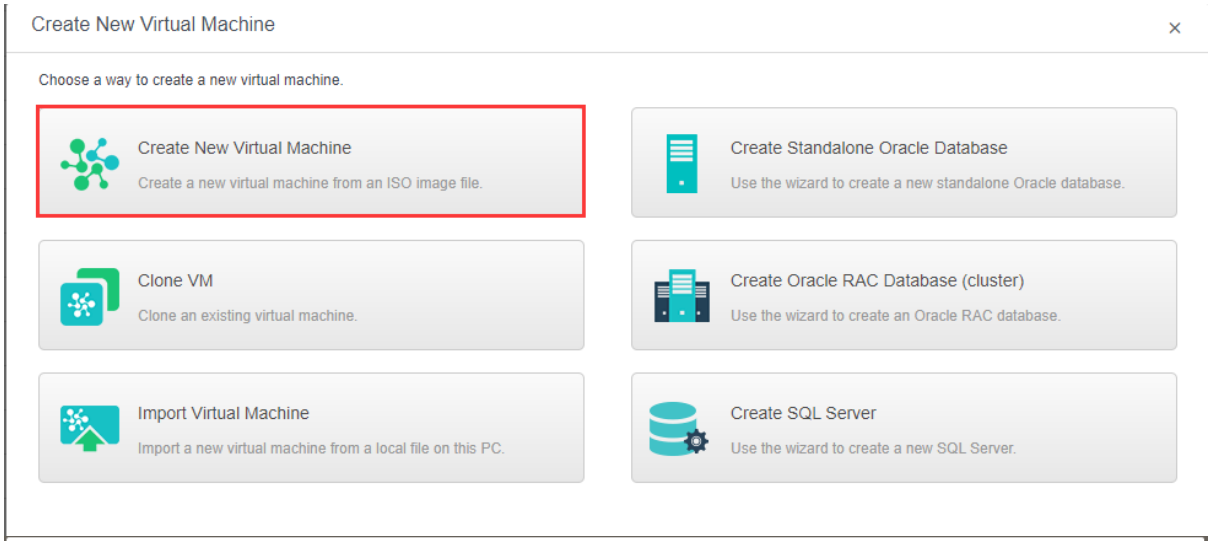
Permissions: Displays admin permissions.

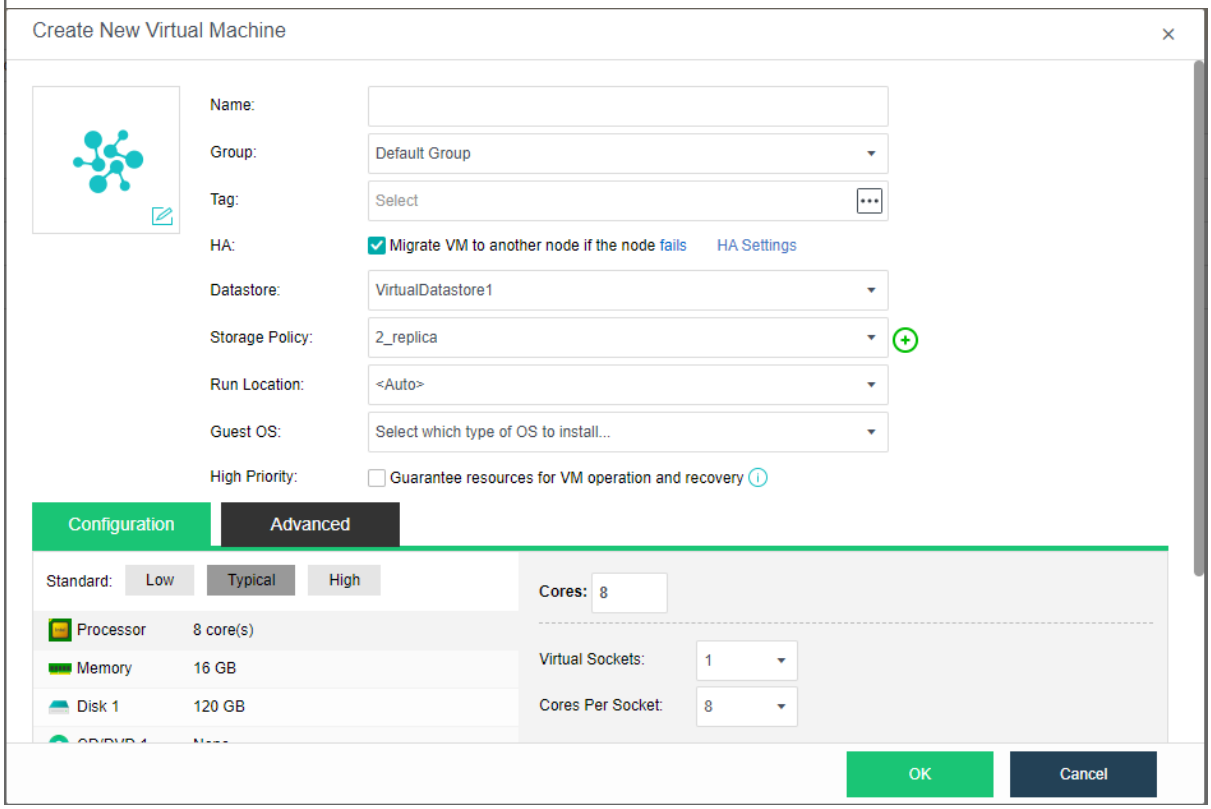


2.2.1.2 Creating Virtual Machine

To create a new virtual machine, click **New** in **Compute** and then select **Create New Virtual Machine** to enter the following page.

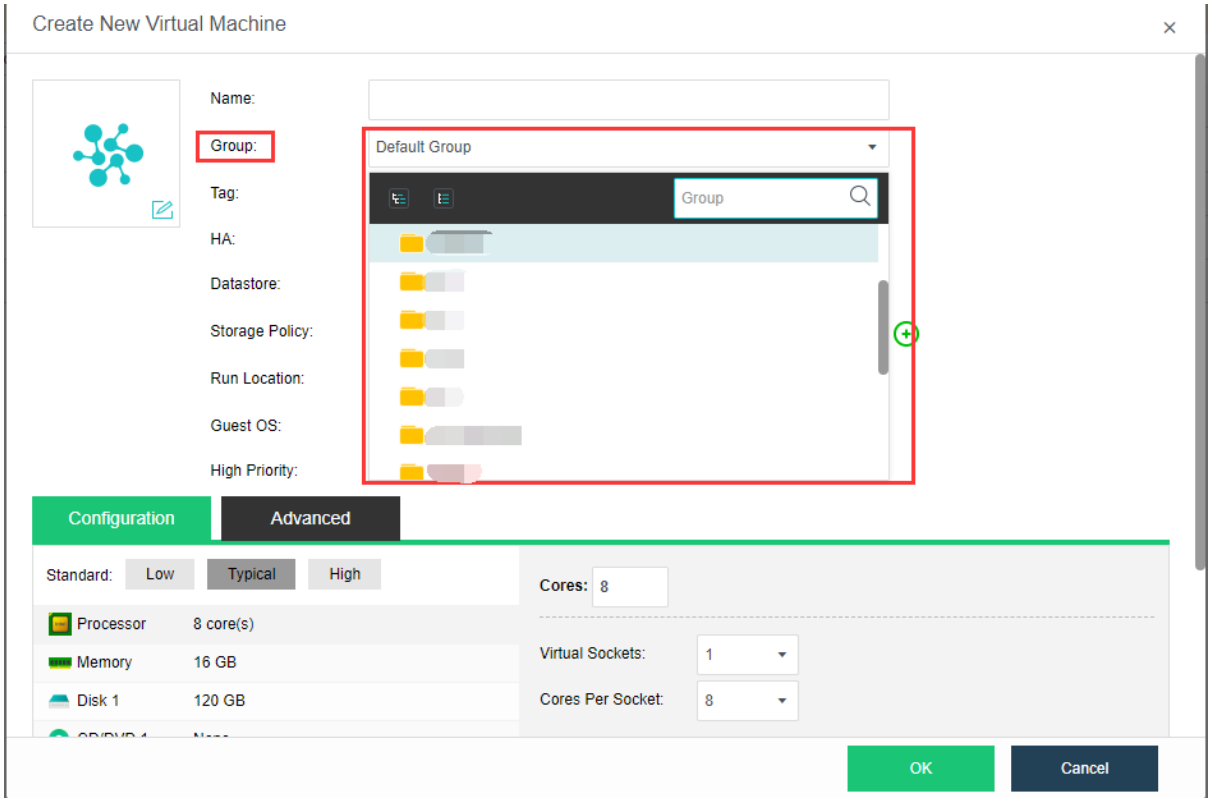




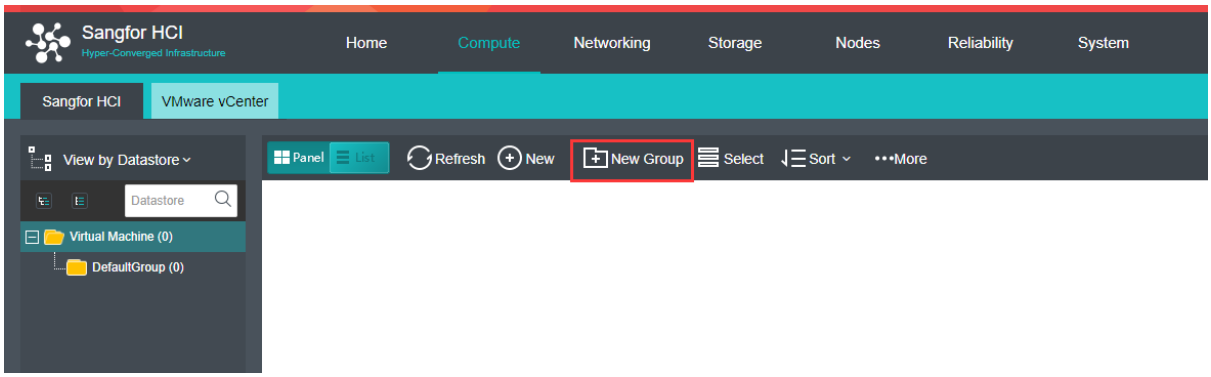


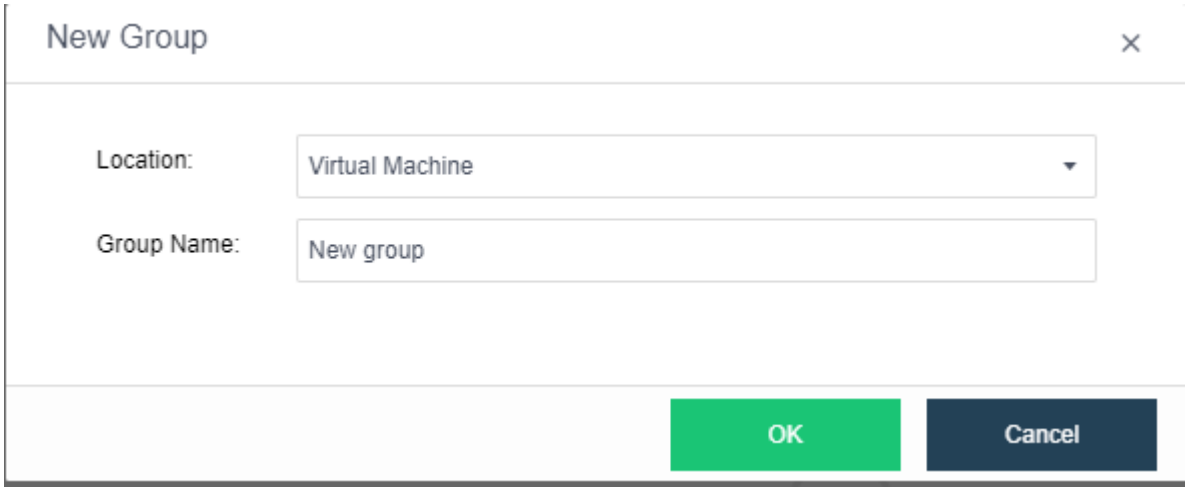
Name: Specifies a distinguishable name for the virtual machine.

Group: Specifies a group to which this virtual machine belongs.

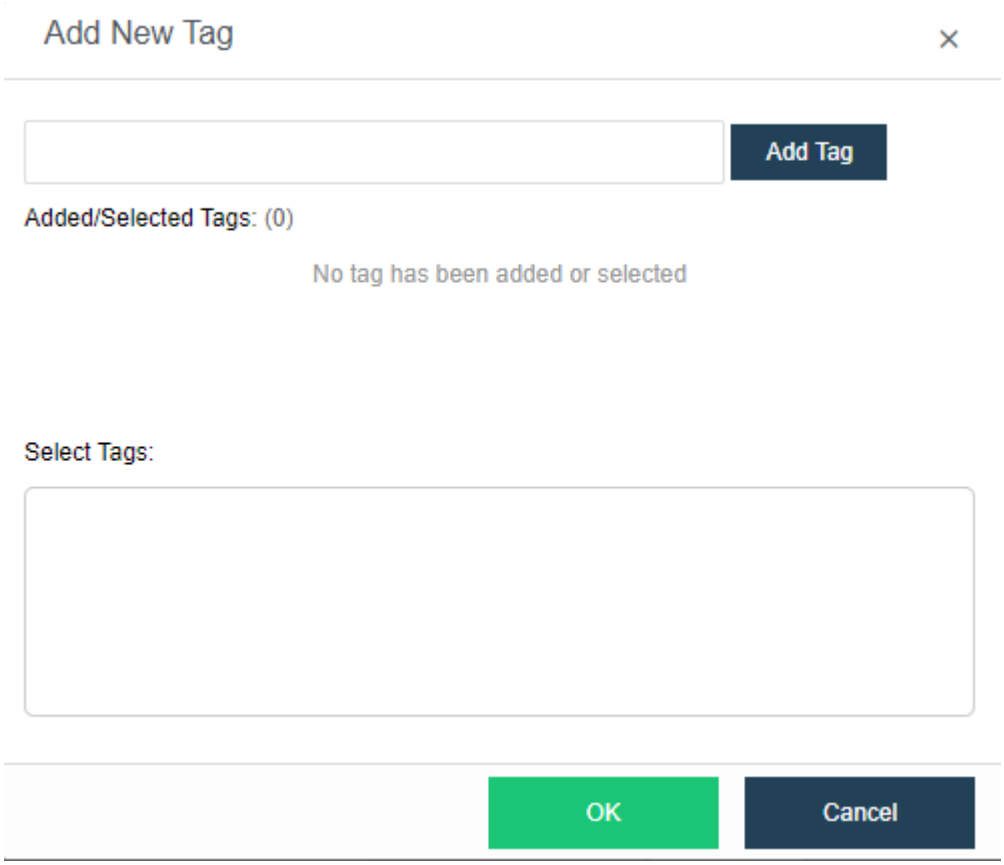


To add a new group, click "add new group"

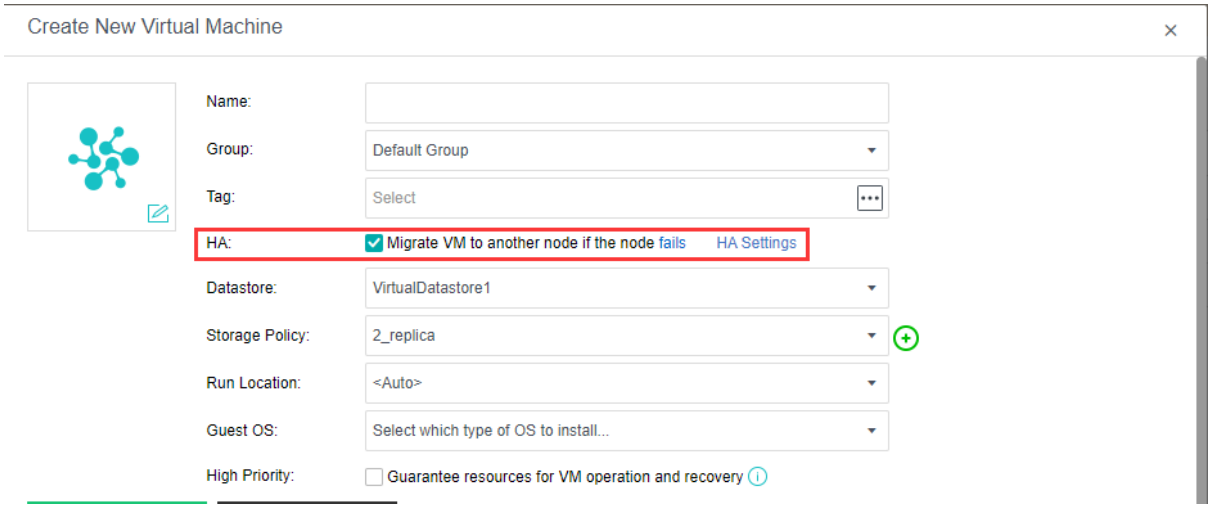




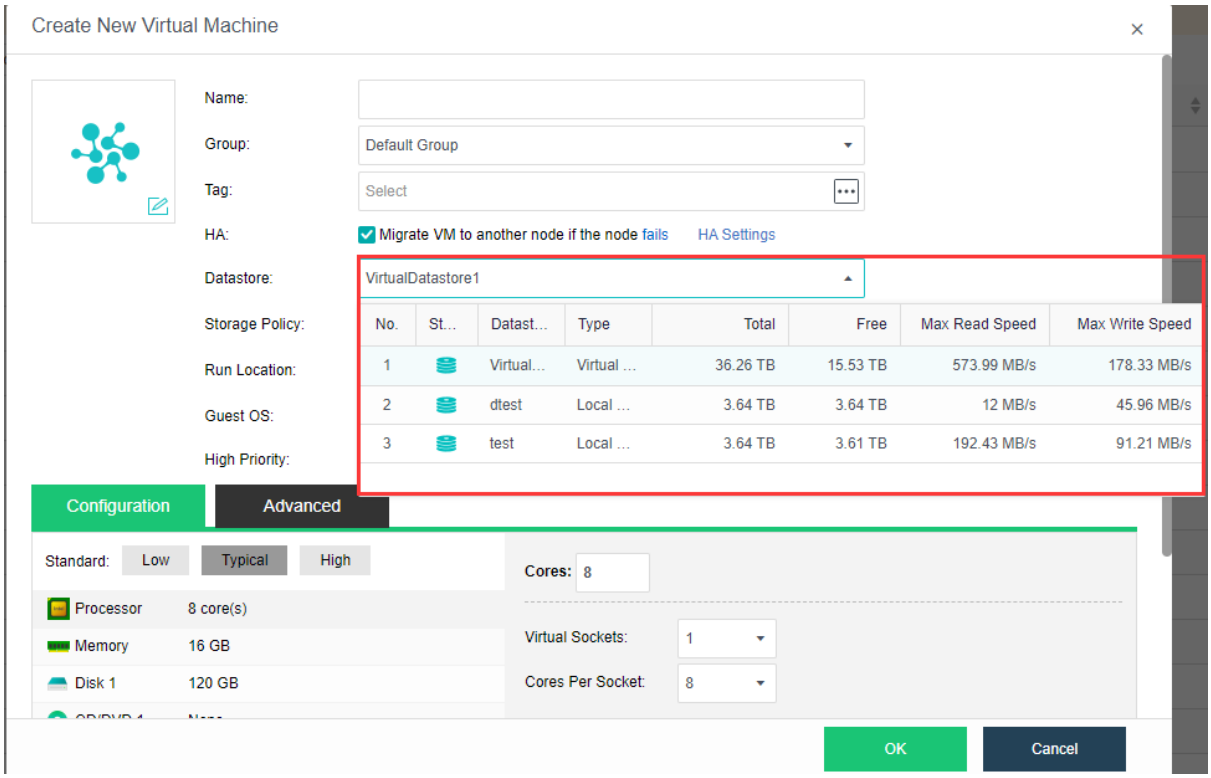
Tag: Specifies one or more than one tags for the virtual machine.



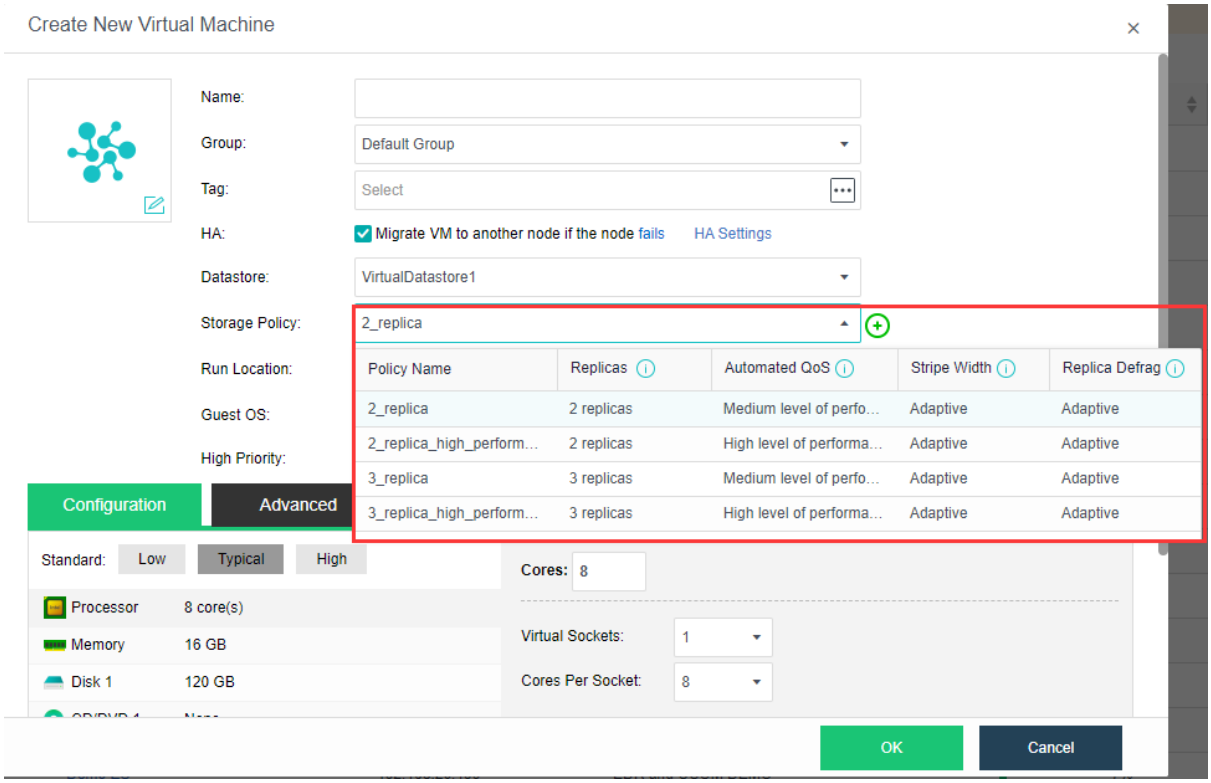
HA: If the option Migrate **to another node if the node fails** is selected, virtual machine will be recovered onto another node in case the node running the VM fails.



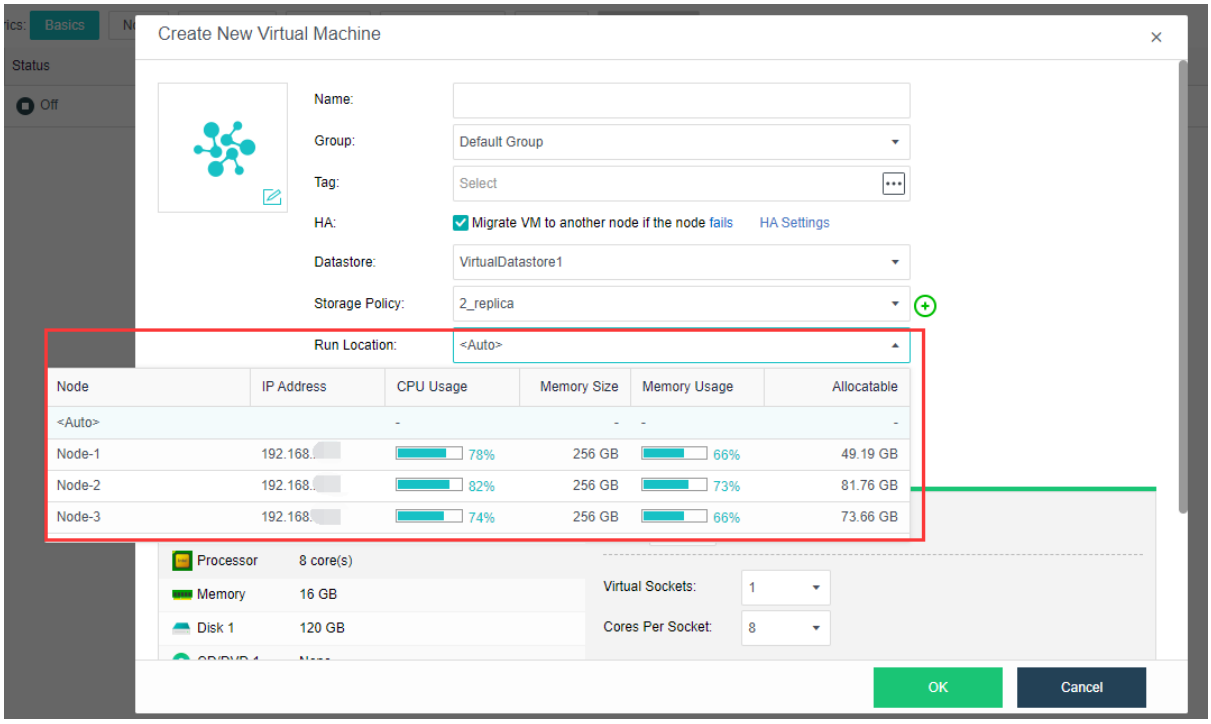
Datastore: Specifies a datastore to store virtual machine. HA is configurable only when a shared datastore is selected.



Storage Policy: Specifies the number of replication and performances.

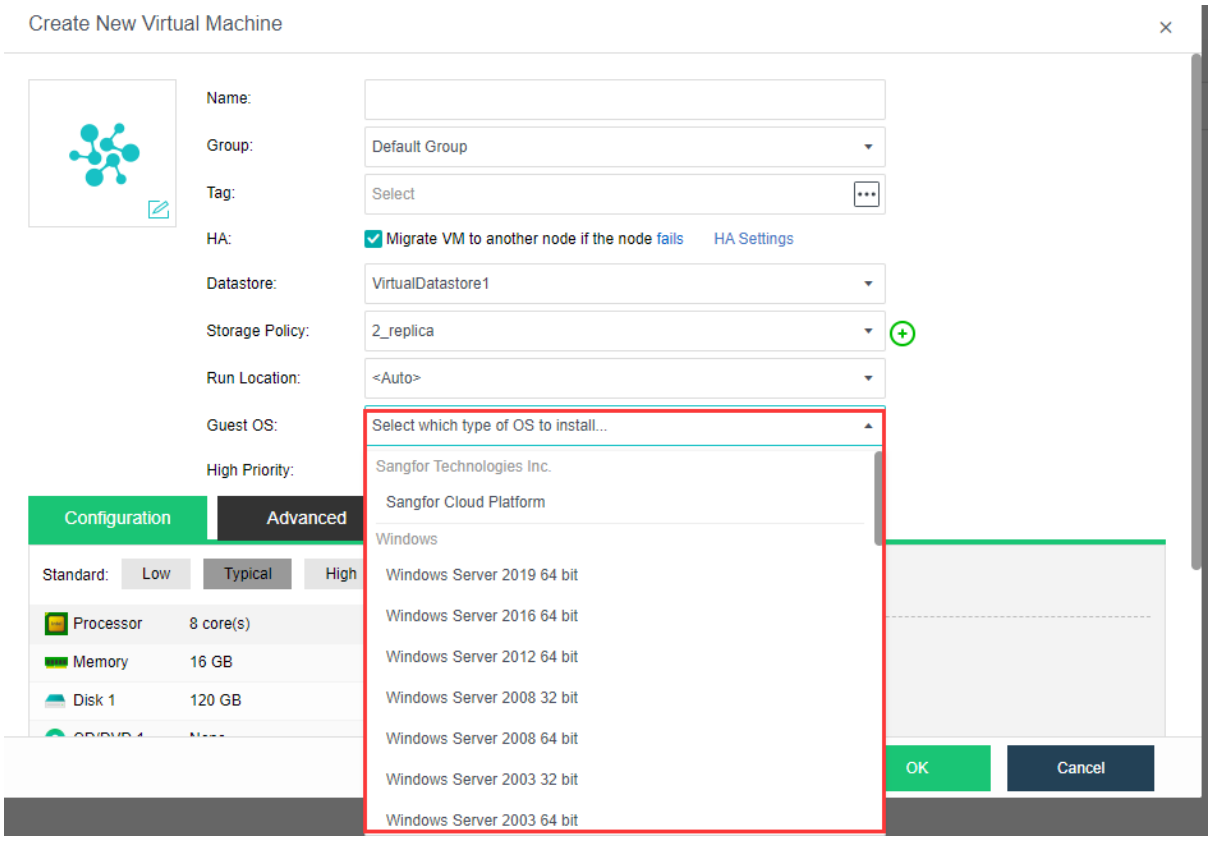


Run on Node: Specifies a node on which the virtual machine runs.

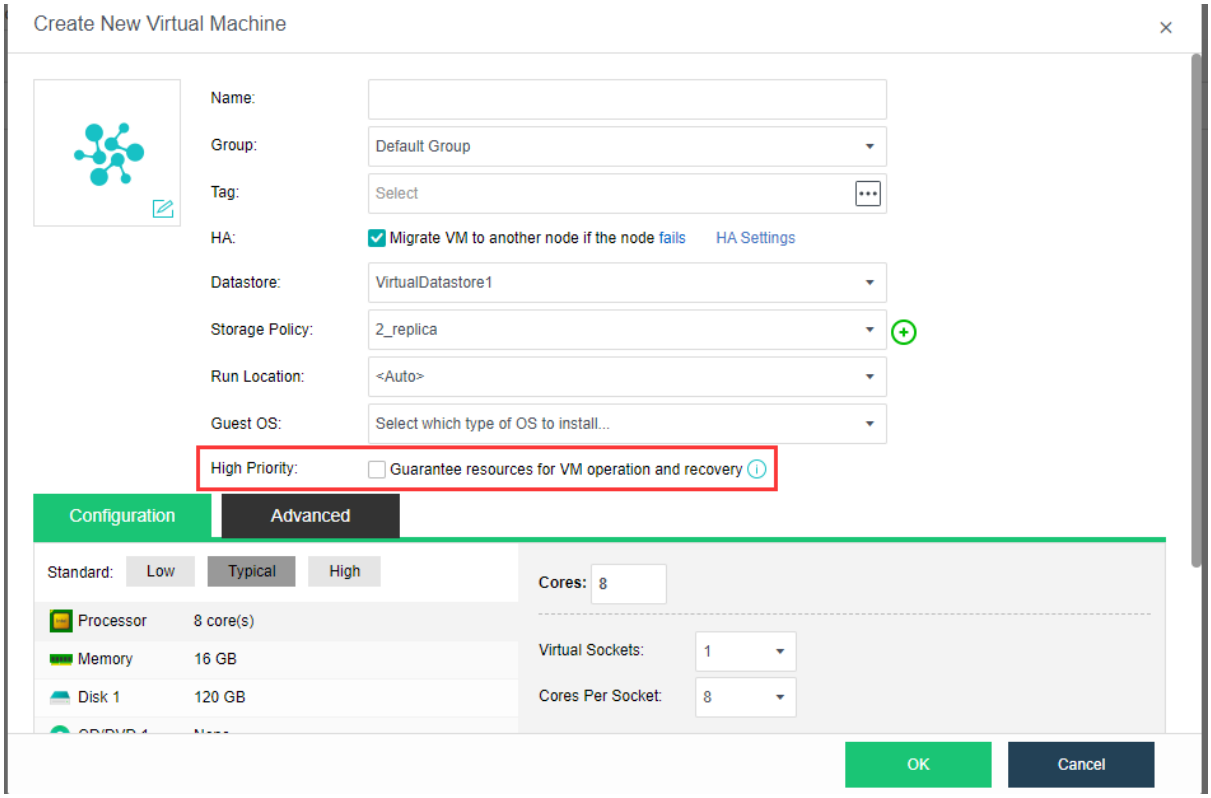


Guest OS: Specifies an operating system for the virtual machine. The following types of guest OSes are supported: Sangfor, Windows, Linux, Linux distributions and others. Sangfor

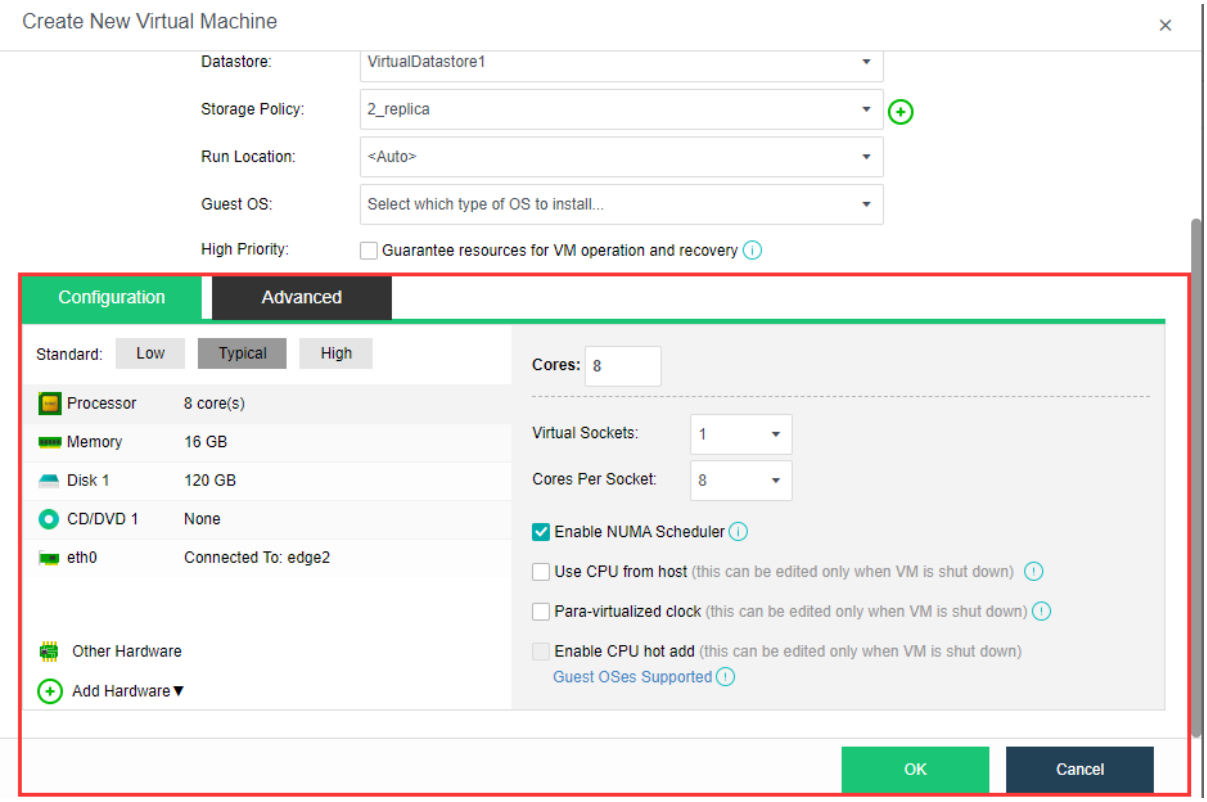
operating system is mainly for software aCenter.



High priority: Once it is selected, resources will be preferentially allocated to virtual machine if overall resources are inadequate.

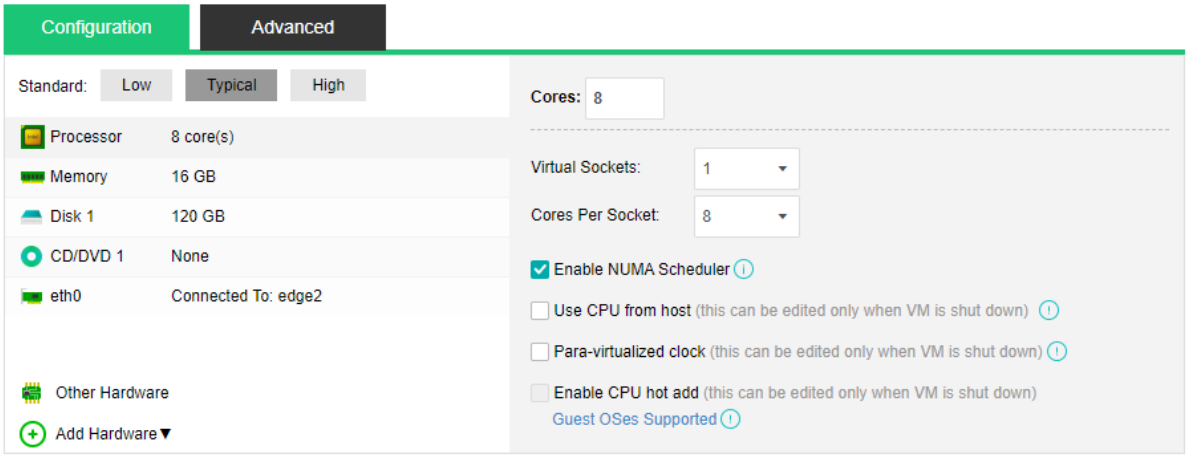


Configuration: It allows you to configure hardware resources, such as **Processor**, **Memory**, **Disk**, **CD/DVD** and **NIC**, etc. Configuration falls into **Low** configuration, **Typical** configuration and **High** configuration. If the current configuration fails to meet business requirements, you can configure the corresponding hardware resource as required, as shown below:



- **Default Low Configuration**: 4 processor, 8 GB memory, 60 GB disk, one CD/DVD, one NIC.
- **Default Typical Configuration**: 8 processor, 16 GB memory, 120 GB disk, one CD/DVD, one NIC.
- **Default High Configuration**: 16 processor, 32 GB memory, 120 GB disk, one CD/DVD, one NIC.

Processor: Specifies the number of virtual sockets and cores per socket for the virtual machine respectively. Once Cores field is configured, Virtual Sockets and Cores Per Socket fields will be automatically filled with optimum values, so as to achieve best VM performance.



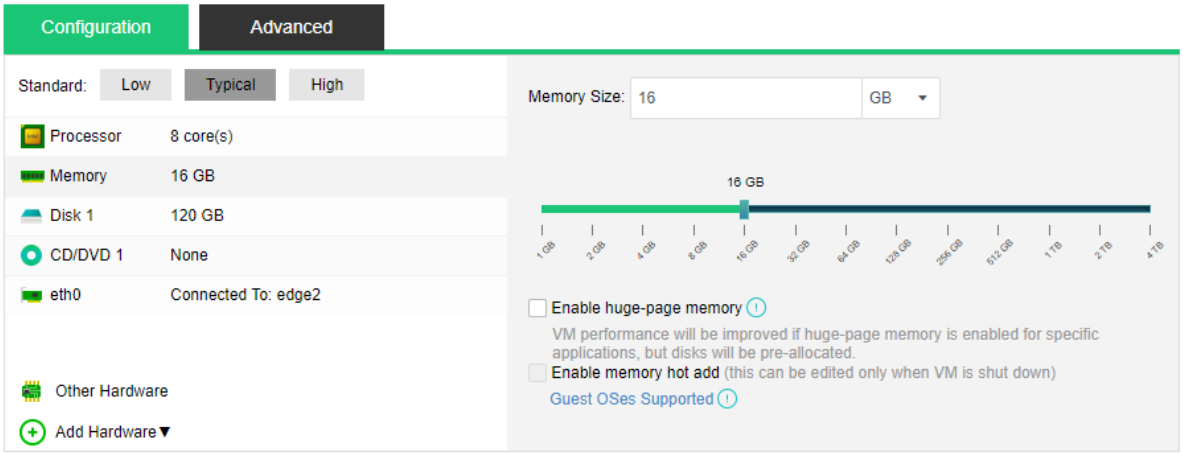
Enable NUMA Scheduler: Once enabled, memory access and VM performance will be enhanced. To enable NUMA scheduler for VM, go to **System > Advanced Settings** to enable NUMA scheduler first. To project NUMA topology into a virtual machine, make sure that virtual machine has more than 8 cores and vmTools have been installed.

Use CPU from host: Live migration might be affected because of the tight association between the virtual machine and the host CPU.

Para-virtualized clock: It is applicable to Windows virtual machines only. It can improve performance of Windows virtual machines running database but requires the option Use CPU from host to be enabled.

Enable CPU hot add: Once CPU hot-add is enabled, CPU resources can be hot-added manually for the virtual machine.

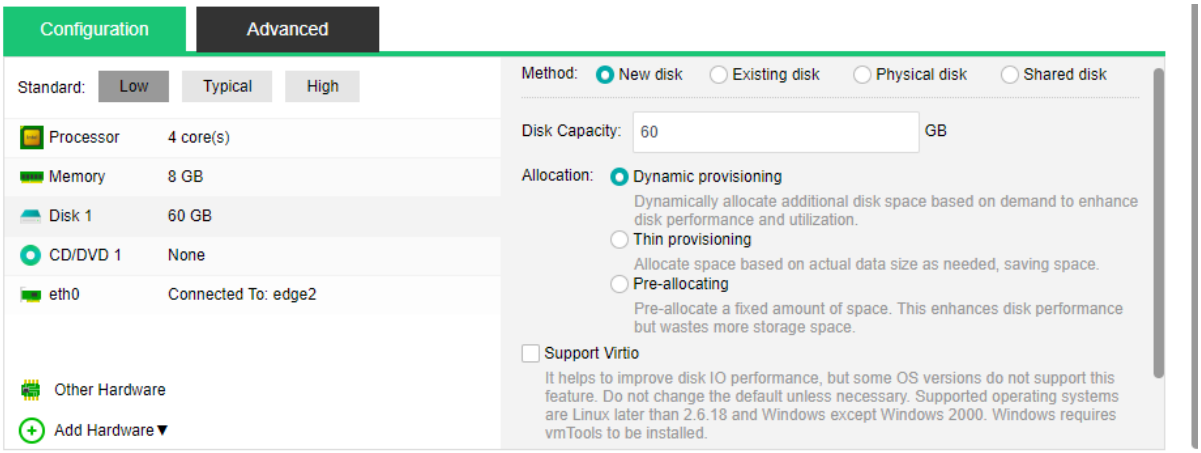
Memory: Specifies the memory size for the virtual machine. The minimum is 1 GB, and the maximum is 4 TB.

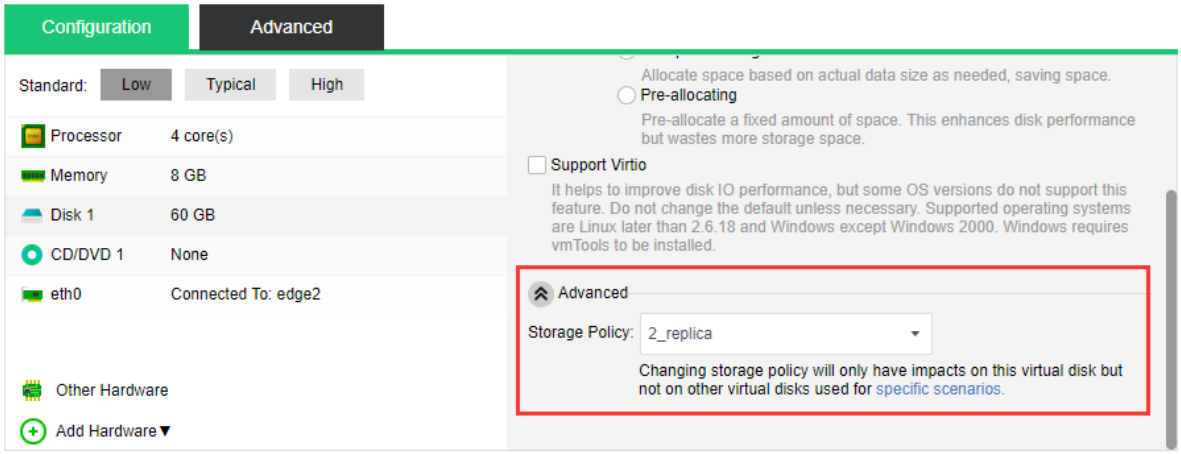


Enable memory hot add: Once memory hot-add is enabled, memory resources can be hot-added manually for the virtual machine.

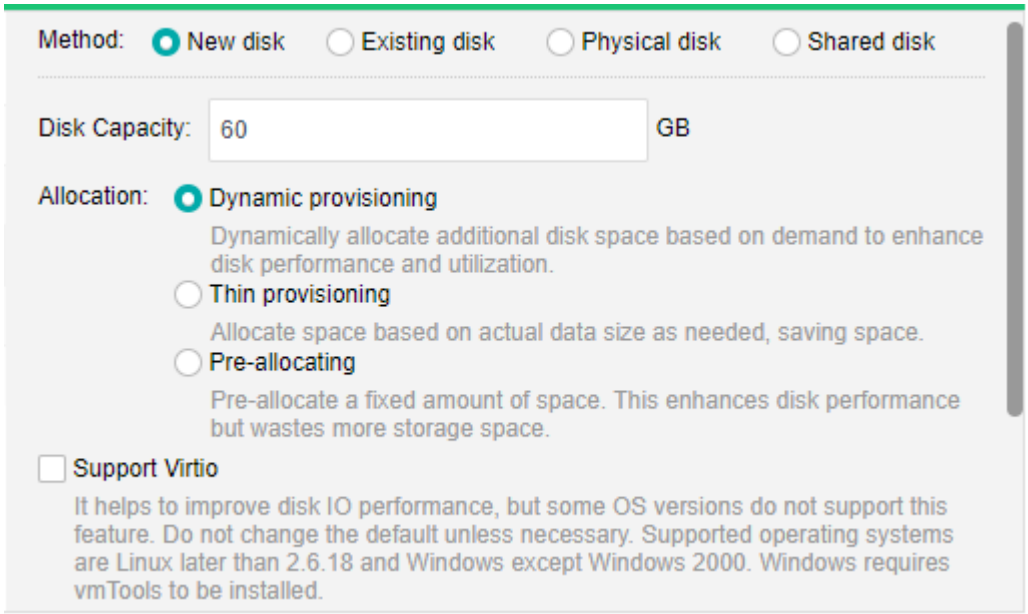
Disk: Specifies the disk for the virtual machine.

To specify a disk for a virtual machine that is not stored on local storage, make sure the disk is on a NFS, iSCSI or FC storage that the virtual machine has access to.





New disk: You may choose to create a new disk or use an existing disk. If you'd like to create a new disk, configure related fields on the following page:



Disk Capacity: Specifies the capacity(GB) of the virtual disk.

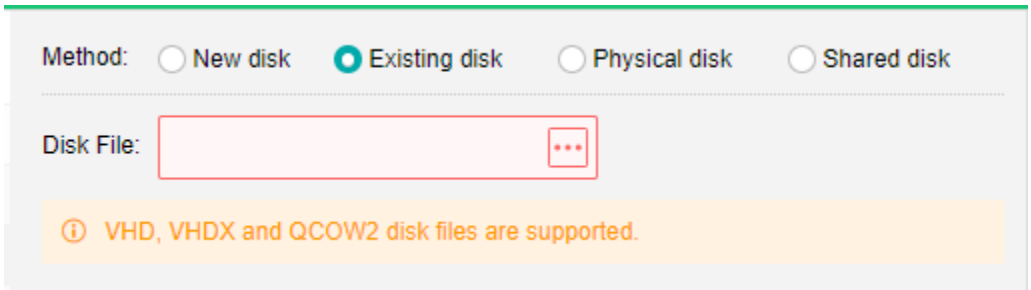
Dynamic provisioning :Allocate space based on pre-allocated space and actual demands, to enhance disk performance and utilization.

Thin Provisioning: Allocate space based on actual data size as needed, saving space.

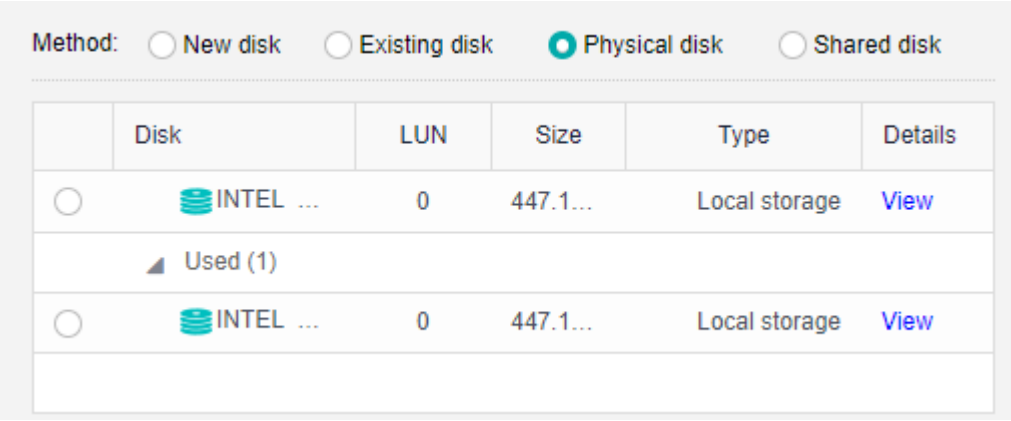
Pre-allocating: Pre-allocate a fixed amount of space, enhancing disk performance but wasting more storage space.

Support Virtio : It helps to improve Disk IO performance, but some versions does not support this feature. Do not change the default unless necessary.

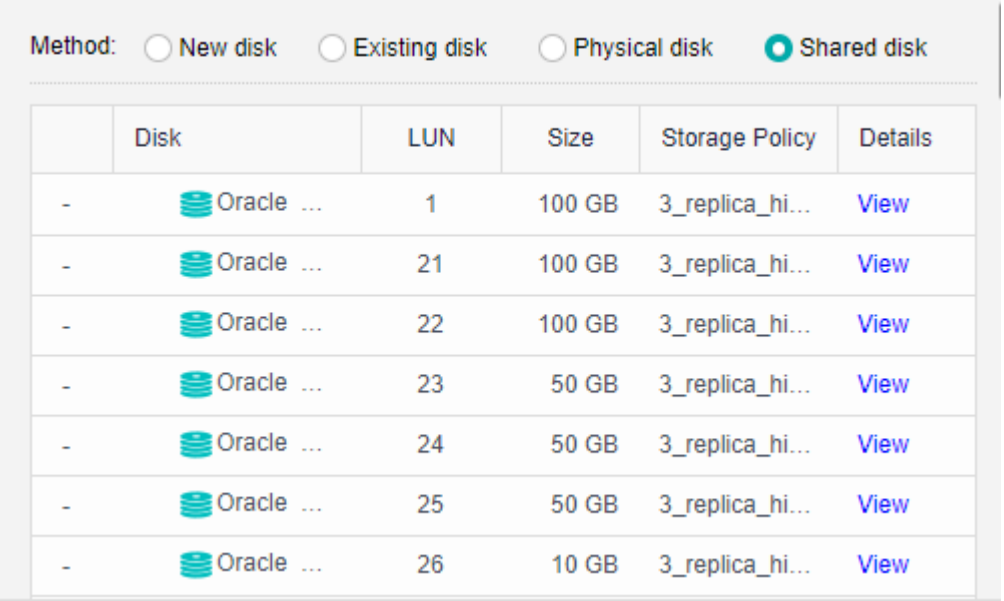
Existing disk: To use an existing disk, select the option **Existing disk** and then select the corresponding disk file.



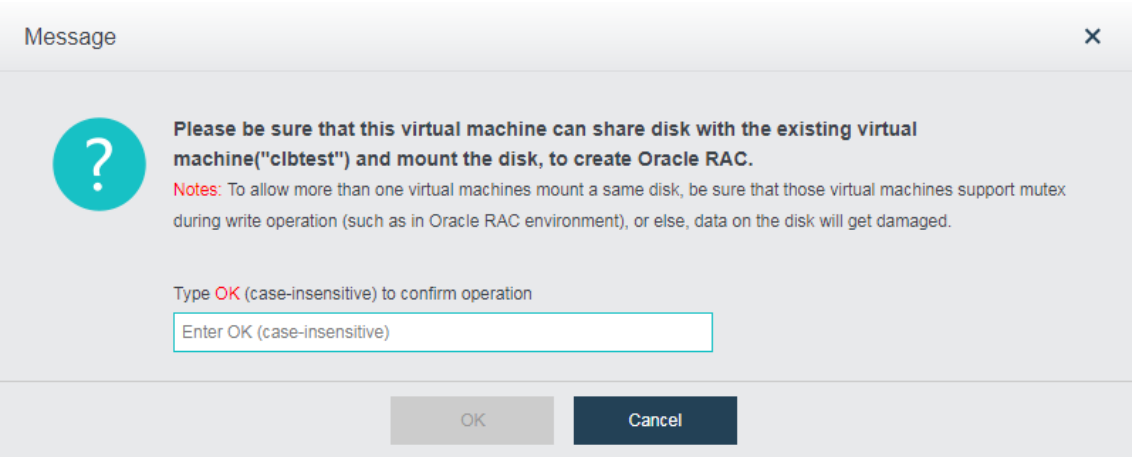
Physical disk: To use a physical disk, select the option **Physical disk** and choose a physical disk which will be mapped to the virtual machine.



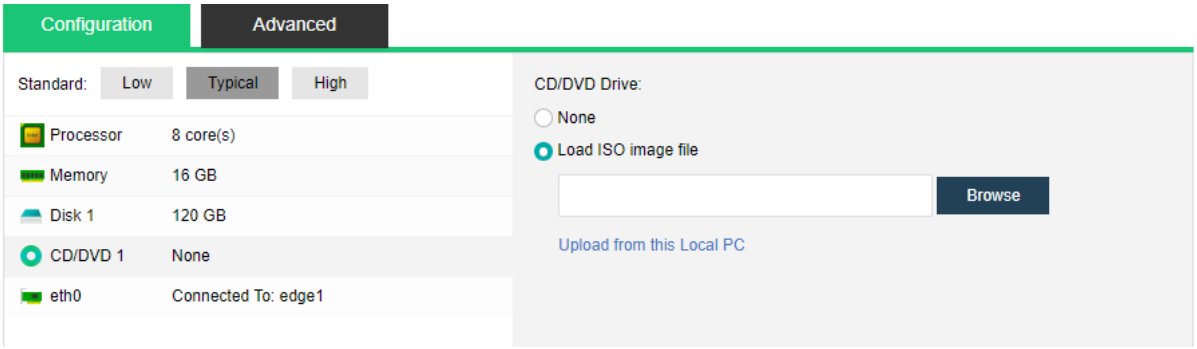
Shared disk: To use a shared disk, select the option Shared **disk**.



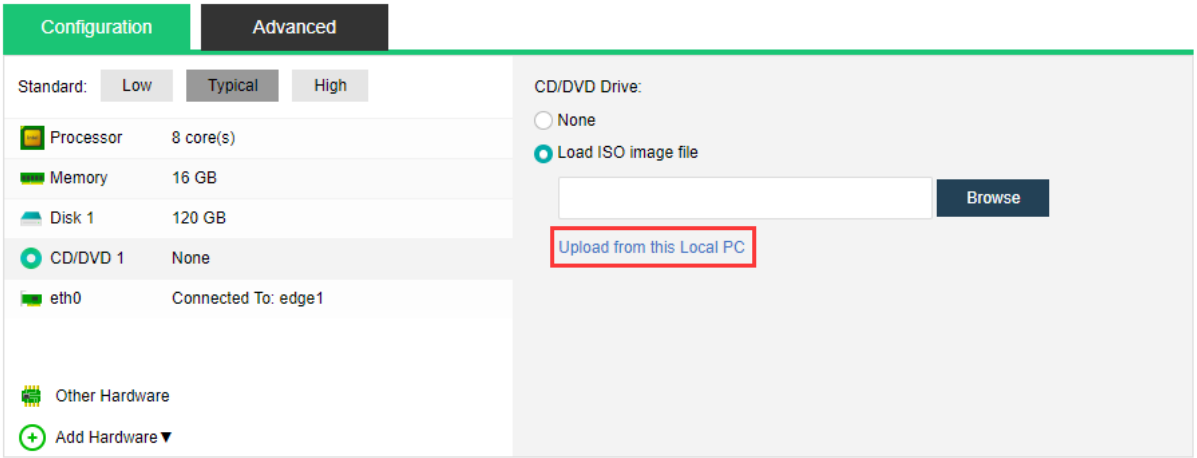
To allow more than one virtual machines mount a same disk, be sure that those virtual machines support mutex during write operation (such as in Oracle RAC environment), or else, data on the disk will get damage.



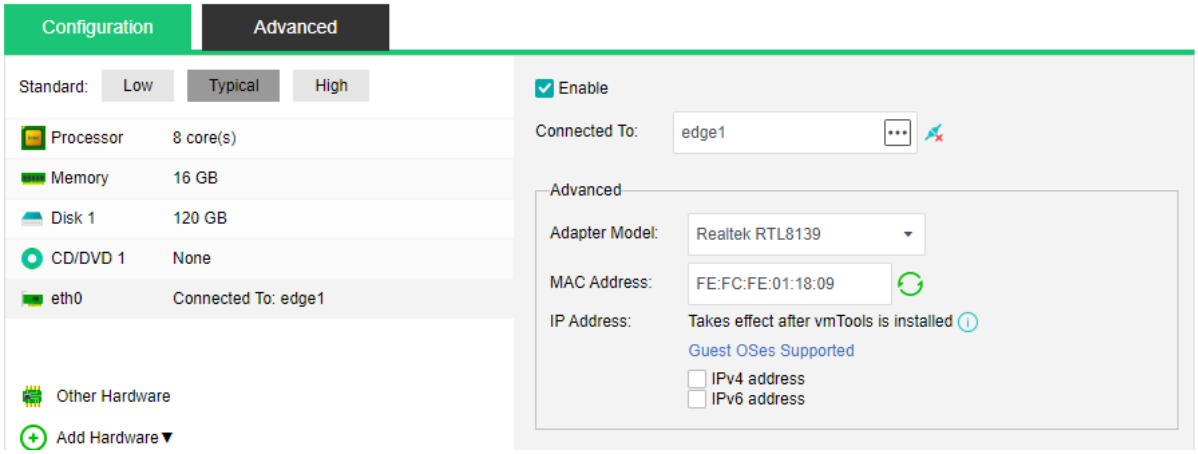
CD/DVD 1: Specifies an ISO image file of CD/DVD drive to be used by the virtual machine. You may also select **None**, which indicates that the virtual machine does not use CD/DVD drive.

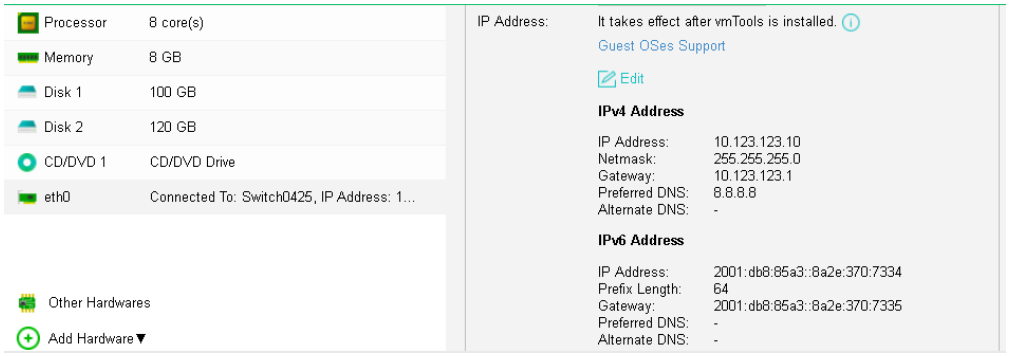


If the option **Load ISO image file** is selected, you need to select the corresponding ISO image file. If there is no ISO image file, you may upload an image file to the datastore from local disk. Click **Upload from this Local Disk,** select an ISO image file and upload it.



etho: Specifies what the virtual machine is connected to.





Enabled: If it is selected, it indicates that the specified virtual network adapter is enabled.

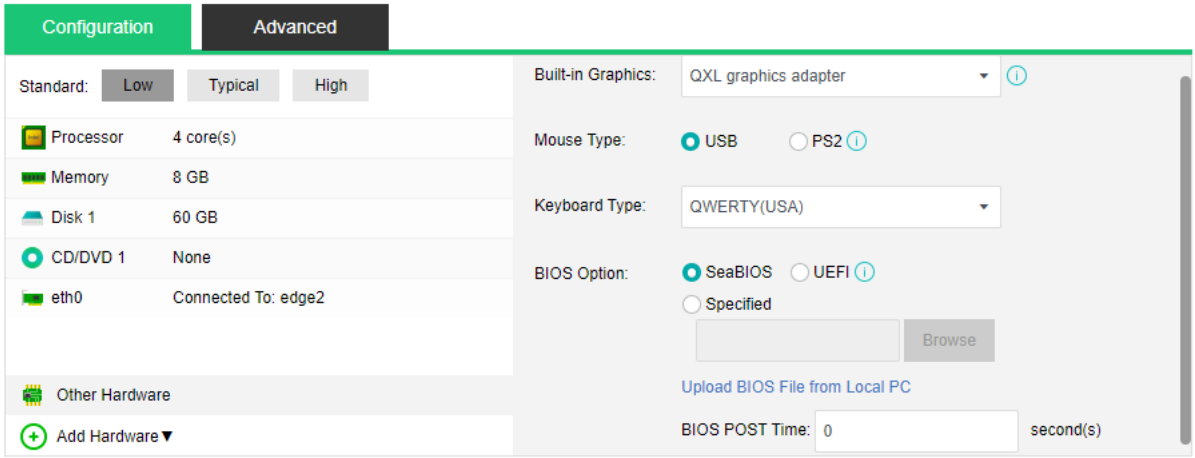
Connected To: Specifies an edge or a virtual switch to be connected to the virtual machine.

Adapter Model: Specifies the adapter model: **Realtek RTL8139** or **Intel E1000**.

MAC Address: It can be automatically generated or manually specified. MAC address examples: 00-11-22-33-44-55, 00:11:22:33:44:55.

Support IPv4 and IPv6 address: Support IPv4 and IPv6 address: It can set IPv4 and IPv6 addresses on the network card. It only supports certain Guest OS and required to install the VM tools as well.

Other Hardwares: Includes **Graphics Adapter, Mouse Type** and **BIOS Option**.



Built-in Graphics: Options are **Standard VGA graphics adapter, VMWare compatible graphics adapter, QXL graphics** adapter and **Cirrus graphics adapter**. Graphics adapter has close relation with desktop display. If selected graphics adapter is not supported by guest OS or display error exists, try another type of graphics adapter.

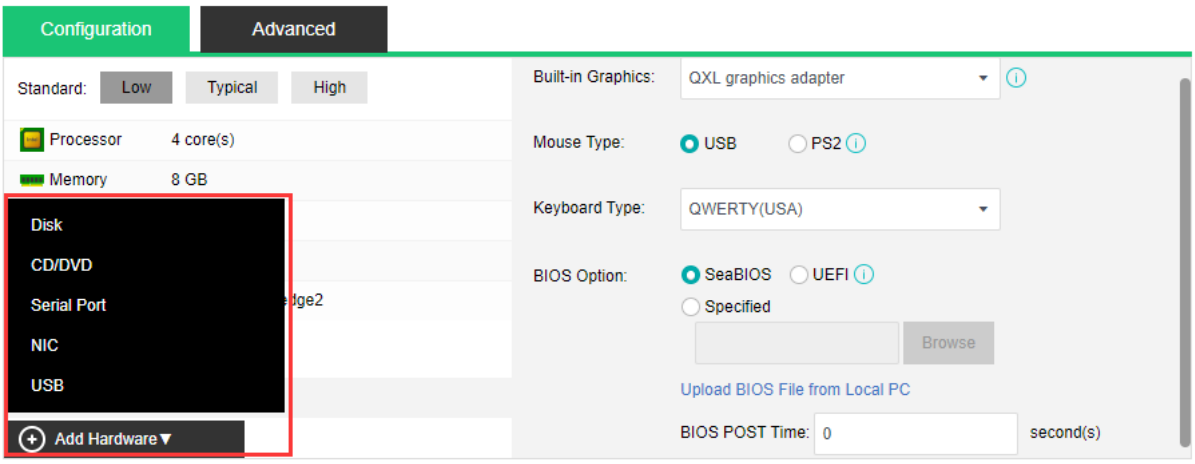
Mouse Type: Options are **USB** and **PS2**.

Keyboard Type: QWERTY (USA) and QERTY (Italy).

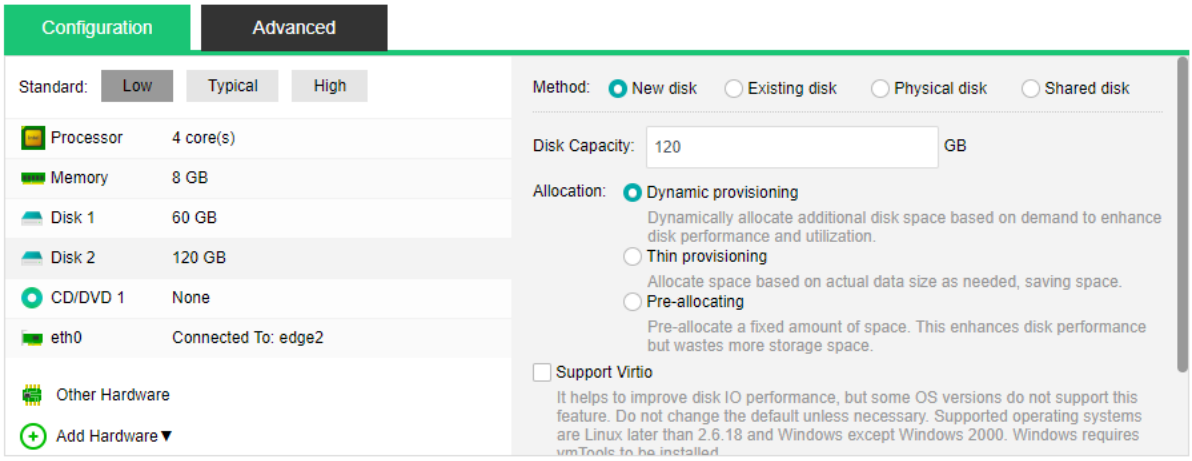
This is not recommended unless the virtual mouse does not work properly or USB mouse refuses to work for some reason. It takes effect after the console is re-opened. Mouse type can be changed to PS2 if USB mouse refuses to work for some reason.

BIOS Option: Options are **SeaBIOS, UEFI BIOS** and **Custom**. You can also specify **BIOS POST Time**.

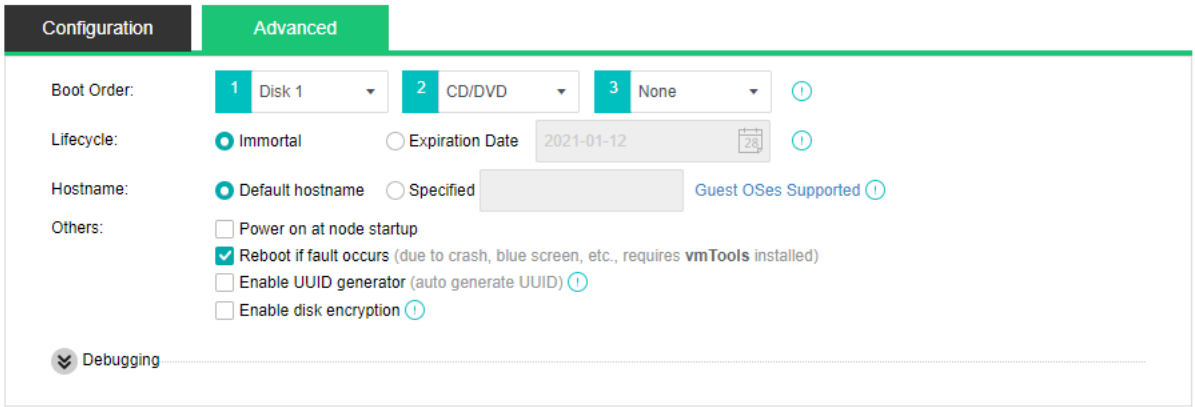
To add more hardwares, click **Add** Hardware. Then, you can add disk, CD/DVD, serial port, NIC and USB as per your need.



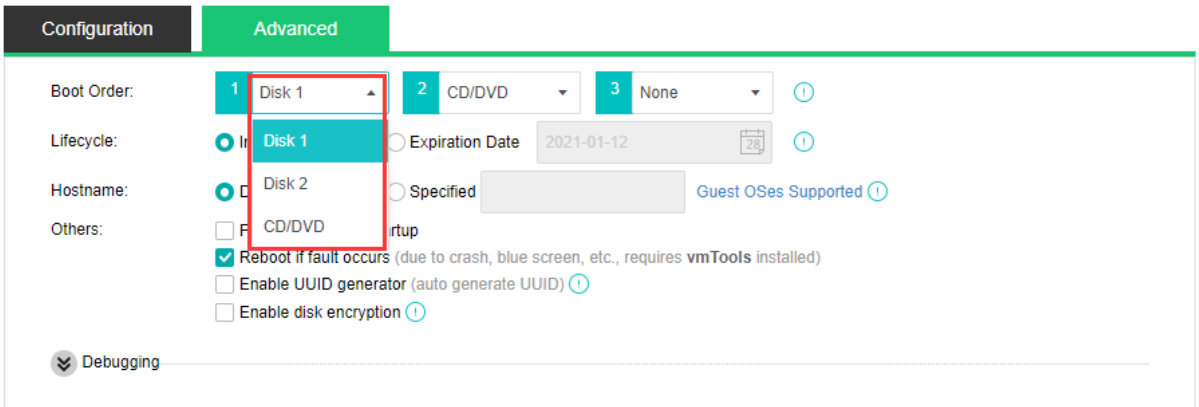
For example, click **Add Hardware** and select **Disk**. Then, disk 2 will be added to the configuration (as shown in following figure). You can add that disk by creating a new disk or using an existing disk. To delete a disk, click on this  icon.



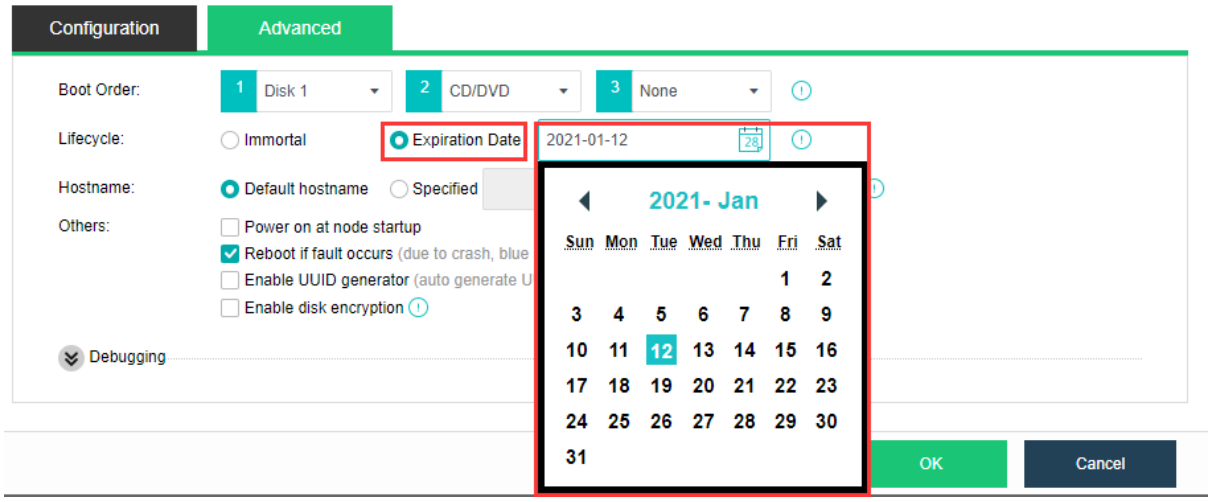
On the **Advanced** tab, you can configure more, such as **Boot Order**, **Lifecycle**, **Others** and **Debugging**.



Boot Order: Specifies the boot order for the virtual machine. You can choose an item (disk or CD/DVD) from the pull-down list.



Lifecycle: Specifies virtual machine's lifecycle. It can be immortal or a specified expiration date. A powered-on virtual machine will occupy CPU and memory resources if it has not been used for a long period of time, while a powered-off virtual machine will occupy disk space if it has not been used for a long period of time. You can specify **Expiration Date** for **Lifecycle** so that you may delete the expired virtual machine when the end of its lifecycle is reached.



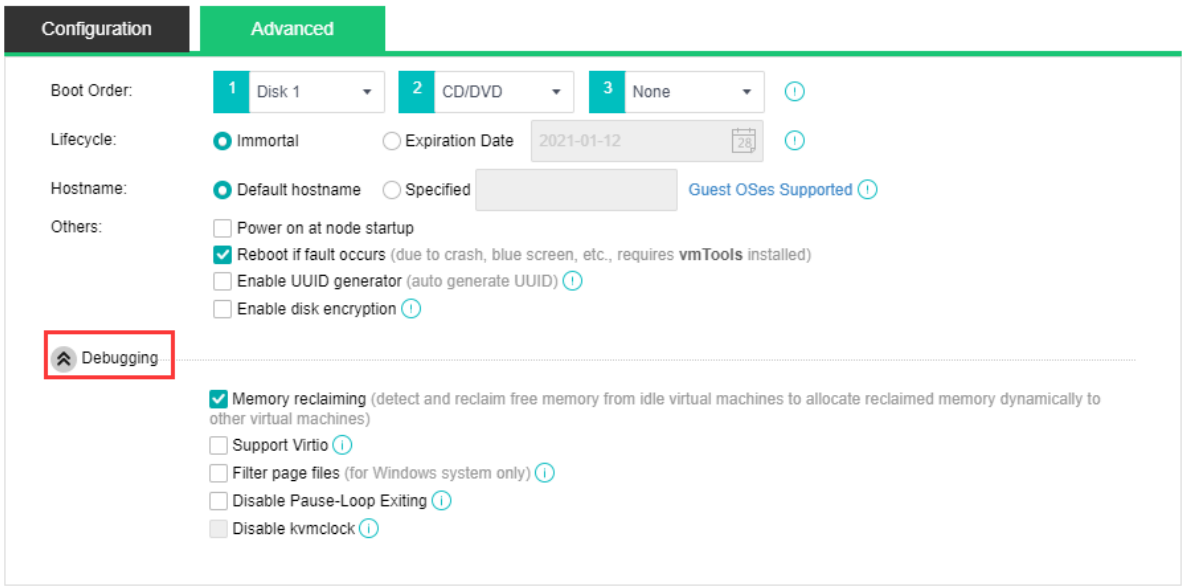
Others includes the following options:

Power on at node startup: Once it is selected, virtual machine will be automatically powered on once the node starts up.

Reboot if fault occurs: Once it is selected, virtual machine will be automatically restarted in case of stuck, blue screen. To make thhis option take effect, vmTools should be installed.

Enable UUID generator: Every time UUID generator is enabled, a new UUID will be generated. Universally Unique Identifier, UUID in short, is an identifier of a virtual machine. Certain software running on the VM need the UUID to work properly. Please do not change this at will, since changes of UUID may cause some functionalities to be invalid. You may choose to re-generate UUID for the new virtual machine while cloning virtual machine or deploying virtual machine from a template.

To show more options, click on Debugging and you will see the following options:



Enable memory reclaiming: Once it is enabled, free memory of idle virtual machines will be detected and reclaimed for other virtual machines.

Support Virtio: Once it is enabled, all disks associated with this virtual machine will support Virtio, to improve IO performance, but some software versions do not support this feature. Please do not change the default setting unless necessary.

Filter page files: Once it is enabled, it helps to save backup storage and time. Page files will not be filtered when a virtual machine is backed up during powered-off status. It takes effect after vmTools are installed. This debugging option is for Windows system only.

Disable Pause-Loop Exiting: Once it is selected, Pause-Loop Exiting will be disabled. Select this option to avoid VM EXIT caused by PAUSE instruction of VM, which improves adaptive spinning performance of multi-core VM (more than 16 cores) to some extend but requires extra costs of physical CPU. The default is recommended unless otherwise required.

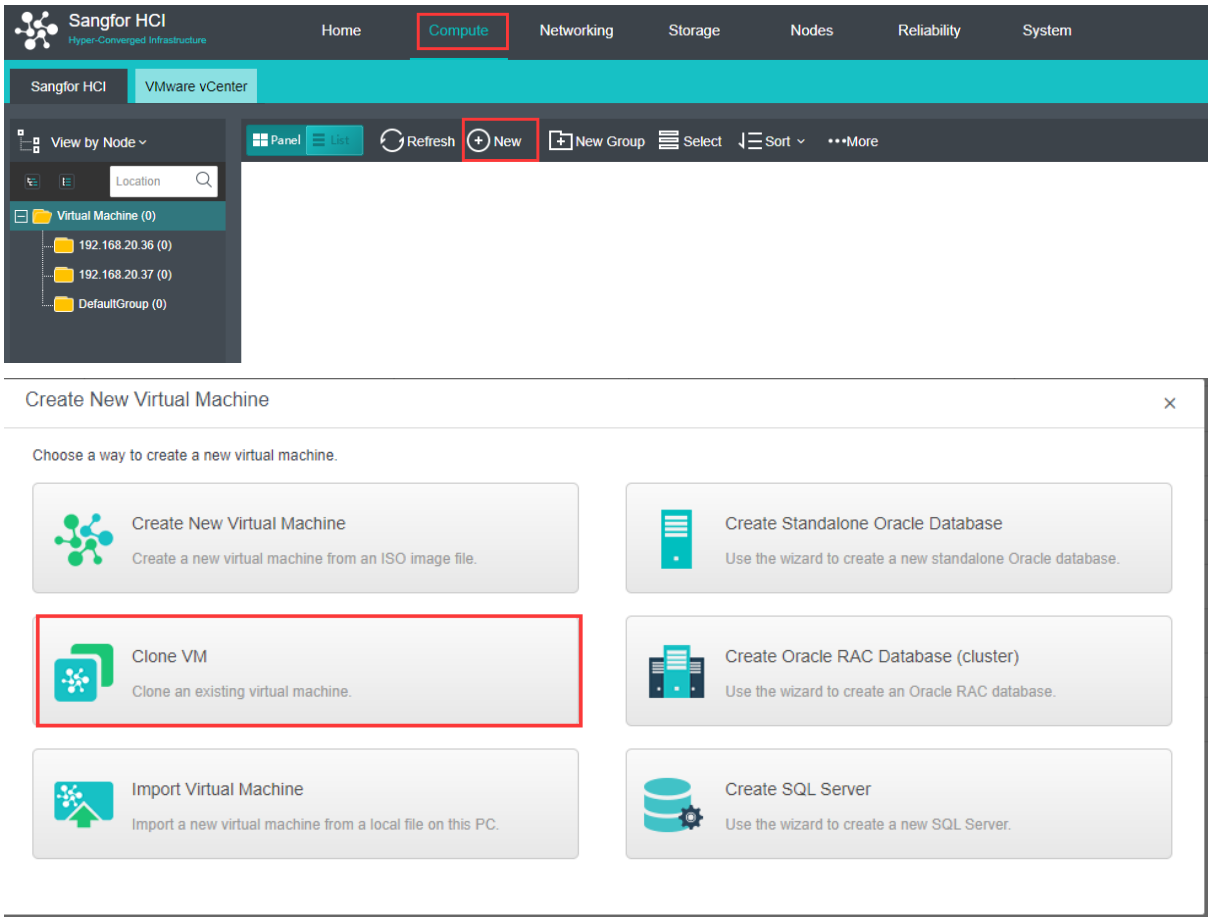
Disable kvmclock: Once it is selected, kvmclock will be disabled. On Linux kernel 2.6.32 or earlier version, you may disable kvmclock to improve system stability.

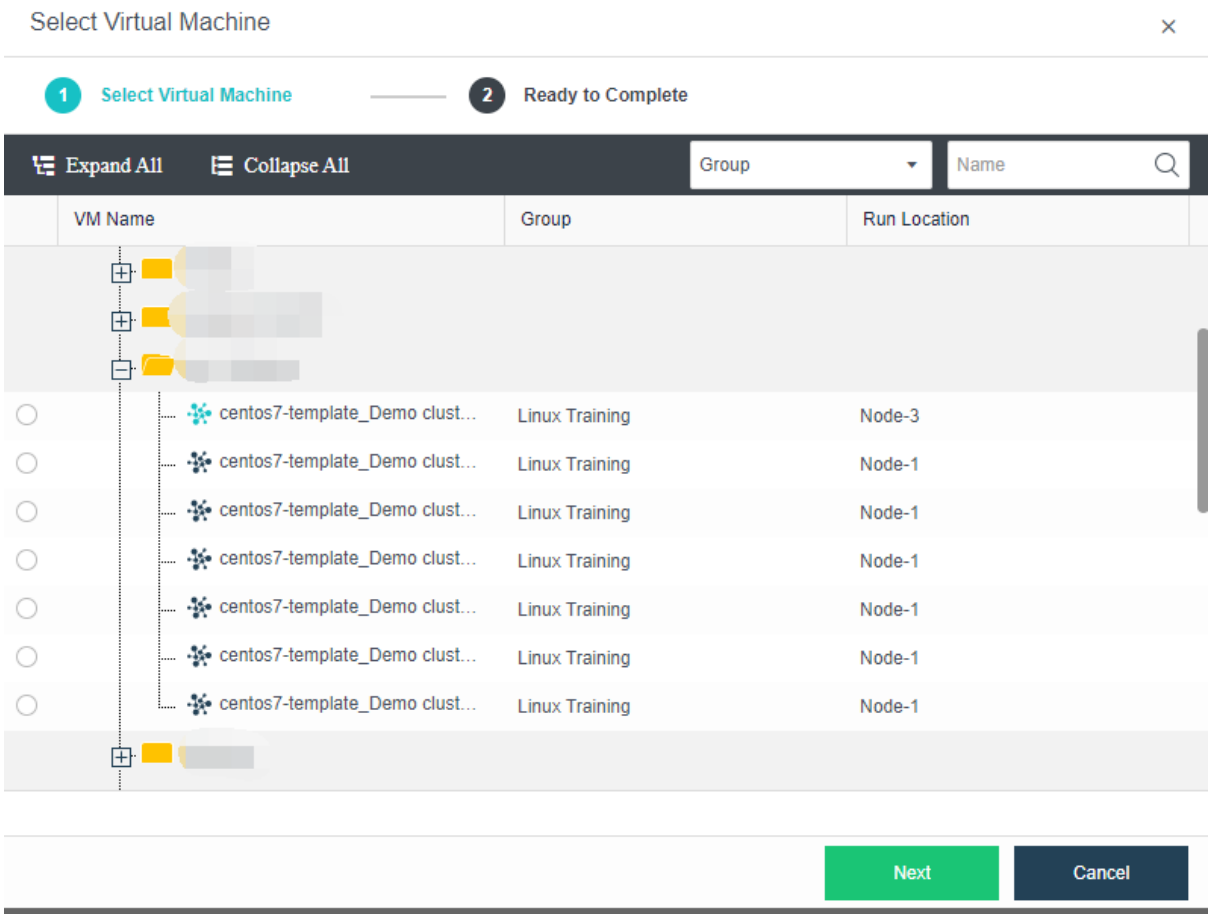
2.2.1.3 Cloning Virtual Machine

Cloning virtual machine means duplicating a virtual machine, which applies to virtual machines that can be used as sources for new virtual machines. The cloned resources will not

affect source virtual machines.

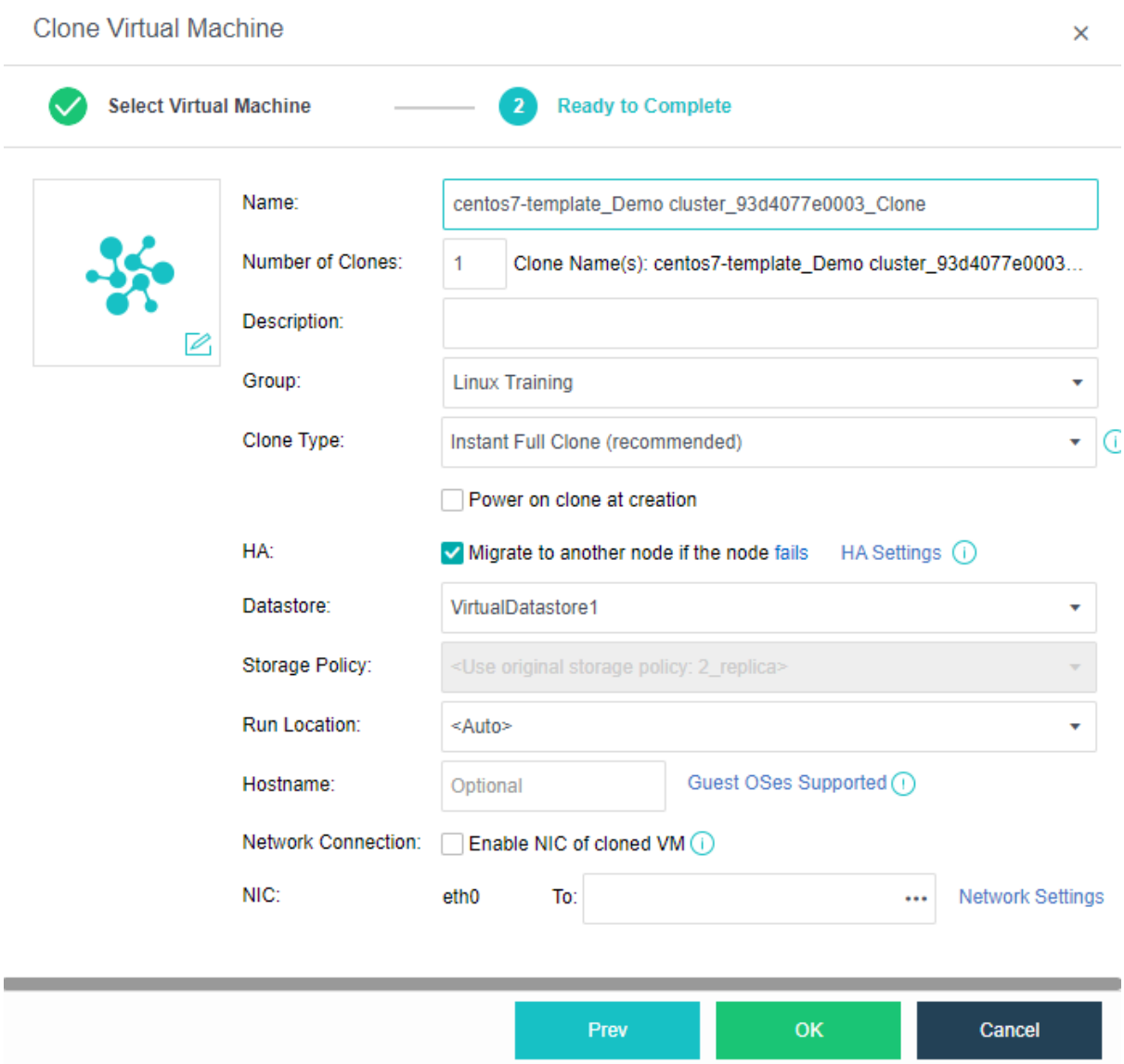
To clone a virtual machine, click **New** in **Compute** and select **Clone VM** on the **Create New Virtual Machine** page to enter the following page. On that page, select a virtual machine that you want to clone.





- A powered-off virtual machine cannot be cloned.
- A virtual machine being migrated or being cloned cannot be cloned.
- Backup task will be canceled if the clone operation is performed against a virtual machine which is being backed up.
- Guest operating system settings of a cloned virtual machine remain the same as that of the source virtual machine, exclusive of MAC address. Thus, IP address of one of the two virtual machines should be modified, otherwise, it may result in IP address conflict.

Cloning a virtual machine creates a duplicate of a virtual machine, including VM configurations and disk files, On the following page, you can customize parameters of a clone.



To clone a virtual machine, you need to specify the following parameters for the clone: **Name, VM number, Description, Clone Type, Group, HA, datastore, Storage Policy, Run on Node, Hostname, Network Connection, and NIC.** To have the cloned virtual machine powered on upon creation, select the option **Power on virtual machine at creation**.

There are three types of cloning available starting from version 6.0.1:

a. Instant Full Clone

Description: Instantly clone the selected virtual machine as a new independent virtual machine. Instant full clone is the default clone option for 3 nodes and above which recommended to be use.

Features:

1. Cloning process can be complete in short time.

2. The disk file of the clone VM is independent to the original VM
3. Performance will not affected after cloning completed.

Requirement: Required 3 nodes and above to support. The datastore of both source virtual machine and cloned virtual machine must be in virtual storage.

b. Linked Clone

Description: Clone the virtual machine by linking the disk file to the original virtual machine. This method is recommended to be use during development and testing phase while the performance is not the essential point.

Features:

1. Cloning process can be complete in short time.
2. The disk file of the clone VM is dependent to the original VM and storage occupation can be reduced.
3. Performance might be slightly affected after cloning completed.

Requirement: Required 3 nodes and above to support. The datastore of both source virtual machine and cloned virtual machine must be in virtual storage.

c. Full Clone

Description: Perform full clone of the selected virtual machine and create a new independent virtual machine.

Features:

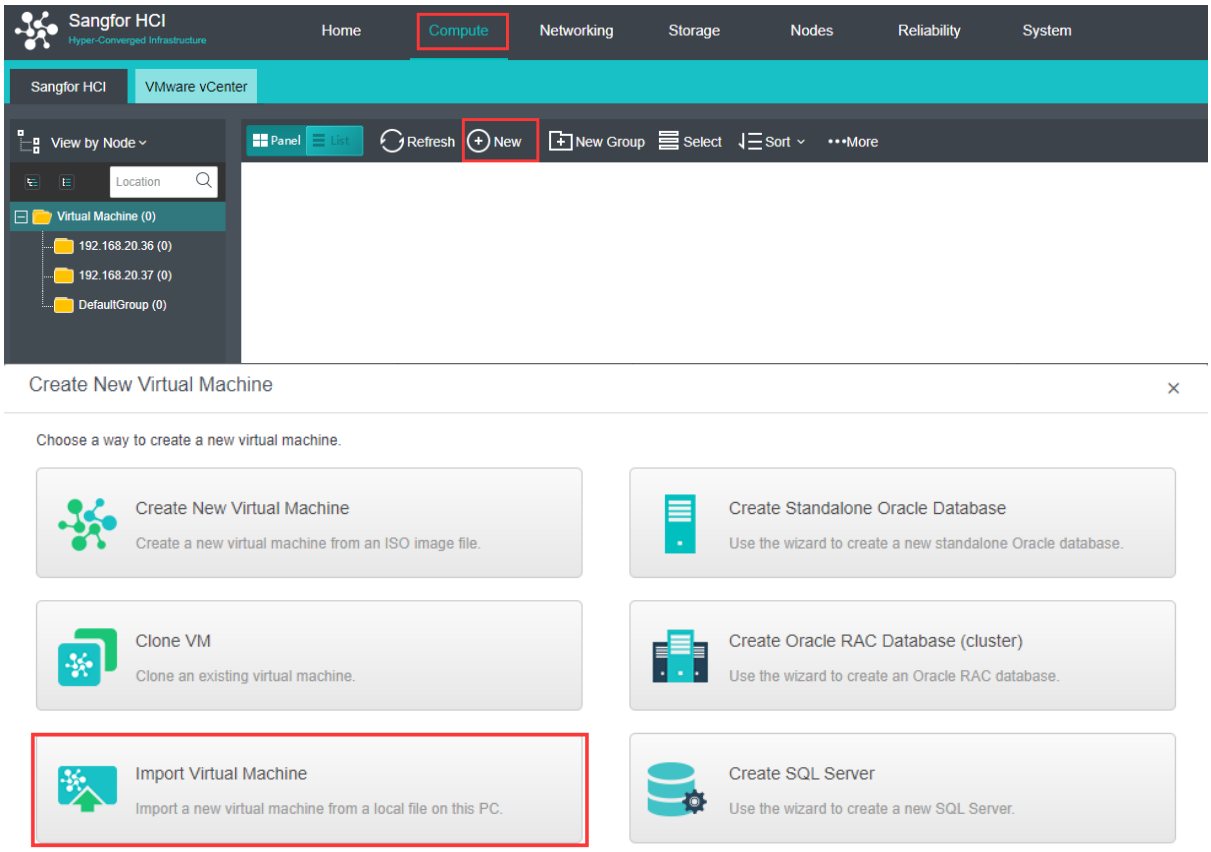
1. The disk file of the clone VM is independent to the original VM.
2. Datastore of the source and cloned vm can be external storage.

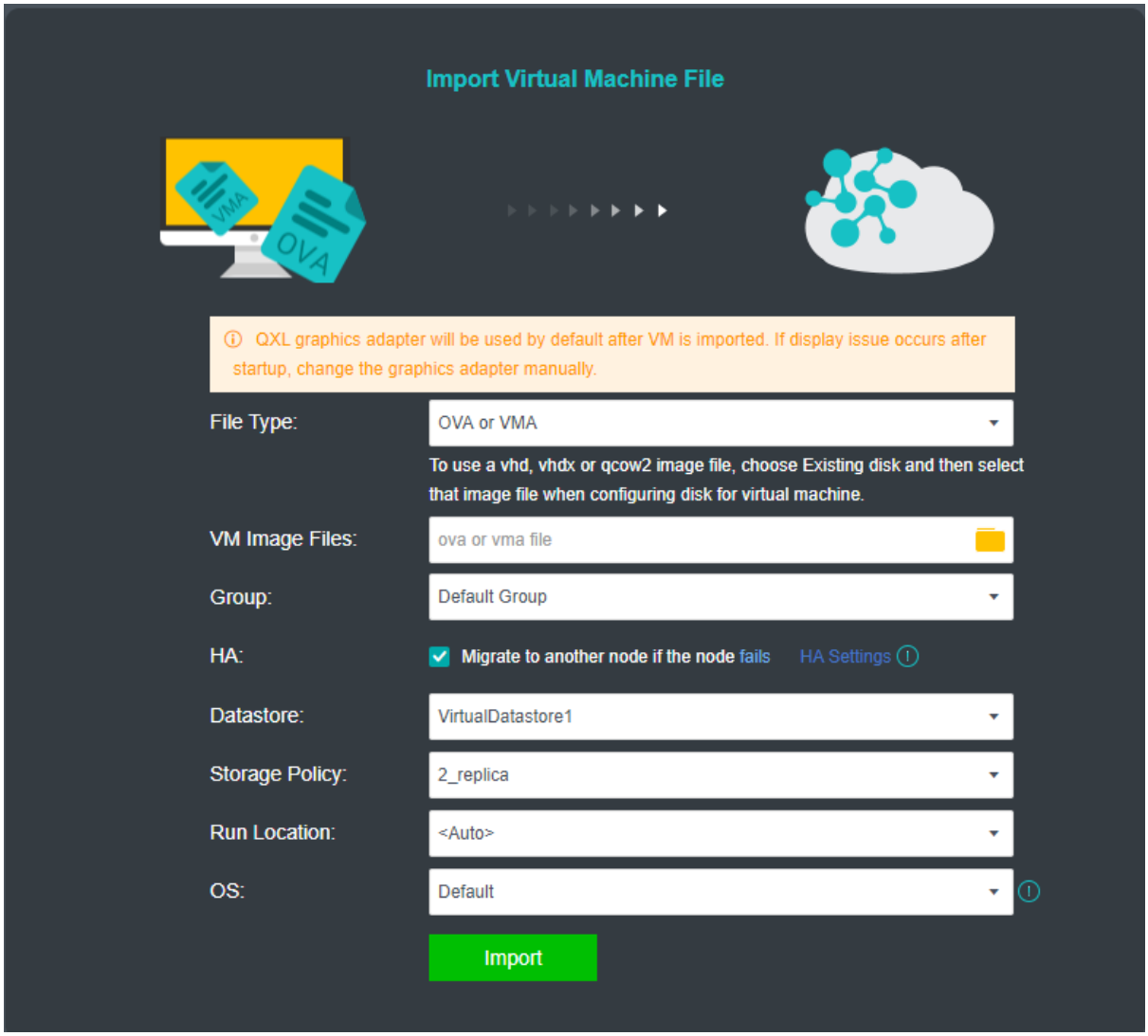
The following factors will affect efficiency of clone task: amount of the source virtual machine data and performance of the server where Sangfor HCI software is installed.

2.2.1.4 Importing Virtual Machine

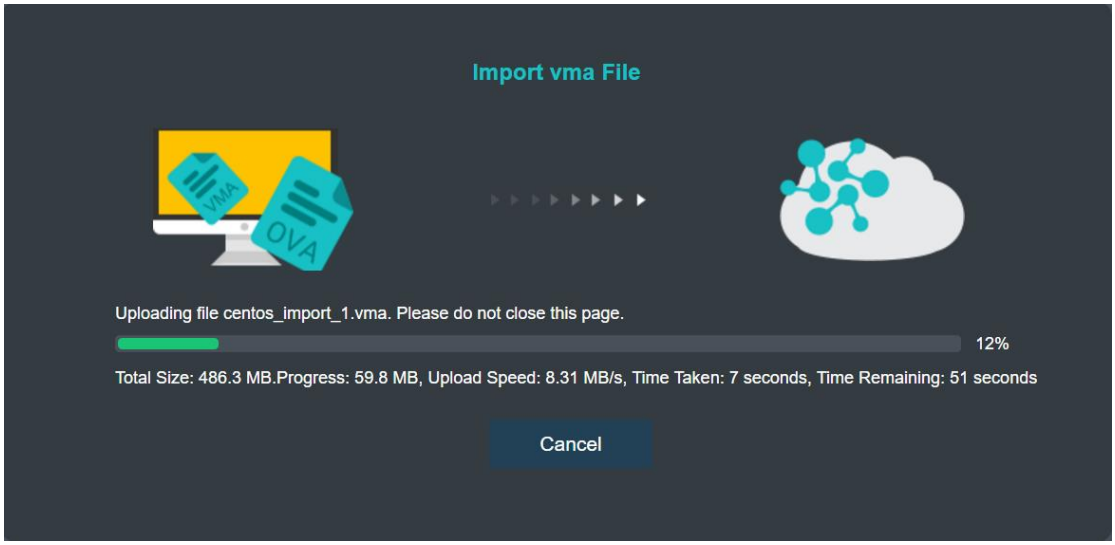
The following types of VM files can be imported onto Sangfor HCI platform: OVA files exported from VMware virtualization platform, VMA files exported from other Sangfor HCI platforms.

To import a virtual machine file, click **New** in **Compute**, select **Import Virtual Machine** on the **Create New Virtual Machine** page to enter the following page.





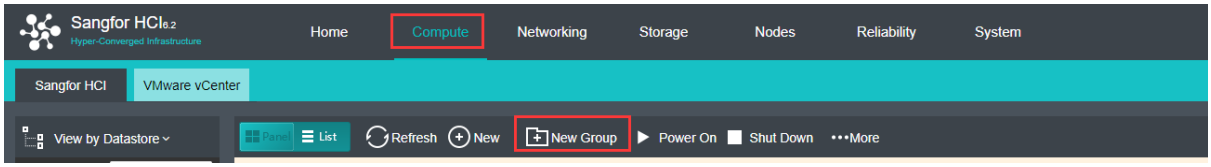
On the above page, select an OVA or VMA file from local disk, specify **Group, HA, Datastore, Run on Node** and **OS**, then click **Import**.

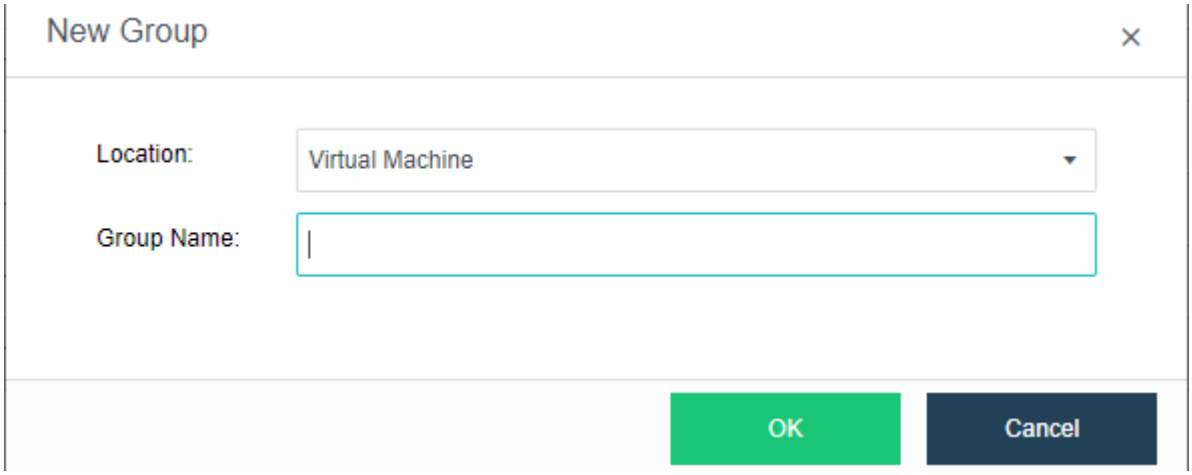


- If an ova file of a Windows based virtual machine is imported, USB mouse driver needs to be updated and you will be prompted to install that driver.
- If an ova file of a Linux based virtual machine is imported, you need to configure IP address for NIC.
- After the ova file is imported, the virtual machine will be automatically created. The Import Virtual Machine File page can be closed while the virtual machine is being created.

2.2.1.5 Adding New Group

In **Compute**, you can add a new group by clicking **New Group**. On the **New Group** page, as shown below, you need to specify a name for the new group.

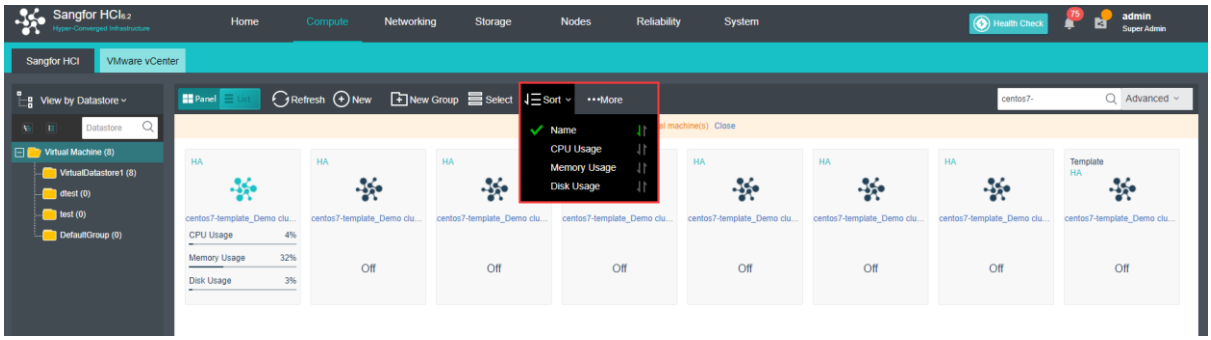


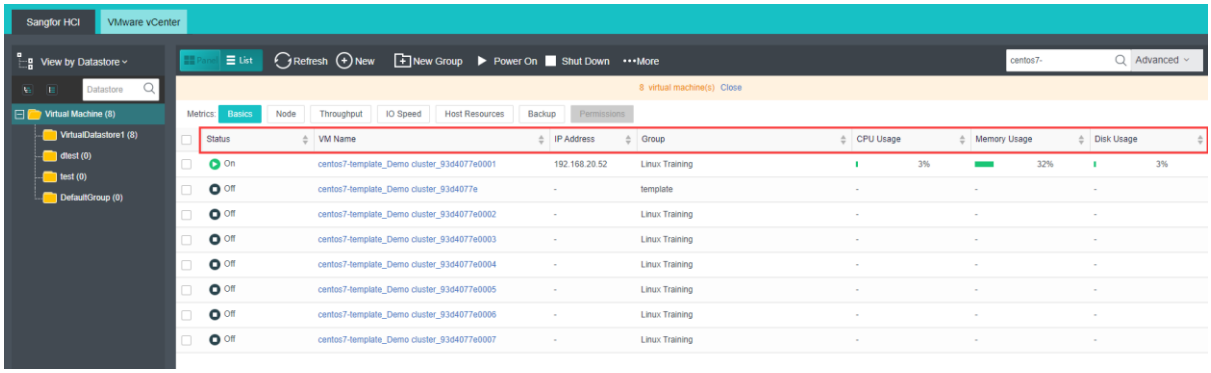


2.2.1.6 Sorting Virtual Machines

Virtual machines can be sorted by **Name, CPU Usage, Memory Usage, Disk Usage** in Panel View.

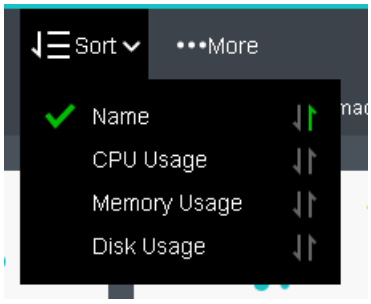
While for the List View, you can sort the virtual machines with any option.



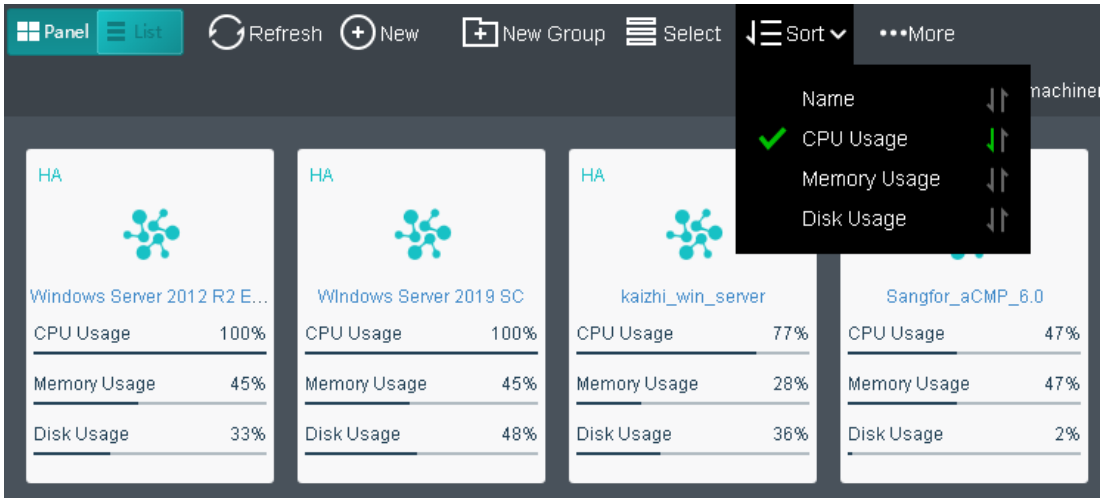


To sort virtual machines by name, select **Sort > Name** in **Compute**. You may click on the

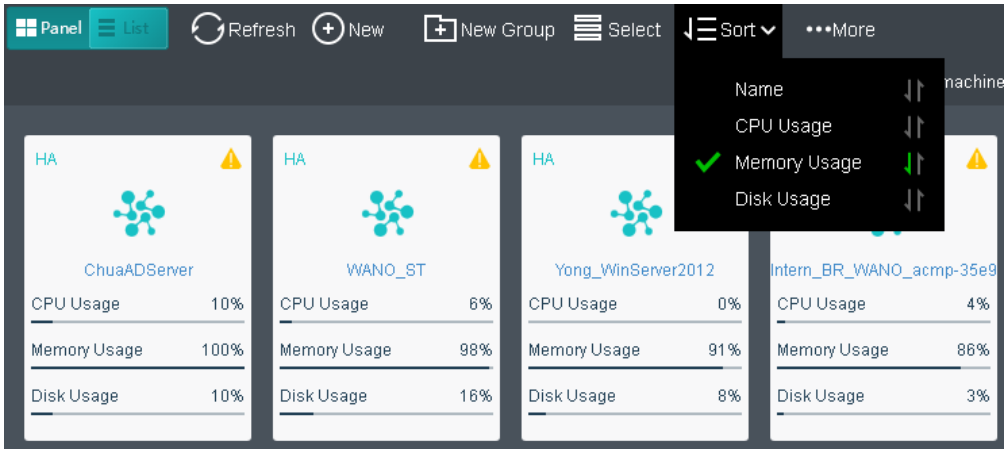
arrow  to sort VMs in ascending or descending order.



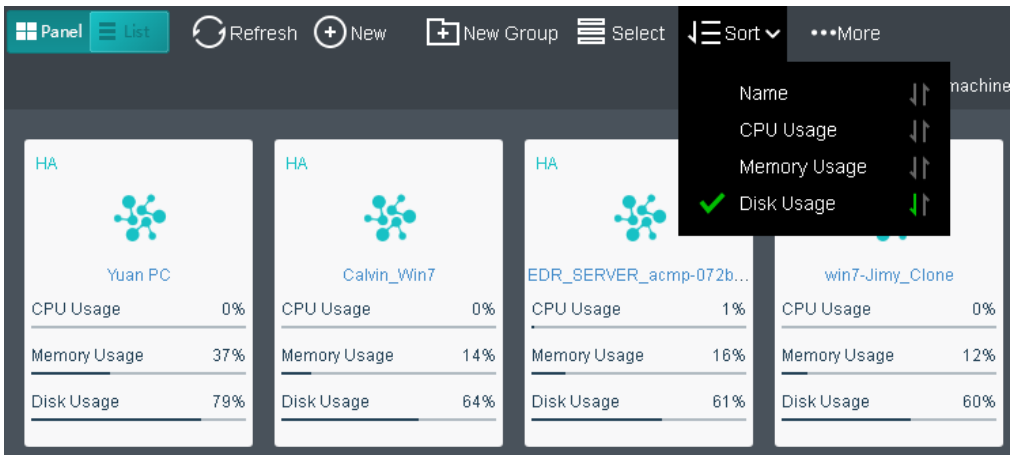
To sort virtual machines by CPU usage, select **Sort > CPU Usage** in **Compute**. By clicking on that arrow, virtual machines can be sorted based on CPU usage in ascending order or descending order. The following figure shows that the virtual machines are sorted by CPU usage in a descending order.



To sort virtual machines by memory usage, select **Sort > Memory Usage** in **Compute**. By clicking on that arrow, virtual machines can be sorted by memory usage in ascending or descending order. The following figure shows that the virtual machines are sorted by memory usage in a descending order.

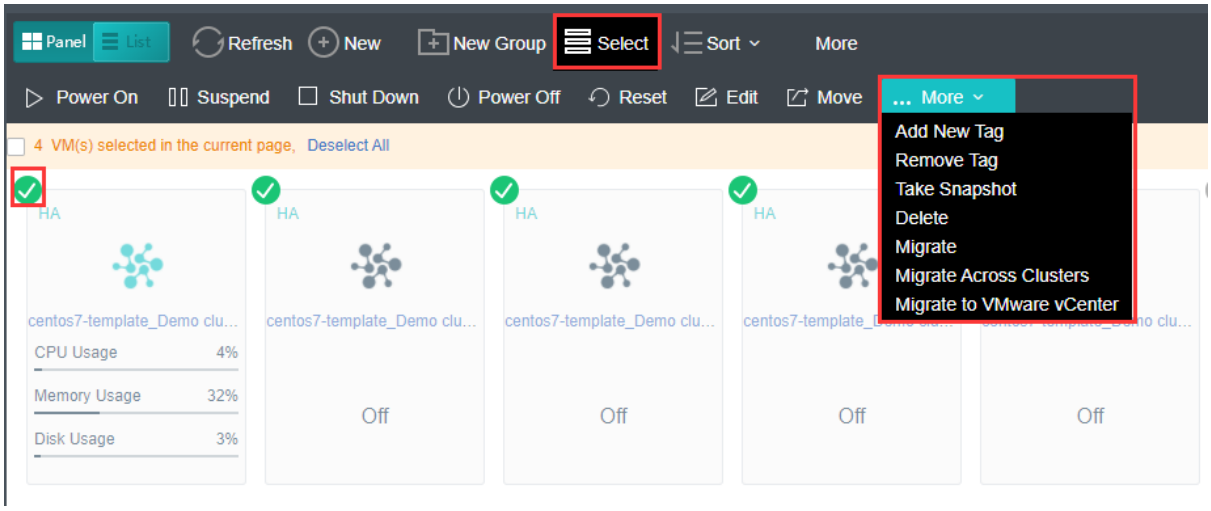


To sort virtual machines by disk usage, select **Sort > Disk Usage** in **Compute**. By clicking on that arrow, virtual machines can be sorted by disk usage in ascending or descending order. The following figure shows that the virtual machines are sorted by disk usage in a descending order.



2.2.1.7 Batch Operation

Administrator can perform the following operations against multiple virtual machines: **Power On, Suspend, Shut Down, Power Off, Reset, Move, Edit, Add New Tag, Remove Tag, Take Snapshot, Delete, Migrate, Migrate Across Cluesters, and Migrate to Vmware vCenter**.



Power On -To power on virtual machines(s), select one or more than one virtual machines and then and click on Power On.

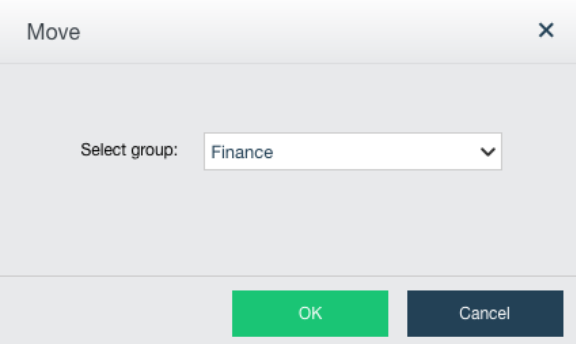
Suspend -To suspend virtual machines(s), select one or more than one virtual machines and then and click on Suspend.

Shut Down -To shut down virtual machine(s), select one or more virtual machines and then click on Shut Down.

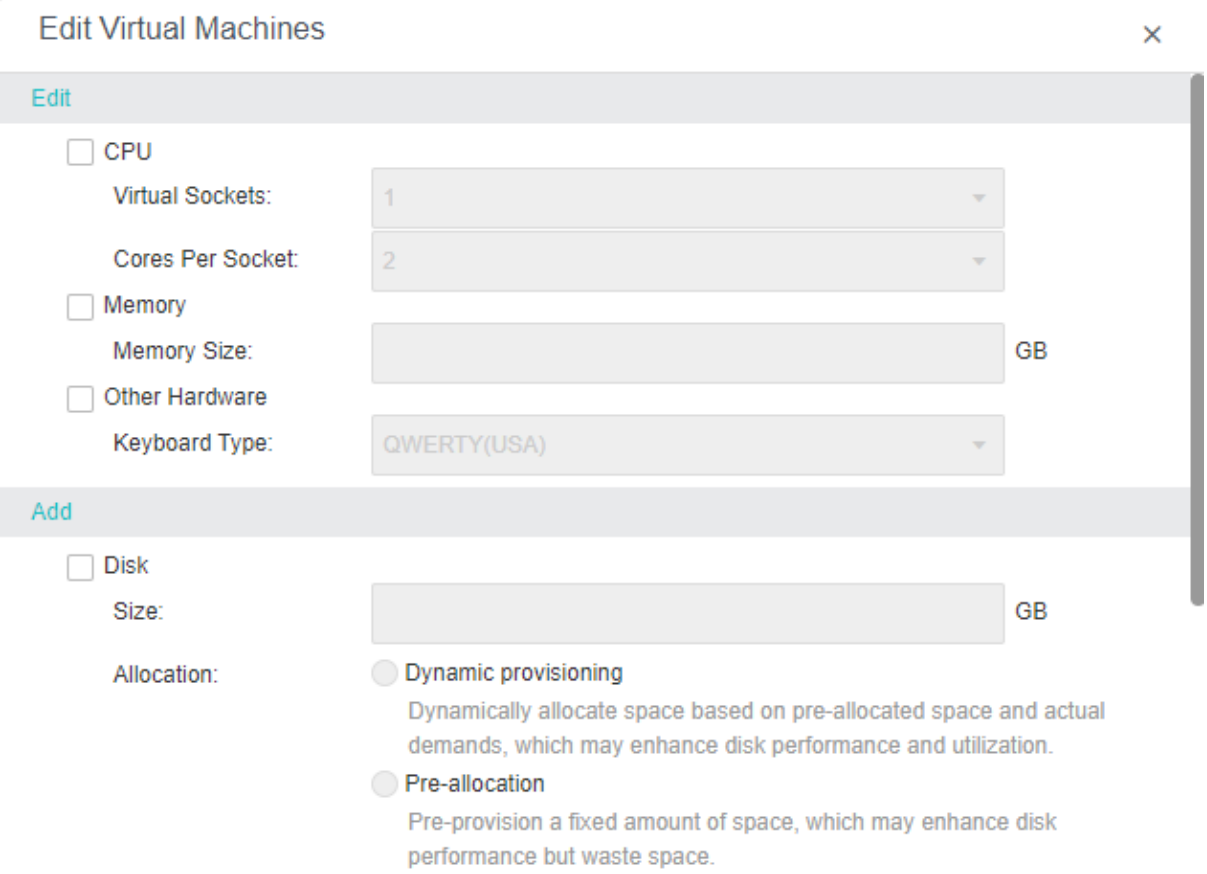
Power Off - To power off virtual machine(s), select one or more virtual machines and then click on Power Off.

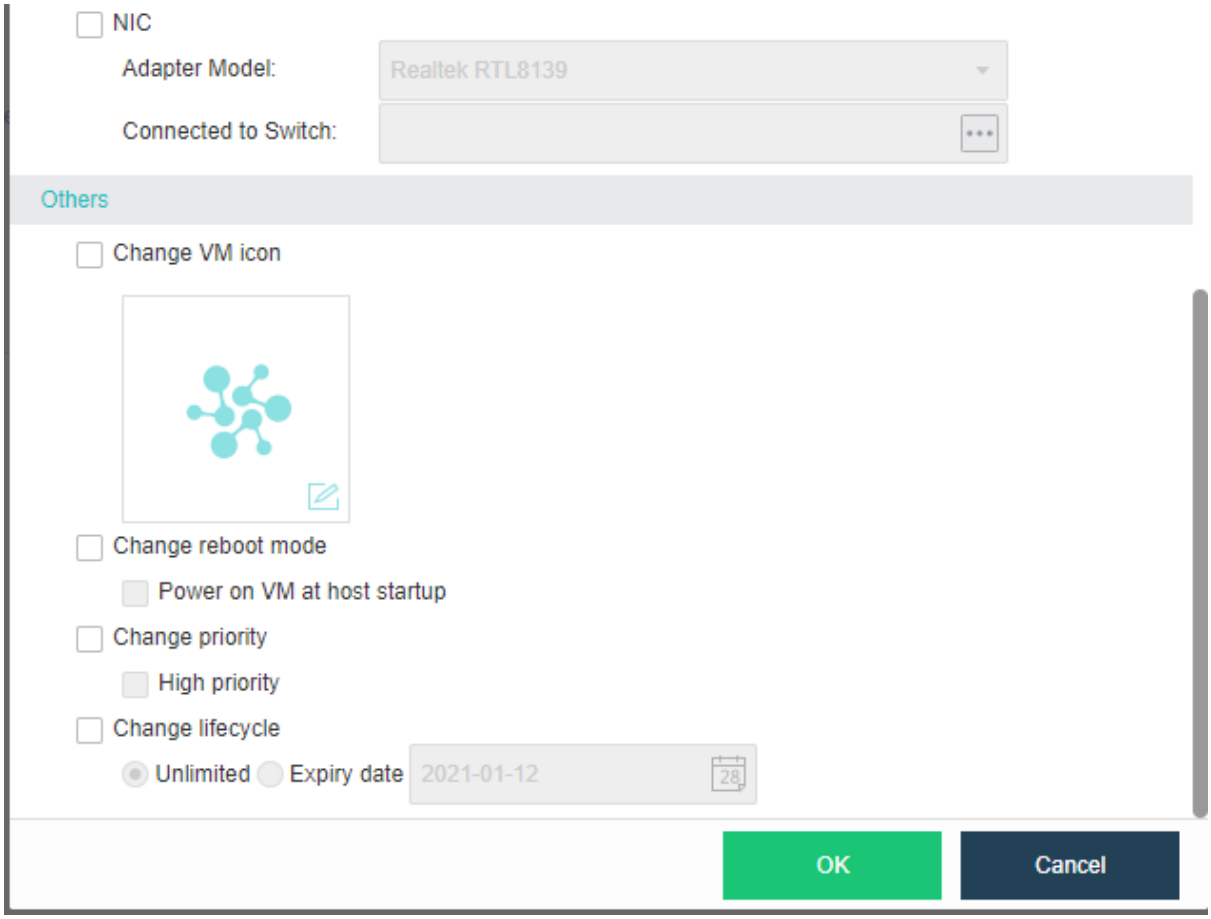
Reset -To restart virtual machine(s), select one or more virtual machines and then click on Reset.

Move -To move virtual machine(s) to a specific group, select one or more virtual machines and then click on Move.

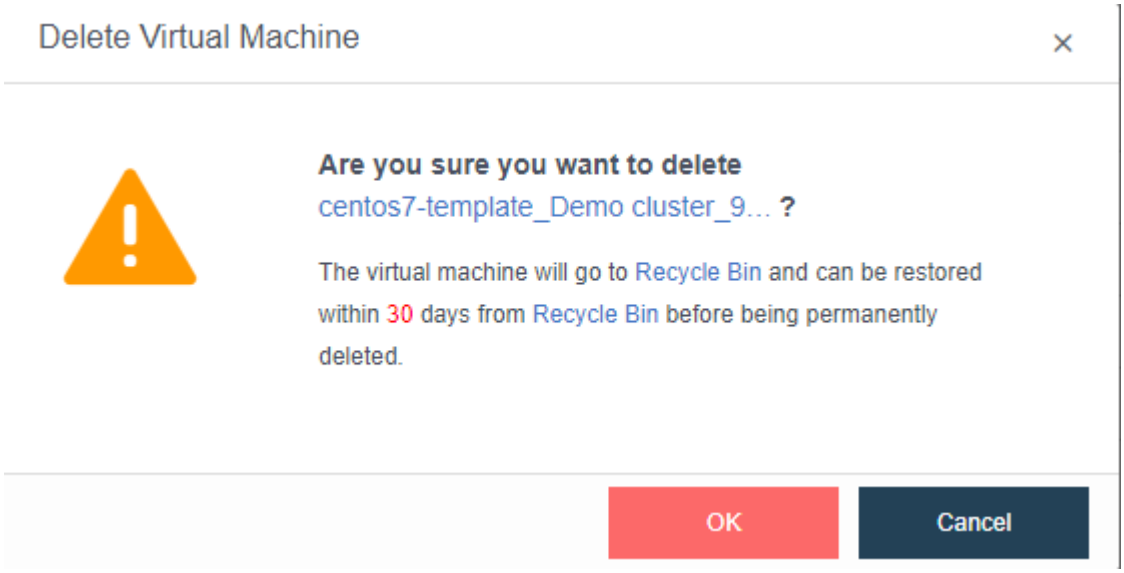


Edit -To edit virtual machines(s), select one or more than one virtual machines and then click on Edit.

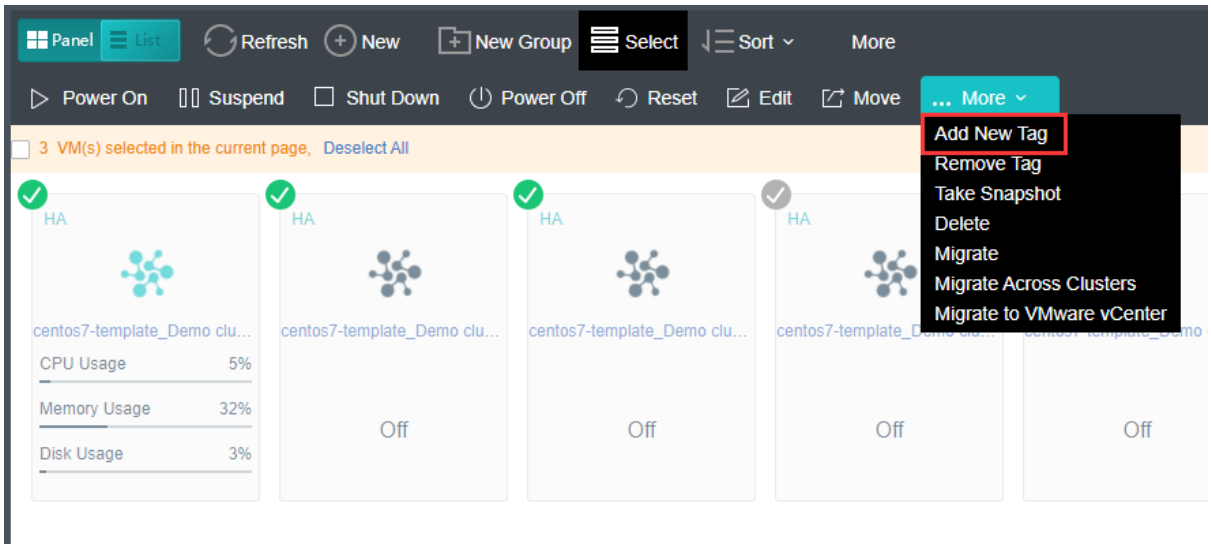


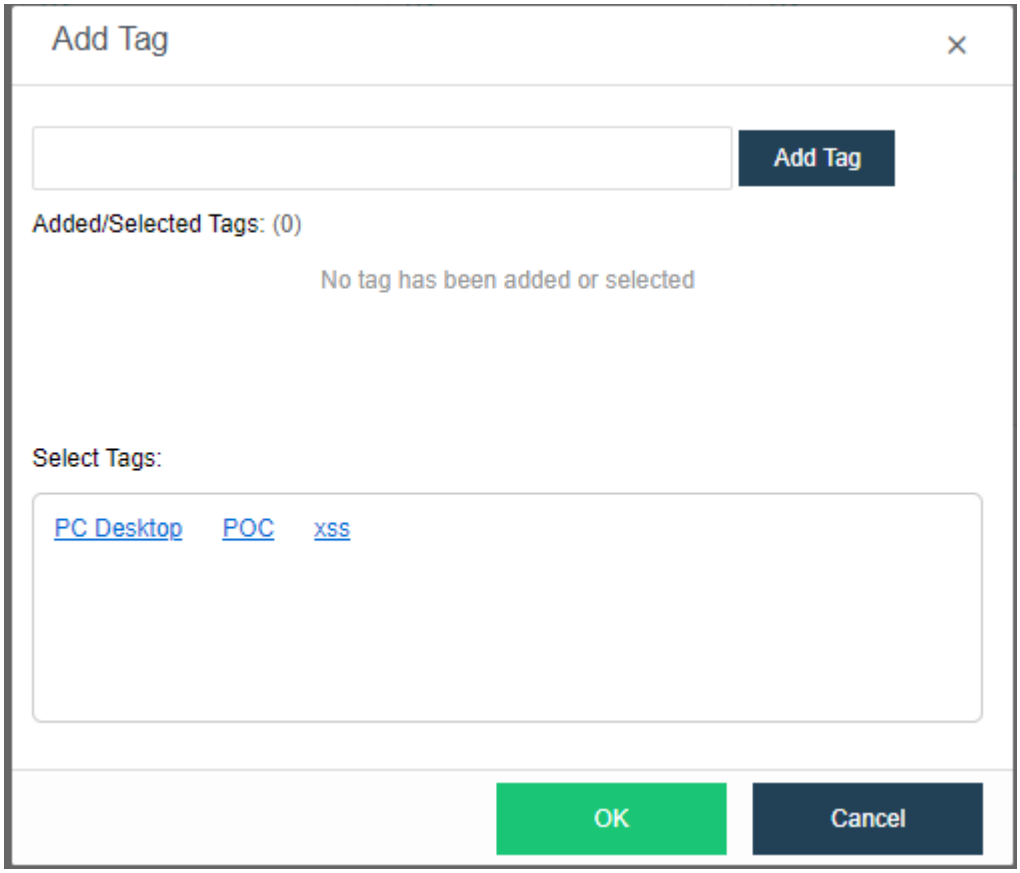


Delete - To delete virtual machines(s), select one or more than one virtual machines and then click on Delete. Virtual machines will go to Recycle Bin after being deleted and can be recovered within 30 days. To delete virtual machine(s) permanently, select the option **Delete the data completely and never restore them**. Thus, configuration files and disk files of virtual machines will be deleted completely and cannot be restored any more.

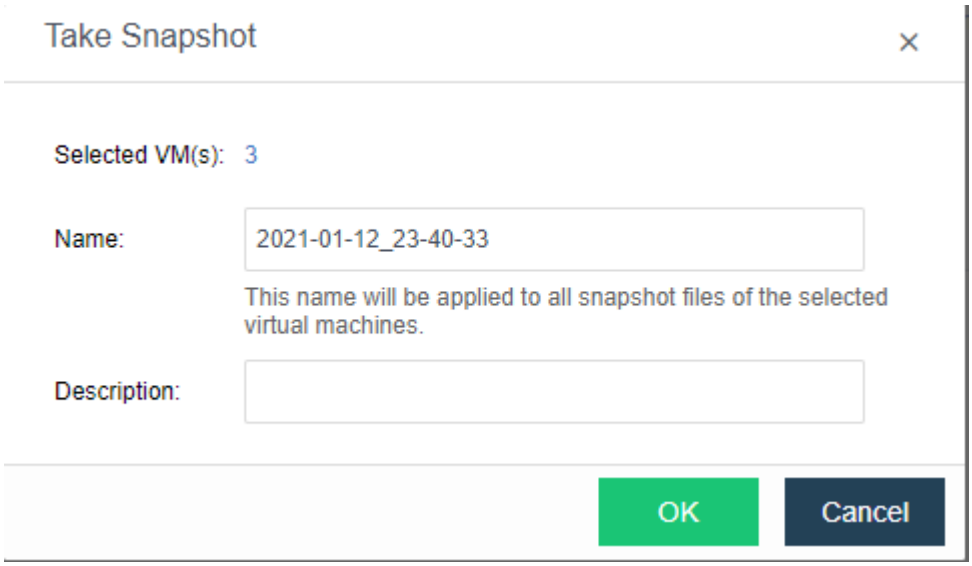


Add Tag -To add new tags to virtual machine(s), choose one or more than one virtual machines and select **Add Tag**. You can choose the existing tags or add new tags for those virtual machines. To remove tags of virtual machine(s), choose one or more than one virtual machines and select **Remove Tag**.

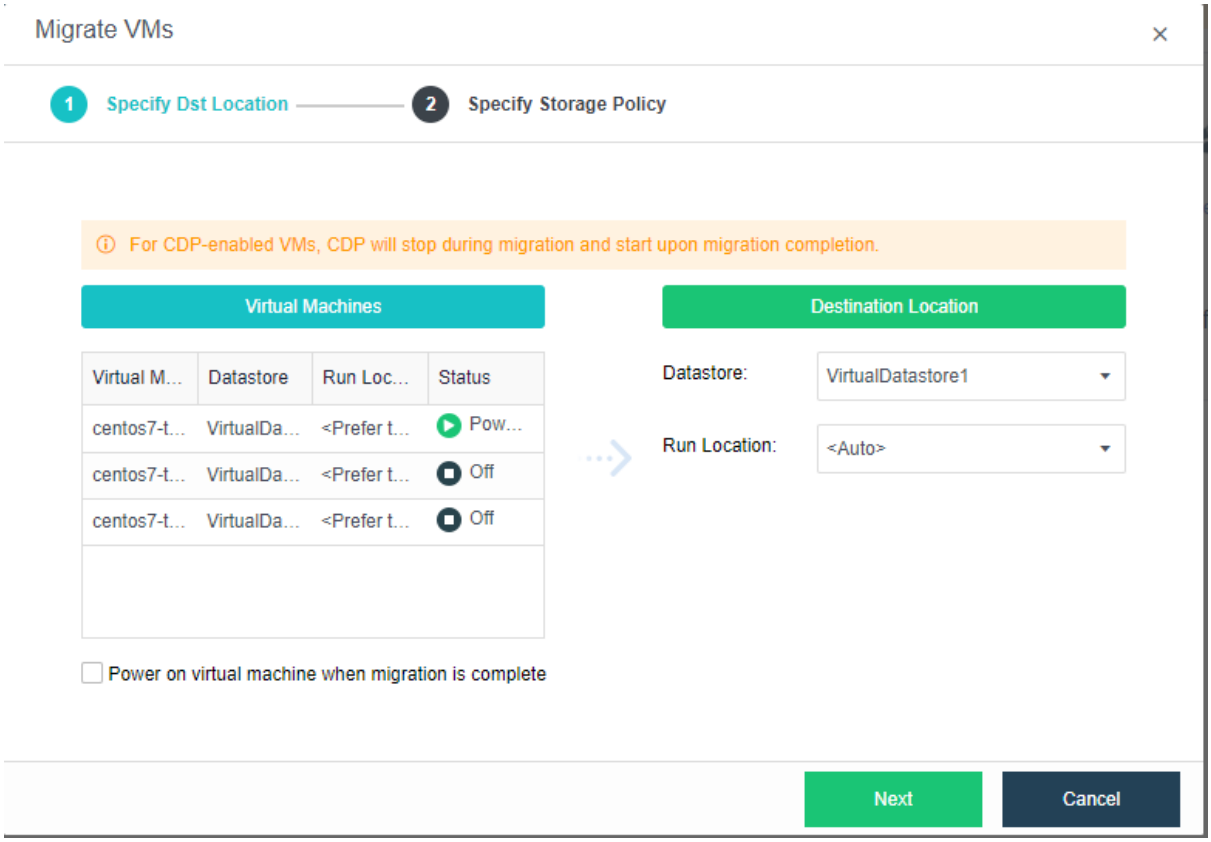


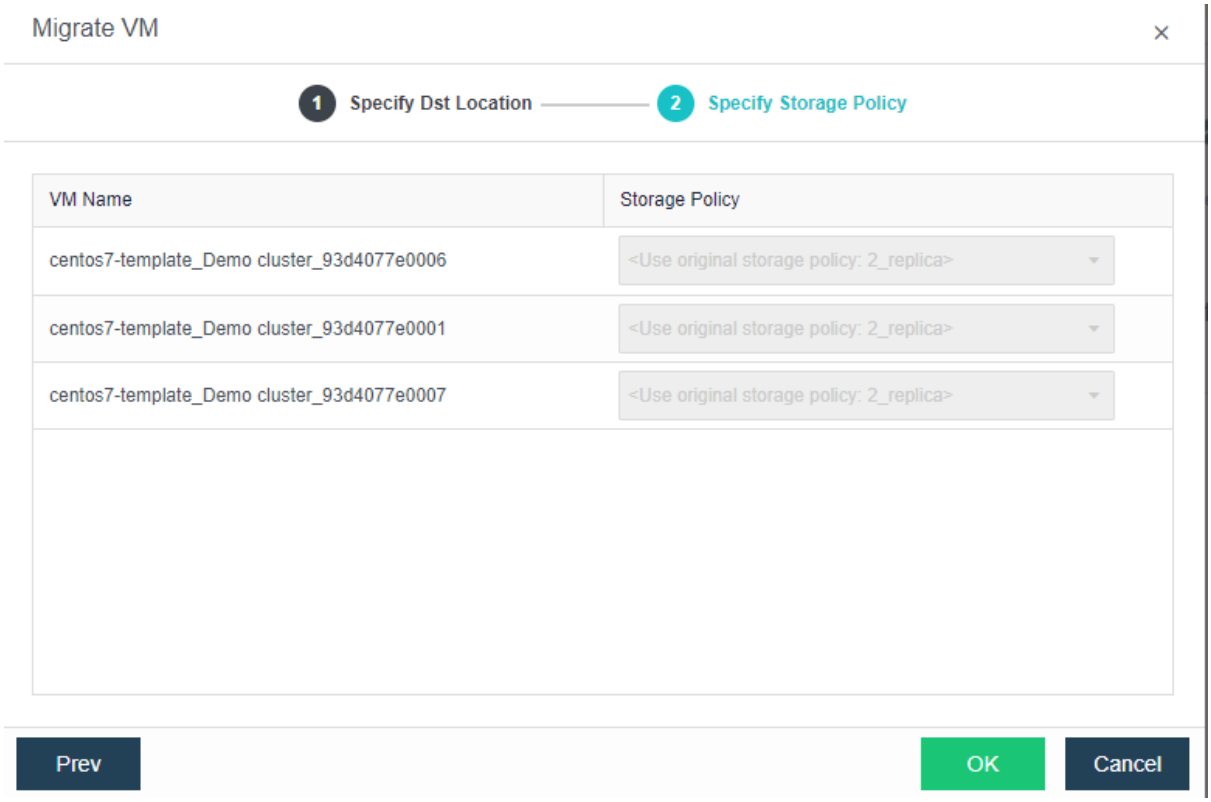


Take Snapshot – To take a snapshot according to the VM, choose one or more than one virtual machines and select Take Snapshot.

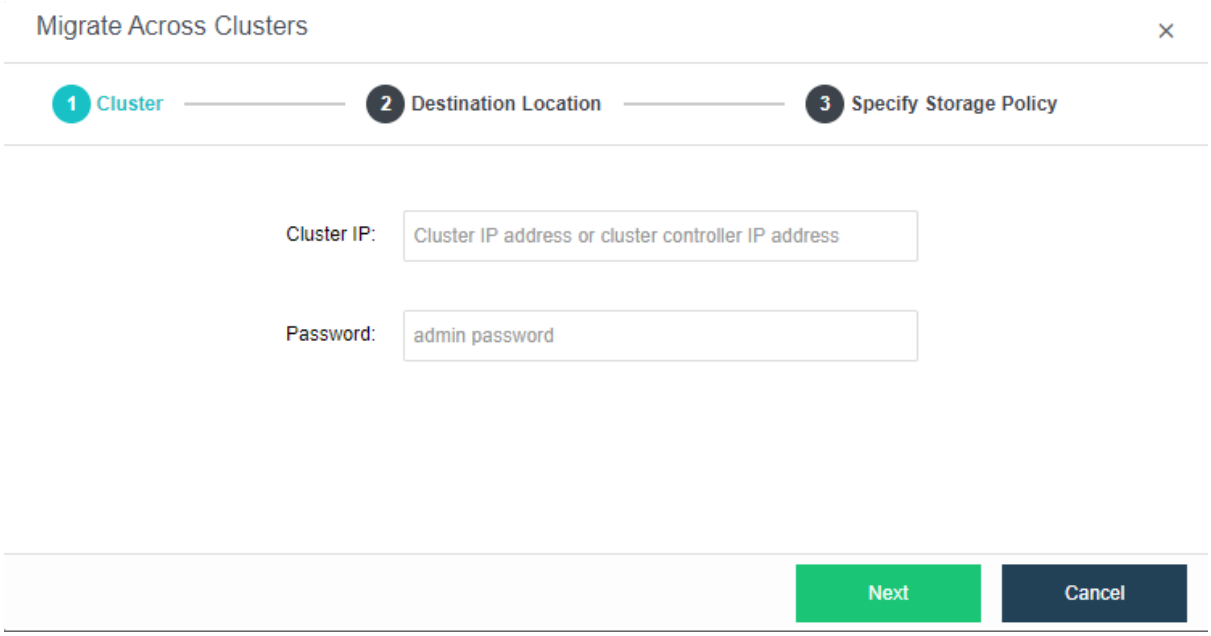


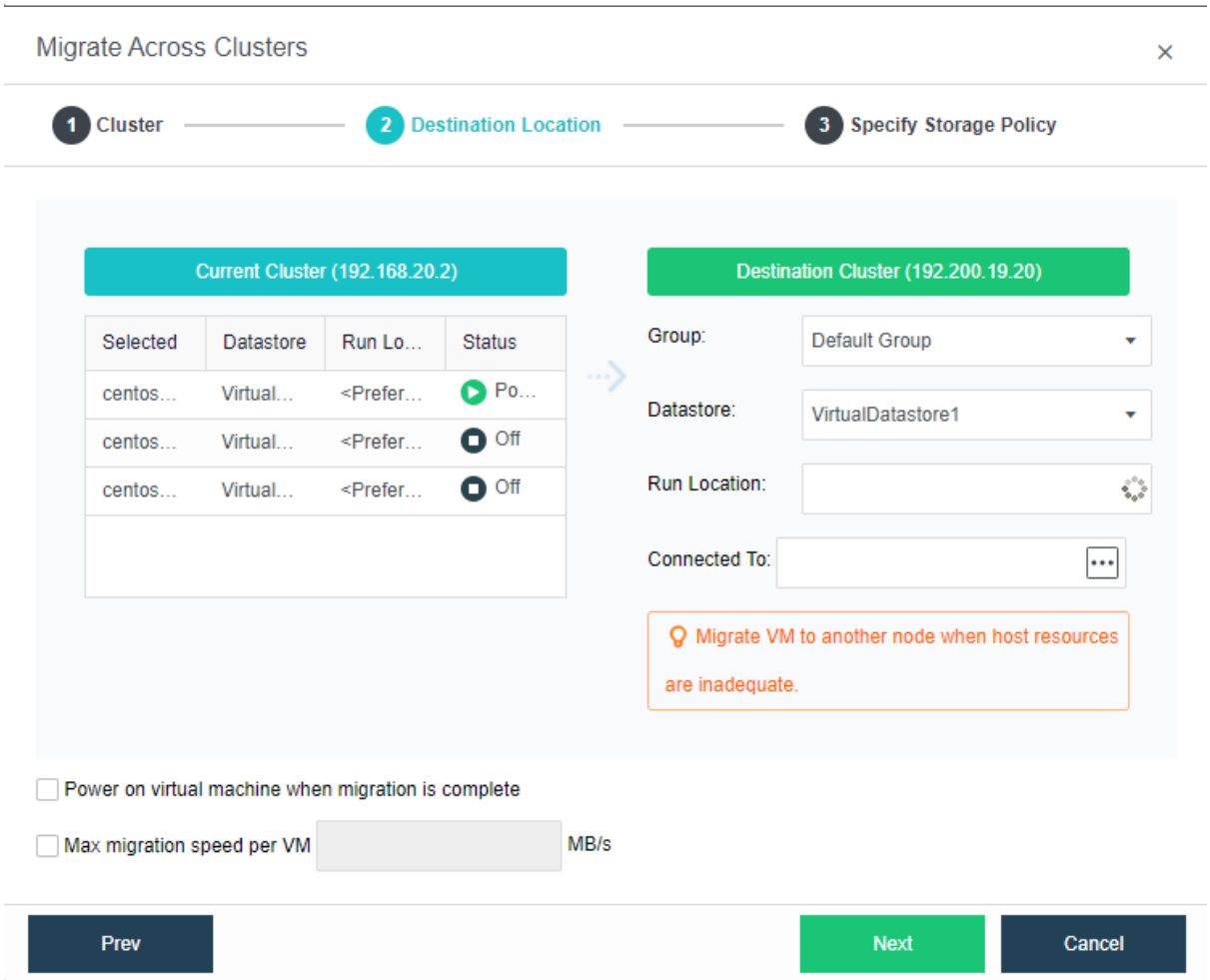
Migrate – To migrate the VM, choose one or more than one virtual machinese and select Migrate.

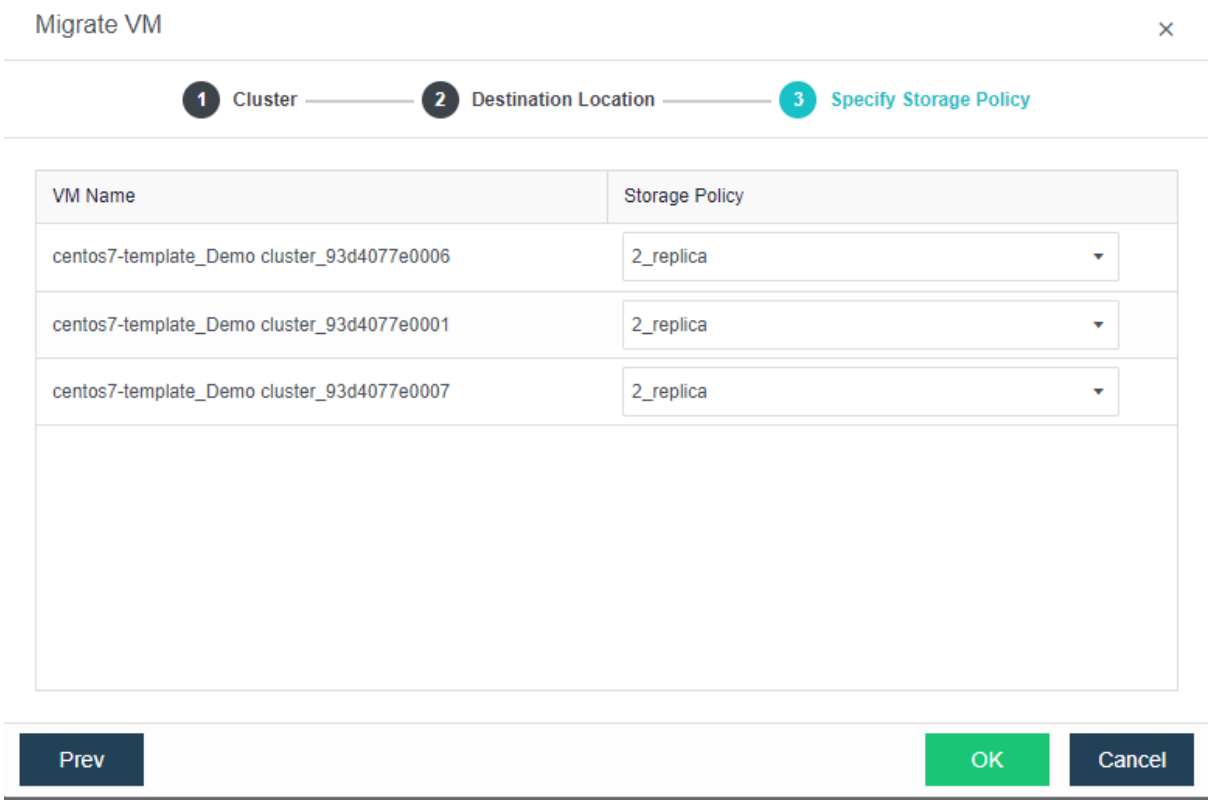

Migrate VMs
1 Specify Dst Location
2 Specify Storage Policy
For CDP-enabled VMs, CDP will stop during migration and start upon migration completion.
Virtual Machines
Destination Location
Virtual M...
Datastore
Run Loc...
Status
centos7-t...
VirtualDa...
<Prefer t...
Pow...
Off
Datastore:
VirtualDatastore1
Run Location:
<Auto>
Power on virtual machine when migration is complete
Next
Cancel


Migrate VM
1 Specify Dst Location
2 Specify Storage Policy
VM Name
Storage Policy
centos7-template_Demo cluster_93d4077e0006
<Use original storage policy: 2_replica>
centos7-template_Demo cluster_93d4077e0001
<Use original storage policy: 2_replica>
centos7-template_Demo cluster_93d4077e0007
<Use original storage policy: 2_replica>
Prev
OK
Cancel

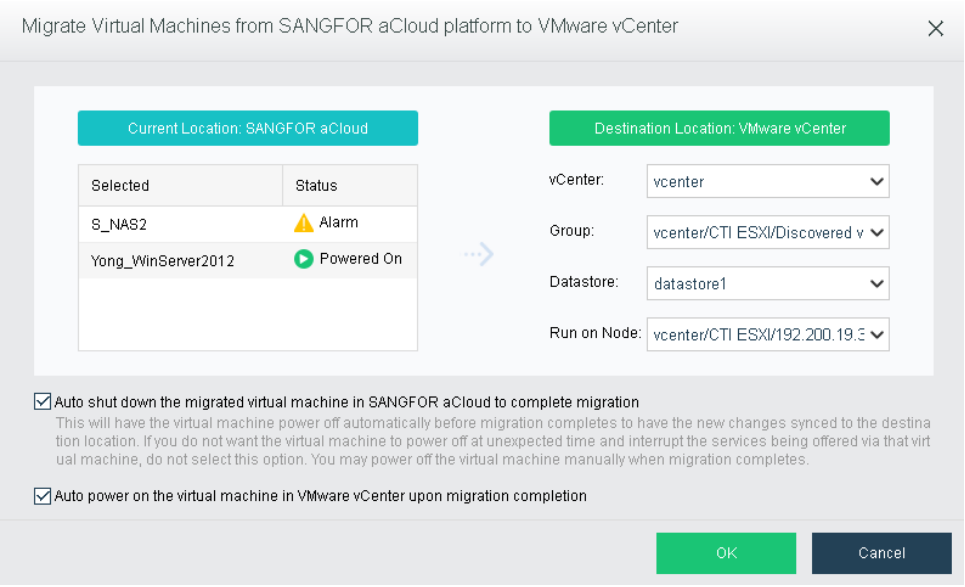
Migrate Across Cluster - To migrate the VM across cluster , choose one or more than one virtual machinese and select Migrate Across Cluster.



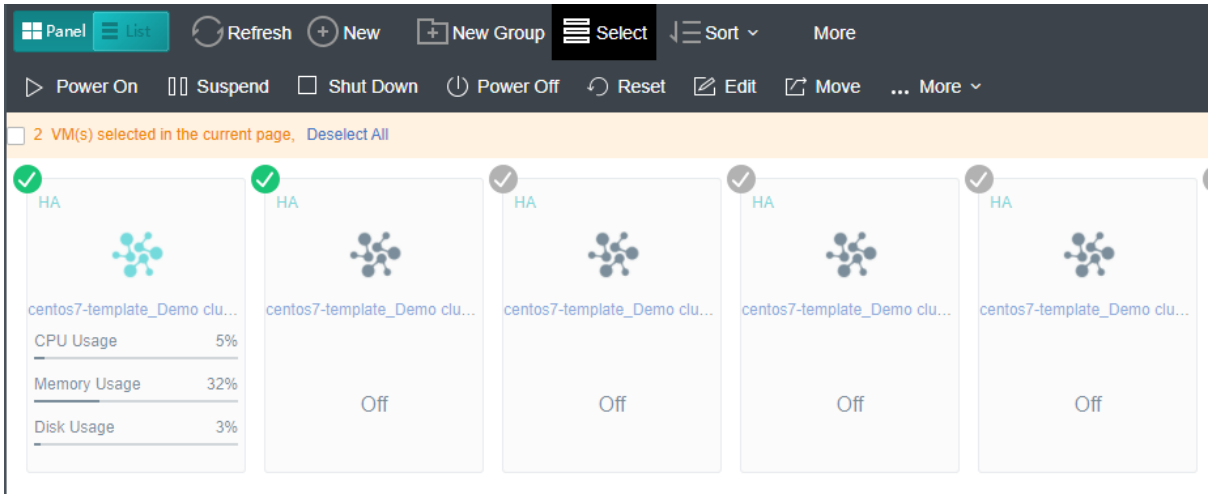




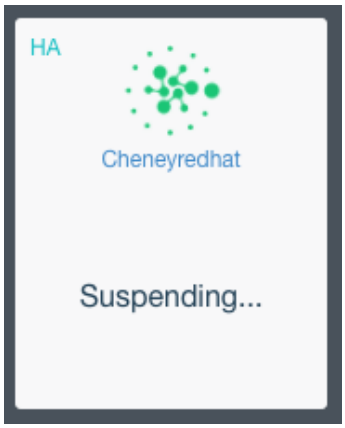
Migrate to VMware VCenter - To migrate the VM to VMware VCenter, choose one or more than one virtual machinese and select Migrate to Vmware VCenter.



If a virtual machine is chosen, the color of the icon at the upper left corner of the corresponding card will turn to green from gray.



If a virtual machine is being powered on, suspended or shut down, there will be the corresponding information displayed on the panel. For example, **Suspending**, as shown in the following figure, shows that the virtual machine is being suspended.



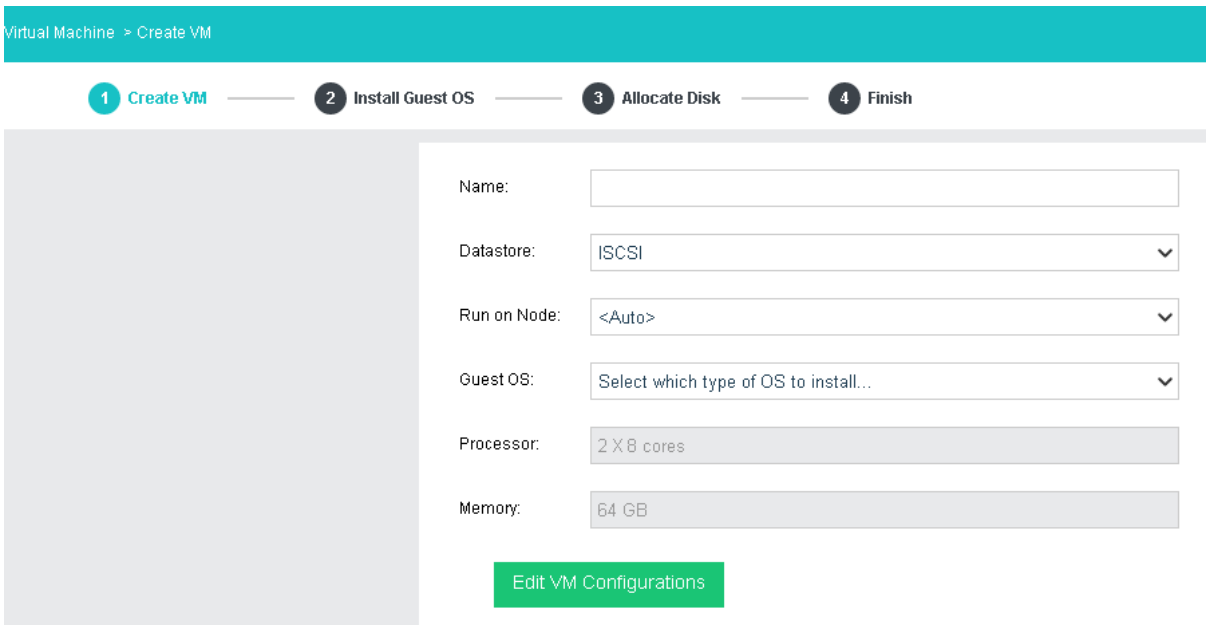
To exit from selecting the virtual machines, click on the **Exit** button on the upper right corner.

2.2.1.8 Deploying Oracle/SQL Server

2.2.1.8.1 Creating Standalone Oracle Database

To create a standalone Oracle database, follow the steps described below:

1. Go to **Compute,** click **New** and then select **Create Standalone Oracle Database** on the **Create New Virtual Machine** page.
2. Create virtual machine. For how to create a virtual machine, see the **2.2.1.2 Creating Virtual** Machine section.



Name: Specifies a distinguishable name for the virtual machine.

Datastore: Specifies a datastore to store virtual machine. HA is configurable only when a shared datastore is selected.

Run on Node: Specifies the node to run the virtual machine.

Guest OS: Specifies an operating system for the virtual machine. The following types of guest OSes are supported: Windows, Linux, Sangfor and others.

Processor: Specifies the number of virtual sockets and cores per socket for the virtual machine respectively.

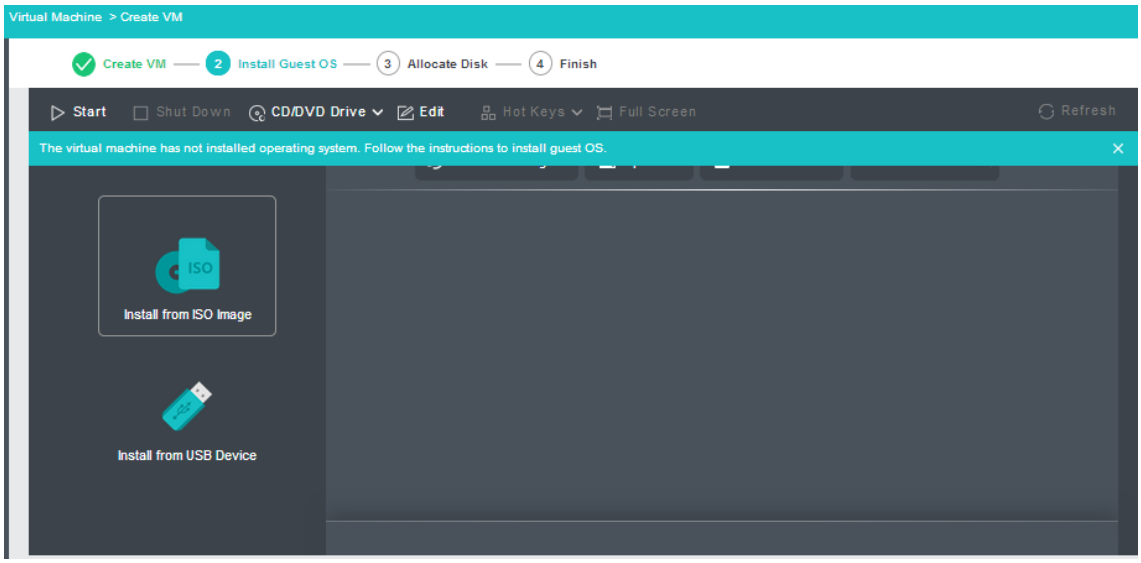
Memory: Specifies the memory size for the virtual machine. The minimum is 512 MB, and the maximum is 1TB.

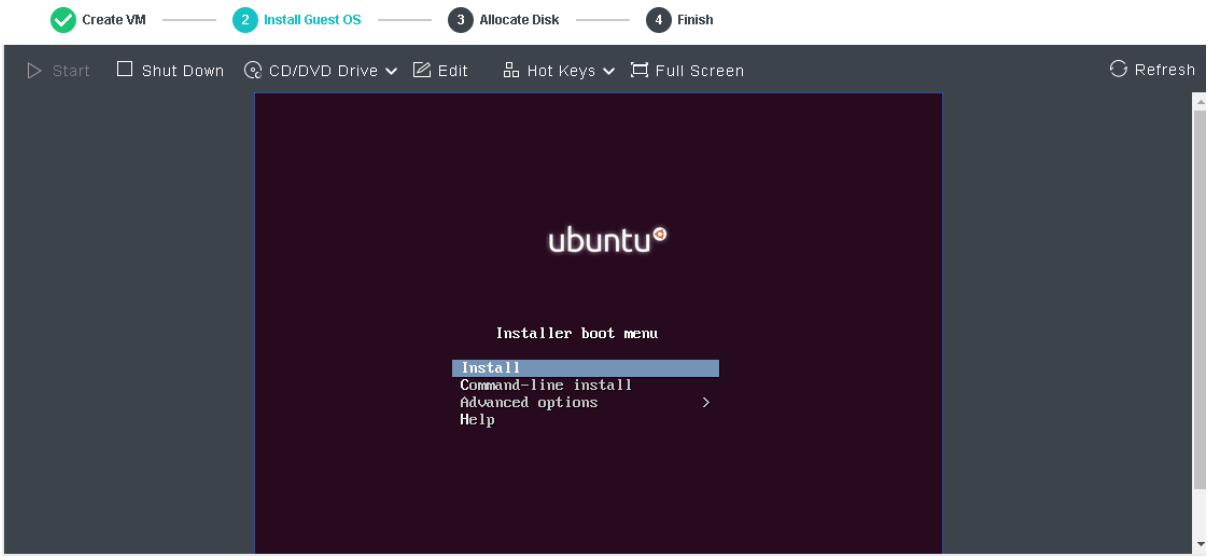
3. Install guest OS.

After VM name and guest OS are specified, click **Next** to install OS. If the image file of a

specified guest OS has not been uploaded to Sangfor HCI platform, you may upload it in the same way of uploading an ISO image introduced in the **2.2.1.2 Creating Virtual** Machine section.

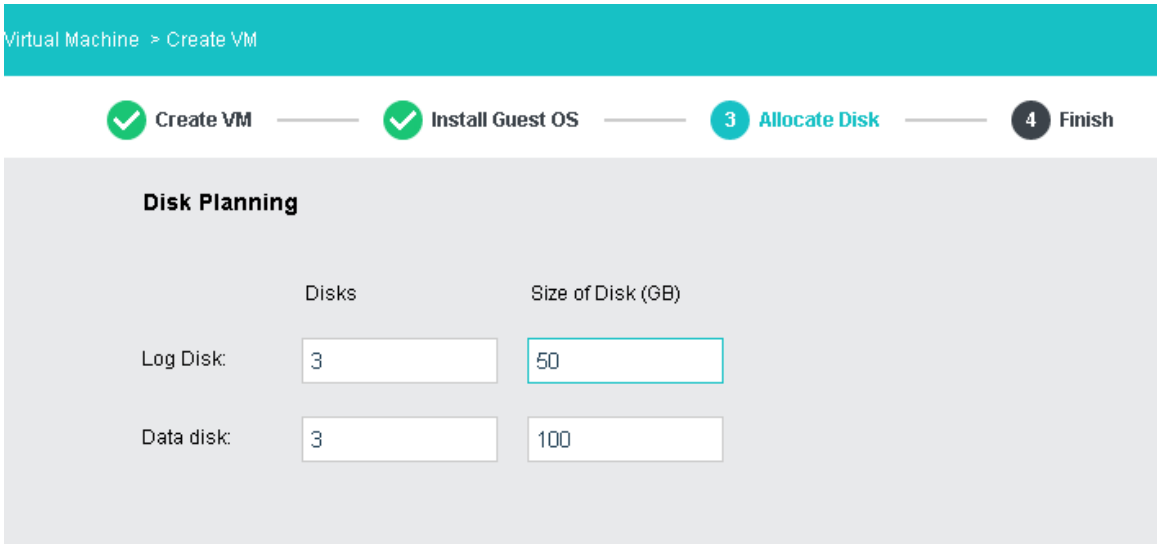
After guest OS is installed, vmTools must be installed before you go to next step.





4. Configure use of disk.

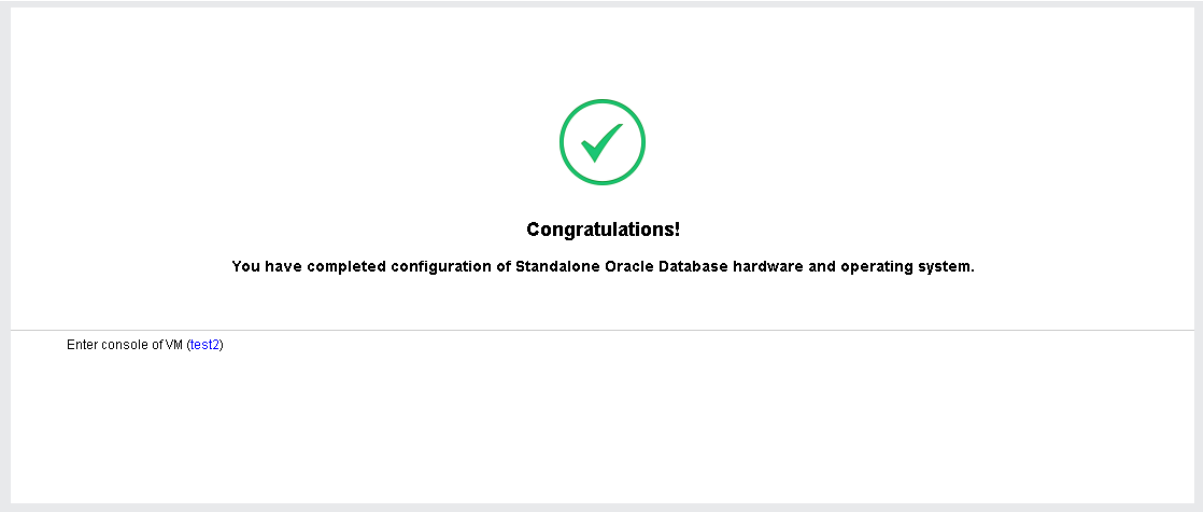
In this step, you need to configure log and quorum disks. More specifically, specify **Disk Name, Total Number, Size of Each Disk** on the following page.



Log Disk: It is used to store Oracle database logs.

Data Disk: It is used to store Oracle database data.

5. After you have configured standalone Oracle database, you may download deployment guide by clicking **Download Deployment Guide in the** following **figure**.



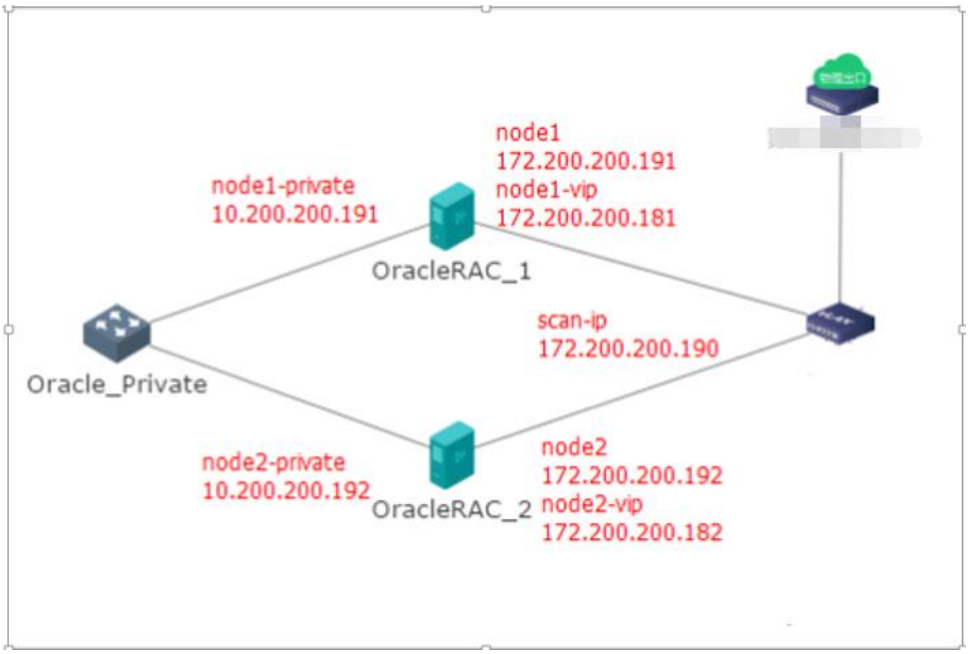
2.2.1.8.2 Creating Oracle RAC Database (cluster)

To create Oracle RAC database(cluster), follow the steps described below:

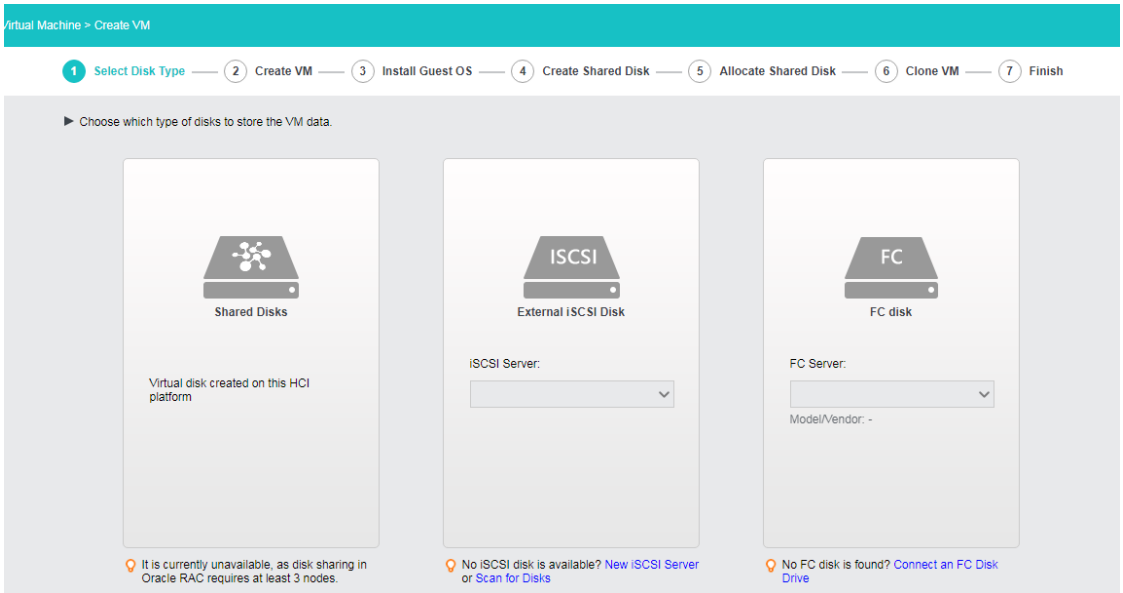
1. Go to **Compute,** click **New** and then select **Create Oracle RAC Database** on the **Create New Virtual Machine** page.

2. Select disk type.

Each node in Oracle RAC needs to be configured a public IP address, a virtual IP address and a private IP address at least, and a cluster has a public IP address. Address allocation and network deployment is shown below:



First, select a type of disk to store VM data: Shared **Disks, External iSCSI Disk, FC Disk**.



3. Create virtual machine.

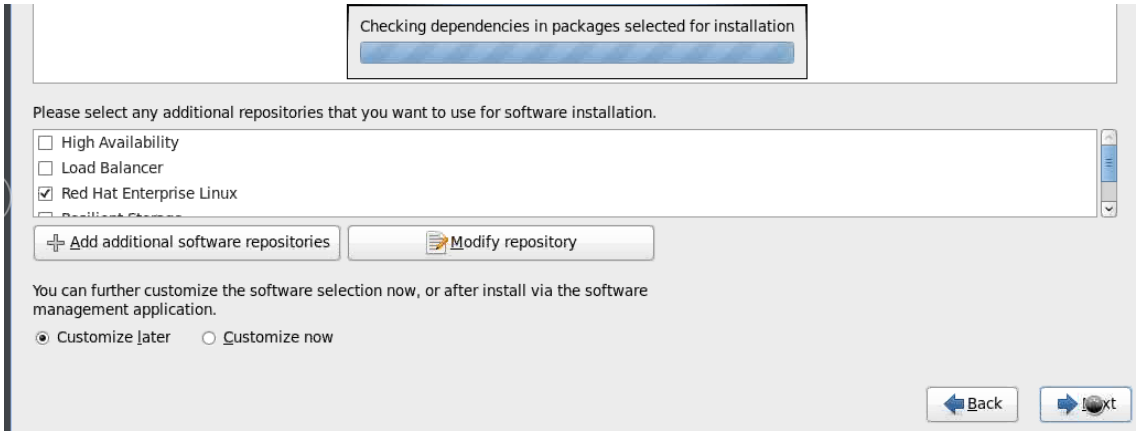
See the **2.2.1.2 Creating Virtual** Machine section for how to configure virtual machine. Note that datastore must correspond to the type of disk you have chosen in the previous

step.

4. Install guest OS.

   After VM name and guest OS are specified, click **Next** to install OS. If the image file of a specified guest OS has not been uploaded to Sangfor HCI platform, you may upload it in the same way of uploading an ISO image introduced in the **2.2.1.2 Creating Virtual** Machine section.

After guest OS is installed, vmTools must be installed before you go to next step.



5. Create shared disk.

   In this step, you need to configure log, quorum and data disks. More specifically, specify **Disk Name, Total Number, Size of Each Disk**.

   Log Disk: It is used to store Oracle database logs.

   Data Disk: It is used to store Oracle database data.

   Quorum Disk: It is used to provide quorum service.

6. Allocate shared disks.

   After shared disks are configured, you may allocate them.

7. Clone virtual machine.

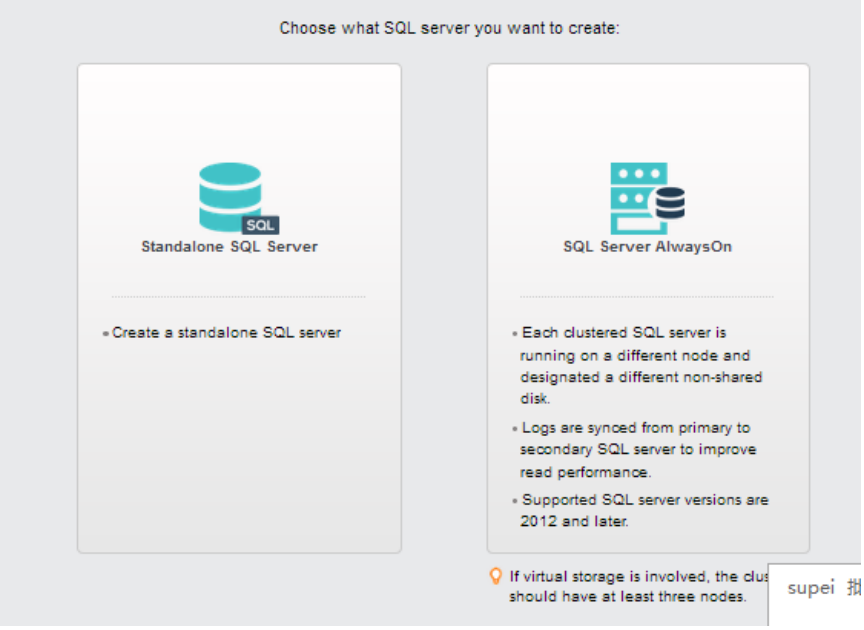
   Here, you may specify VM name, description and the number of virtual machines to be created.

8. Click **OK** to save the settings.

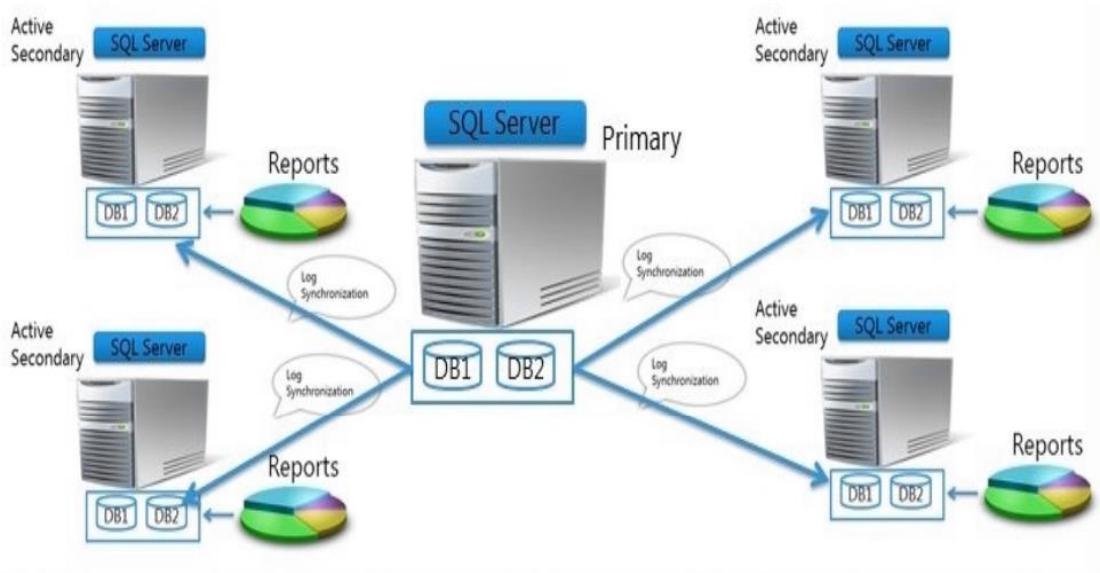
Creating SQL Server

To create SQL server, do as follows:

1. Select **SQL Server AlwaysOn**, as shown below:



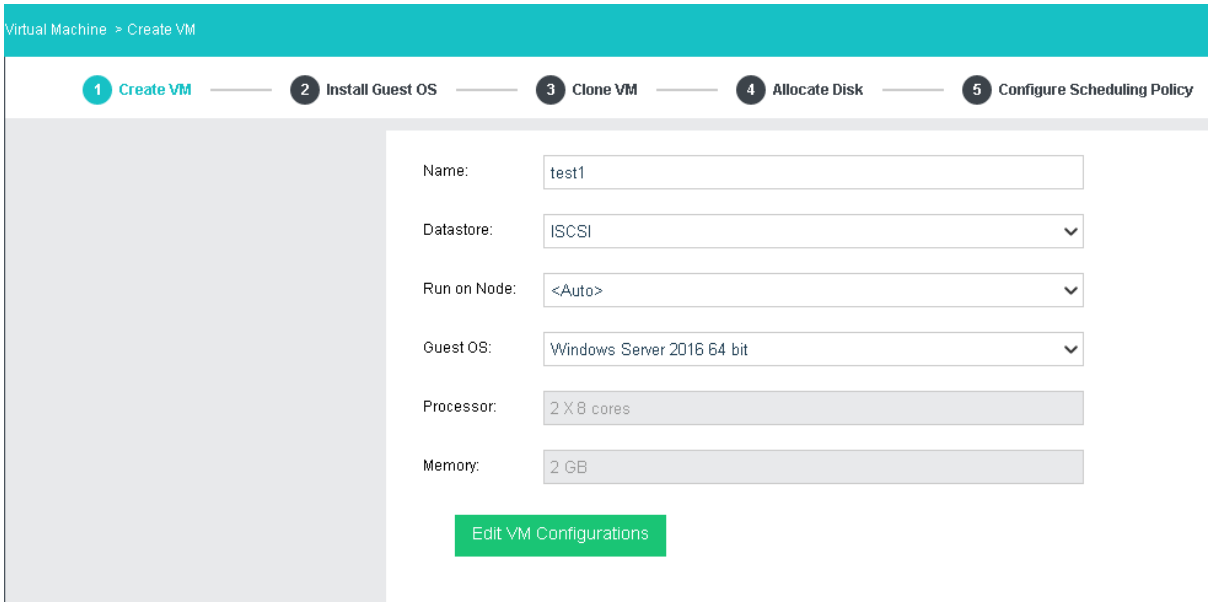
2. Select disk type.



On the two nodes in an AlwaysOn availability group that host two SQL servers, the network adapter name and use should be the same. For example, both the etho ports on the two nodes are business interfaces and both the eth1 ports are heartbeat interfaces.

3. Create virtual machine

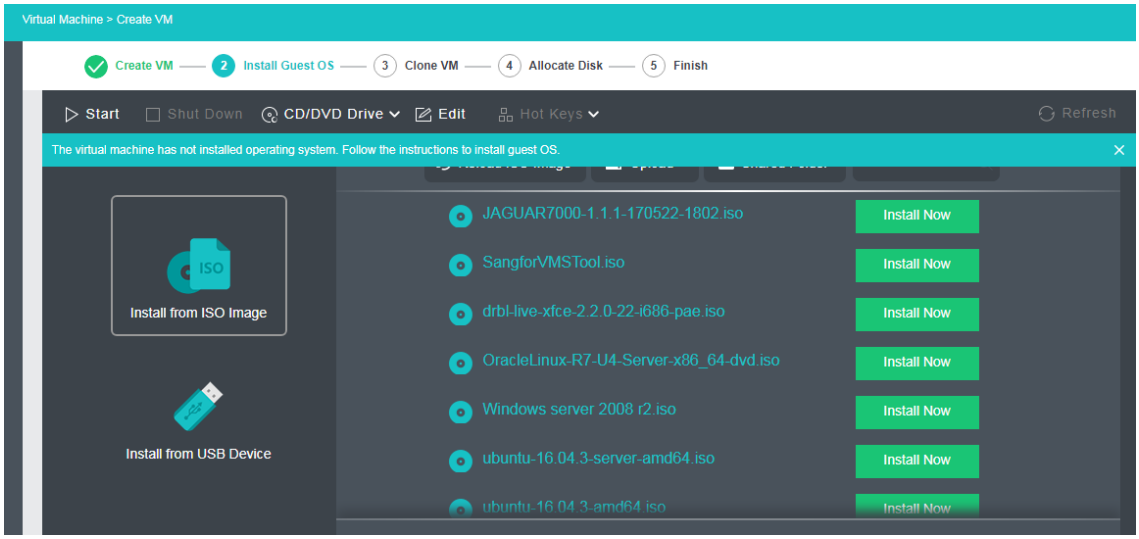
See **2.2.1.2 Creating Virtual** Machine section for how to configure virtual machine.



4. Install guest OS.

After VM name and guest OS are specified, click **Next** to install OS. If the image file of a specified guest OS has not been uploaded to Sangfor HCI platform, you may upload it in the same way of uploading an ISO image introduced in the **Creating Virtual Machine** section.

After guest OS is installed, vmTools must be installed before you go to next step.



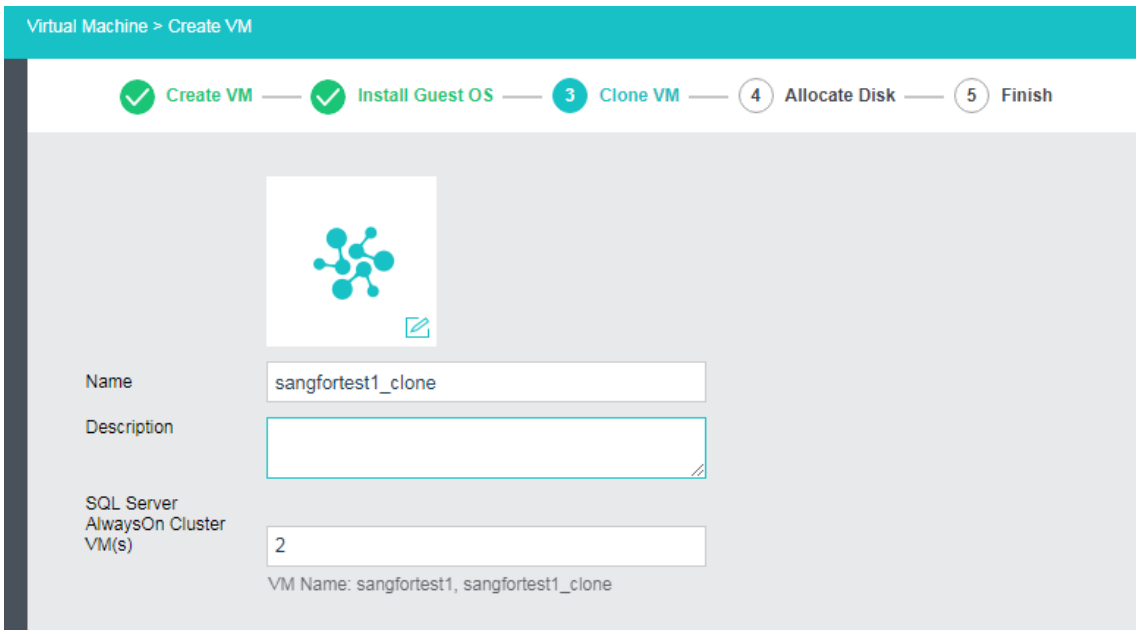
- After guest OS is installed, firewall must be disabled.
- As for database, SQL Server 2012 Enterprise SP1 is recommended(SQL Server 2012 and

later versions are also supported). As for operating system, Windows Server 2012 R2 Datacenter is recommended(Windows Server 2008 R2 and later versions are also supported).

5. Clone virtual machine.

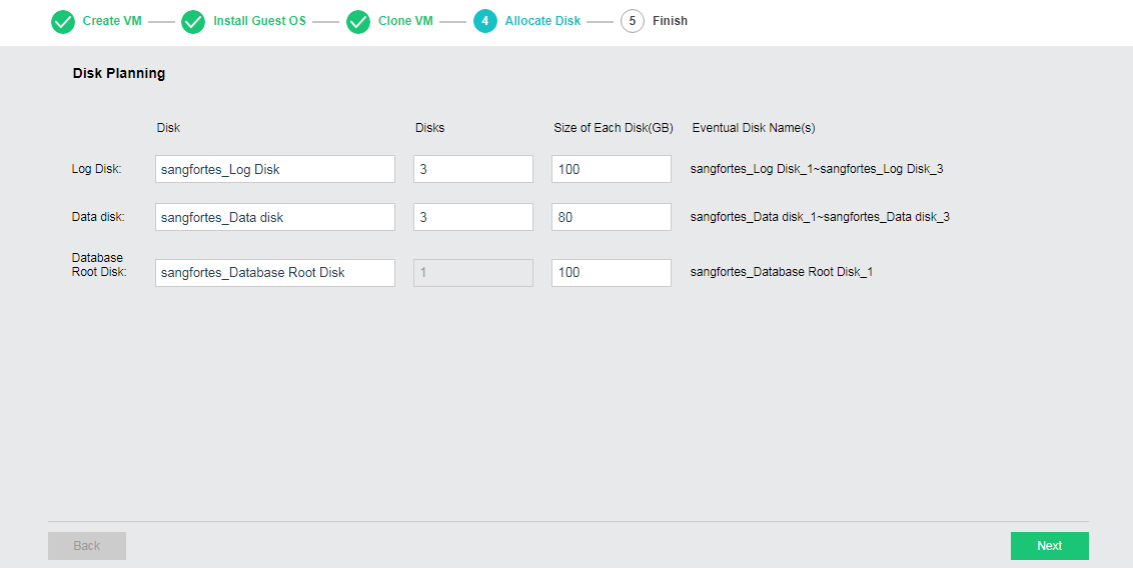
After one SQL server AlwaysOn virtual machine is created, you may create other virtual machines by cloning the previous one so as to enhance deployment efficiency and to ensure that the configurations of all SQL server AlwaysOn virtual machines are exactly the same.

As for number of cloned SQL Server AlwaysOn nodes, enter the number directly. For example, to create two SQL server AlwaysOn virtual machines, enter 2.



6. Allocate disks.

Allocate disks by specifying number of log disks, data disks and database root disks and size of.each disk respectively.



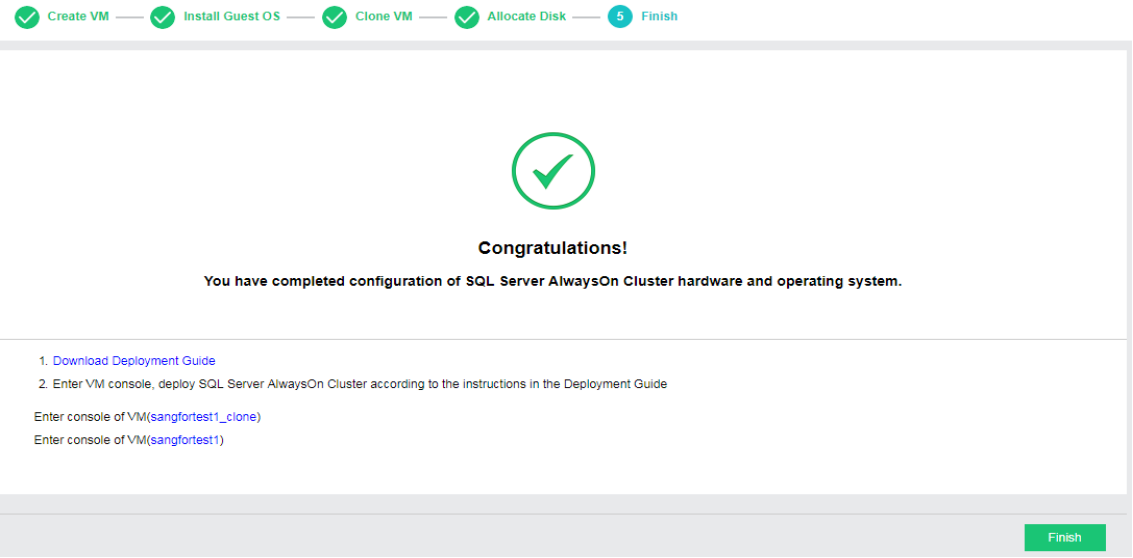
Log Disk: It is used to store log files of SQL server.

Data Disk: It is used to store data of SQL server.

Quorum Disk: It is used to store logs and data files of system database tempdb.

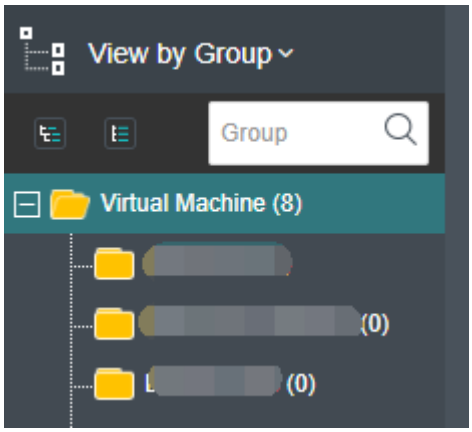
7. Click **OK** to save the settings.

After configuration, you may download deployment guide by clicking **Download Deployment Guide**.

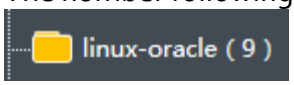


2.2.1.9 Viewing VM Groups

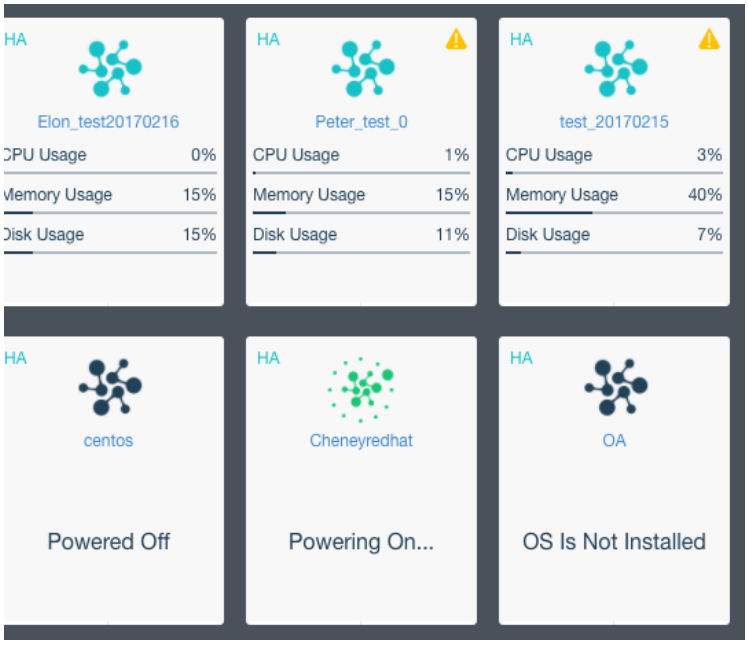
In **Compute**, all VM groups can be expanded or collapsed by clicking on the button. To expand or collapse a specific group, click on the & button next to that group.



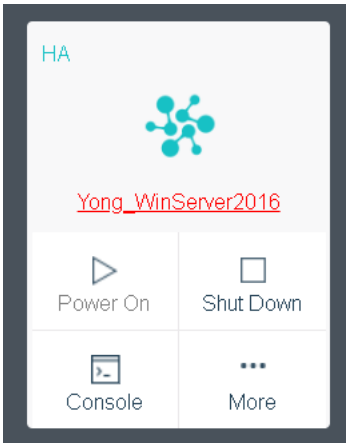
The number following a group name indicates the number of virtual machines in that group.



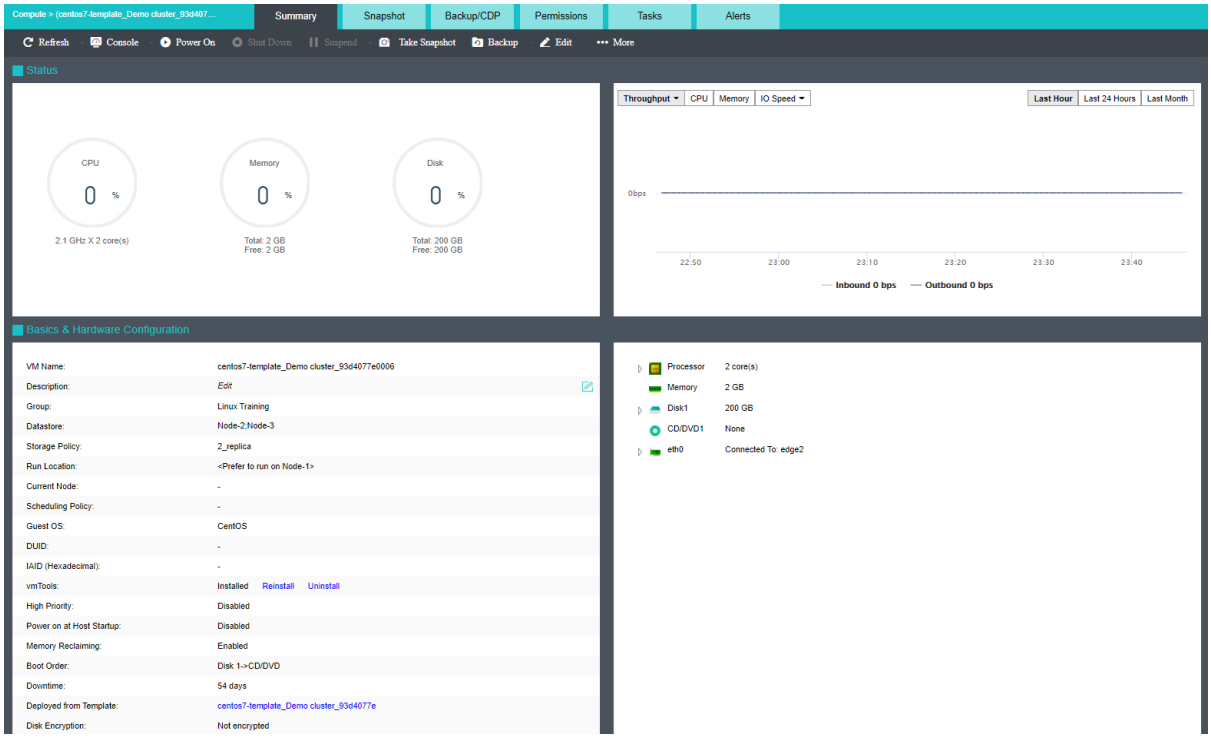
You can get the following information on virtual machine panel: power status(powered on or powered off), CPU, memory and disk usage. Blue VM icon indicates virtual machine is powered on, while gray VM icon indicates virtual machine is powered off.



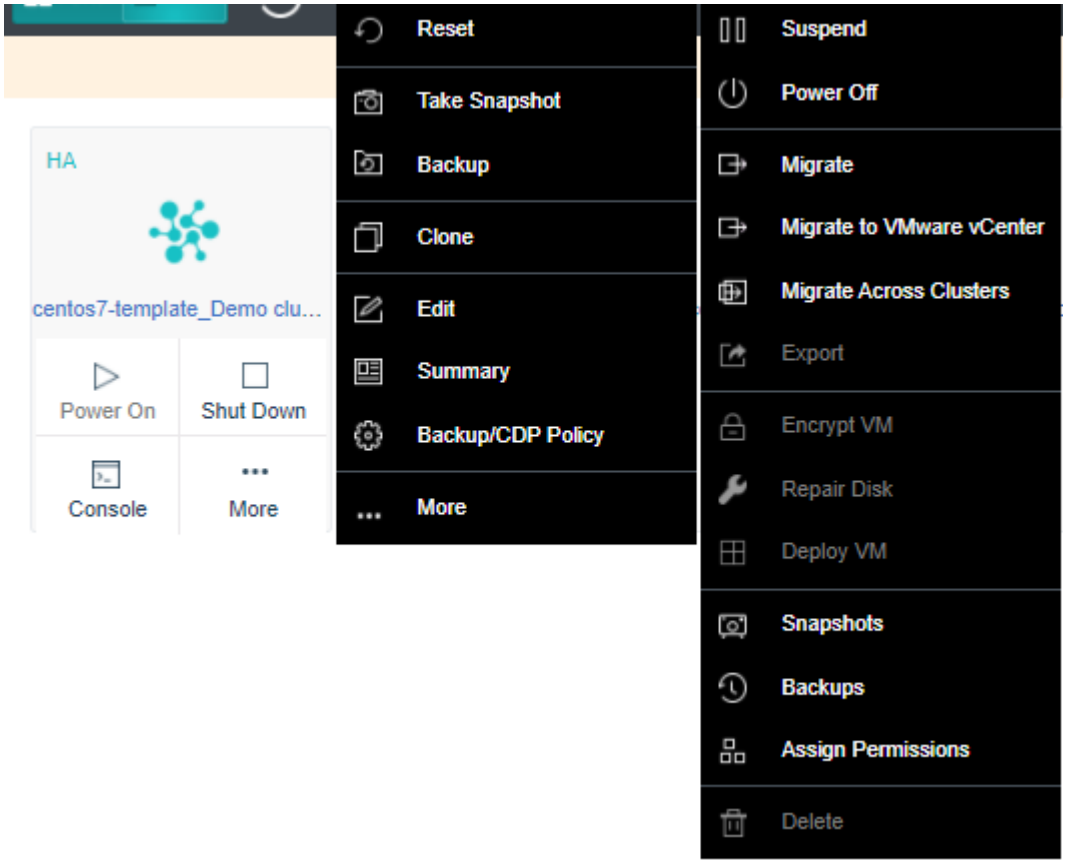
Move the cursor onto VM card and the following buttons will appear on that card, as shown in the following figure:



For virtual machine details, you may click on VM name to redirect to the **Summary** page, as shown below:



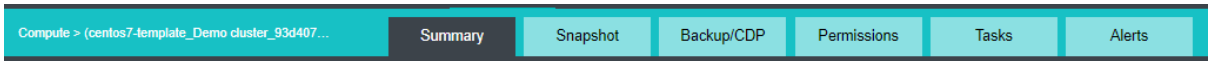
To perform more operations against virtual machine, click **More,** as shown below:



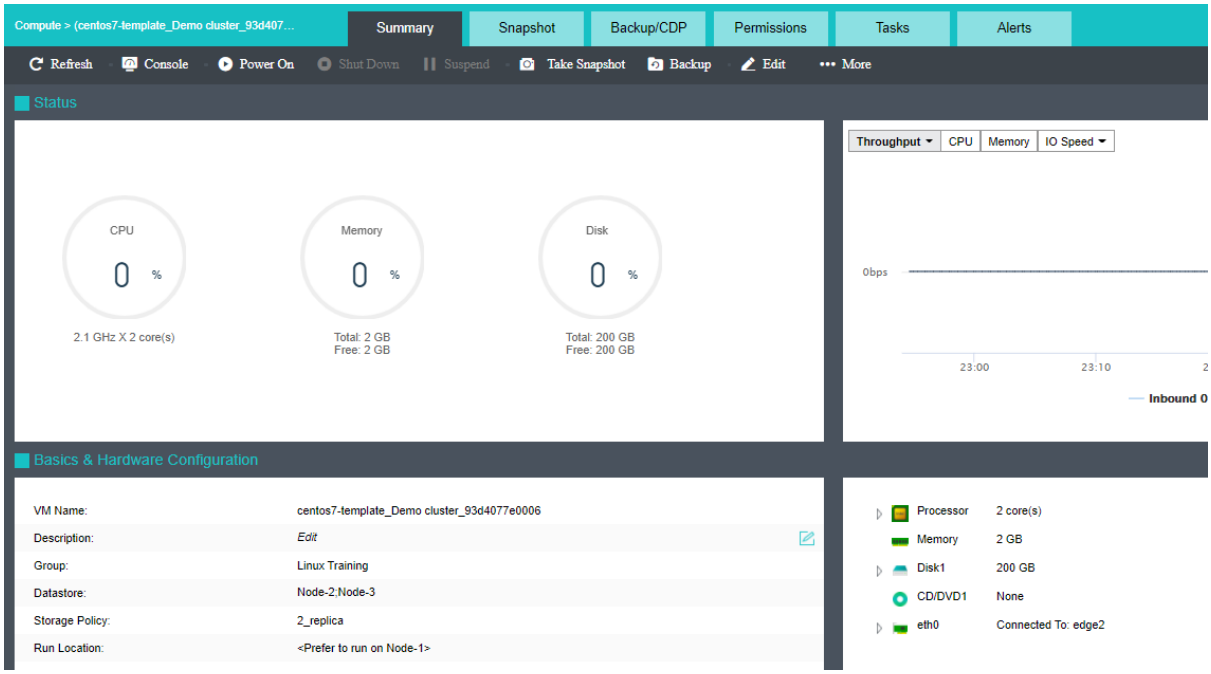
If VMware vCenter is not added to Sangfor HCI platform, the option Migrate to VMware vCenter will not be displayed.

2.2.1.10 Viewing VM Details

There are the following tabs: **Summary, Snapshot, Backup/CDP, Permissions, Tasks** and **Alarms,** as shown below.

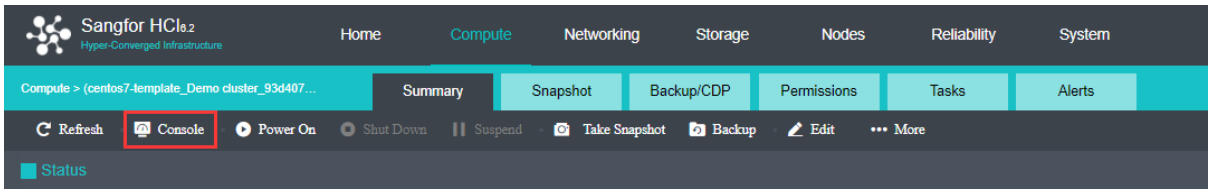


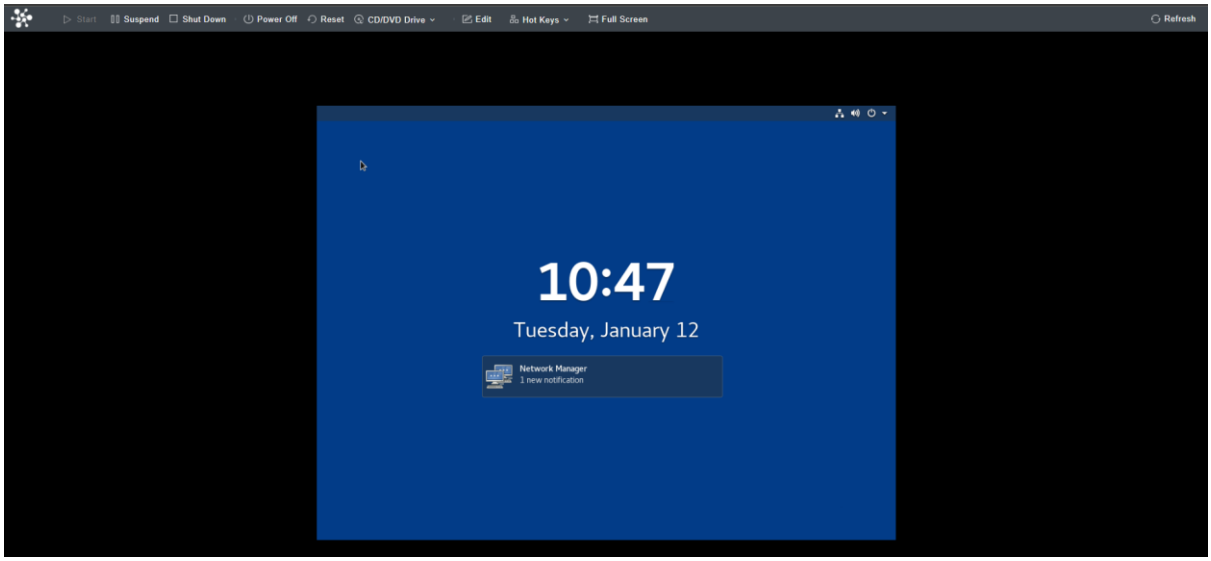
On the **Summary** tab, you may perform such operations as **Power On, Shut Down,** etc., and view basic information and hardware configurations of virtual machine.



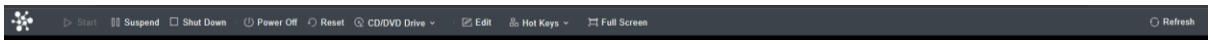
To refresh the **Summary** page, click on **Refresh** on the upper left corner.

To open virtual machine's console, click **Console** on the **Summary** page, or click on the **Console** button on the virtual machine panel to enter the following page.

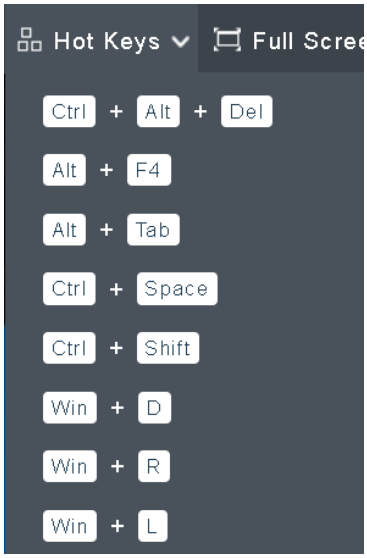




On the above page, you can perform the **following** operations: **Start, Suspend, Shut Down, Power Off, Reset, CD/DVD Drive, Edit, Hot Keys, Full Screen, Refresh**.



Hot keys lists combinations of commonly-used keys.



Full Screen to have console of the virtual machine displayed in full screen, click **Full Screen**. To exit from **full** screen, you may click **Exit**.

If the console encounters error, you may click **Refresh**.

To power on virtual machine, you may click **Power On**.

To shut down virtual machine, you may click **Shut Down**.

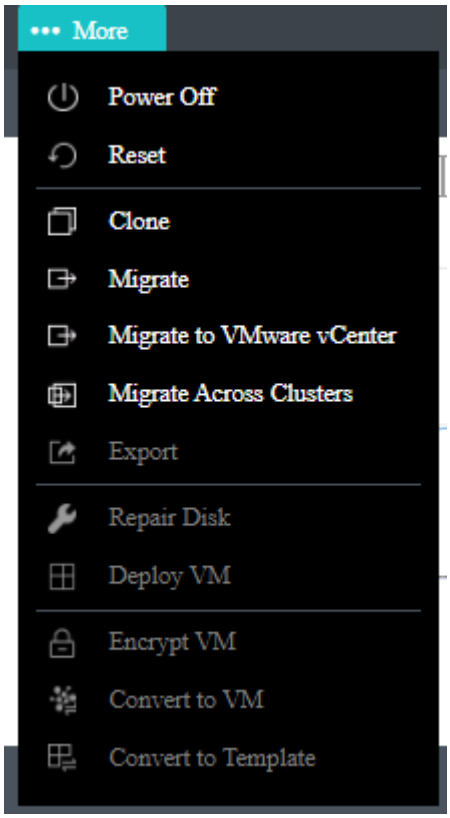
To suspend virtual machine, you may click **Suspend**.

To take snapshot of virtual machine, you may click **Take Snapshot**.

To back up virtual machine, you may click **Backup**.

To edit virtual machine, you may click **Edit.**

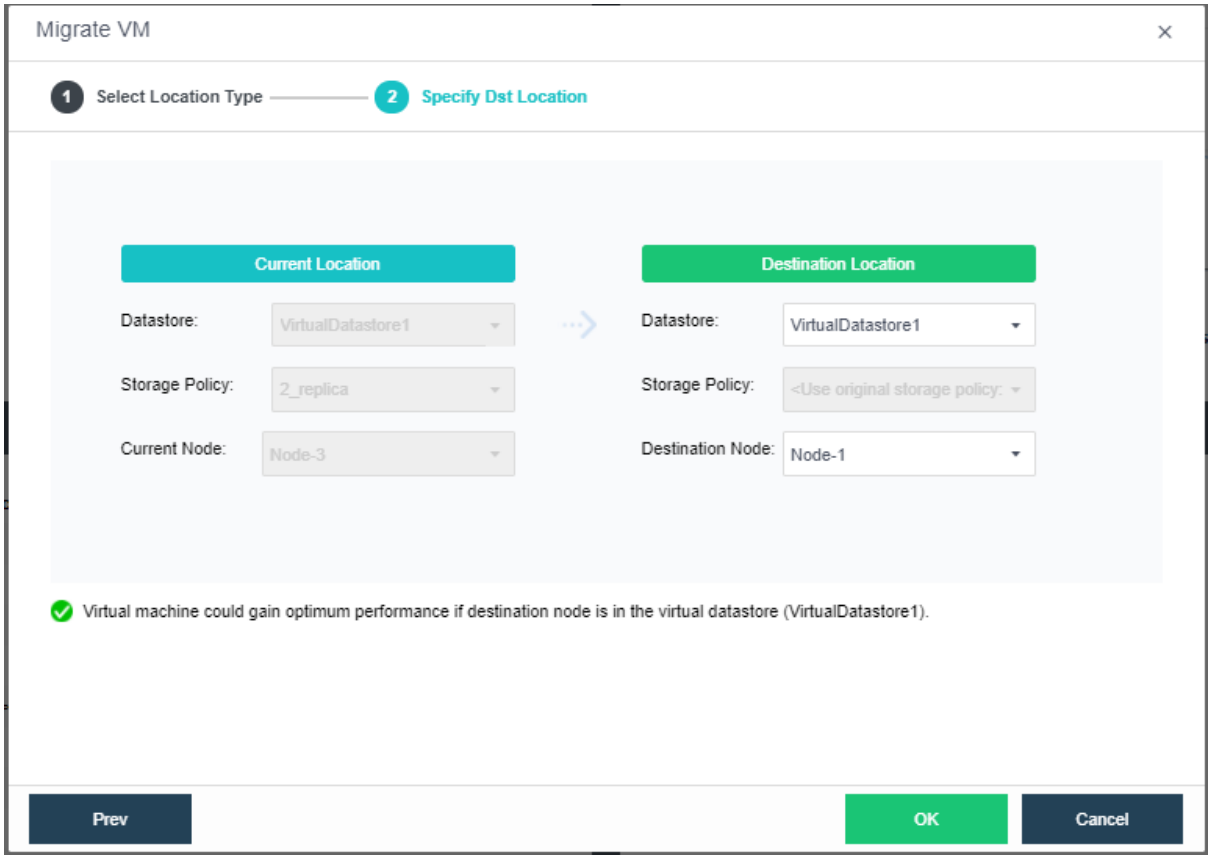
On the **Summary** page, you may perform the following operations by clicking **More**: **Power Off**, **Reset**, **Clone**, **Migrate**, **Migrate to VMware vCenter**, **Migrate Across Clusters**, **Export**, **Repair Disk**, **Deploy VM**, **Convert to VM**, **Convert to template**, as shown below:



If VMware vCenter is not added to Sangfor HCI platform, the option Migrate to VMware vCenter will not be displayed.

2.2.1.11 Migrating VM

A virtual machine can be migrated to another node or another datastore.



Current Location: Displays the current datastore and node of the virtual machine.

Datastore: Indicates the datastore where virtual machines is stored.

Storage Policy: Indicates the number of replication.

Current Node: Indicates the node where virtual machine resides.

Destination Location: Displays the destination datastore and node.

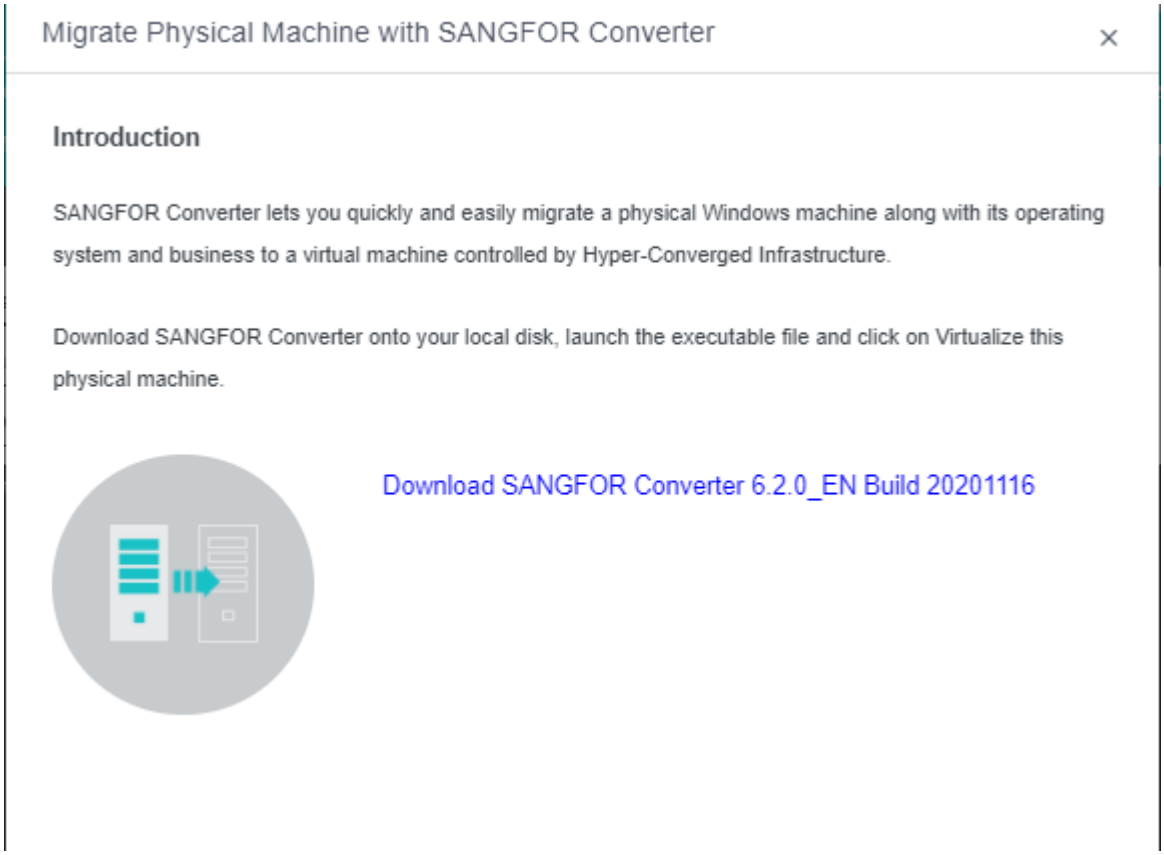
Destination Node: Indicates the node where virtual machine resides.

Datastore: Indicates the destination datastore. For virtual machines that have been mounted any physical disk, migration to another datastore is not allowed before the physical disk is removed.

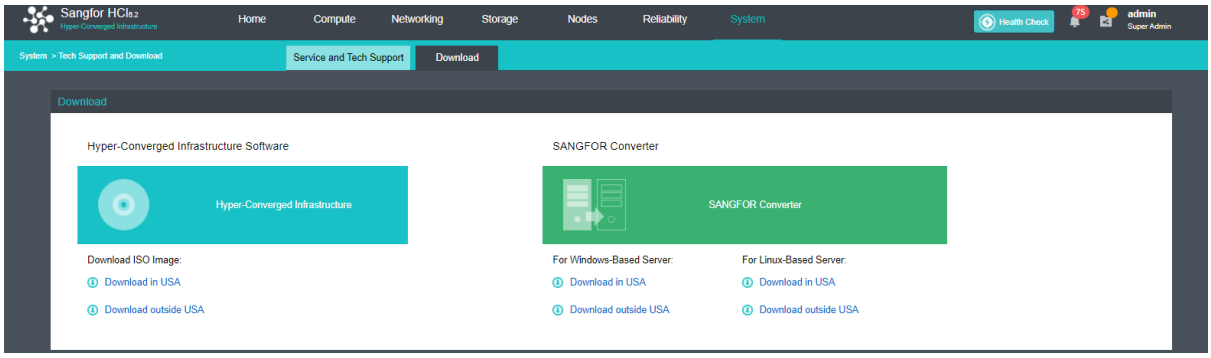
Which destination datastore can be chosen depends on destination node. If the destination node is **Auto**, destination datastore can only be a shared datastore. If the destination node is specified, destination datastore can only be a local disk on that node, or a shared datastore.

2.2.1.11.1 Migrating Physical Machine

Sangfor Converter is designed for easy and quick migration of physical machines along with their operating systems and business to virtual machines managed by Sangfor HCI platform.



To download Sangfor converter, click **Download Sangfor Converter** and you will be redirected to the following page:



Requirements for physical servers:

CPU: 64bits

Memory: >=2GB

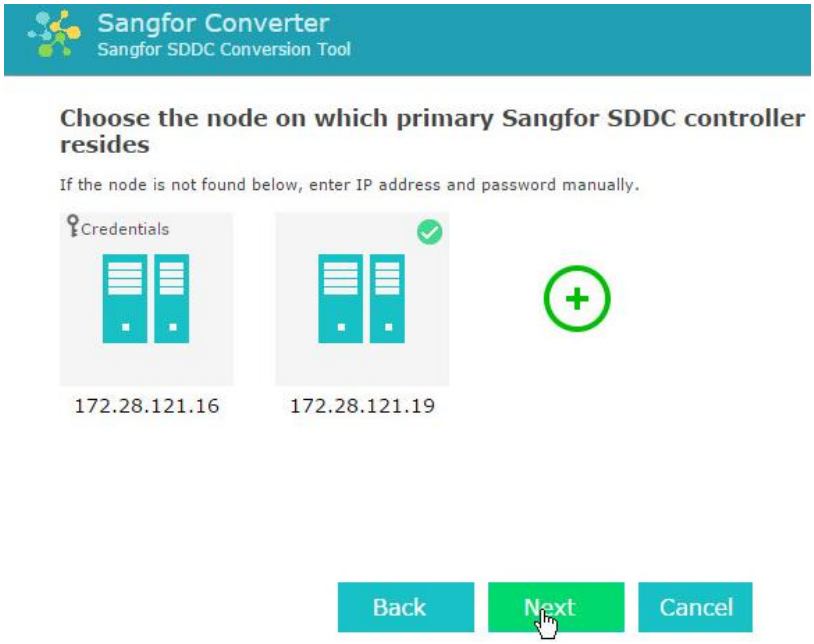
Disk: All supported except for dynamic disks

NICs: >=1

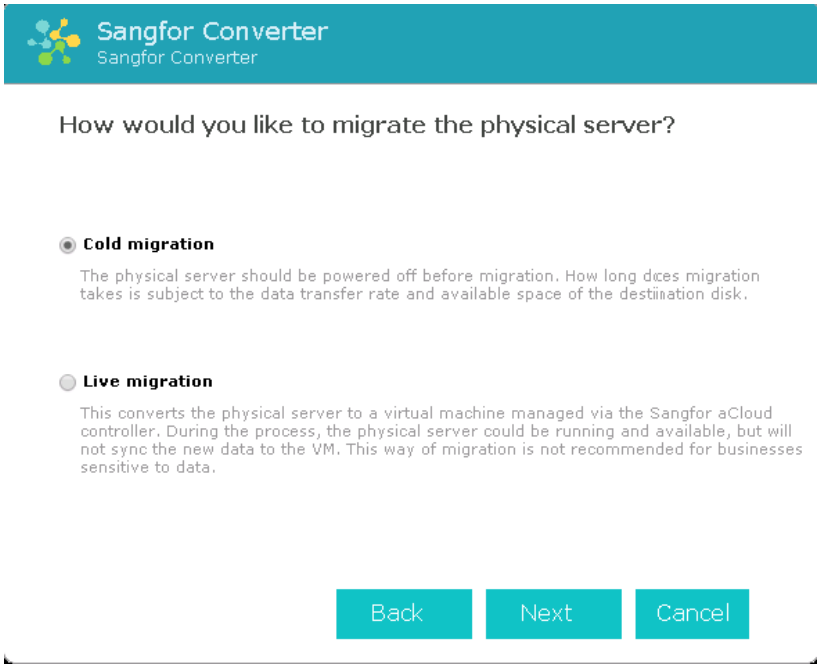
OS: 32-bit or 64-bit Windows XP/7/2003/2008/2012, Linux (Kernel version 2.6.18 and later)

2.2.1.11.1.1 Converting Windows-based Server to VM

Download and install Sangfor Converter on Windows system, and then launch it. Select **Virtualize this physical machine** and click **Start Now**.

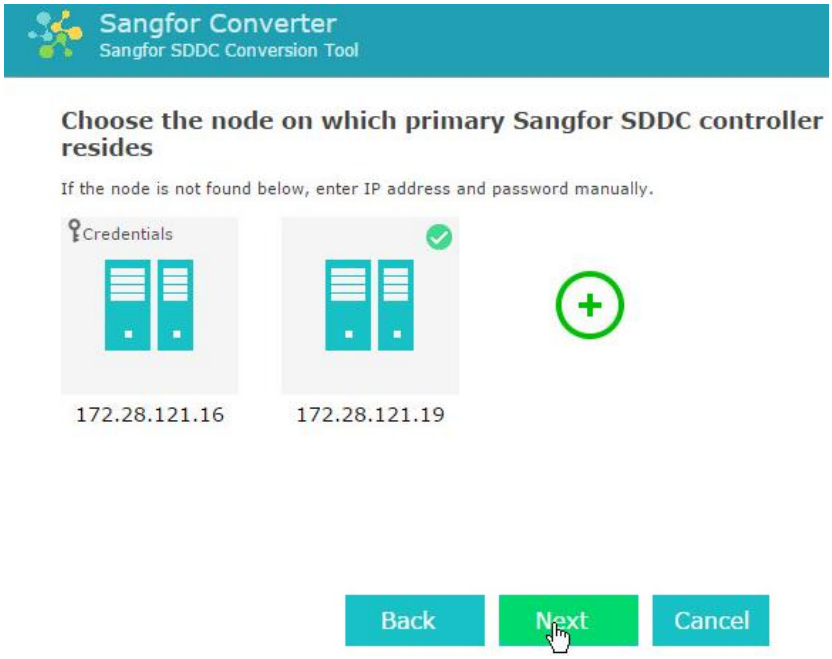


On the following page, select **Cold migration** or **Live migration**,

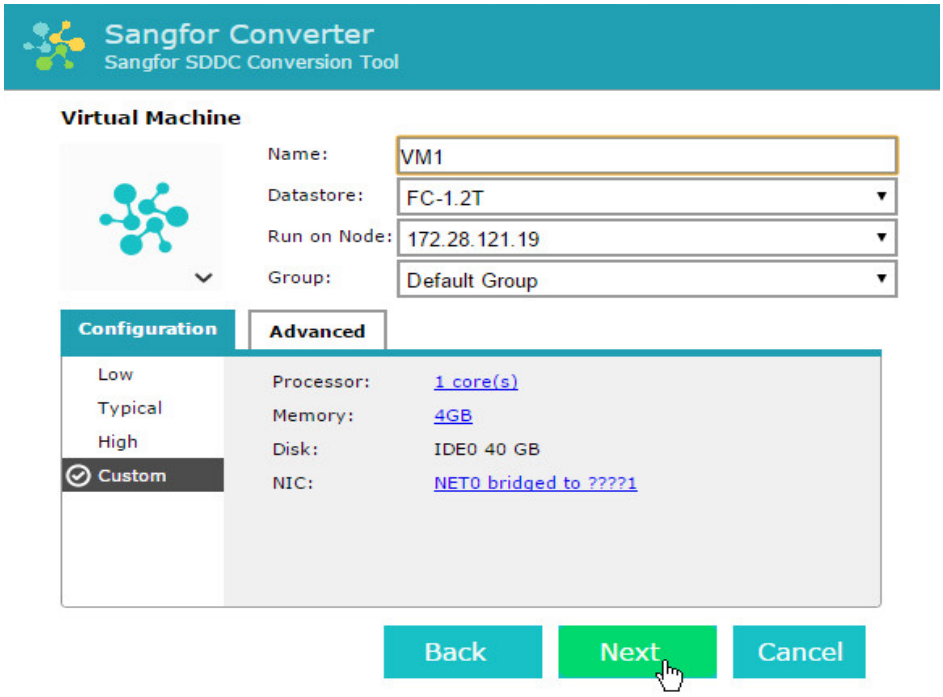


Select a target node. Target nodes on a same subnet as the physical server to be migrated will be discovered automatically, To migrate physical server to a node which resides on a different subnet, you need to add that node first by clicking 『+』 and entering username and password.

The target node must be reachable from the physical server to be migrated. If there is a firewall appliance between them,access to that target node from that physical server must be allowed. Only the cluster controllers residing on a same subnet as a physical server to be migrated will be discovered.



Configure the virtual machine to which the physical machine is converted, as shown below:

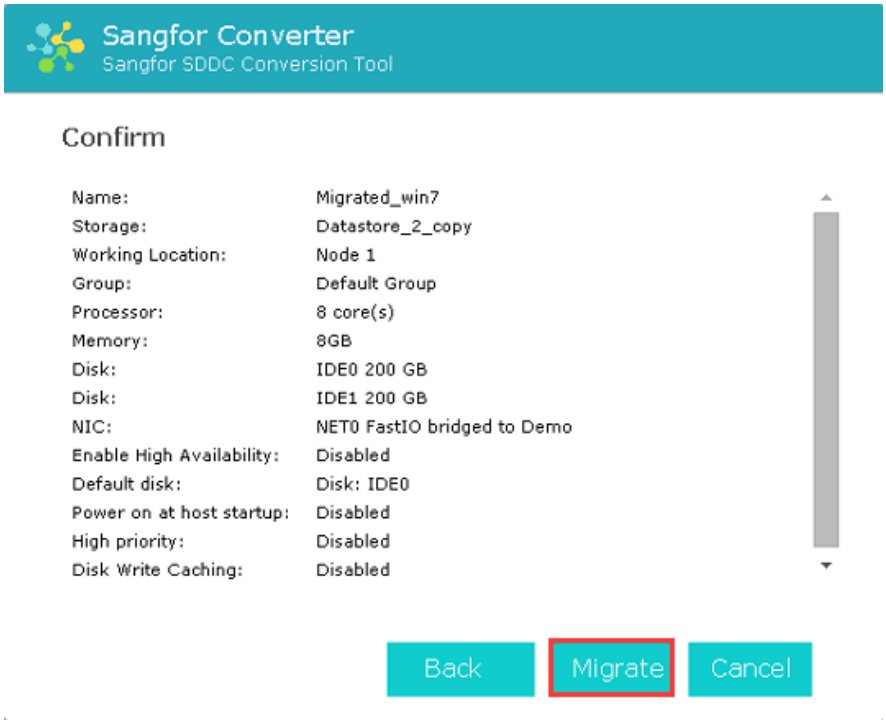


Configure processor and memory according to the need for your business system.

Disk cannot be configured. System will assign disks and disk size according to business system.

You can add or delete NIC according to the need for your business system, and select a virtual switch to connect.

After the virtual machine is configured, you will enter the following page to confirm configurations. Then, click **Install**.

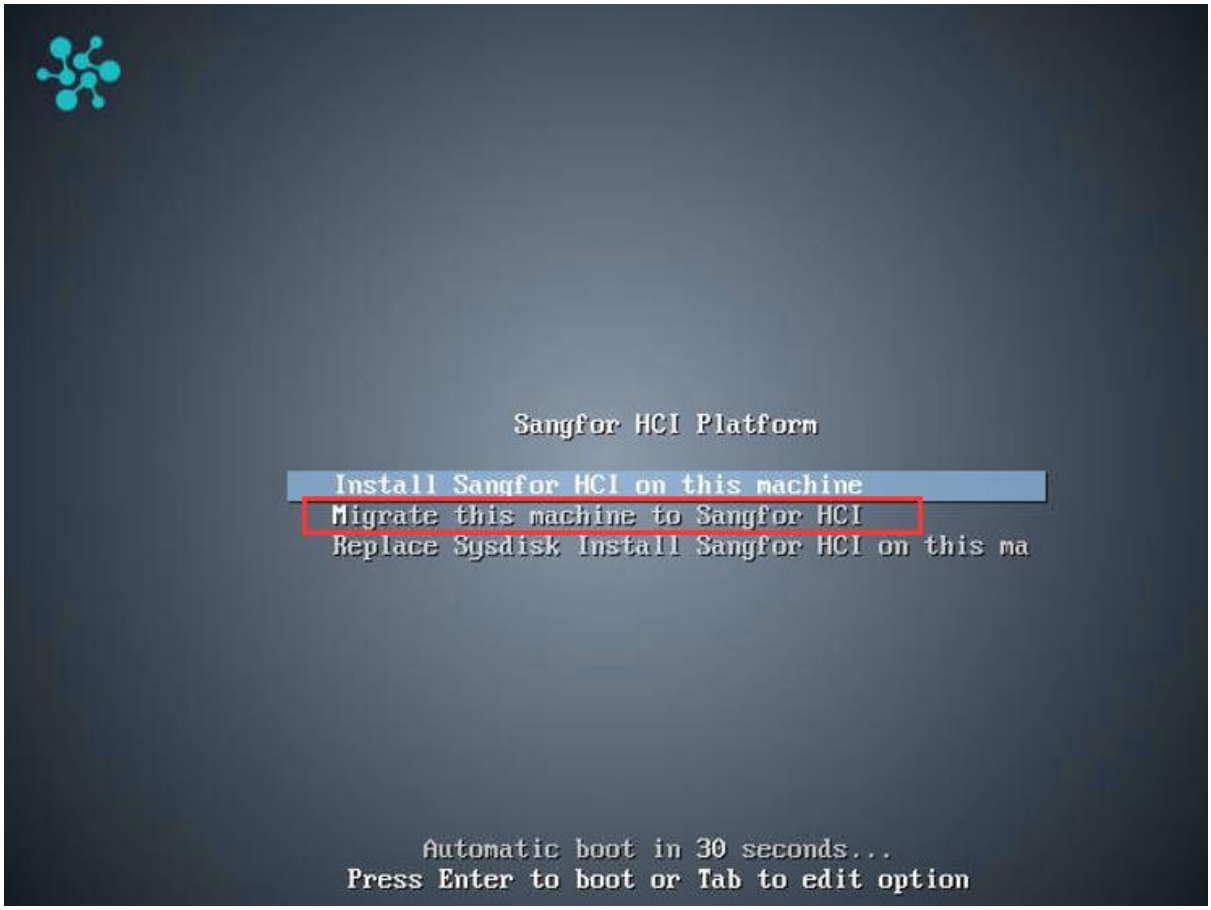


After installation of Sangfor Converter completes, you need to select an operation which will be performed upon migration completion. To see the migration process, log in to Web admin console of Sangfor HCI platform.

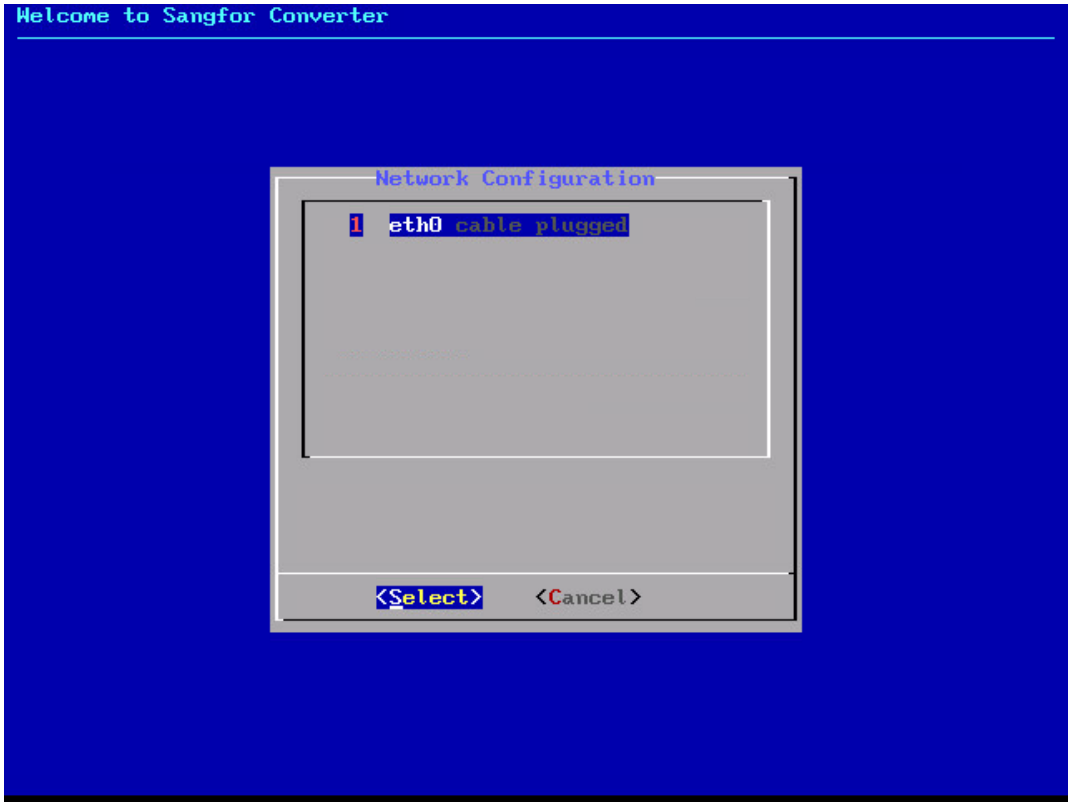
- Make sure that only one of the physical server and virtual machine is powered on and NCI address of that virtual machine is modified after migration is successful.
- Intermittent lose of network connection during migration is allowed, but not supported if the corresponding program on client and server side is closed.
- If migration fails due to uncertain factors(e.g,, power outage, etc.), physical server being migrated can go back to its operating system by restarting it.

2.2.1.11.1.2 Converting Linux-based Server to VM

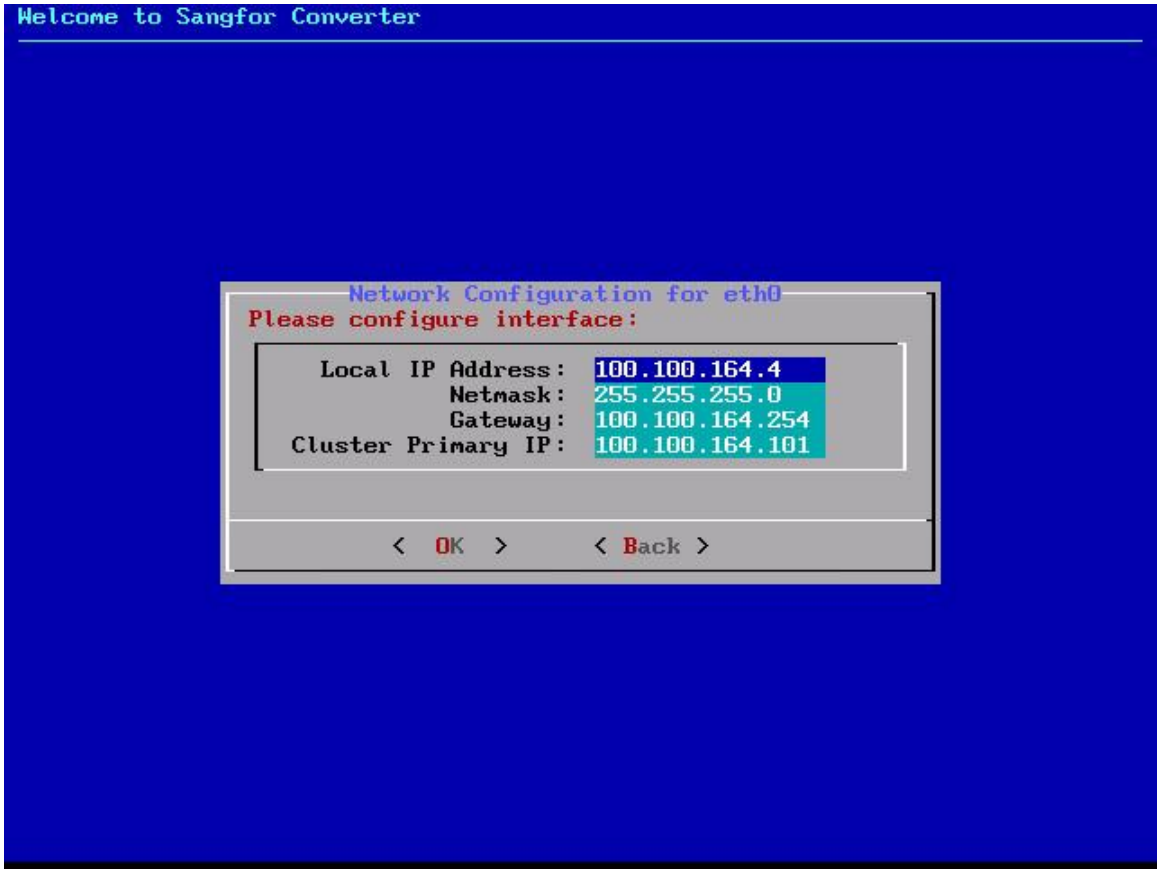
Insert the USB drive that Sangfor HCI software image file is written to, into a physical server running Linux, boot the system from that USB drive, and select **Migrate physical server to VM with P2V**.



Network configuration is required before performing migration. Select a physical network adapter for the current node, for the purpose of communication with the destination node.

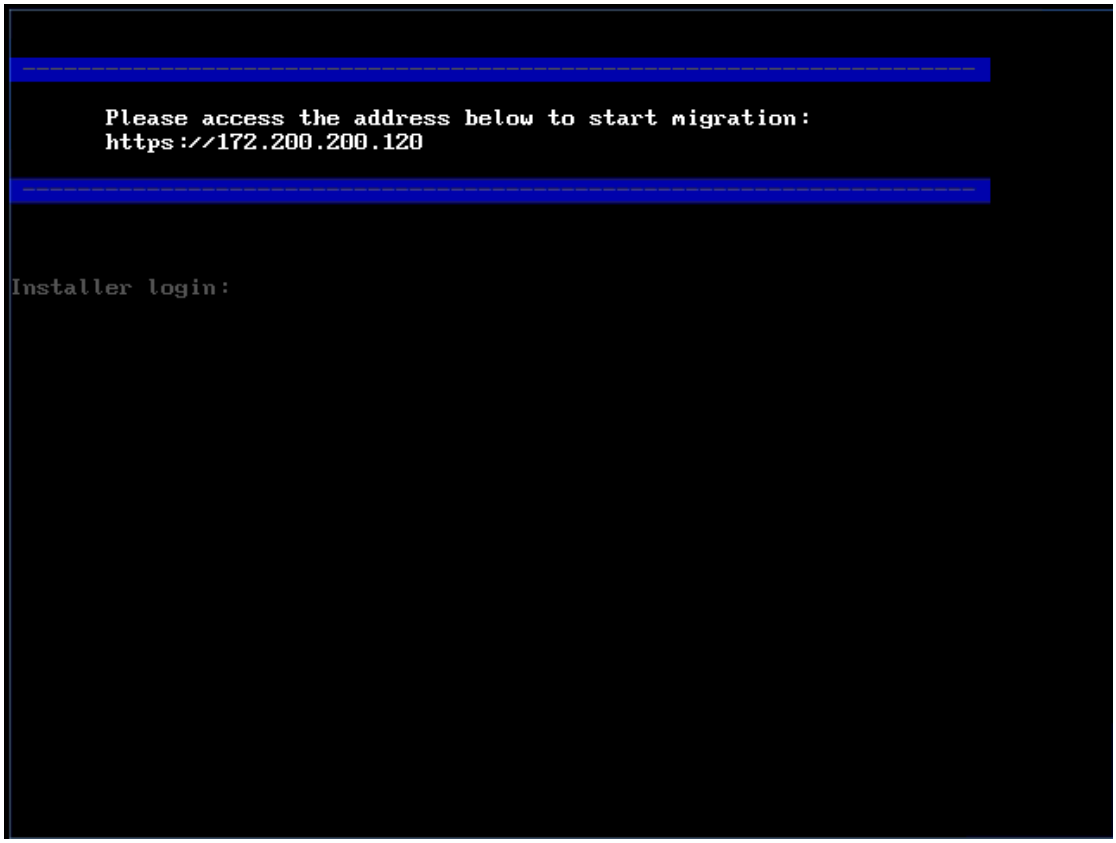


Configure an available local IP address, netmask and gateway for the physical network adapter, and enter IP address of the destination node. Make sure the server to be migrated can access that destination node.

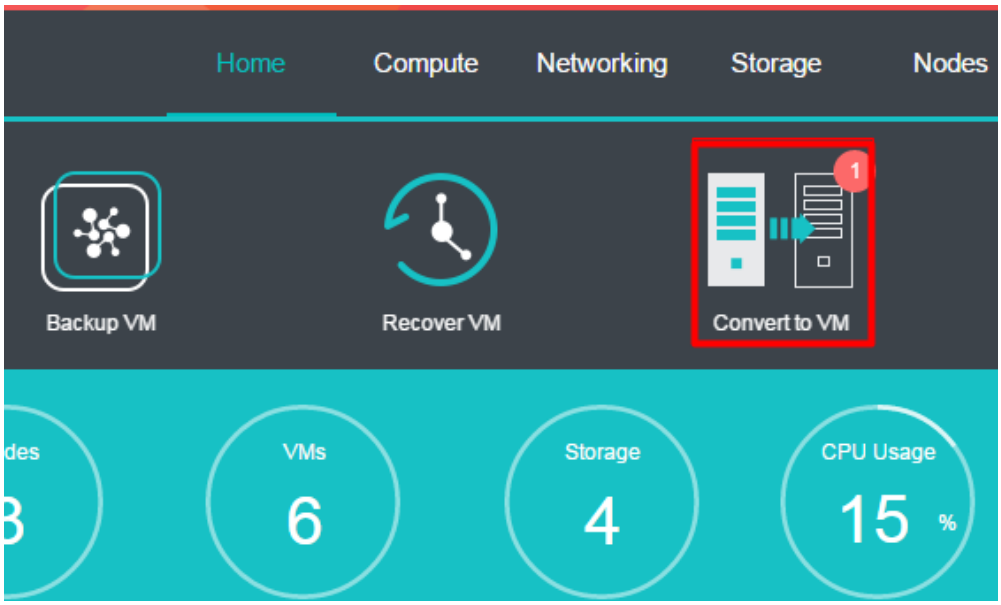


After specifying the above fields, the migration program will verify whether the current node and the destination node can communicate with each other. If not, it will be redirected to the network configuration page for you to make some changes, if so, click **OK** to proceed.

The following page will display if network communication succeeds, indicating that the node gets ready for migration. (The Installer login is for the purpose of debugging in case of migration failure)

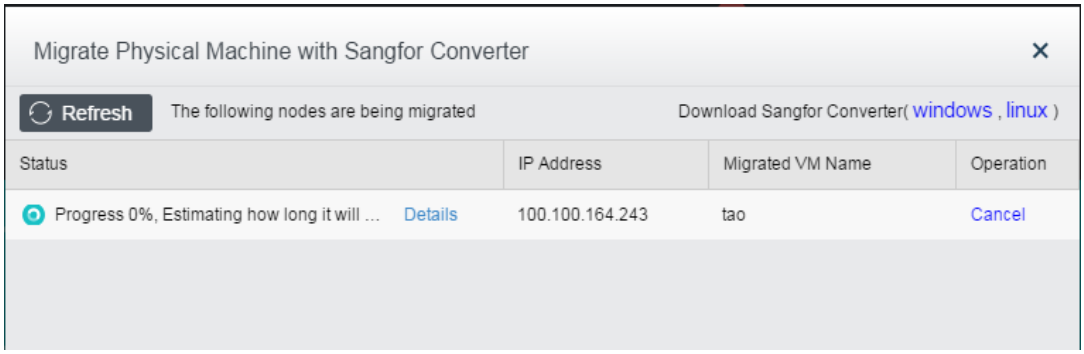


To view migration tasks, log in to Web admin console of Sangfor HCI platform and click **Convert to VM** in **Home**.

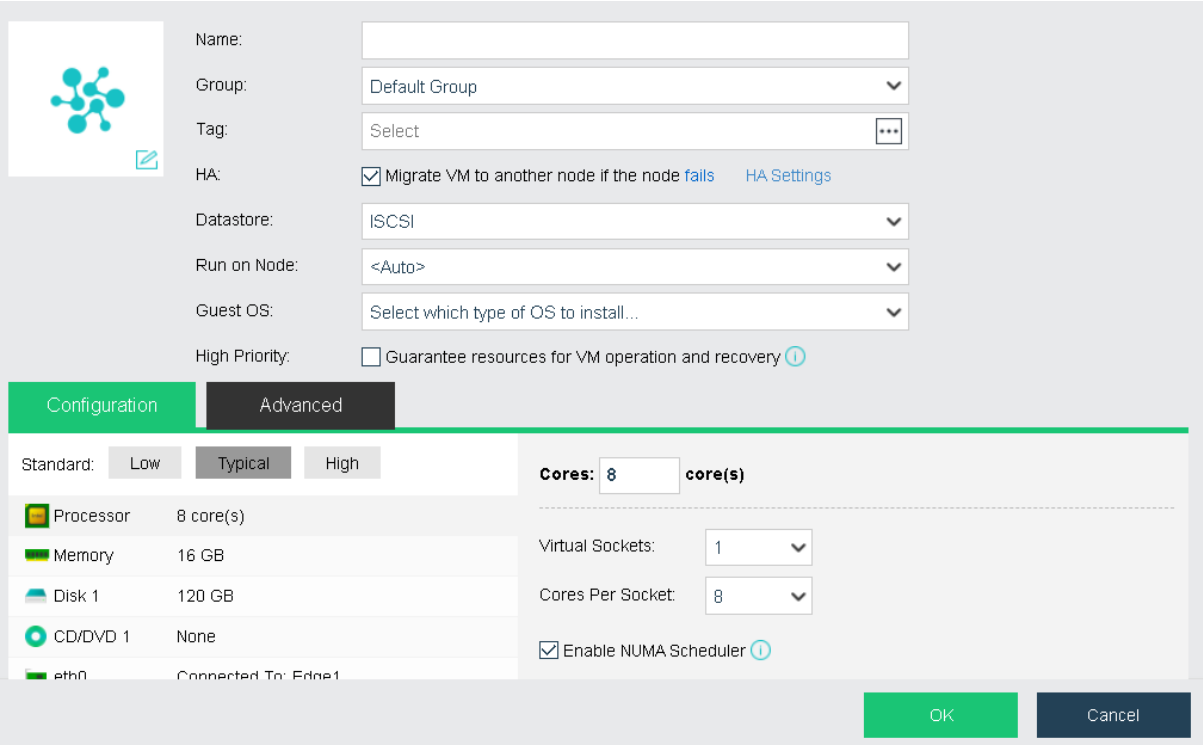


On the following page, you will see migration tasks and physical machines waiting for

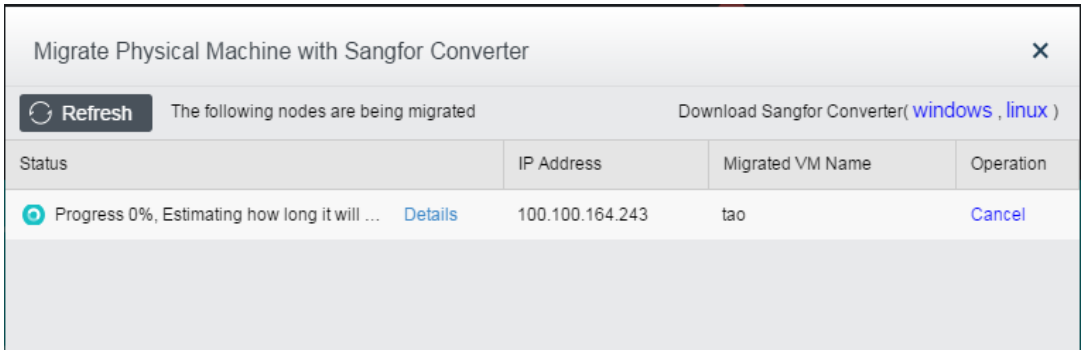
migration. To migrate a physical machine, you need to click **Migrate** to enter the **Destination VM** page and configure destination virtual machine.



Make relevant configurations, including VM name, datastore, run on node, hardware configurations, etc, as shown below:



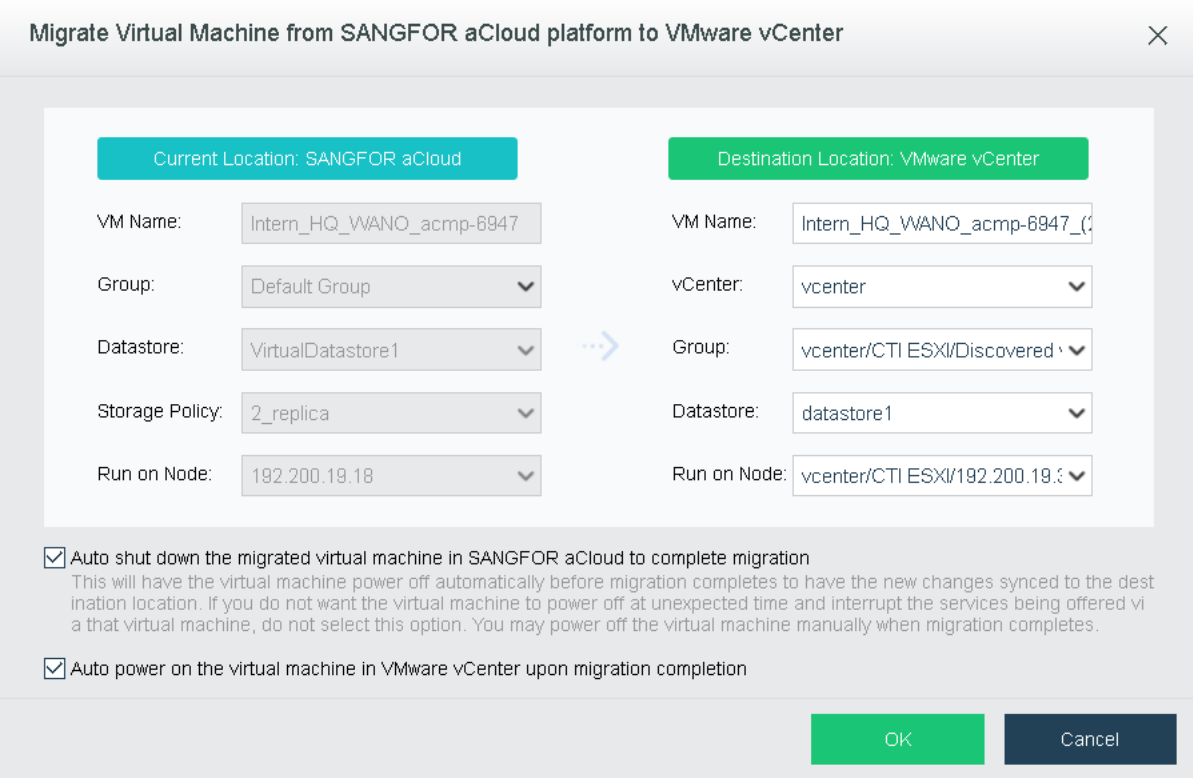
After making the above configurations, start migration.



- Conversion of physical machine is supported by Sangfor HCI3.3 and later versions. Sangfor conversion tool for Windows based server is a separate .exe file; for Linux based server, that tool is integrated into Sangfor HCI software.
- The progress of migration depends on physical network bandwidth and disk IO performance of the host having Sangfor HCI software installed.
- It is recommended that physical network bandwidth should be 1 GBps at least.
- Since migration will affect disk performance of the host having Sangfor HCI software installed, it is recommended to perform migration when business system is not busy and ensure that number of migration tasks is less than 3.
- Storage capability of Sangfor HCI platform should be larger than the used space of disk of the physical machine to be migrated, or else migration will fail.

2.2.1.11.2 Migrating VM to VMware vCenter

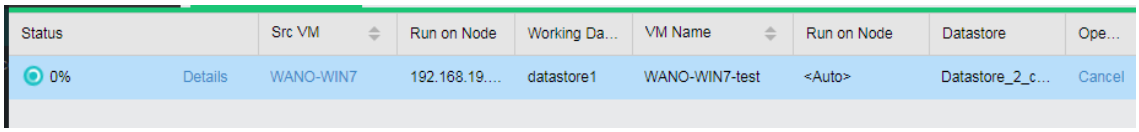
Powered-on virtual machines on Sangfor HCI platform can be migrated to VMware vCenter



Before migration, you need to specify the fields under **Current Location** and **Destination Location.** Whether to select the options **Auto shut down the migrated virtual machine in Sangfor HCI to complete migration** and **Auto power on the virtual machine in VMware vCenter upon migration completion** depends on your own needs.

Auto shut down the migrated virtual machine in SANGFOR HCI to complete migration: This will have the virtual machine power off automatically before migration completes to have the new changes synced to the destination location. If you do not want the virtual machine to power off at unexpected time and interrupt the services being offered via that virtual machine, do not select this option. You may power off the virtual machine manually when migration completes.

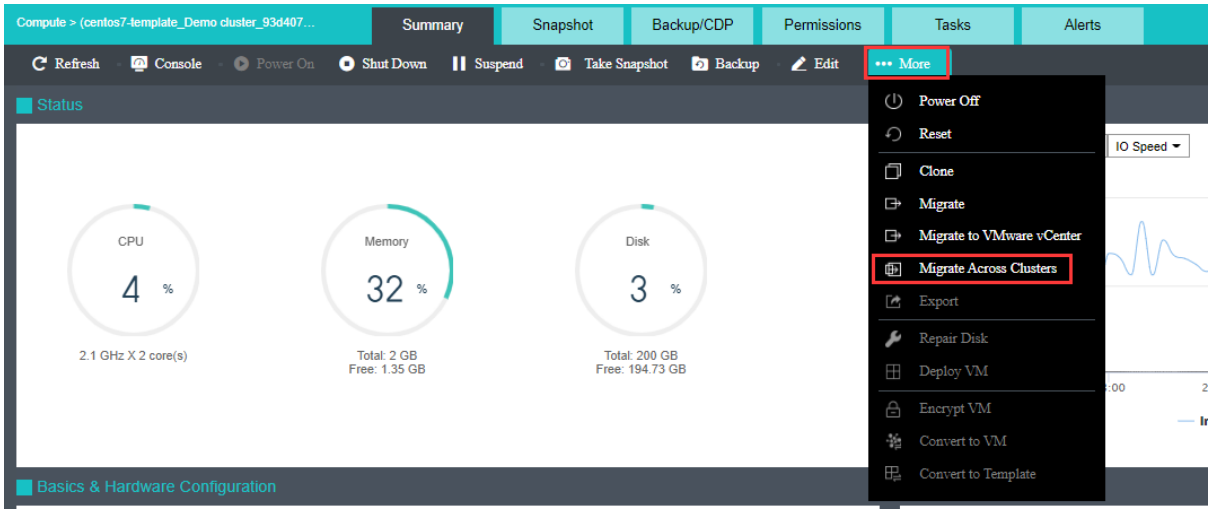
After configuring relevant fields, click **OK** to start migrating virtual machine and you will see the migration process. You can also view migration progress and more details in tasks, as shown below:



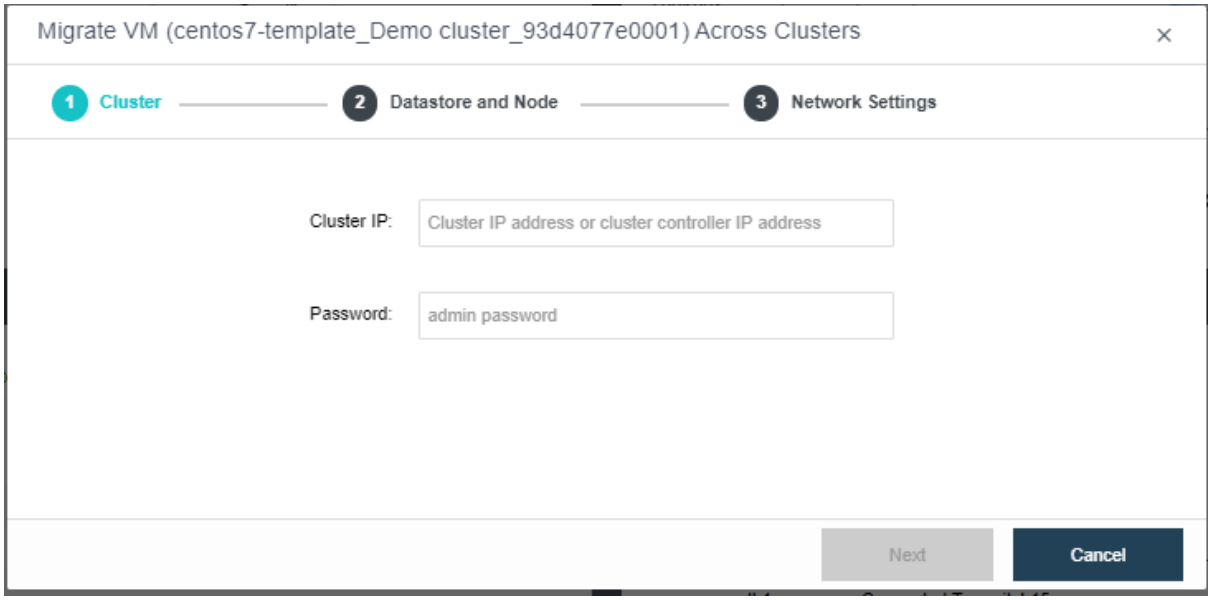
2.2.1.11.3 Migrating VM Across Clusters

This feature enables virtual machine to be migrated to a different cluster.

Live Migration

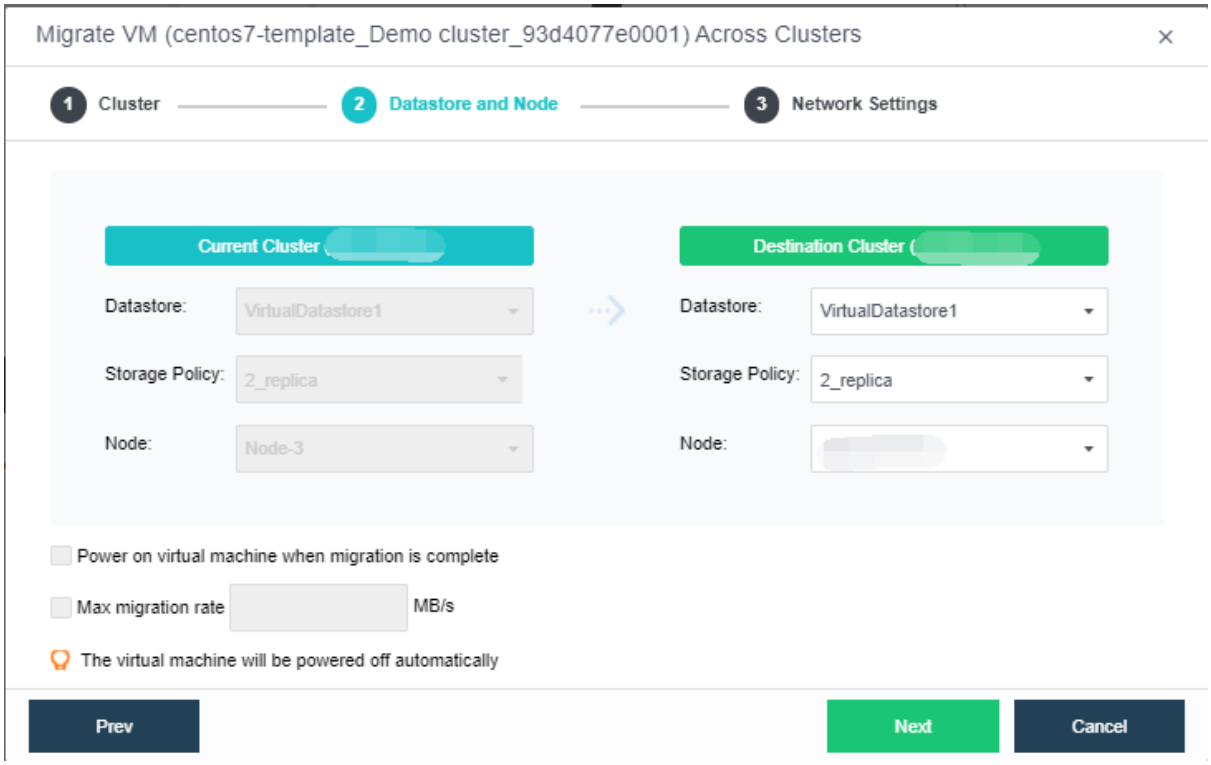


And then



Cluster IP: Specifies IP address of destination cluster.

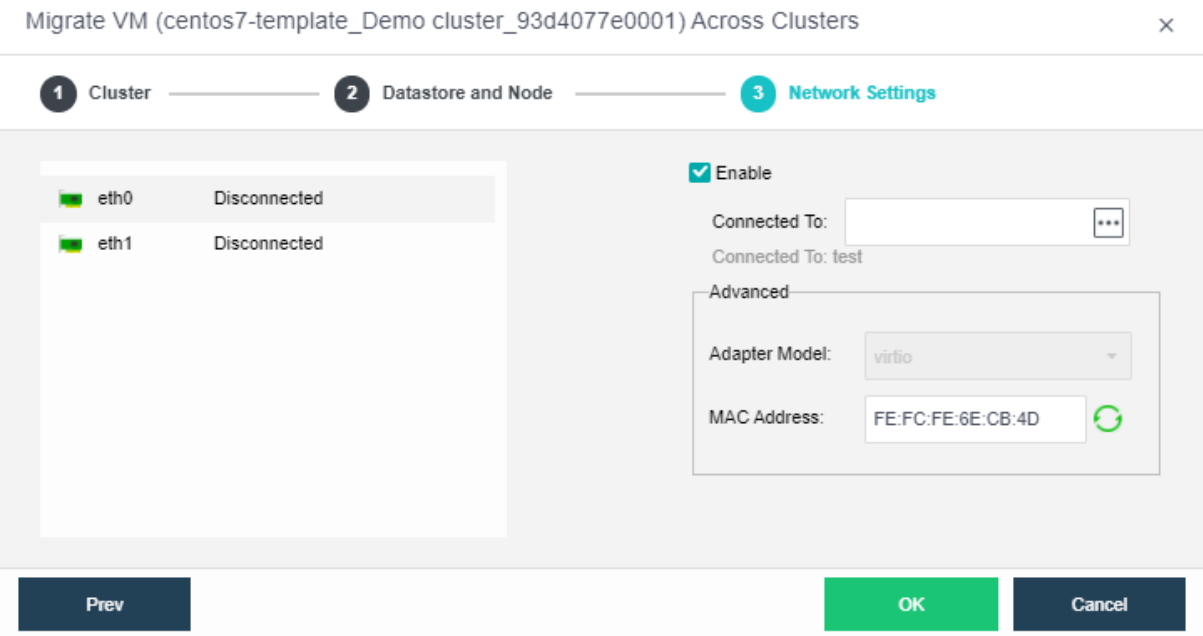
Password: Specifies admin password.



Reboot upon migration completion: It is applicable to cold migration only.

Max migration rate: Specifies the maximum migration speed. The minimum is 5MB/s and the maximum is 1000MB/s.

After specifying destination datastore and node, click **Next** to configure network.



Enabled: If it is selected, it indicates that the specified virtual network adapter is enabled.

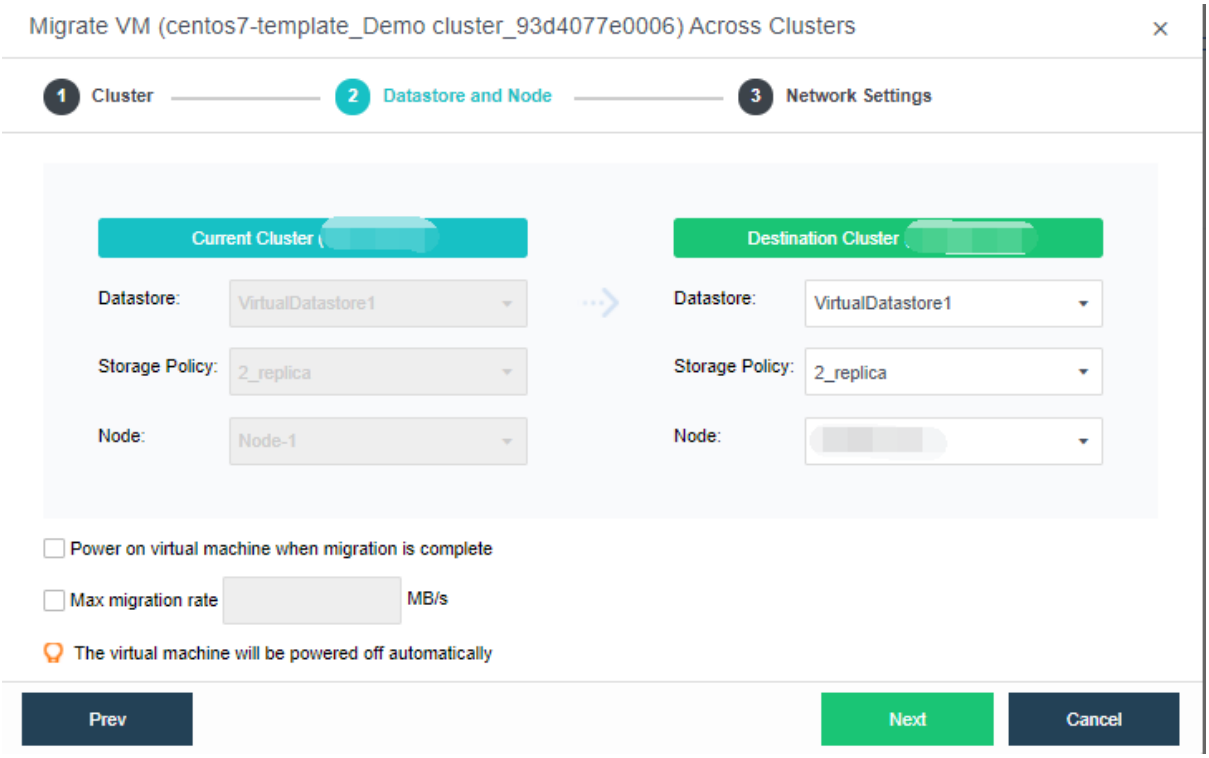
Connected To: Specifies an edge or a virtual switch to be connected to the virtual machine.

Adapter Model: Specifies the adapter model. Options are **Realtek RTL8139** and **Intel E1000**.

MAC Address: MAC address can be automatically generated or manually specified. MAC address examples: 00-11-22-33-44-55, 00:11:22:33:44:55. MAC address will be changed after the migration operation completes and you may edit the MAC address if you do not want the MAC address to be changed.

The virtual machine will be powered off automatically and added into the default VM group.

Cold Migration

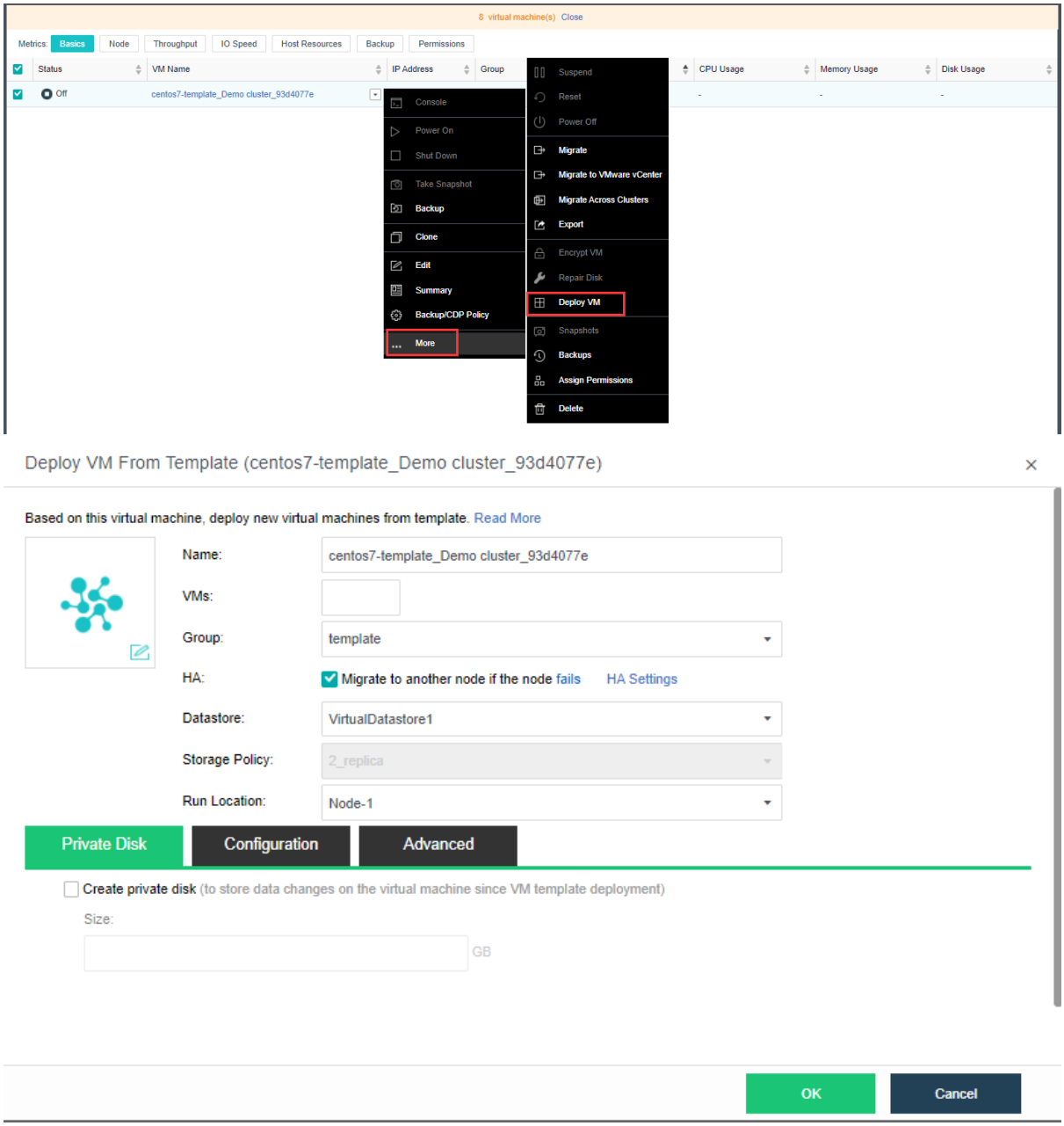


Other configurations are the same with that of live migration. You may refer to the **Live Migration** section.

2.2.1.12 Deploying VM

Generally speaking, a VM template is a virtual machine which has been configured, and can be used to deploy multiple virtual machines with the same configurations. The difference from cloning VM is that disk files will not be replicated when a virtual machine is deployed from a template. What's more, changes made to template will be saved to de virtual machine incrementally.

Deploy VM: Only the virtual machine converted to template can be used to deploy virtual machines. Disk settings of the virtual machine after being converted to template cannot be changed any more. You may deploy new virtual machines when converting a virtual machine to template. Deployed virtual machines have the same configurations as that of its template.



Name: Specifies name of the deployed virtual machine(s).

Name of the deployed VM depends on the **Name** and the number of virtual machines. For instance, name of VM is **name** and number of virtual machines is 2, then names of the two new virtual machines are **name_0001** and **name_0002** respectively.

Migrate to another node if the node fails: If this option is selected, deployed virtual machines will be automatically migrated to another node if the working node fails.

Datastore: Specifies a datastore where configuration files of deployed virtual machines are

stored.

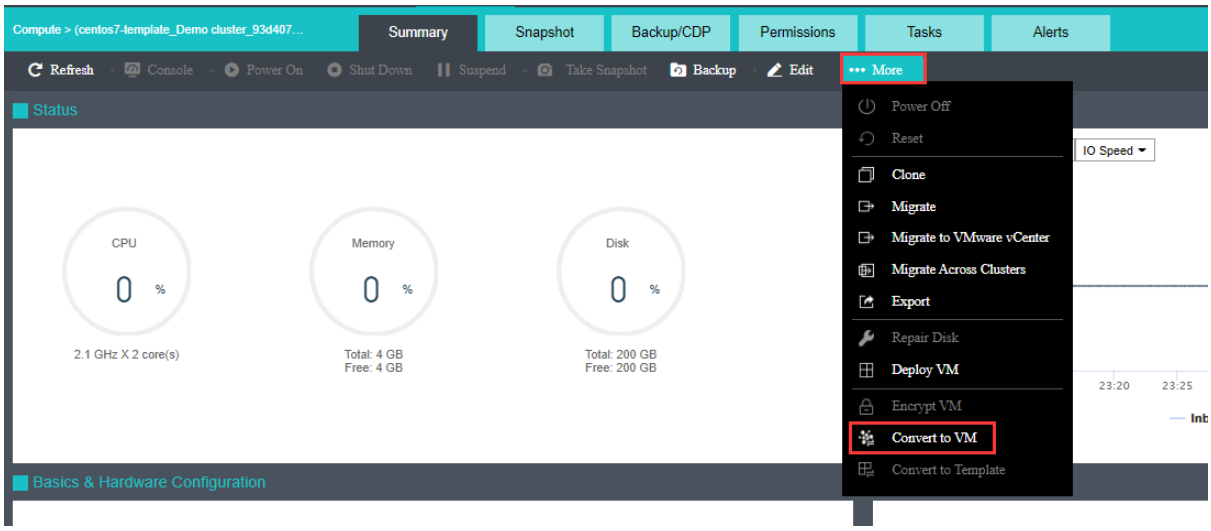
Working Location: Specifies a node where the deployed virtual machines resides.

Create Private Disk: You may create a private disk and assign a specified disk size to each deployed virtual machine.

After deploying virtual machine from template completes, go to VM template Summary page and click the number next to Deployed VM(s) to enter the following page to view deployed virtual machine.

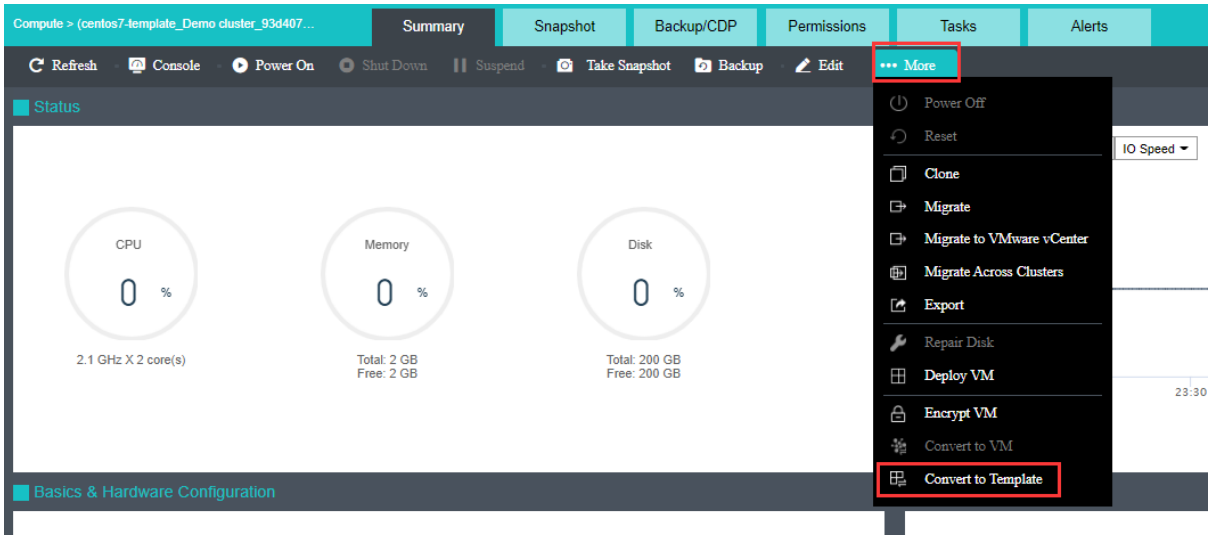
2.2.1.13 Converting VM Template to VM

You may convert a VM template to an ordinary virtual machine. Before converting template to VM, template must be powered off first. To convert template to VM, make sure that template is powered off. If it is powered on, click Power **Off** or **Shut Down** and select **More > Convert to VM** on the **Summary** page, as shown below:



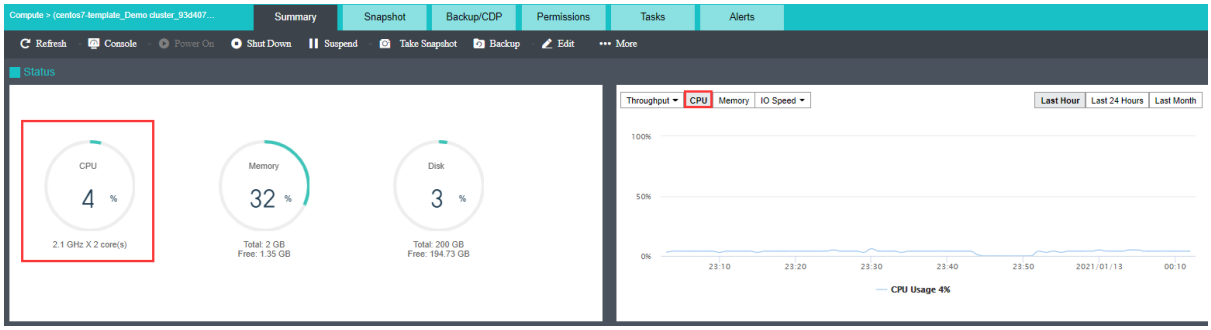
2.2.1.14 Converting VM to Template

A virtual machine can be converted into template so that it can be used as a template to create multiple virtual machines. Before converting virtual machine to template, make sure that VM is powered off; if it is powered on, click **Power Off** or **Shut Down** and then select **More > Convert to template** on the **Summary** page, as shown below:

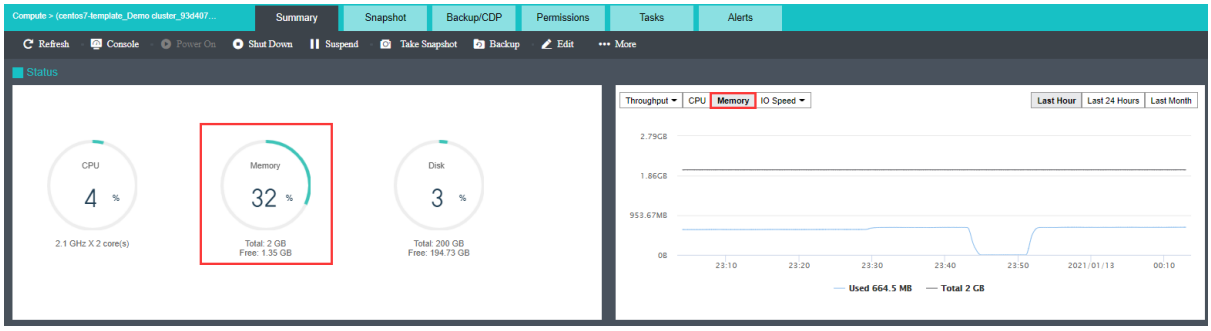


Status: Displays the following information about virtual machine: **CPU Usage, Memory Usage, Disk Usage, Throughput, CPU, Memory, IO Speed, IOPS**.

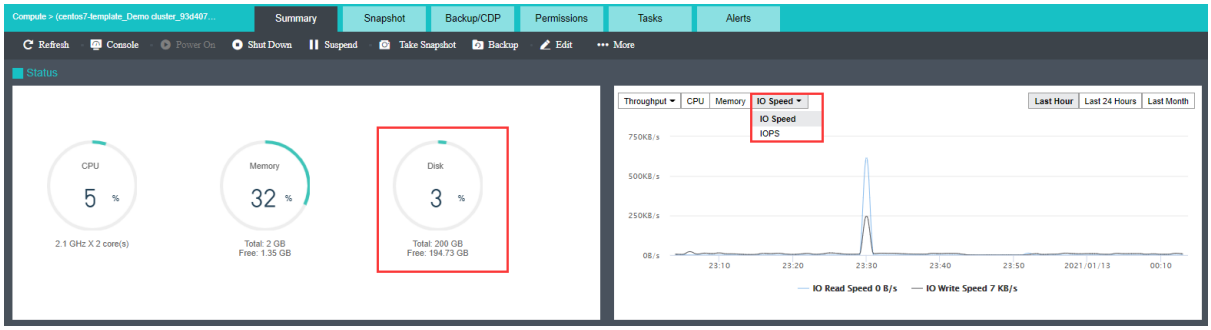
CPU Usage: Displays CPU usage of virtual machine. On the right side, you may view CPU usage in the last hour or last 24 hours.



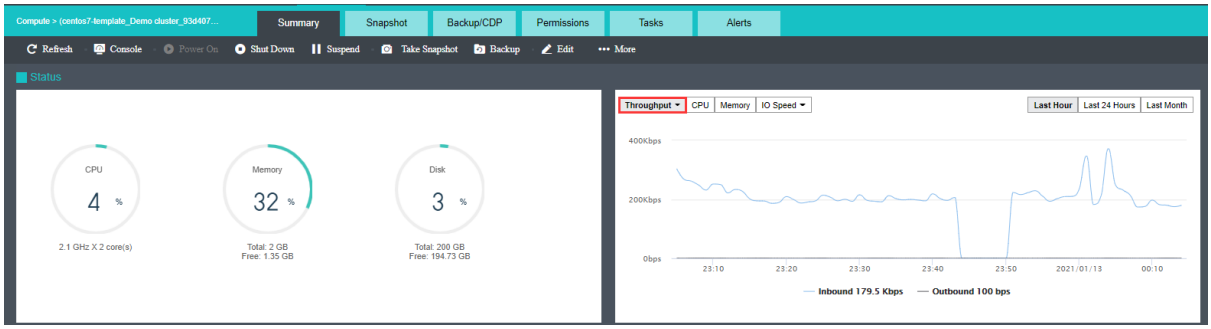
Memory Usage: Displays the total and free memory size respectively, as well as memory usage. On the right side, you may view memory usage in the last hour or last 24 hours.



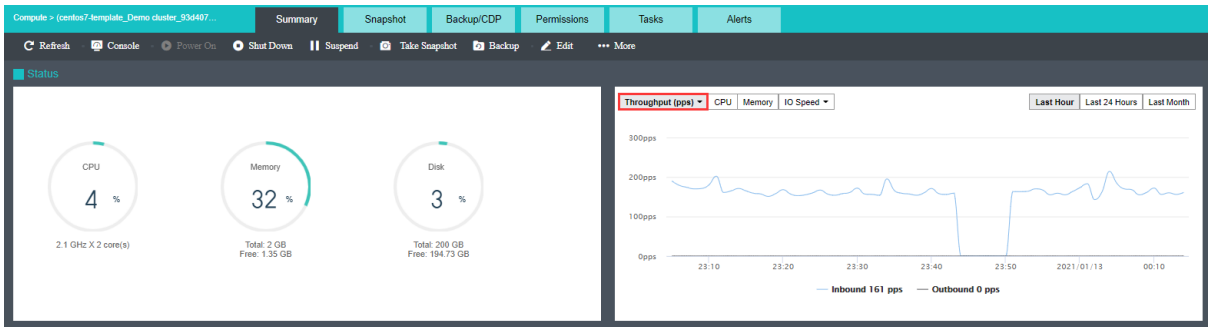
Disk Usage: Displays the total and free disk size respectively, as well as disk usage. On the right side, you may view disk IO speed and IOPS.



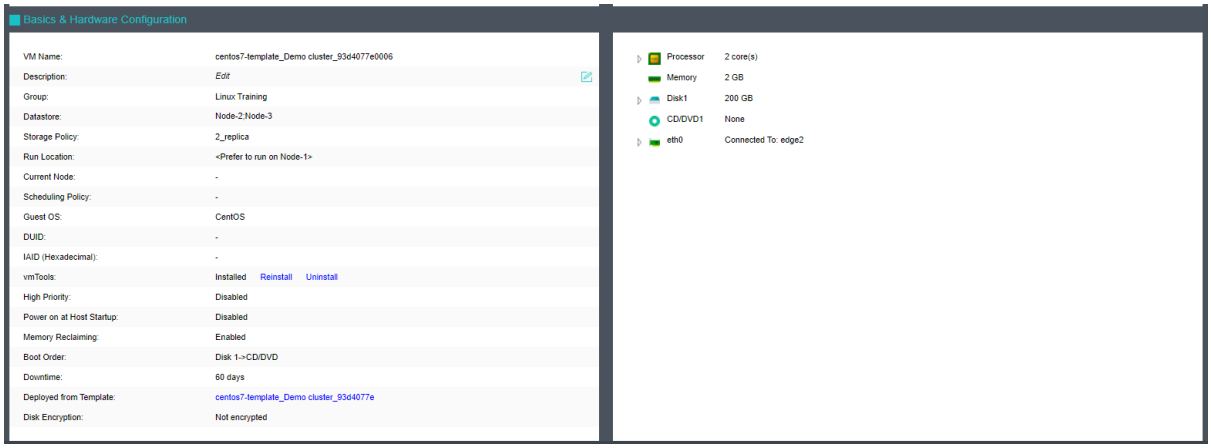
Throughput: Displays overall throughput.



Throughput(pps): Displays inbound and outbound packets per second.



The **Basics & Hardware Configuration** section displays basic information and hardware configuration of virtual machine. Basic information includes **VM Name, Description, Group, Datastore, Storage Policy, Run Location, Current Node, Scheduling policy, Guest OS,DUID, IAID(Hexadecimal), vmTools, High Priority, Power on at host startup, memory reclaiming, Boot Order, Downtime, Deployed from Template and Disk Encryption**.



2.2.1.15 Taking Snapshot

There are 2 types of snapshot starting from version 6.0.1.

a. Storage based snapshot

Description: Storage based snapshot with ROW mechanism. This is the default snapshot method for cluster starting from version 6.0.1 for 3 nodes and above environment.

The maximum number of storage based snapshot can be take is 128.

Up to 128 snapshot can be taken for storage based snapshot.

Features:

1. Reduce the impact to the performance after taking a snapshot.
2. Space occupied by the snapshot can be release after deleted the snapshot.

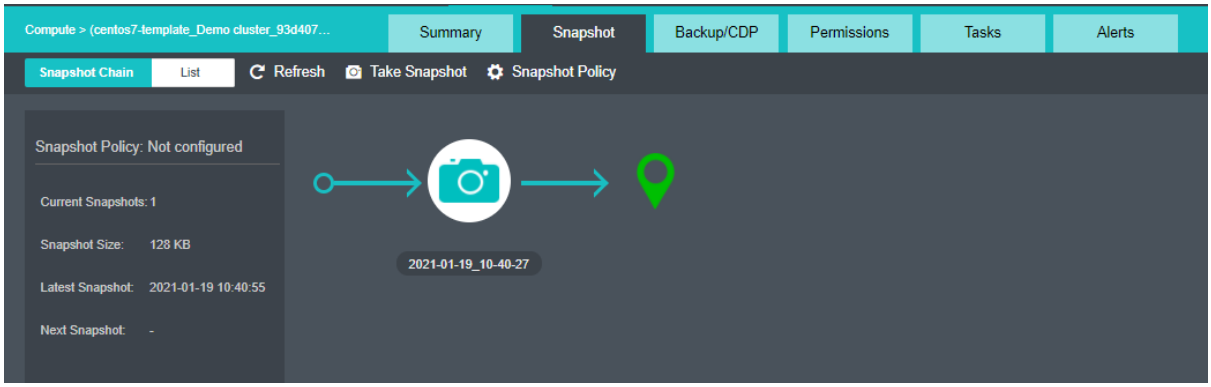
Requirement: To support storage based snapshot, the following requirement must be fulfill.

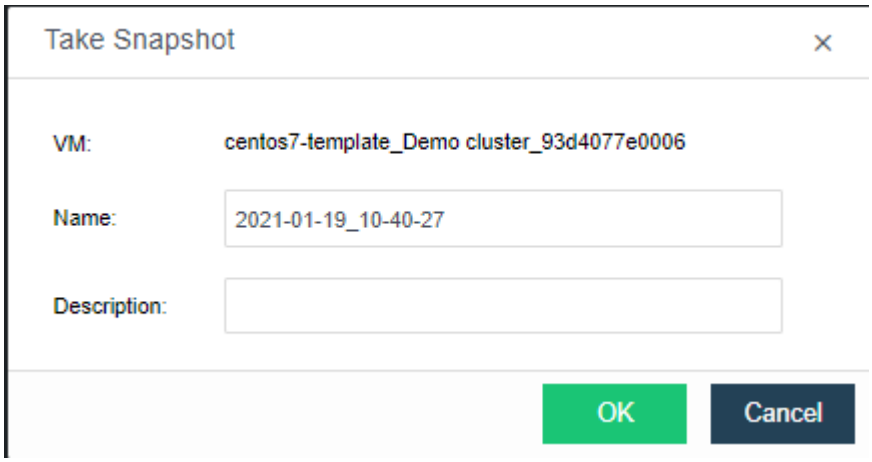
1. Version 6.0.1 and above.
2. 3 nodes and above cluster.
3. VM is running in virtual storage.

b. Virtual disk based snapshot

Description: Qemu based snapshot with COW mechanism. This snapshot will be use for 2 nodes cluster or VM that running on external storage.

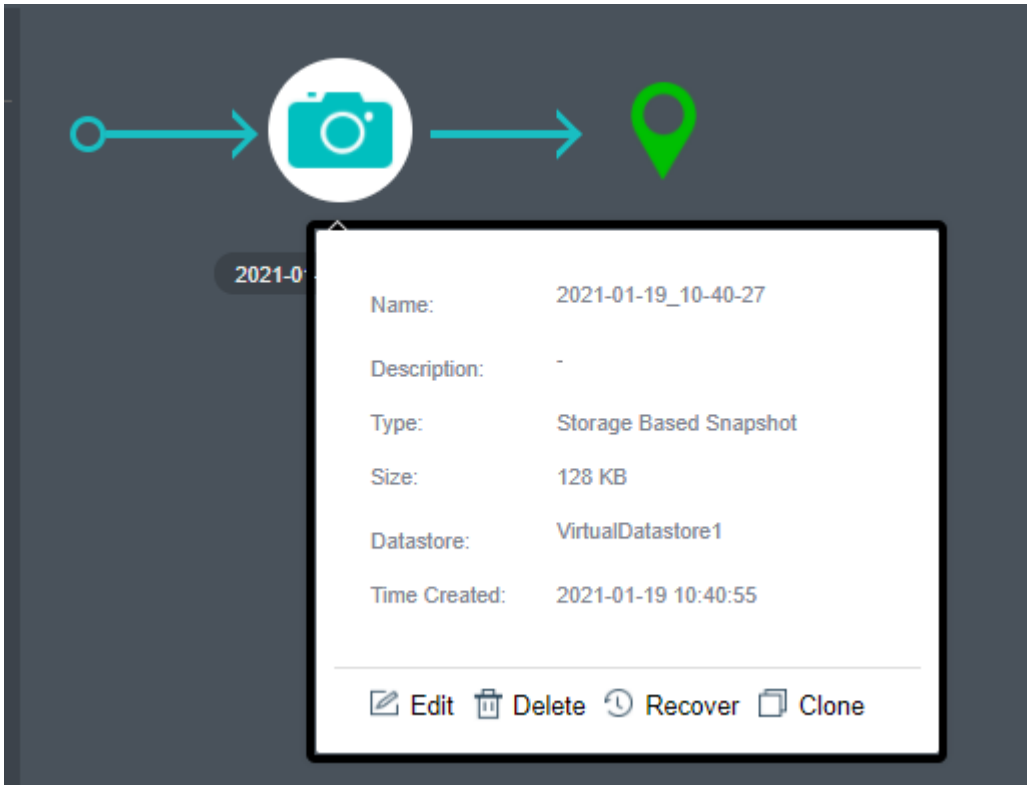
On the **Snapshot** page, you can view the snapshots you have taken and create new snapshot. To create a snapshot, click **Take Snapshot**.





On the above page, specify **Name** and **Description**. Then, click **OK**.

After a snapshot is created, you may click on the snapshot name and then a dialog pops up, as shown below:



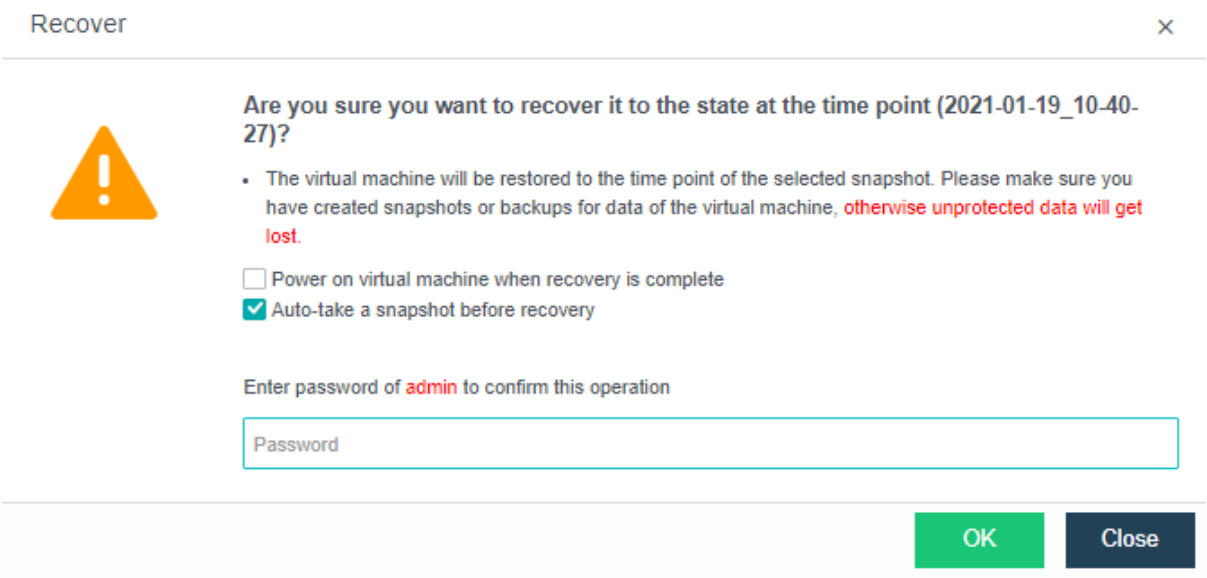
To modify the snapshot name and description, you may click **Edit**.

To delete the snapshot, you may click **Delete**. Snapshots cannot be recovered once deleted. It requires admin password to confirm the operation.

To clone a virtual machine from the snapshot, you may click **Clone**.

To recover virtual machine from snapshot, you may click **Recover**. The virtual machine is running, but will be powered off before being recovered. Please power it on manually after recovery.

Take a snapshot prior to recovery: Once it is enabled, though the changes made since the previous snapshot will get lost, this snapshot is inevitable in case of recovery failure.



To make snapshot before recovery, you may tick the option **Auto-take a snapshot before recovery.**

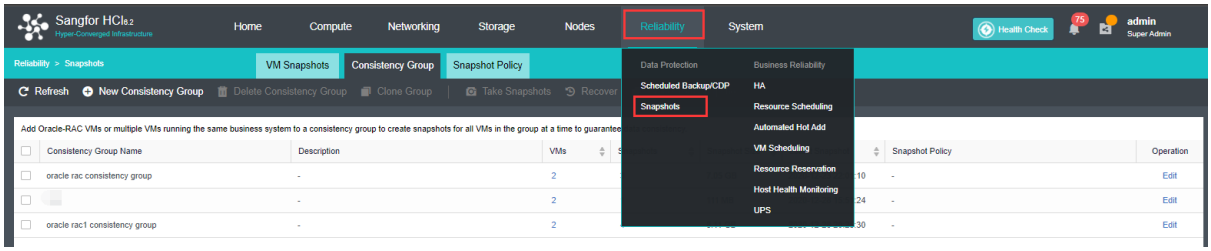
Consistency group snapshot

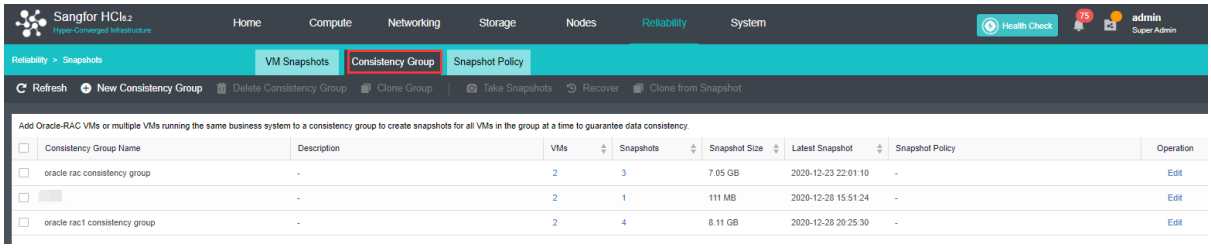
Consistency group snapshot is the feature which allow user to add multiple VM into a consistency group and take snapshot at the same time.

A single consistency group has restricted the number of vm disk which the maximum number of disk is 64.

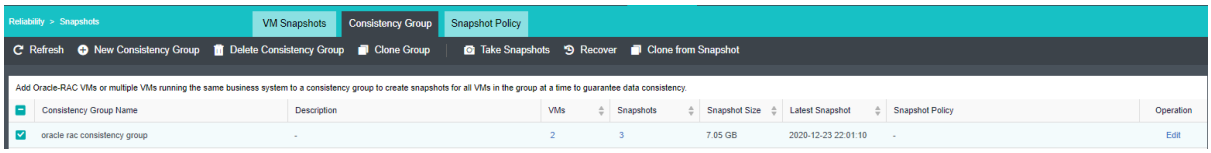
Consistency group snapshot will only process for the virtual disk that running on virtual storage.

Navigate to consistency group snapshot setting under **Reliability** > **Snapshots** > **Consistency Group**.

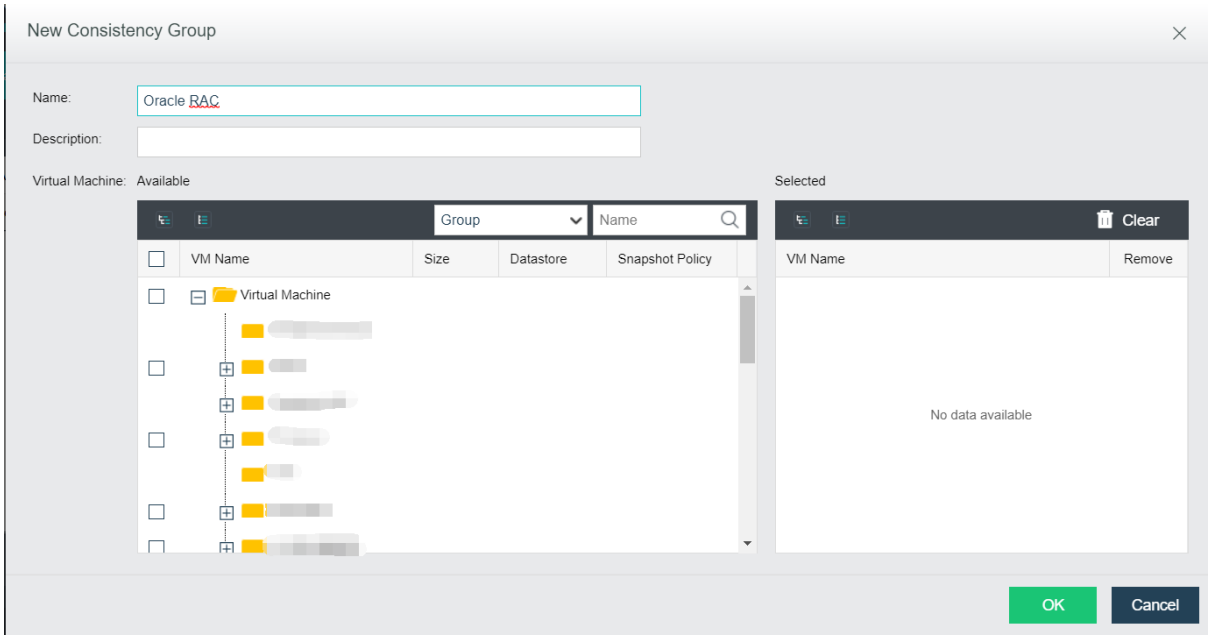




In the Consistency Group tab, you can perform the following:



New Consistency Group: Create a new consistency group with selected VM



Delete Consistency Group: Delete the selected consistency group. Required to enter admin password to proceed.

Clone Group: Clone the VM inside the consistency group and create new consistency group with the cloned VM.

Take Snapshots: Take snapshot for the selected consistency group.

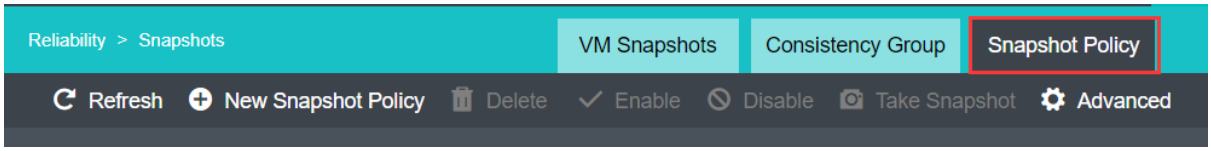
Recover: Recover snapshot for the selected consistency group.

Clone From Snapshot: Clone VM from the selected snapshot.

Schedule Snapshot policy

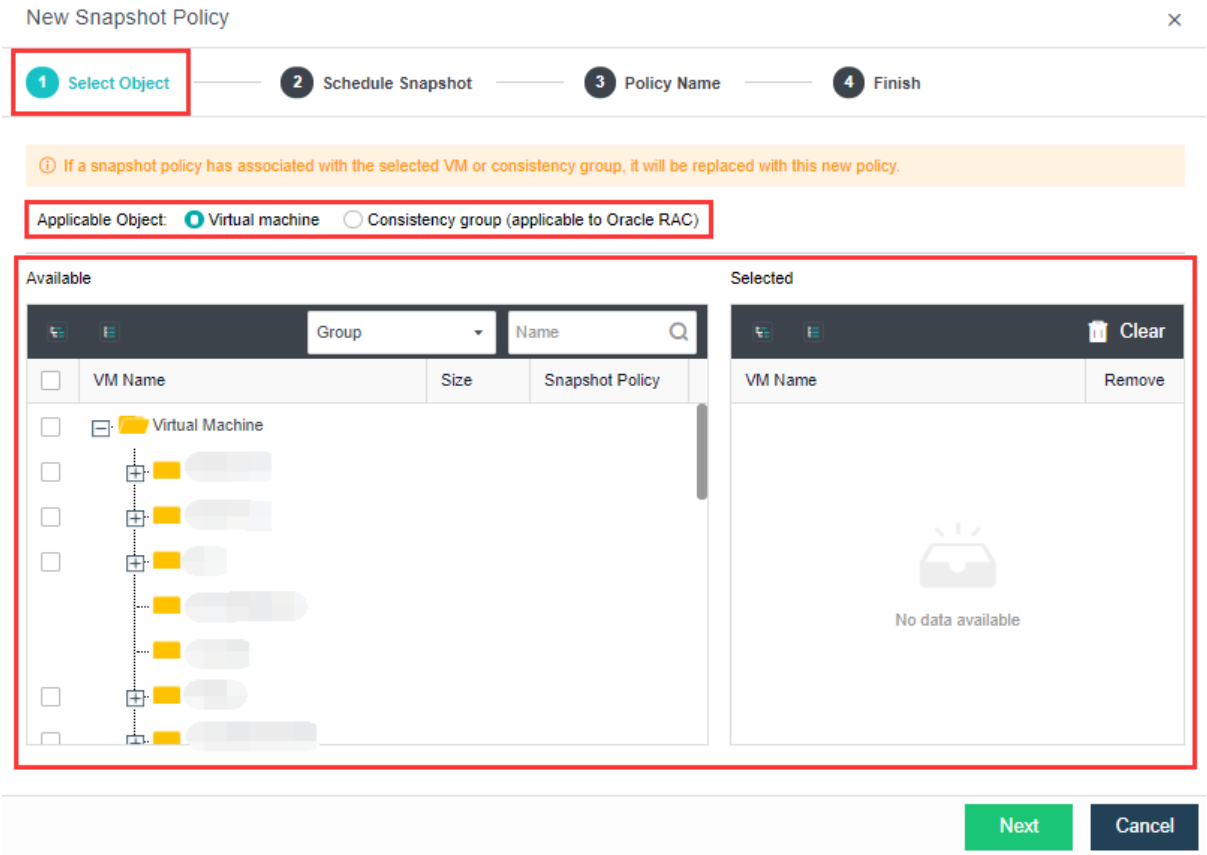
Schedule snapshot policy allow user to take a snapshot and cleaning up the snapshot periodically for security purposes as well as saving the storage space.

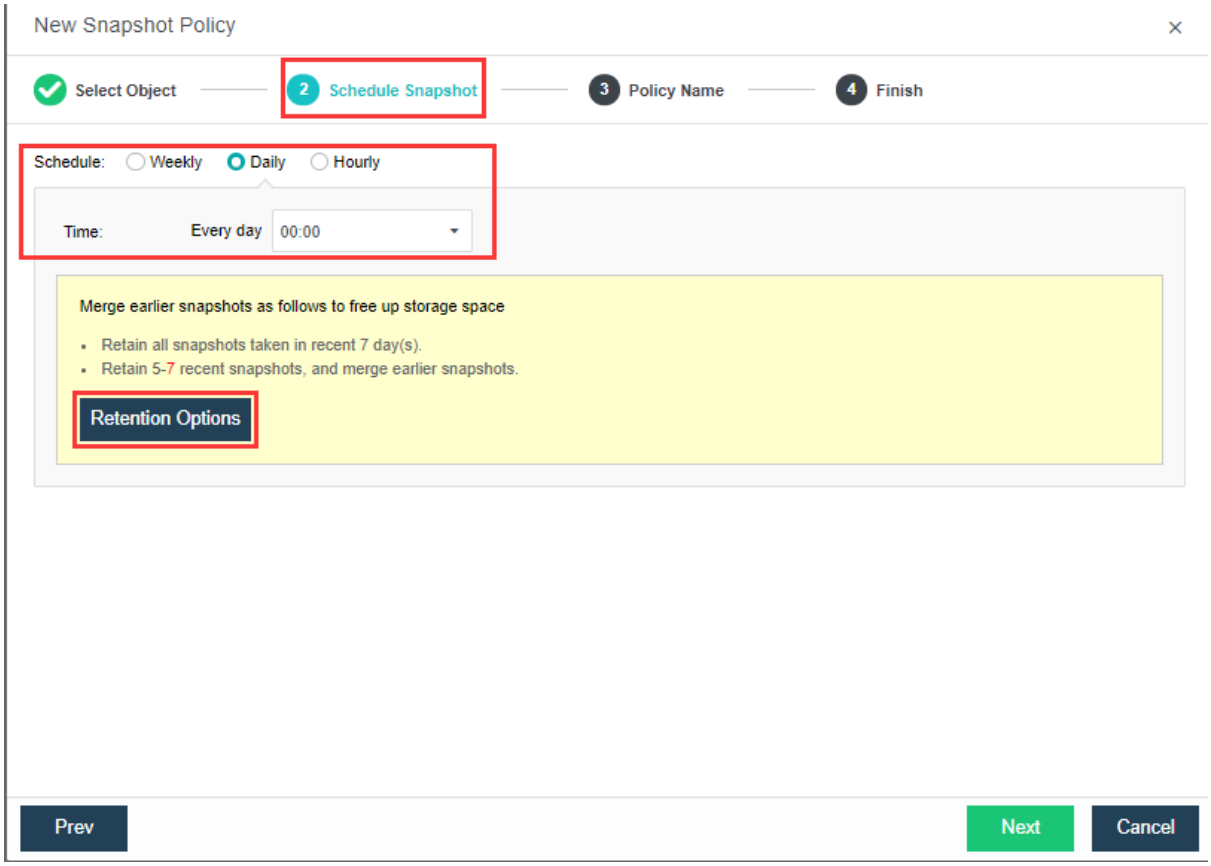
User can configure schedule snapshot policy to take snapshot for the VM periodically under **Reliability** > **Snapshots** > **Snapshot Policy**.

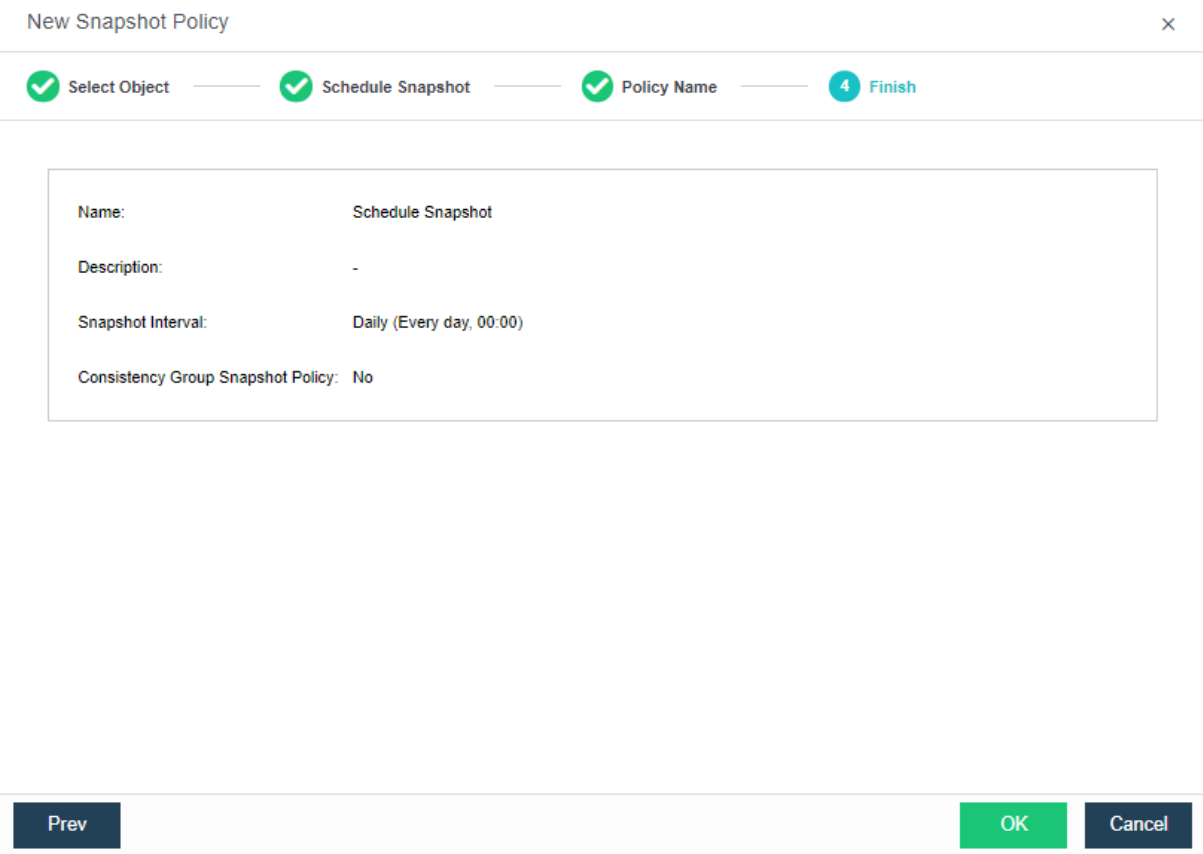


In snapshot policy tab, you can perform the following action.

New Snapshot Policy: Create new snapshot policy by selecting VM/Consistency Group, Schedule, Retention Options and specify the policy name.




New Snapshot Policy
Select Object
2 Schedule Snapshot
3 Policy Name
4 Finish
Schedule: Weekly Daily Hourly
Time: Every day 00:00
Merge earlier snapshots as follows to free up storage space
Retain all snapshots taken in recent 7 day(s).
Retain 5-7 recent snapshots, and merge earlier snapshots.
Retention Options
Prev
Next
Cancel



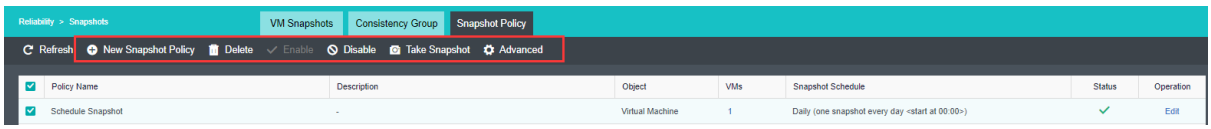
Delete: Delete the selected snapshot policy.

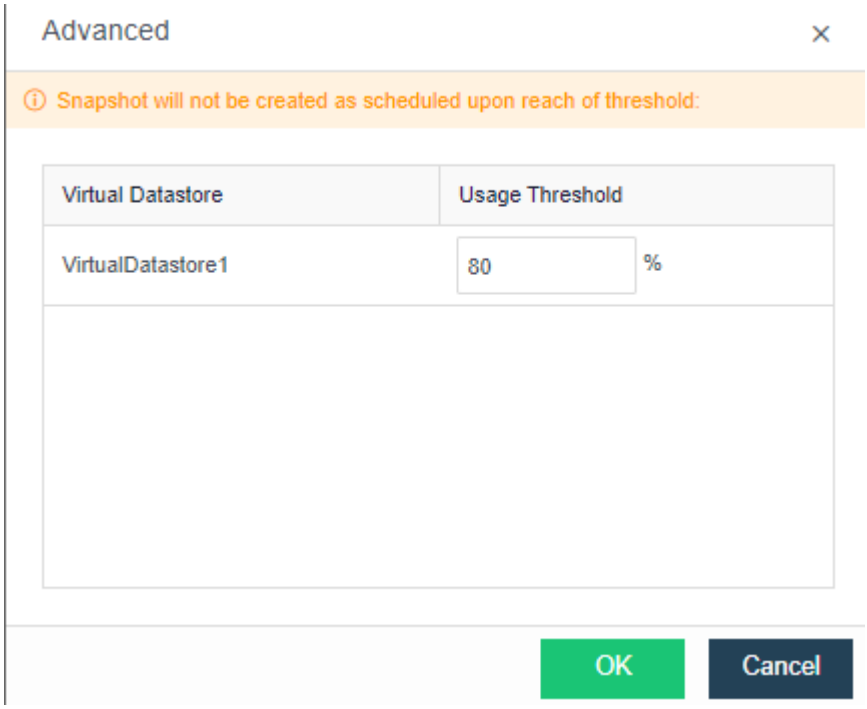
Enable: Enable the selected snapshot policy.

Disable: Disable the selected snapshot policy.

Take Snapshot: Take snapshot for the VM in the snapshot policy.

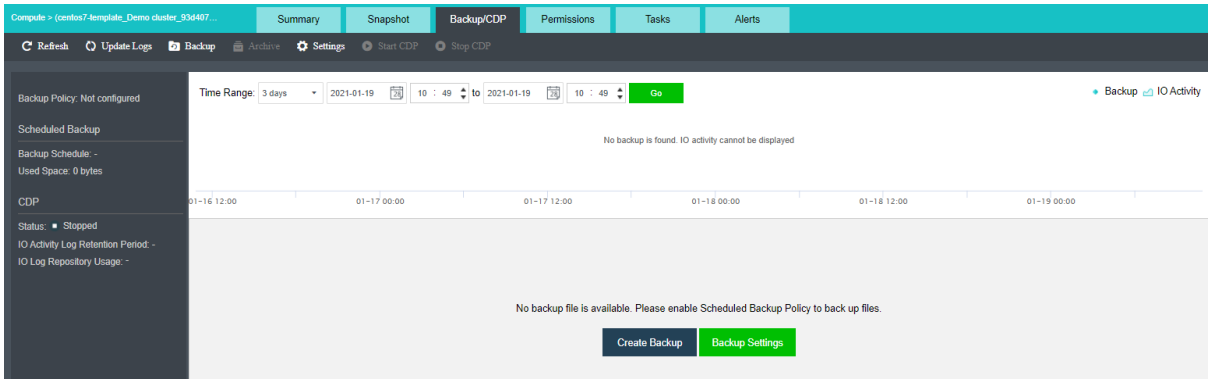
Advanced: Configure the **Threshold** for the storage which will stop the schedule snapshot.



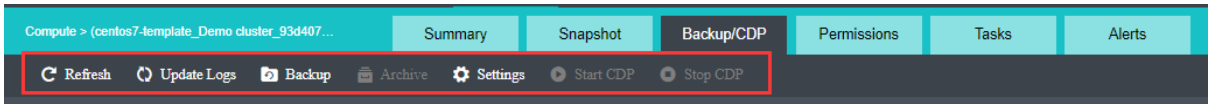


2.2.1.16 Configuring Backup/CDP

Continuous data protection(CDP) is real-time backup which can log every disk IO activity of a virtual machine. It enables administrators to restore virtual machine to any point in time and view or download file created at any point in time, which helps a lot in case that virtual machine encounters file deletion by mistake, virus infection, system crash, data damage, etc.



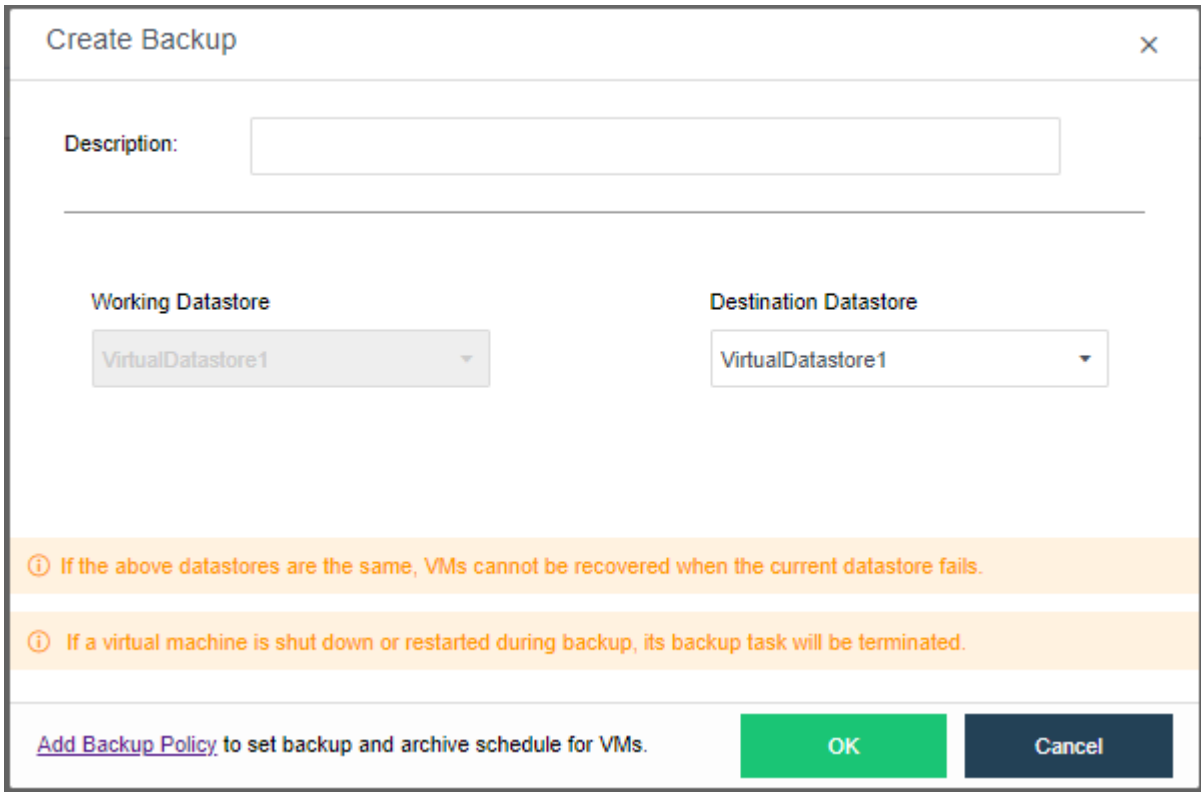
On the toolbar, there are **Refresh, Scan New Backups, Backup, Settings** and **Start CDP**, as shown below:



To refresh the page, you may click **Refresh**.

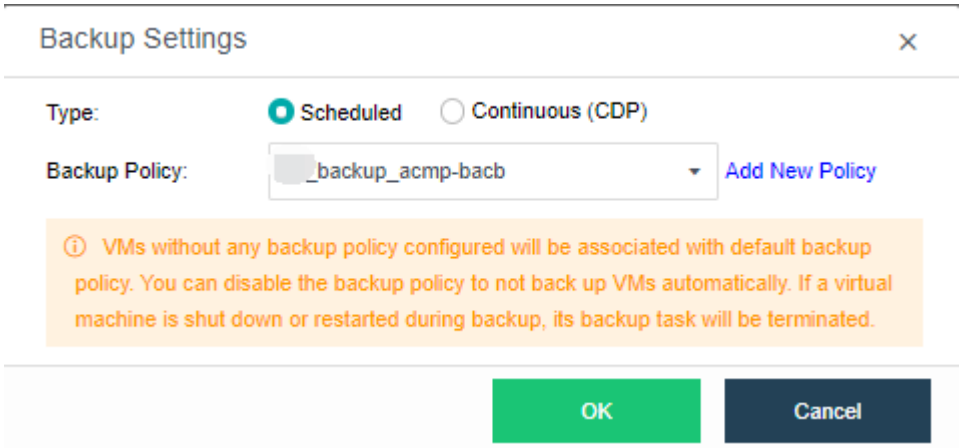
To check whether there are new backups, you may click **Update Logs**.

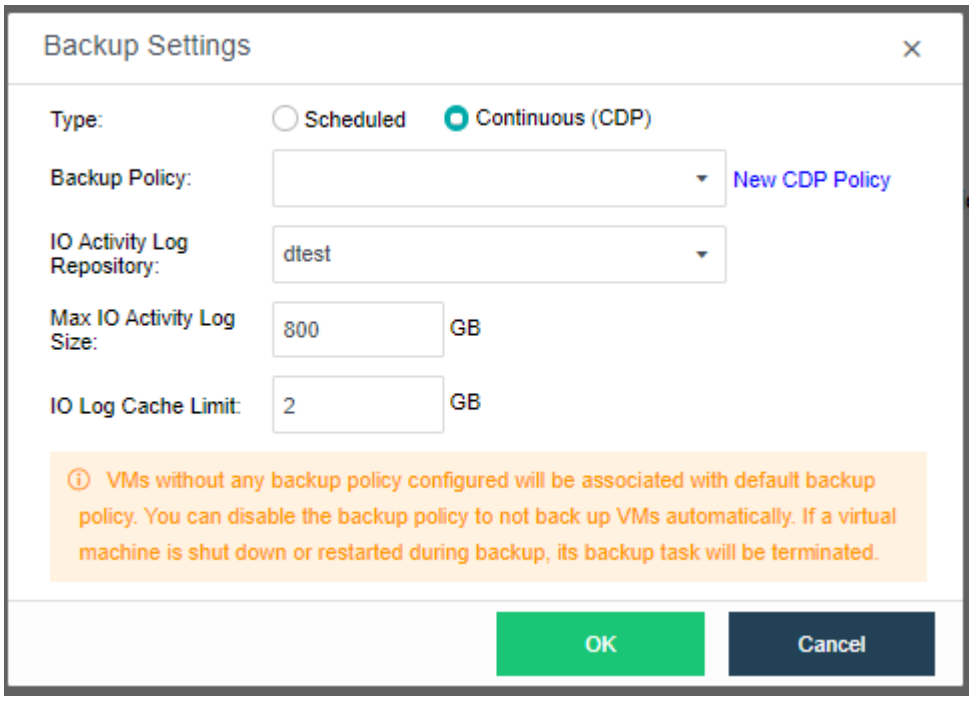
To create backup for the virtual machine, you may click **Backup**.



- If CDP is enabled, the destination datastore is that you have specified in CDP policy and cannot be specified manually.
- If the above datastores are the same, VM cannot recover when the current datastore fails.

To specify backup method and backup policy, click **Settings**. As for backup method, options are **Scheduled** and **Continuous(CDP)**. For details, refer to **2.6.12.1 Sangfor Backup** Policy section.

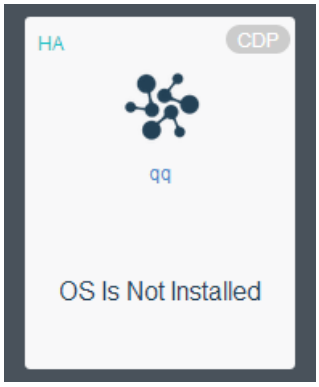




For VMs not associated with any backup policy, they will associate with default backup policy. To not back up a specific virtual machine, simply disable the corresponding backup policy.

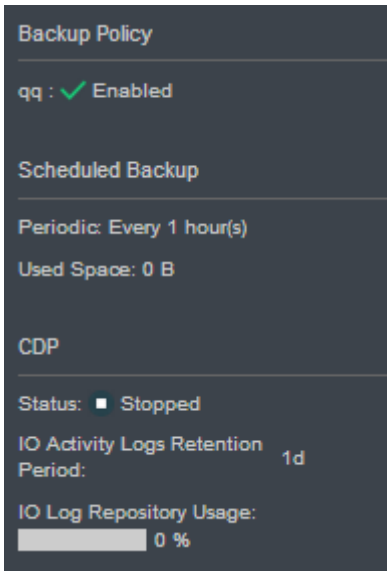
Start CDP: To start CDP, click **Start CDP**, only support when the backup method is **Continuous**(CDP).

When CDP policy is enabled and CDP is started for virtual machine, the CDP icon is green on the VM panel. If the CDP policy is enabled yet CDP is not started, the CDP icon is gray, as shown in the following picture.



CDP can be started only when virtual machine is powered on and associated with a CDP policy. Template and virtual machines deployed from template do not support CDP.

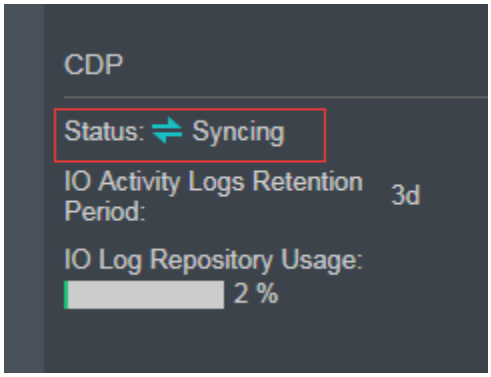
The left panel displays backup policy, backup method and CDP information, as shown below:



Backup Policy: It displays the backup policy that has been selected and its status.

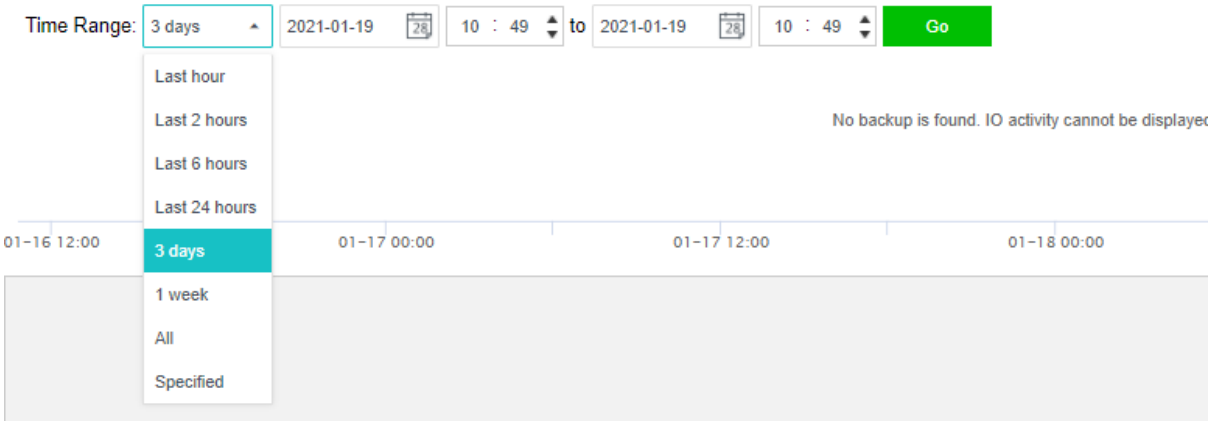
Scheduled Backup: It displays backup method and used space.

CDP: It displays status of CDP, IO Activity Logs Retention Period and IO Log Repository Usage. Status of CDP includes Not configured, Starting, Synchronizing, Started, and Stopped, etc.



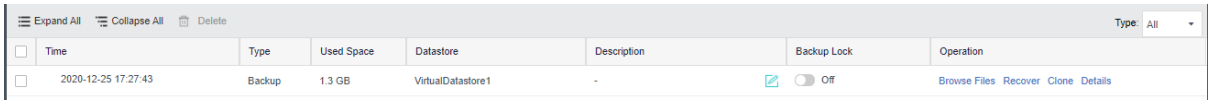
2.2.1.16.1 Viewing IO Activities

As for **Period**, option can be **Last Hour**, Last **2 Hours**, **Last 6 Hours**, **Last 24 Hours**, **Three days**, **One week**, **All** and **Specified**.



2.2.1.16.2 Viewing Backup Details

It displays backup details, including **Time,** Type**, Used Space, Datastore, Description, Backup Lock**, and **Operation**.



Expand All: To display all the IO activity logs, click **Expand All.**

Collapse All: To hide IO activity logs, click **Collapse All.**

Delete: To delete one or more backups, select the backup(s) and click **Delete**. Once backup is deleted, corresponding IO activity logs will also be deleted for they are dependent on

backup(s). Backups cannot be recovered once deleted. Enter password of the current username to confirm operation:

To display IO activity logs, click . To hide IO activity logs, click

Time: Displays time that a backup or IO activity log is created.

Type: Displays backup type, Backup or IO activity log.

Used Space: Displays space used by backup or IO activity log.

Datastore: Displays datastore where backup or IO activity log is stored.

Description: Displays backup description. To edit description, click

Backup Lock: To enable backup lock, click on . To disable backup lock, click on

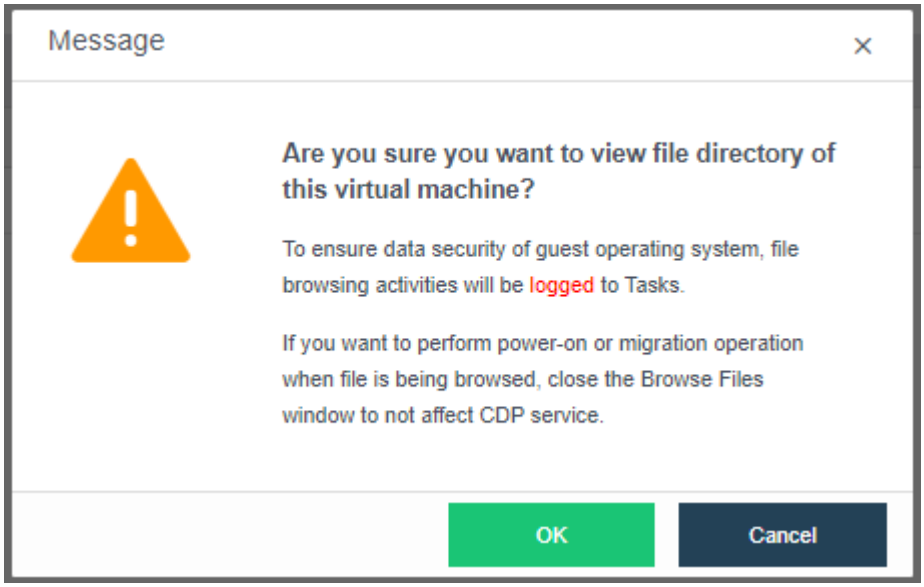
Operation: For Backup, operations can be **Browse Files**, **Recover, Delete** and **Clone**. For IO activity log, operations can be **Browse Files** and **Recover**.

As for details of browsing files, see the **Browsing Files** section. For details on how to recover virtual machine, see the Recovering Virtual Machine section. For details on how to clone virtual machine, see the **Cloning Virtual Machine** section.

2.2.1.16.3 Browsing Files

You may select a backup or IO activity log created at any time point and download the corresponding backup file. This operation will be logged so as to ensure data security.

Click **Browse Files** to enter te following page:

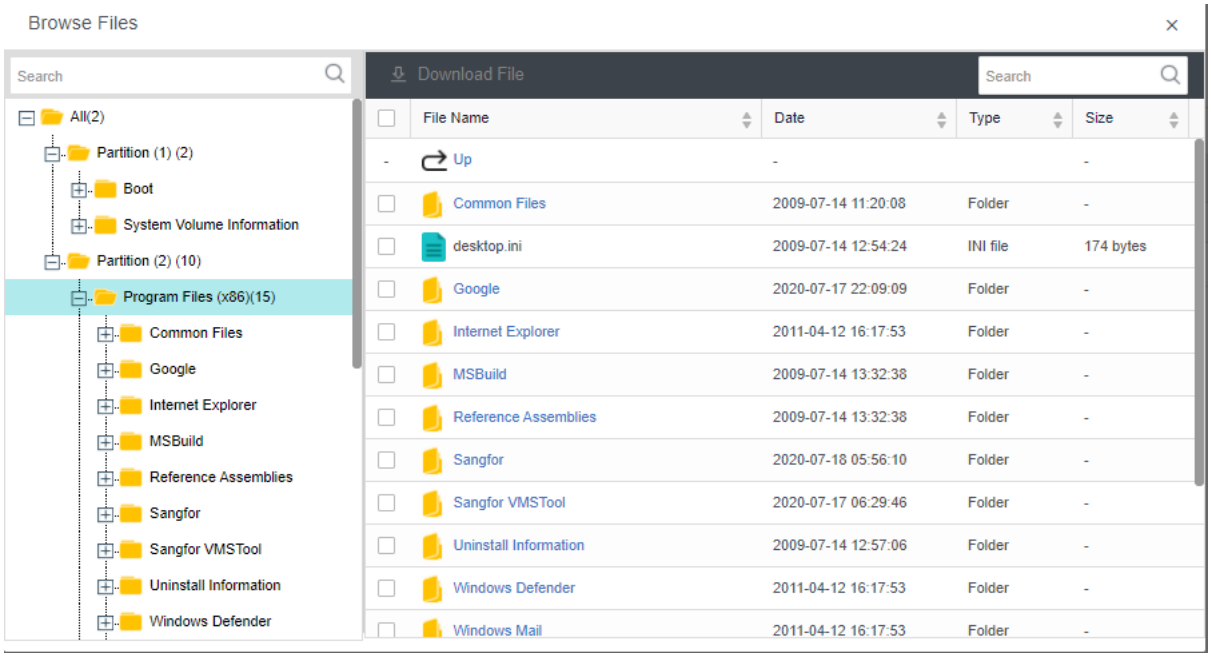


To ensure data security of guest operating system, file browsing activities will be logged to **Tasks**.

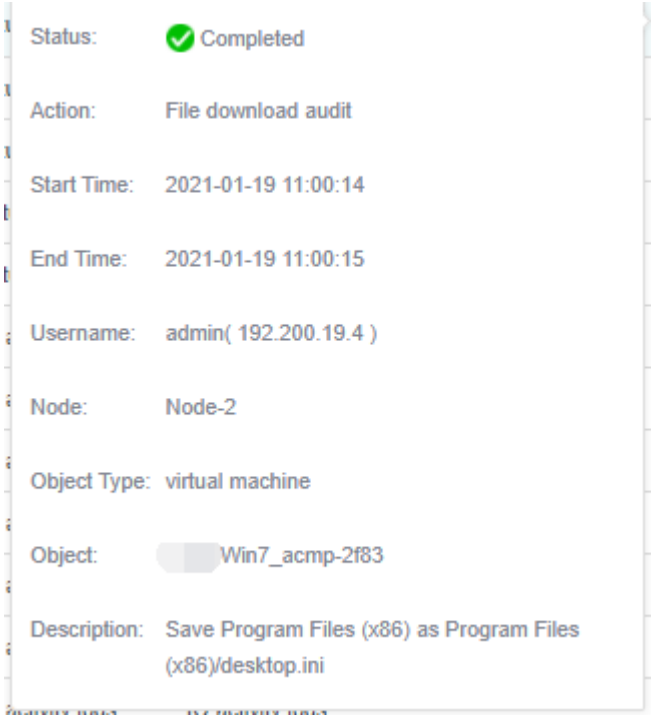
If you want to perform power-on or migration operation when file is being browsed, close the Browse Files window to not to affect CDP service.

As for Linux-based virtual machines, backup files cannot be browsed or saved.

Click **OK** to enter the following page to select partition, select one or more files, click **Download File** to download file to local disk, as shown below:



You may go to **Tasks** to view relevant logs, as shown below:

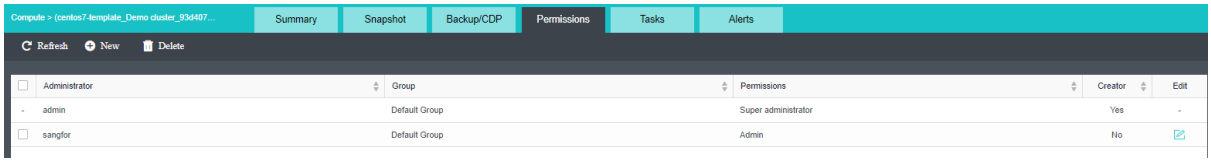


2.2.1.17 Recovering Virtual Machine

2.2.1.18 Disk Encryption

2.2.1.19 Viewing Permissions

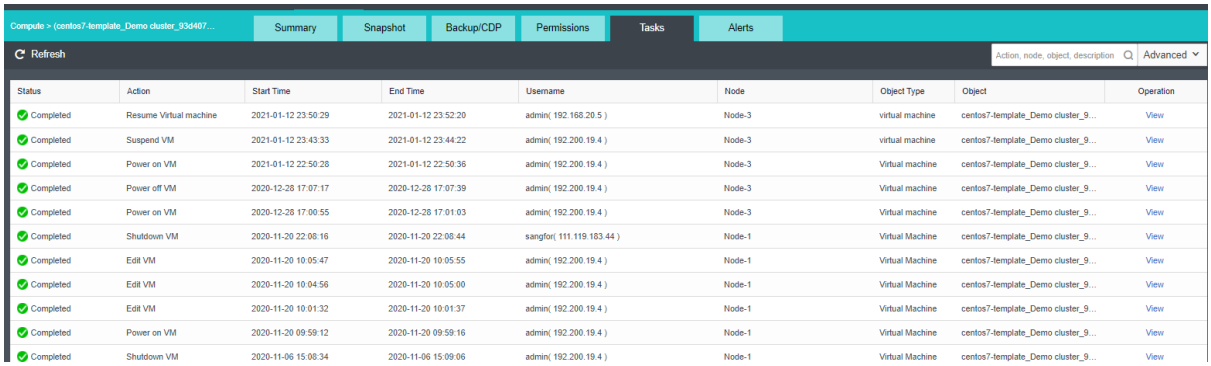
The **Permissions** page shows the permissions of administrator against VM resources.



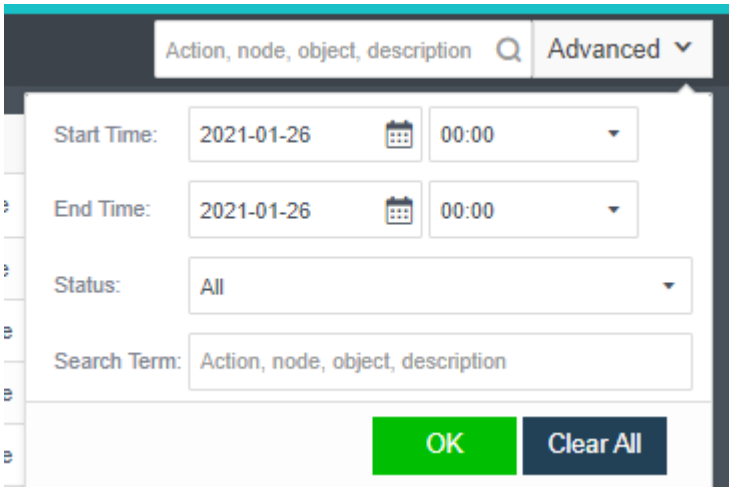
For details, refer to the **2.6.3 System Administrators and** Permissions section.

2.2.1.20 Viewing Tasks

On the **Tasks** page, you can view administrator logs about various operations performed by administrator, such as creating a virtual machine, etc. Each log contains the following information: **Status, Action, Start Time, End Time, Username, Node, Object Type, Object** and **Operation**. To view log details, click **View** in **Operation** column.

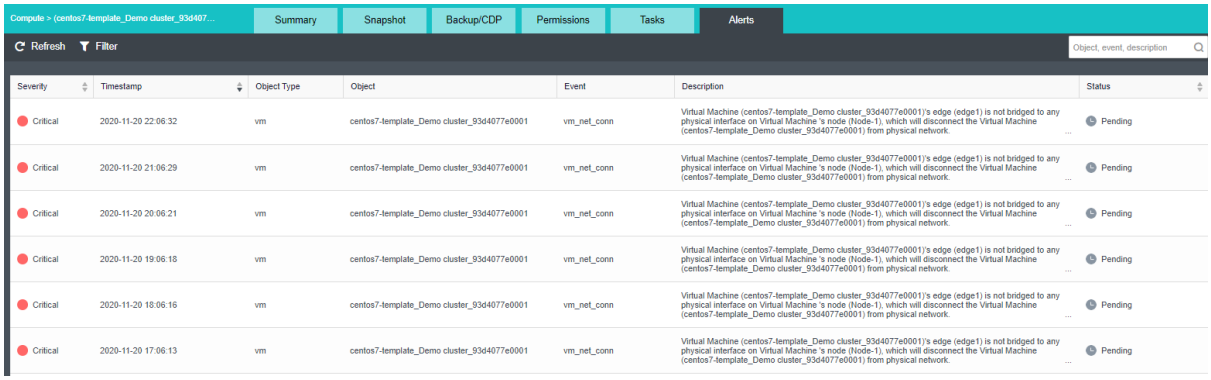


Logs can be searched by action, node, object and description. By clicking **Advanced Search**, you can also specify a period of time, status and search term to filter logs.

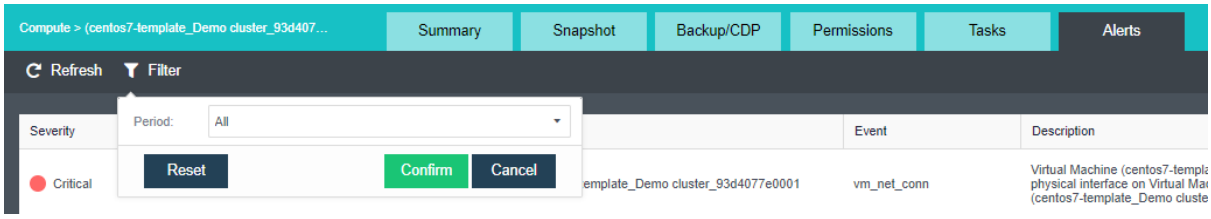


2.2.1.21 Viewing Alerts

This section displays alert logs. For instance, an alert log records that VM CPU usage is above threshold, etc. When an alert-triggering threshold is reached, a corresponding alert will be triggered and an alarm log will be generated. An alert log includes the following information: **Severity, Timestamp, Object Type, Object, Event, Description, Status**.



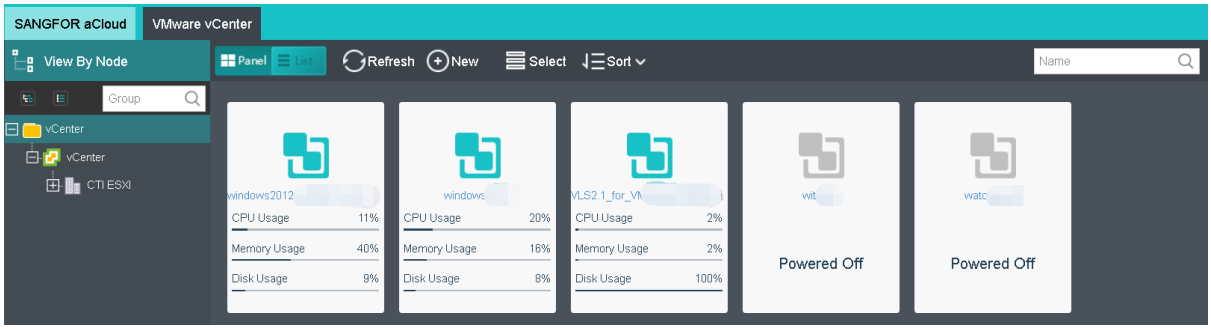
alert logs can be searched by action, node, object and description. By clicking **Filter**, you may also specify a period of time and search term to filter logs.



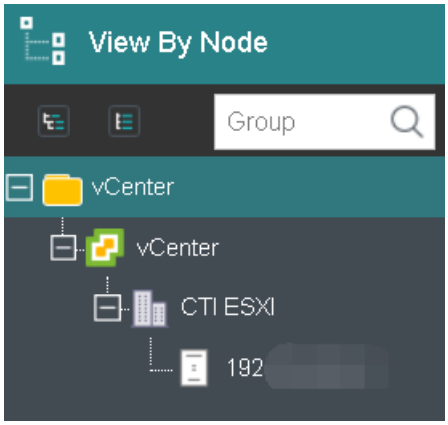
For details about alarm logs, refer to **2.6.4 Alarm** section.

2.2.2 Managing Virtual Machines in VMware vCenter

Navigate to **compute** and you will see a toolbar, as shown in the following figure. On the toolbar, there are the following items: **View By Group/Node/Datastore/Tag, Panel/List, Refresh, New, New Group, Select, Sort, Recycle Bin, Advanced**.

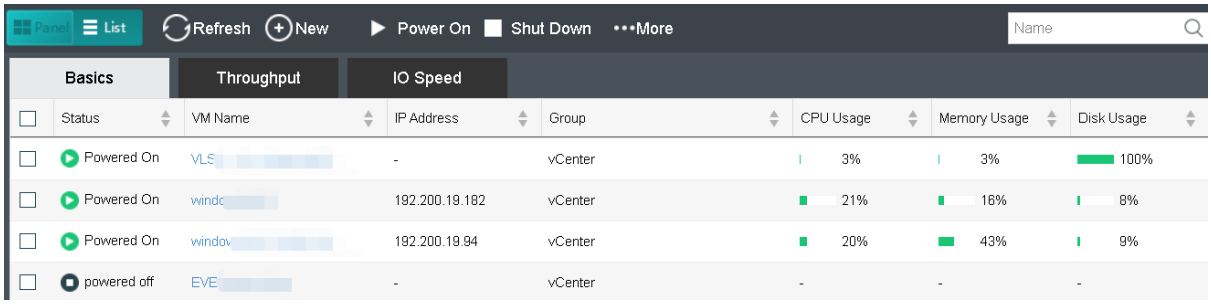


Virtual machines can be viewed by **Node,** as shown below:



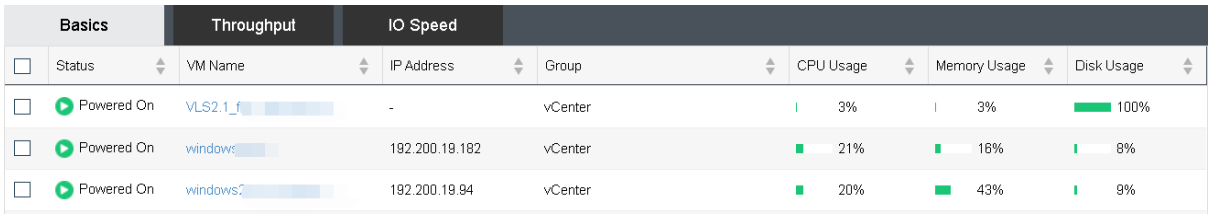
2.2.2.1 Viewing VMs by Panel or List

Virtual machines can be viewed by **Panel** or **List**. By default, virtual machines are displayed by **Panel**. To view VMs by **List,** click on **List,** as shown below:

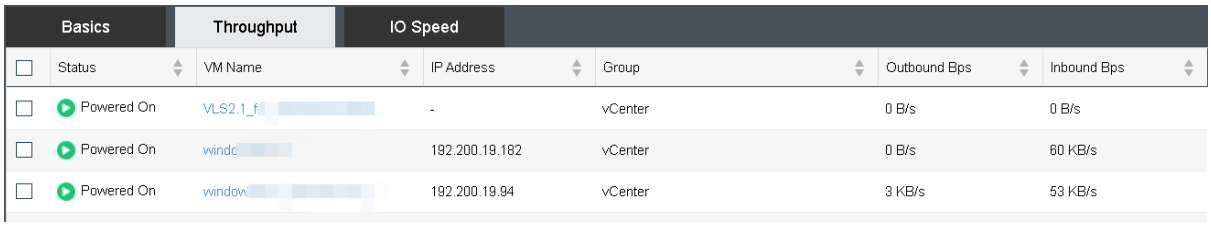


VM details are displayed, as shown below:

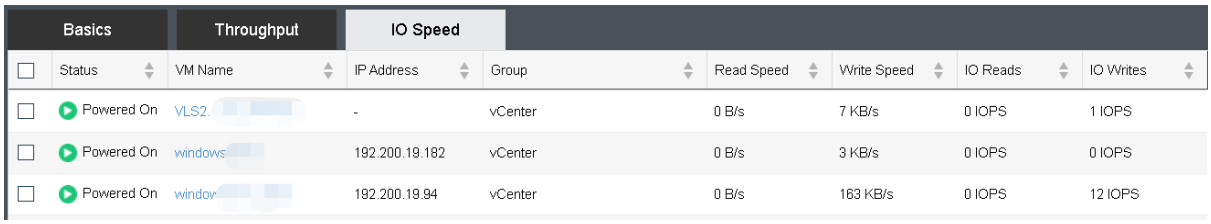
Basics: Displays basic information of virtual machines.



Throughput: Displays outbound and inbound speed.



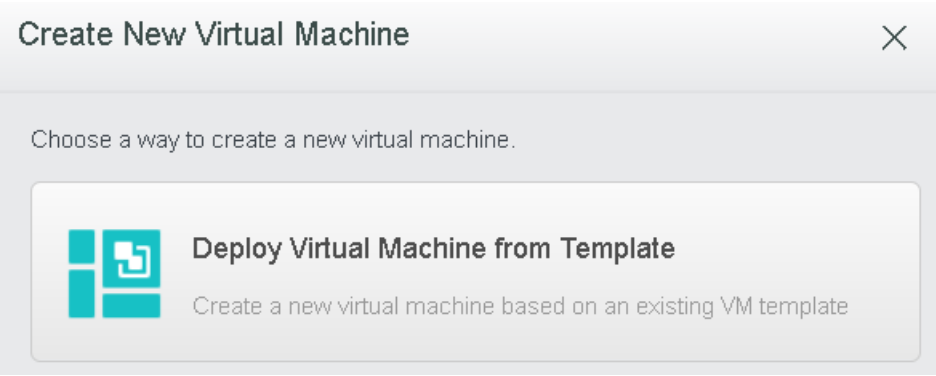
IO Speed: Displays IO speed.



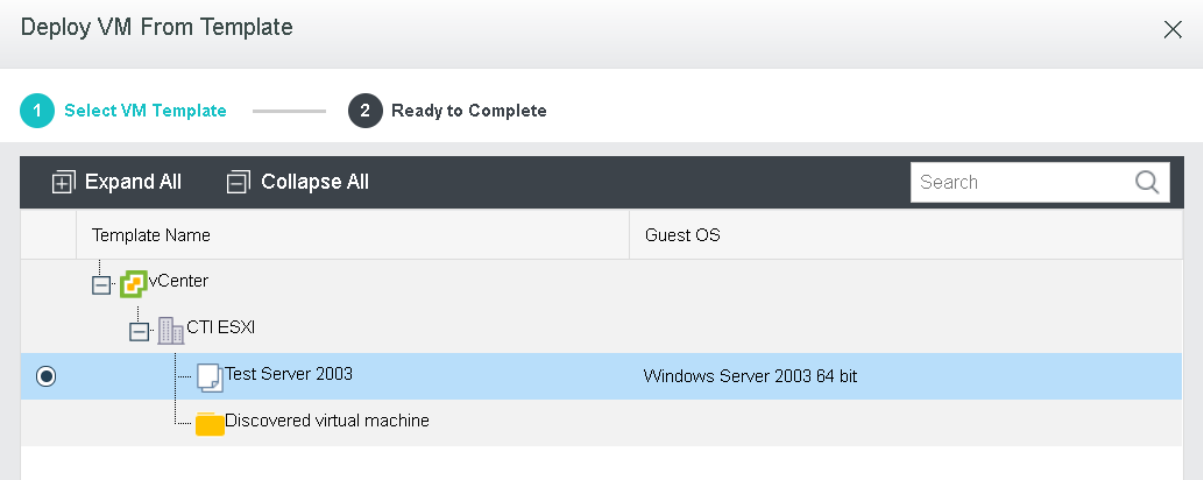
Creating New Virtual Machine

Click 

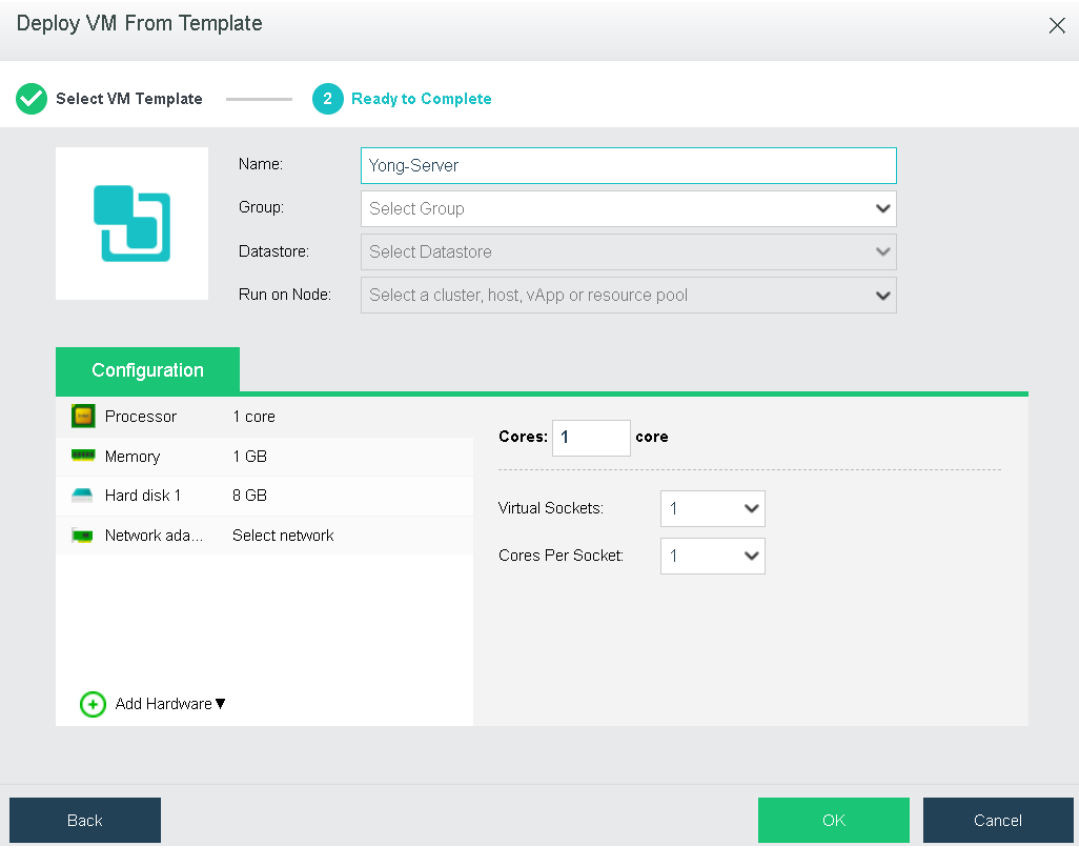
to deploy a new virtual machine from an existing VM template, as shown below:



Select a VM template and then configure relevant fields, as shown below:



Click Next, after the template is selected.



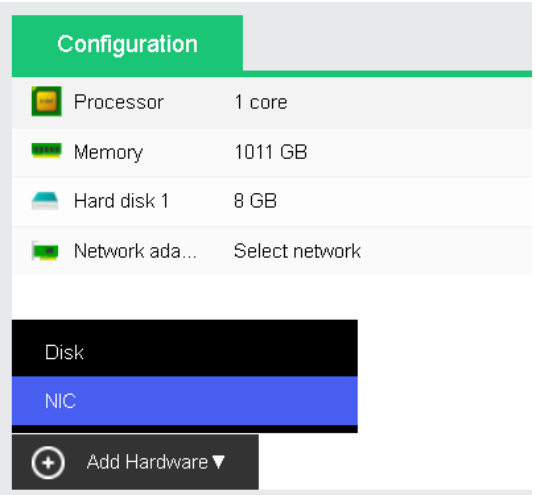
Name: Specifies a distinguishable name for the virtual machine.

Group: Specifies a group to which this virtual machine belongs.

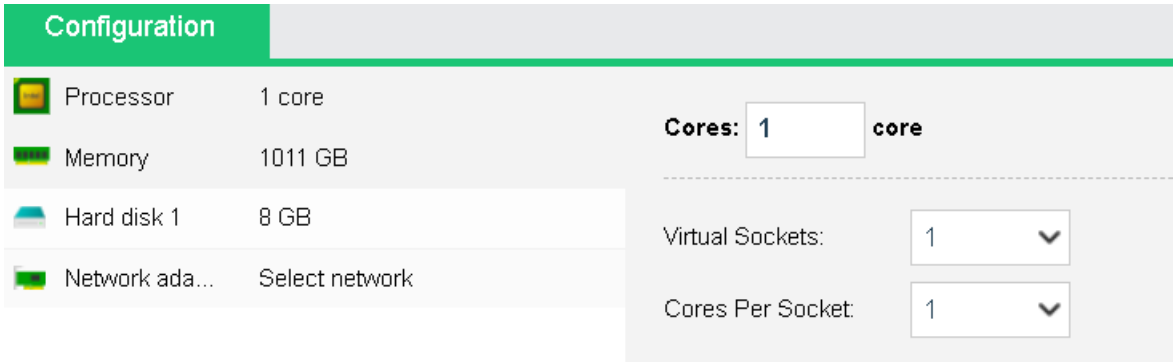
Run on Node: Specifies a node on which the virtual machine runs.

Datastore: Specifies a datastore where configuration files of deployed virtual machine is stored.

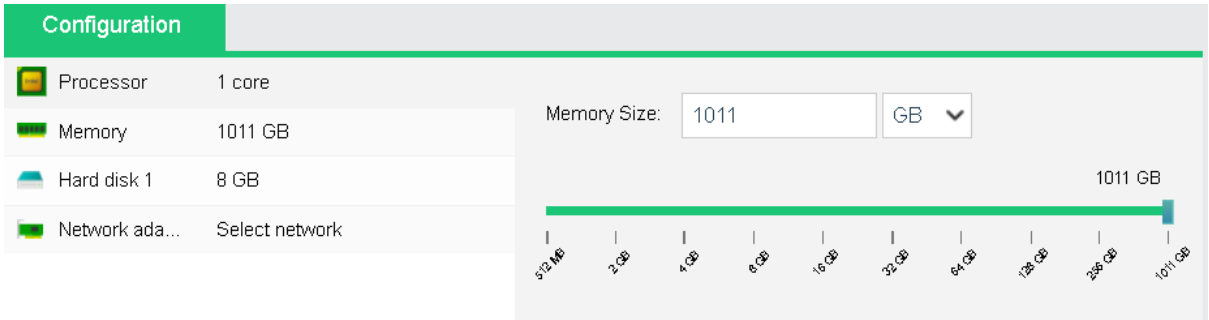
Configuration: It allows you to configure hardware resources, such as **Processor**, **Memory**, **Disk**, **CD/DVD** and **NIC**, etc.



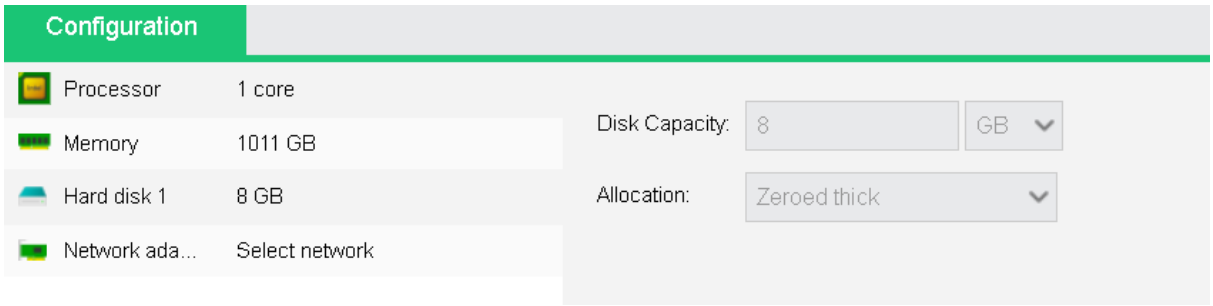
Processor: Specifies the number of virtual sockets and cores per socket for the virtual machine respectively. Once the numbe of cores is configured, Virtual Sockets and Cores Per Socket will be automatically filled with optimum values so as to achieve best VM performance.



Memory: Specifies the memory for the virtual machine. The minimum is 512 MB, and the maximum is 1TB.



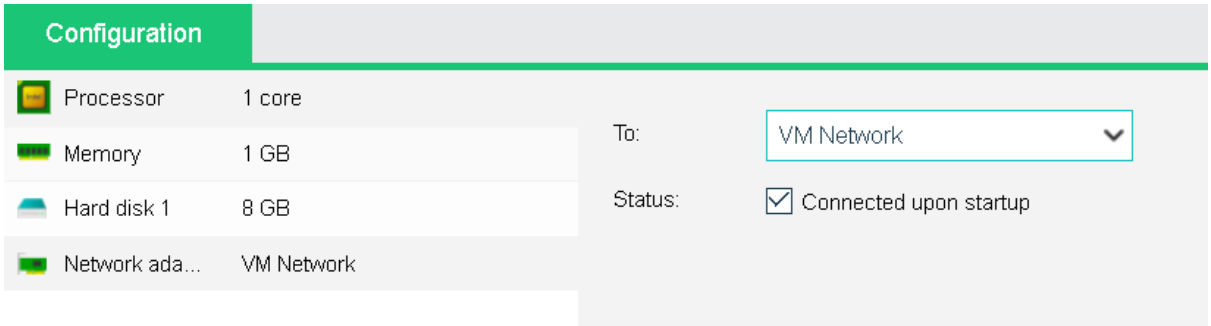
Disk: Specifies the disk for the virtual machine.



Disk Capacity: Specifies the capacity(GB) of the virtual disk.

Allocation: Options are **Thin Provisioning, Eager zeroed thick** and **Zeroed thick**.

Network adapter: Specifies what the virtual machine is connected to.

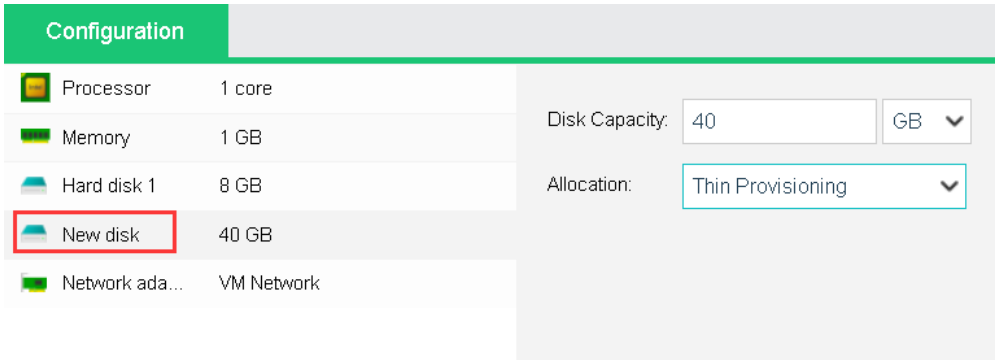


Connected To: Specifies an edge to be connected to the virtual machine.

Status: If it is selected, the VM will auto connect to the edge upon startup.

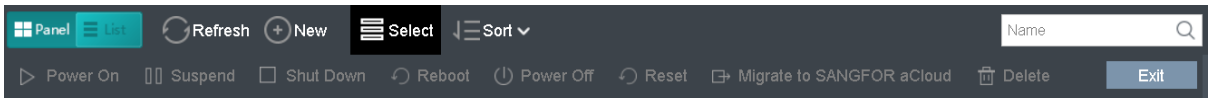
Add Hardware: To add more hardwares, click **Add Hardware**. Then, you can add new Disk and NIC.

For example, click **Add Hardware** and select **Disk**. Then, a new disk will be added(as shown in following figure). To delete a disk, click on the  icon.



Batch Operation

Administrator can perform the following operations against multiple virtual machines: **Power On, Suspend, Shut Down, Reboot, Power Off, Reset, Migrate to SANGFOR HCI, and Delete**.



To power on virtual machines(s), you may select one or more than one virtual machines and then and click on **Power On**.

To suspend virtual machines(s), you may select one or more than one virtual machines and then and click on **Suspend**.

To shut down virtual machine(s), you may select one or more virtual machines and then click on **Shut Down.**

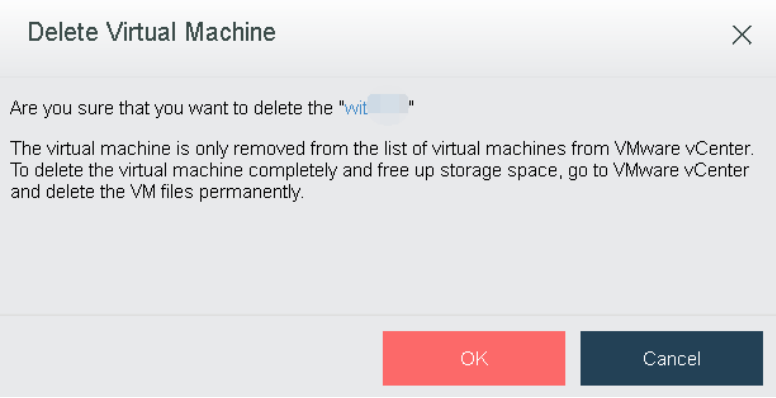
To start virtual machine(s), you may select one or more virtual machines and then click on **Reset**.

To power off virtual machine(s), you may select one or more virtual machines and then click on **Power Off**.

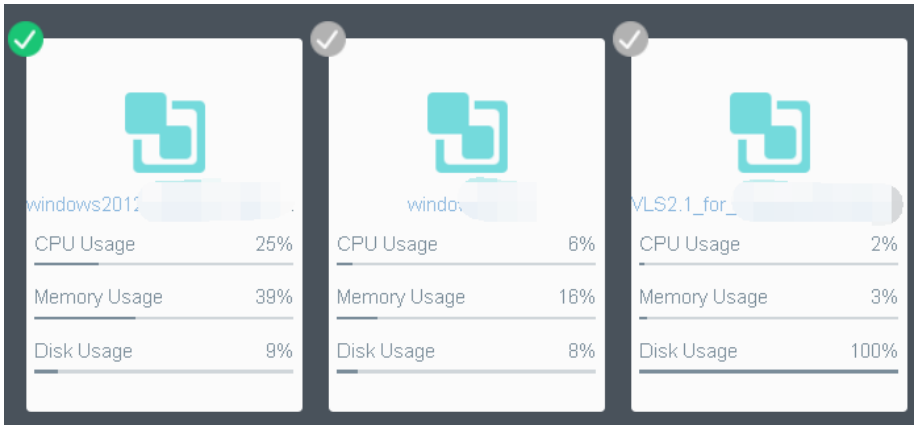
To restart virtual machine(s), you may select one or more virtual machines and then click on **Reboot**.

To migrate the virtual machine(s) to SANGFOR HCI, you may select one or more virtual machines and then click on **Migrate to SANGFOR HCI**.

To delete virtual machines, you may select the virtual machines and click **Delete,** then the virtual machine will be removed from the VMware vCenter yet the storage space occupied by the VM will not be freed up. You may go to VMware vCenter platform to clean up files of the virtual machine.



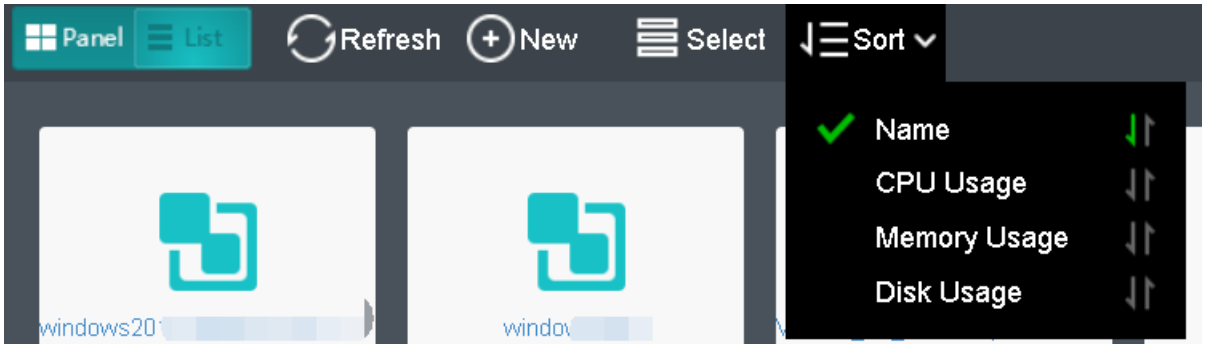
If a virtual machine is selected, the color of the icon at the upper left corner of the corresponding card will turn to green from gray.



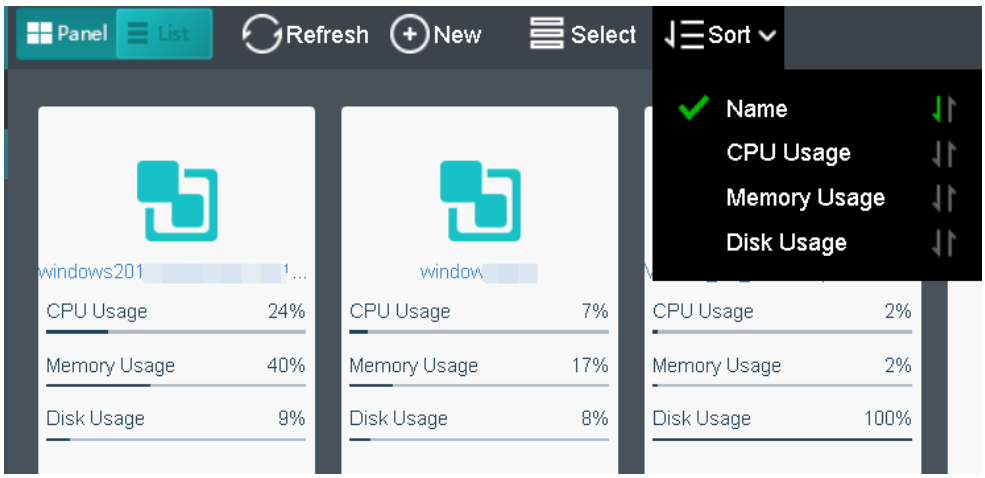
To exit from editing the virtual machines, click on the **Exit** button on the upper right corner.

2.2.2.4 Sorting Virtual Machines

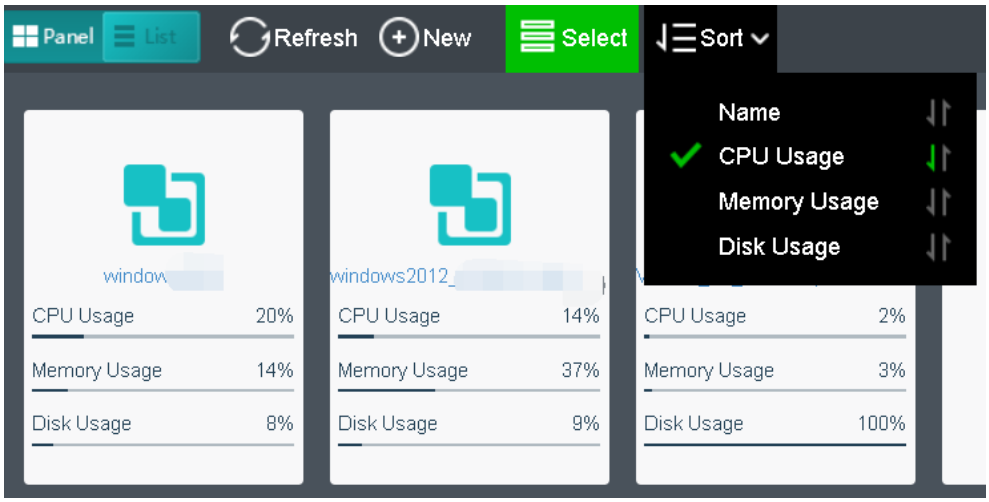
Virtual machines can be sorted by **Name, CPU Usage, Memory Usage, Disk Usage**.



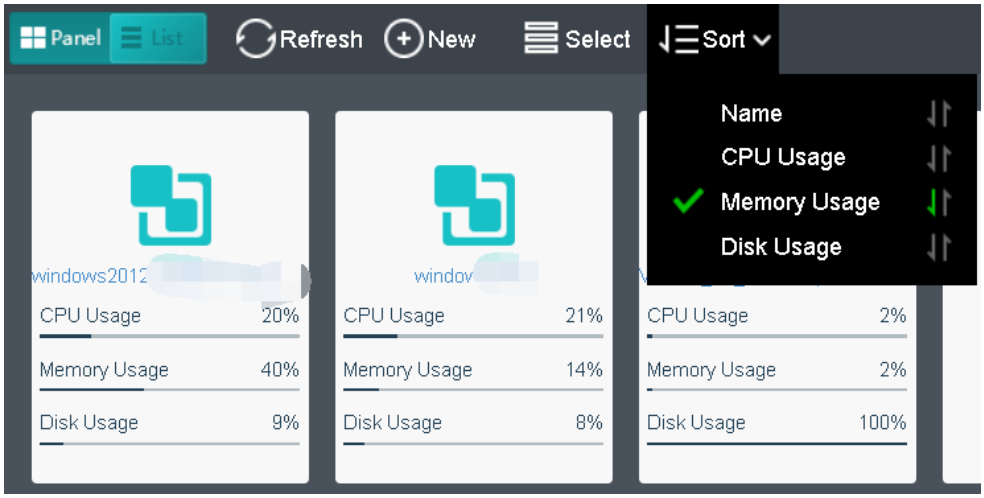
To sort virtual machines by name, select **Sort > Name** in **Compute**. You may click on the arrow  to sort VMs in ascending or descending order.



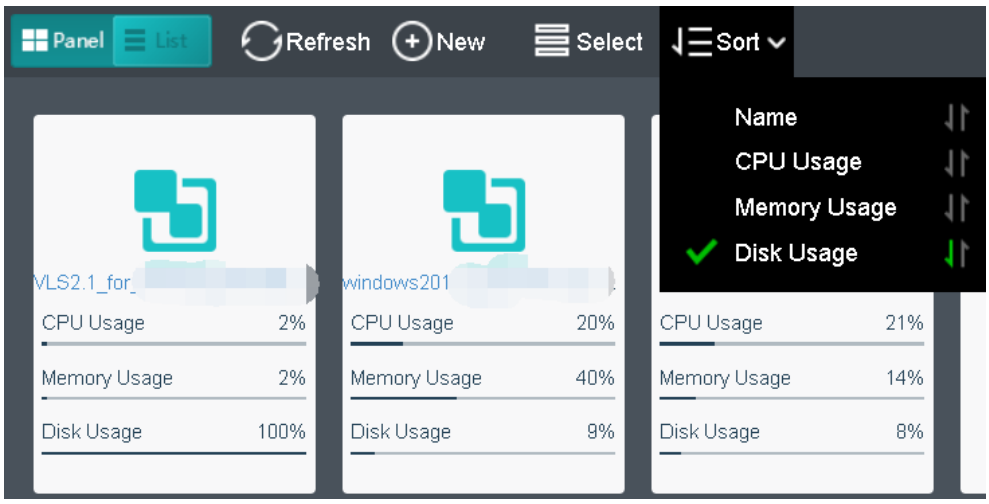
To sort virtual machines by CPU usage, select **Sort > CPU Usage** in **Compute**. By clicking on that arrow, virtual machines can be sorted based on CPU usage in ascending order or descending order. The following figure shows that the virtual machines are sorted by CPU usage in a descending order.



To sort nodes by memory usage, select **Sort > Memory Usage**. By clicking on that arrow, node can be sorted by memory usage in ascending order or descending order. The following figure shows that the virtual machines are sorted by memory usage in a descending order.

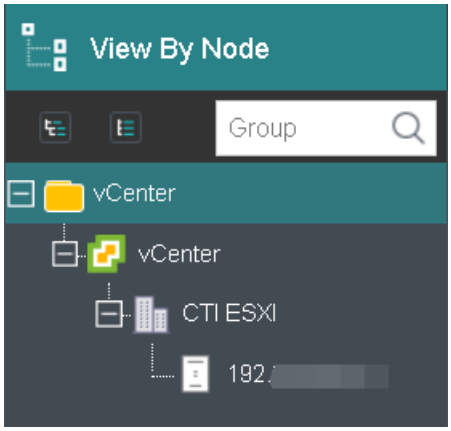


To sort virtual machines by disk usage, select **Sort > Disk Usage** in **Compute**. By clicking on that arrow, virtual machines can be sorted by disk usage in ascending or descending order. The following figure shows that the virtual machines are sorted by disk usage in a descending order.

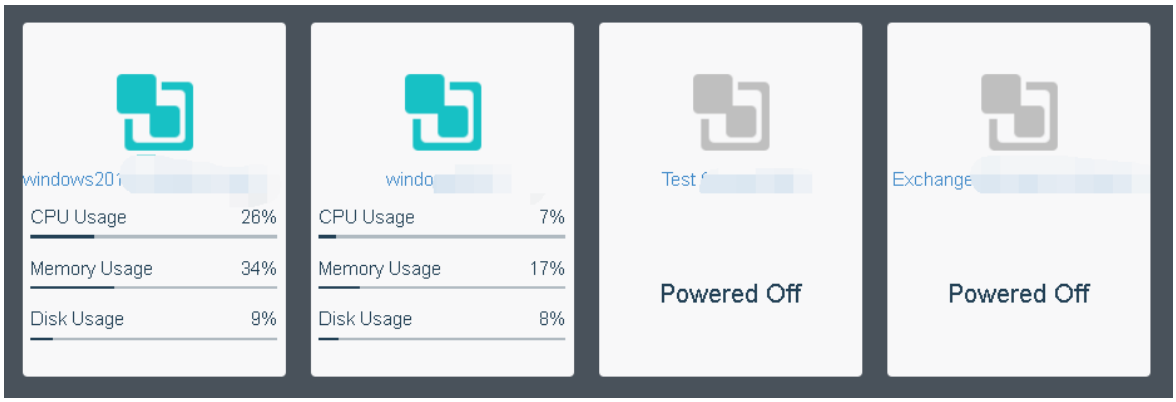


2.2.2.5 Viewing VM Status

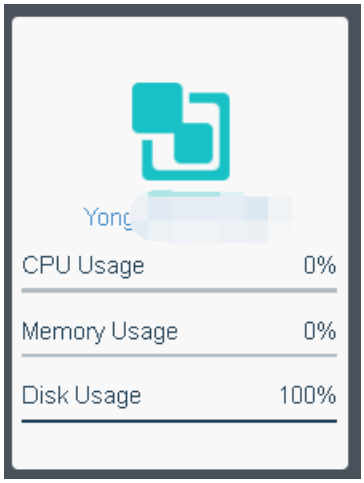
In **Compute**, all VM groups can be expanded or collapsed by clicking on the  button. To expand or collapse a specific group, click on the  button next to that group.



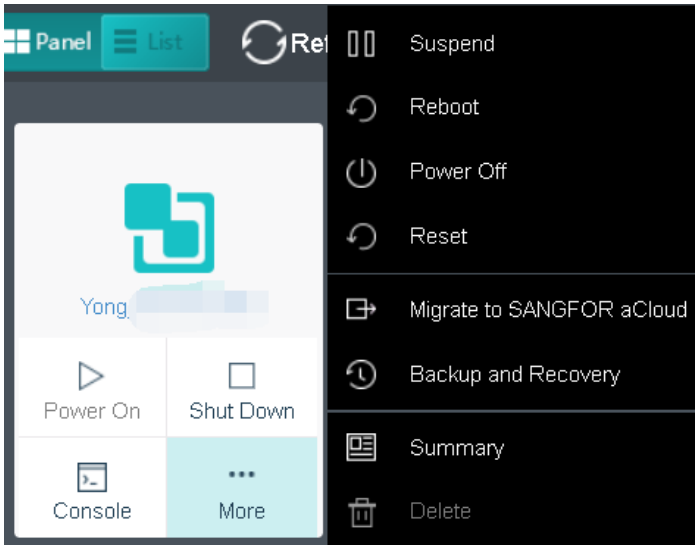
You can get the following information on virtual machine panel: power status(powered on or powered off), CPU, memory and disk usage. Blue VM icon indicates virtual machine is powered on, while gray VM icon indicates virtual machine is powered off.



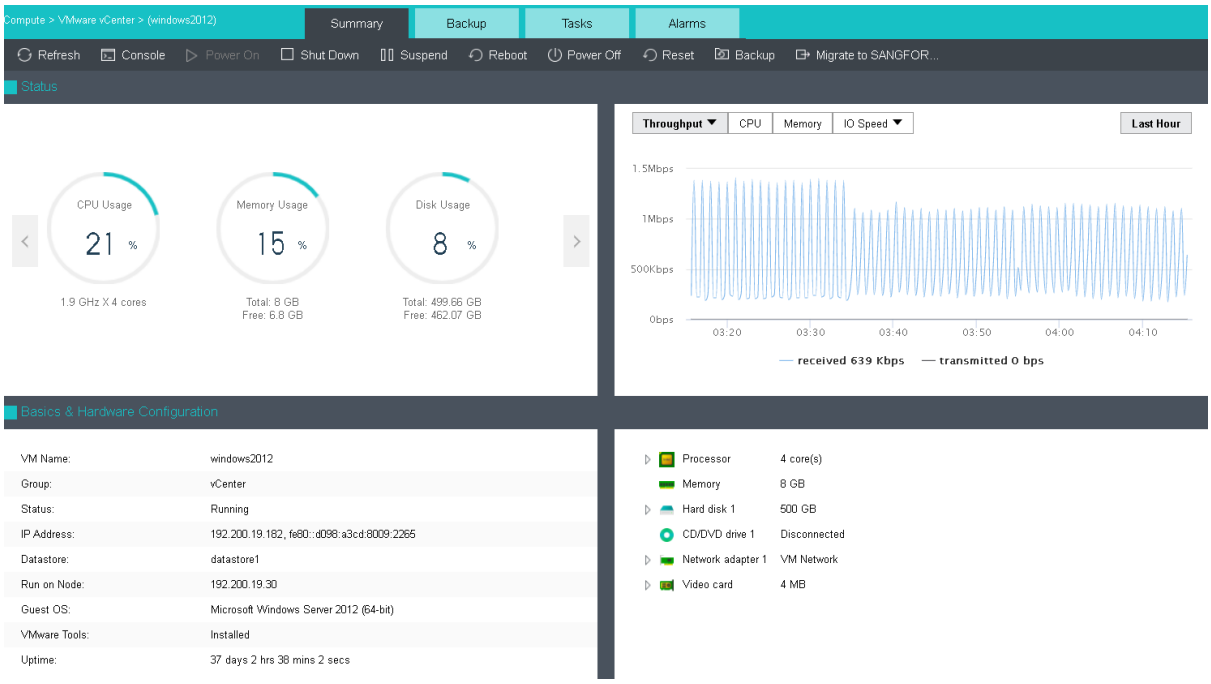
Move the cursor onto VM panel and the following buttons will appear on that card, as shown in the following figure:



To perform more operation against virtual machine, click **More**, as shown below:



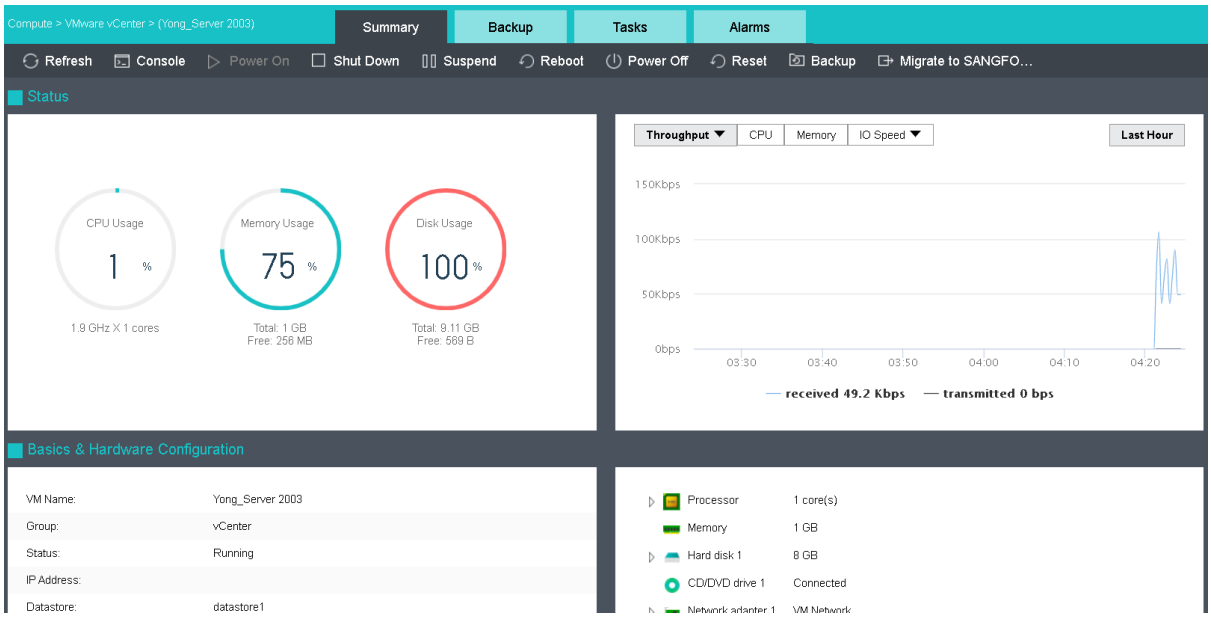
For virtual machine details, you may click on VM name to redirect to the **Summary** page, as shown below:



2.2.2.6 Viewing VM Details

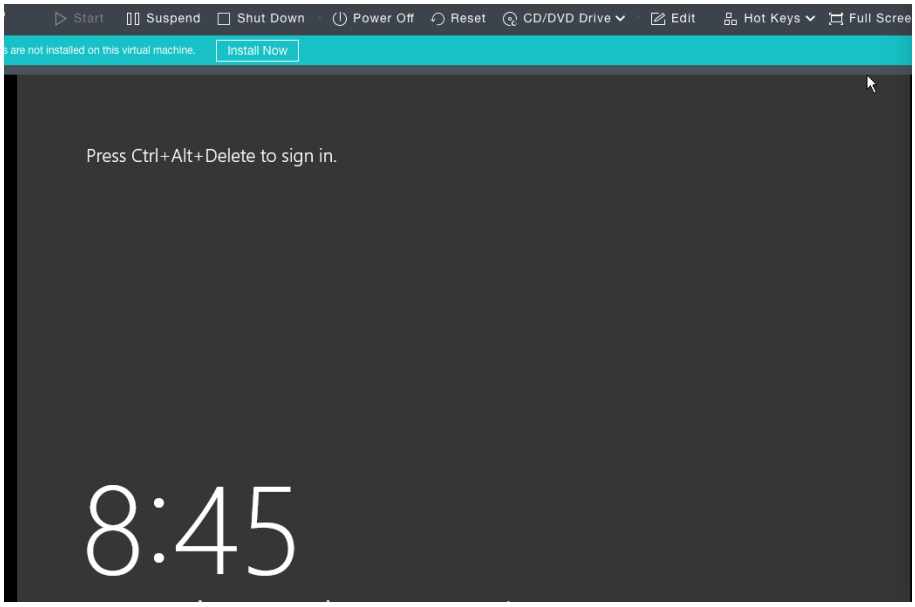
There are the following tabs: **Summary, Snapshot, Backup/CDP, Permissions, Tasks** and **Alarms,** as shown below.

On the **Summary** tab, you may perform such operations as **Power On**, **Shut Down**, etc., and view basic information and hardware configurations of virtual machine.



To refresh the **Summary** page, click on **Refresh** on the upper left corner.

To open virtual machine's console, click **Console** on the **Summary** page, or click on the **Console** button on the virtual machine panel to enter the following page. Before opening VMware vCenter administrator console, make sure the console plug-in has been installed, as shown below:



Click  to send Ctrl+Alt+Delete command to guest OS.

Click  to enter full screen, and press Ctrl+Alt+Enter to exit from full screen.

To power on virtual machine, you may click **Power On**.

To shut down virtual machine, you may click **Shut Down**.

To suspend virtual machine, you may click **Suspend**.

To restart a virtual machine, you may click **Reeboot**.

When a virtual machine is in powered-on state, you can click **Power Off** to force it to be powered off.

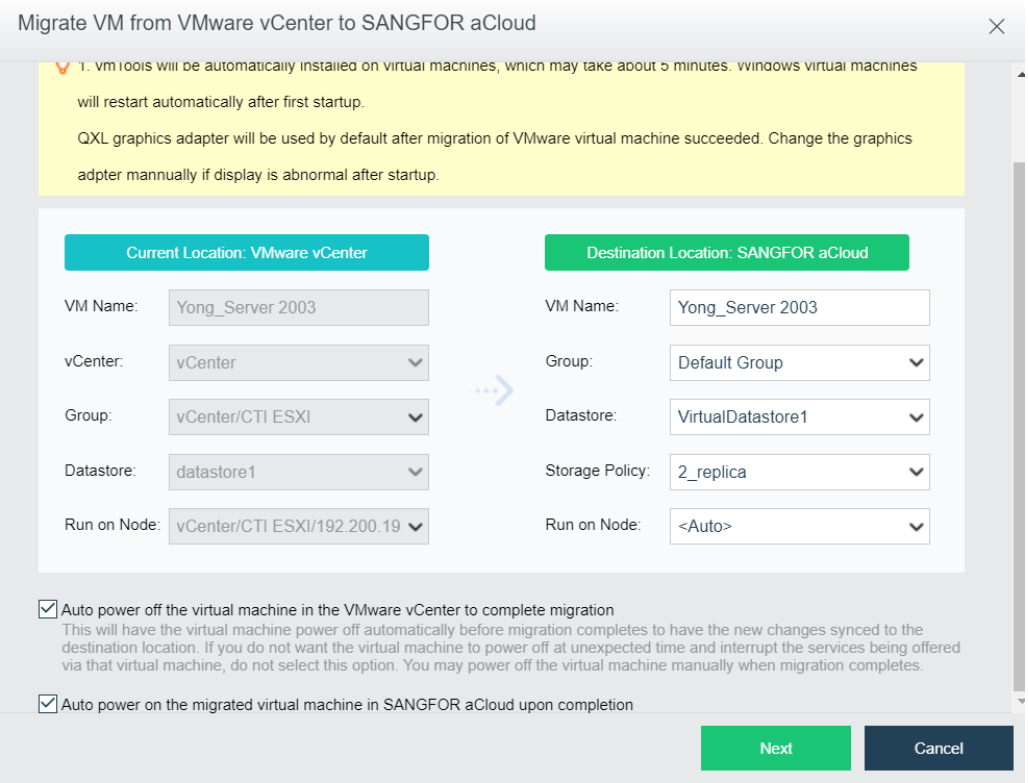
To restart virtual machine, you may click **Reset.**

To back up virtual machine, you may click **Backup**.

To migrate the VM, you may click **Migrate to SANGFOR HCI.**

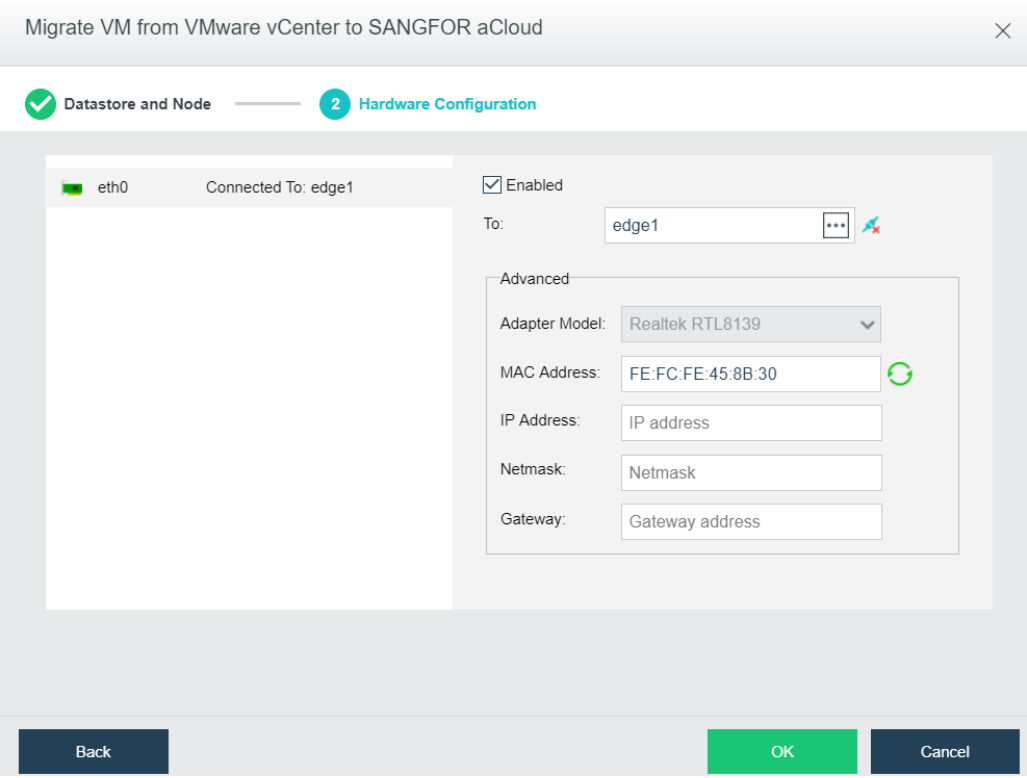
2.2.2.7 Migrating VM From Vmware vCenter to Sangfor HCI

Virtual machines running on VMware vCenter can be migrated to Sangfor HCI.



Specify the required fields under **Current Location** and **Destination Location**. Whether to select the options **Auto power off the virtual machine in the VMware vCenter to complete migration** and **Auto power on the migrated virtual machine in Sangfor HCI upon completion** depends on your own needs, and then start migrating virtual machine.

Auto power-off virtual machines in the VMware vCenter to complete migration: This will have the virtual machine powered off automatically before migration completes to have the new changes synced to the destination location. If you do not want the virtual machine to power off at unexpected time and interrupt the services being offered via that virtual machine, do not select this option. You may power off the virtual machine manually when migration completes.



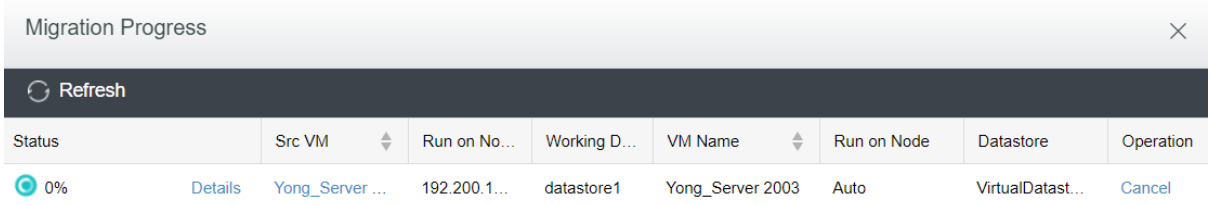
Enabled: If it is selected, it indicates that the specified virtual network adapter is enabled.

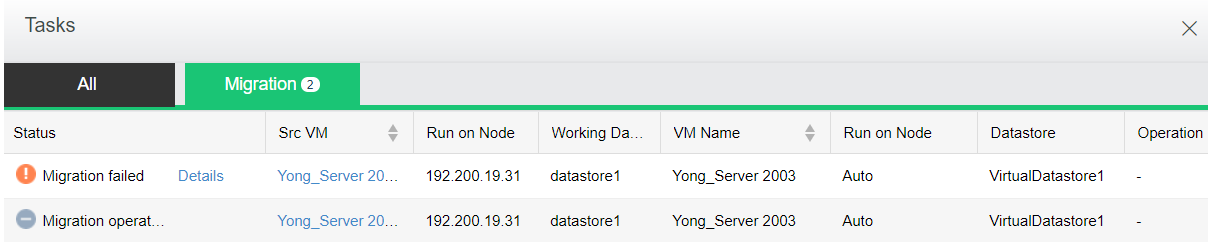
Connected To: Specifies an edge or a virtual switch to be connected to the virtual machine.

Adapter Model: Specifies the adapter model. Options are **Realtek RTL8139** and **Intel E1000**.

MAC Address: MAC address can be automatically generated or manually specified. MAC address examples: 00-11-22-33-44-55, 00:11:22:33:44:55. MAC address will be changed after the migration operation completes and you may edit the MAC address if you do not want the MAC address to be changed.

After configuring relevant fields, click **OK** to start migrating virtual machine. To view migration progress, go to **Migration Process**, as shown below:

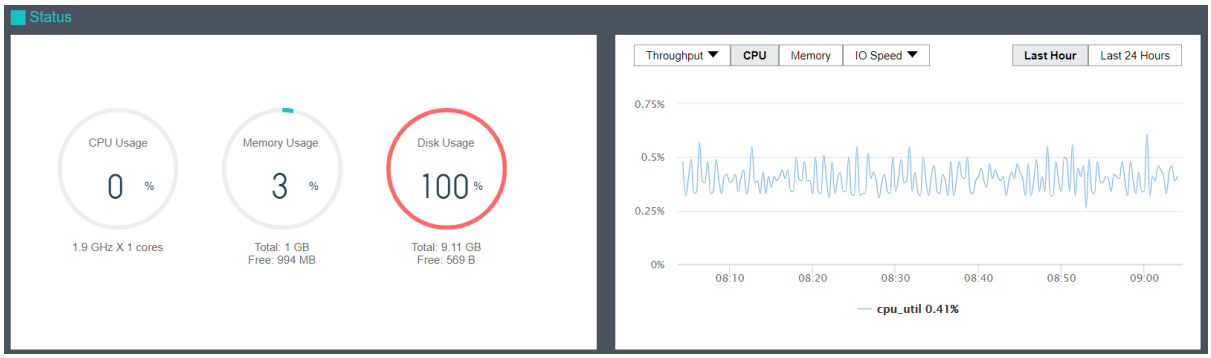




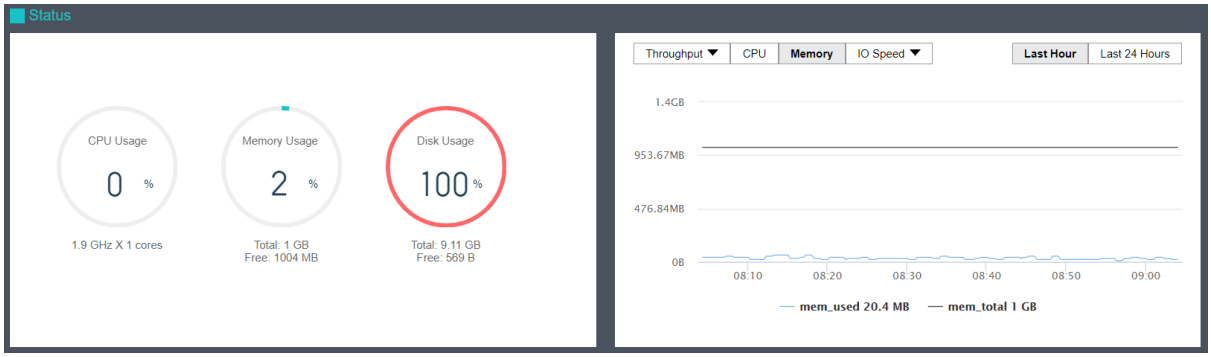
When migration is being performed on a virtual machine in VMware vCenter, do not power on the VM, expand disk capacity, or roll back snapshot of that virtual machine, or else migration may fail.

Status: Displays the following information about virtual machine: **CPU Usage, Memory Usage, Disk Usage, Throughput, CPU,** Memory, **IO Speed, IOPS**.

CPU Usage: Displays CPU usage of virtual machine. On the right side, you may view CPU usage in the last hour or last 24 hours.

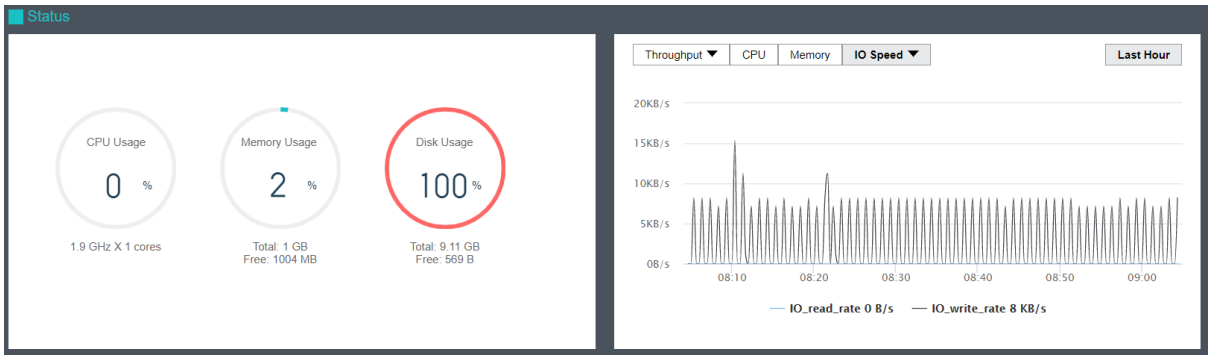


Memory Usage: Displays the total and free memory size respectively, as well as memory usage. On the right side, you may view memory usage in the last hour or last 24 hours.

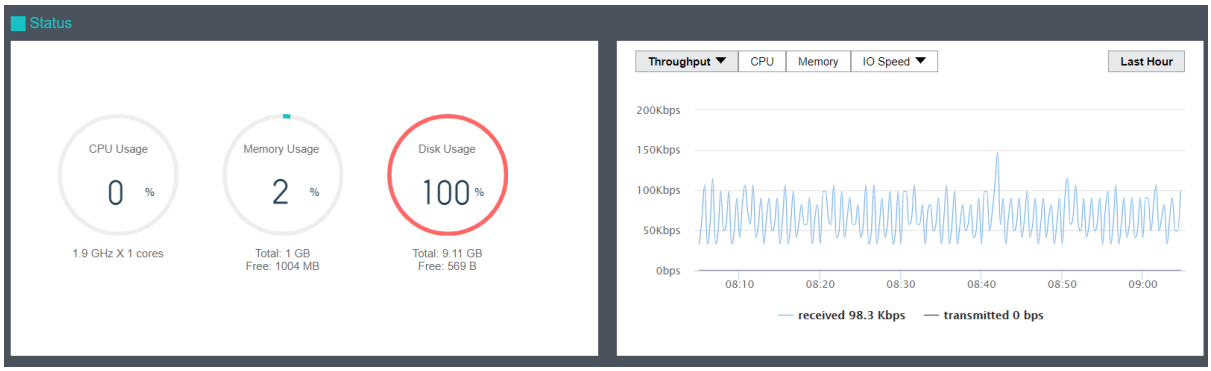


Disk Usage: Displays the total and free disk size respectively, as well as disk usage. On the

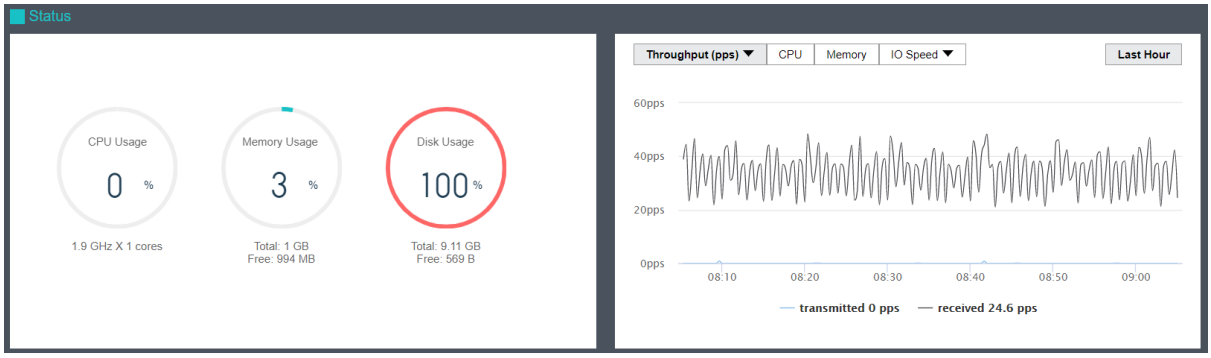
right side, you may view disk IO speed and IOPS.



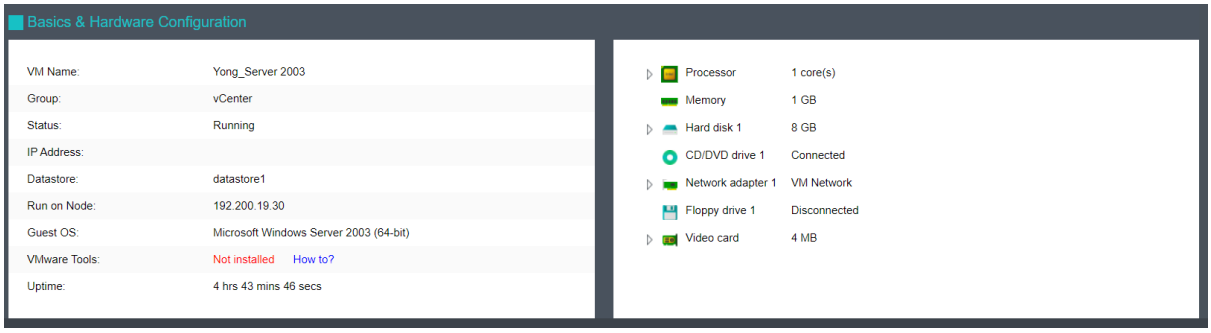
Throughput: Displays overall throughput.



Throughput (pps): Displays inbound and outbound packets per second.

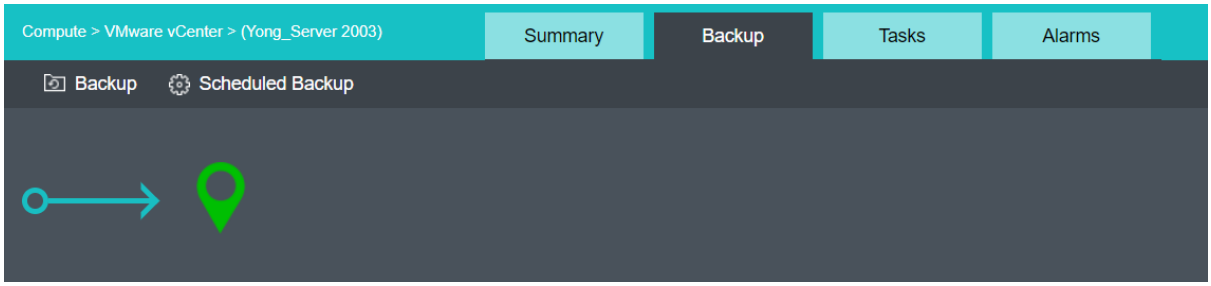


The **Basics & Hardware Configuration** section displays basic information and hardware configuration of virtual machine. Basic information includes **Name**, Description, **Group**, **Datastore**, **Run on Node**, **Guest OS**, **vmTools**, **High Priority**, **Power on at host startup**, **Enable memory reclaiming**, **Boot Order**, and **Uptime**.



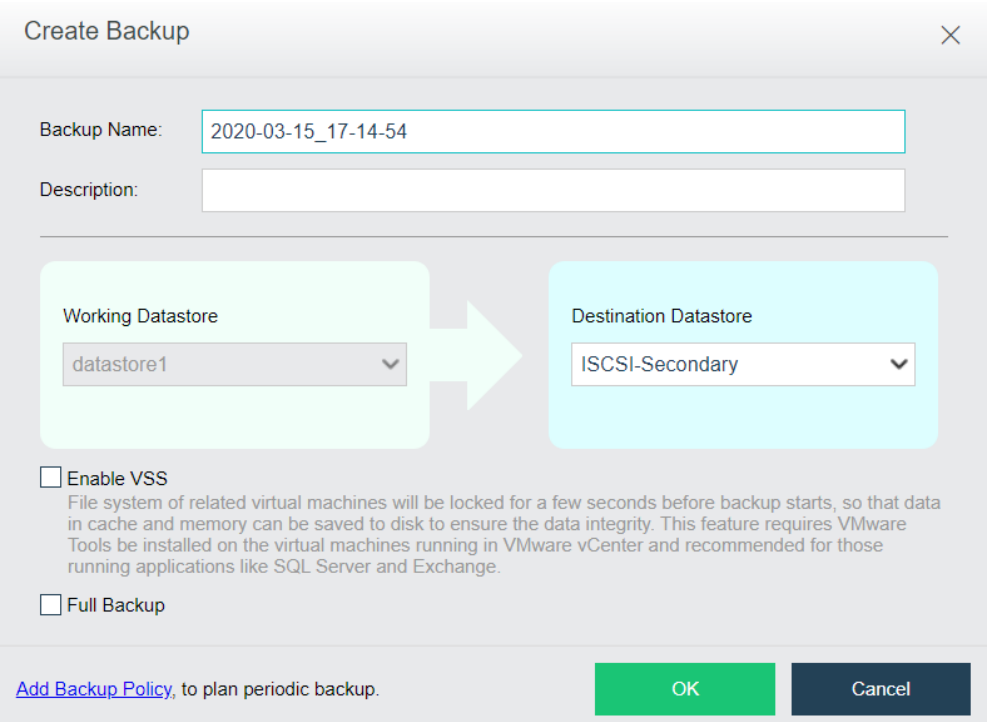
2.2.2.8 VM Backup

Virtual machines in VMware vCenter can be backed up to Sangfor HCI platform without installing any third-party software or plugin or purchasing any backup storage device. Additionally, virtual machines can be recovered on Sangfor HCI from backup or recovered to VMware vCenter.



2.2.2.8.1 Manual Backup

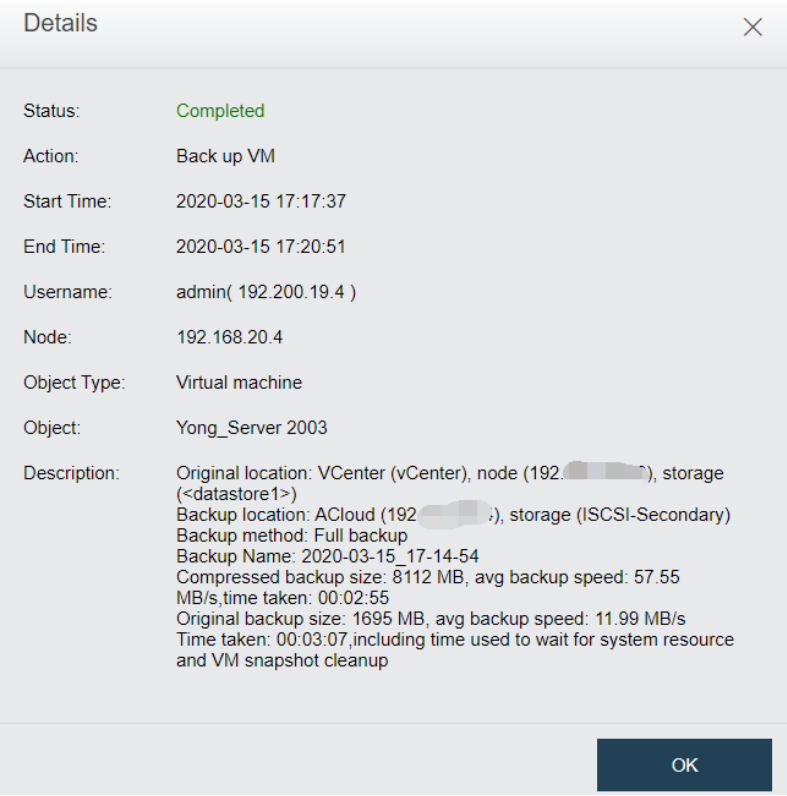
On the **Backup** page, you may back up virtual machine manually or have virtual machine backed up automatically. To back up virtual machine manually, you may click **Backup**.



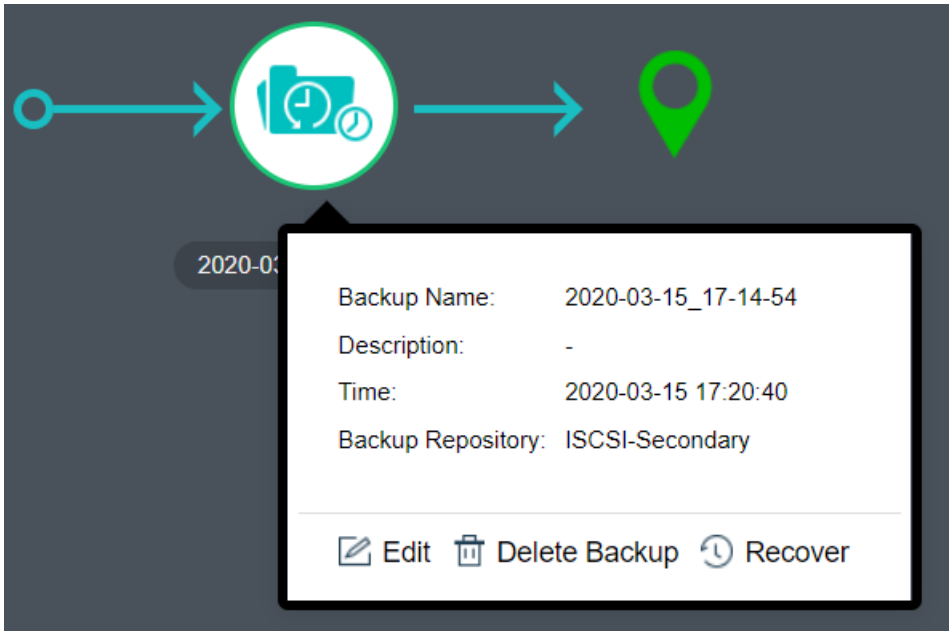
Specify **Backup Name, Description** and **Destination Datastore**. Then, click **OK**. You may select **Enable VSS** and **Full Backup** based on your own needs.

Enable VSS: File system of related virtual machines will be locked for a few seconds before backup starts, so that data in cache and memory can be saved to disk to ensure the data integrity. This feature requires VMware Tools to be installed on the virtual machines running in VMware vCenter and is recommended for those running applications like SQL Server and Exchange.

After specifying relevant fields, click **OK** to start backup operation. You may view backup status in **Tasks**, as shown below:



After a backup is created, you may click on the backup name and then a dialog box pops up, as shown below:



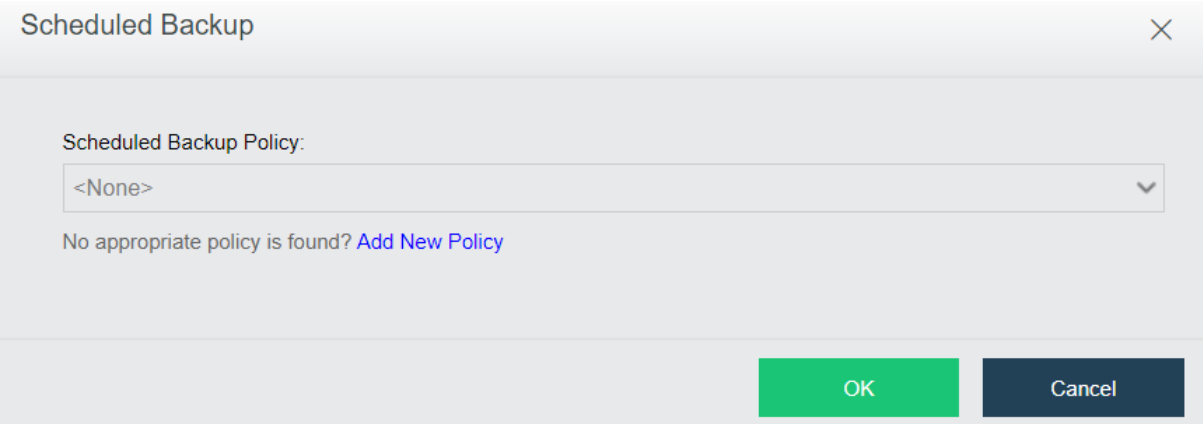
To modify backup name and description, you may click **Edit**.

To delete a backup, you may click **Delete Backup**.

To recover a virtual machine from its backup, you may click **Recover**.

2.2.2.8.2 Scheduled Backup

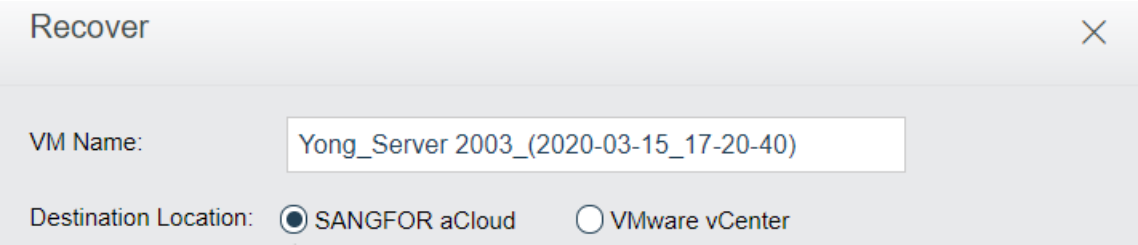
On the **Backup** page, you may also create a scheduled backup by clicking **Scheduled Backup** to enter the following page. On that page, select the option **Enable Scheduled Backup** and select a scheduled backup policy, then click **OK**. You may click **Add New Policy**, if there is no schedule backup policy.



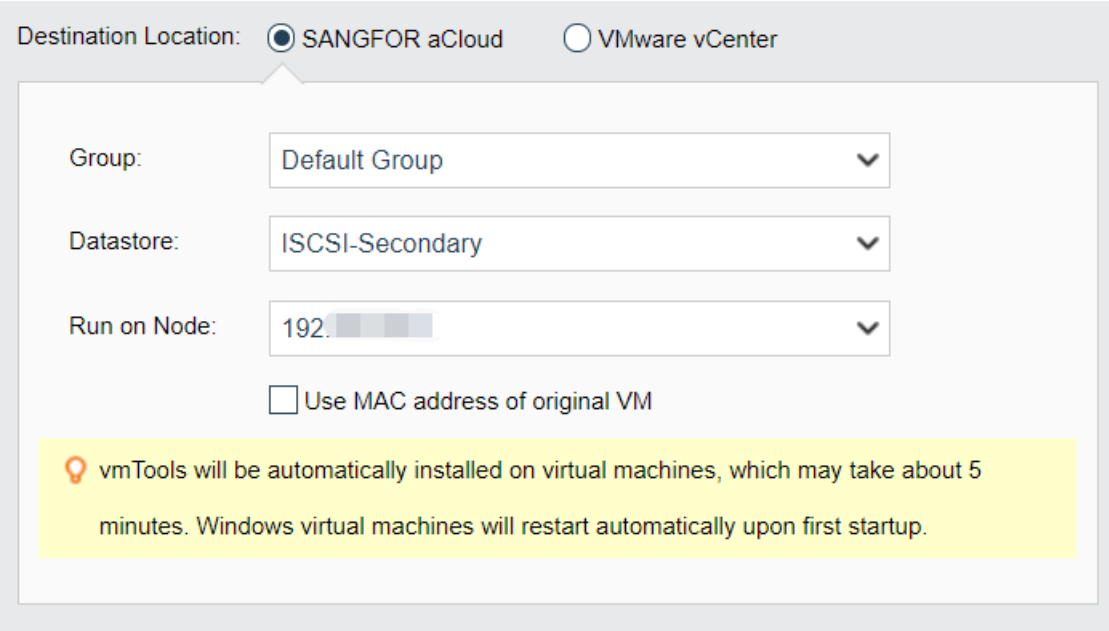
For details about scheduled backup, refer to Error! Reference source not found. section.

2.2.2.9 VM Recovery

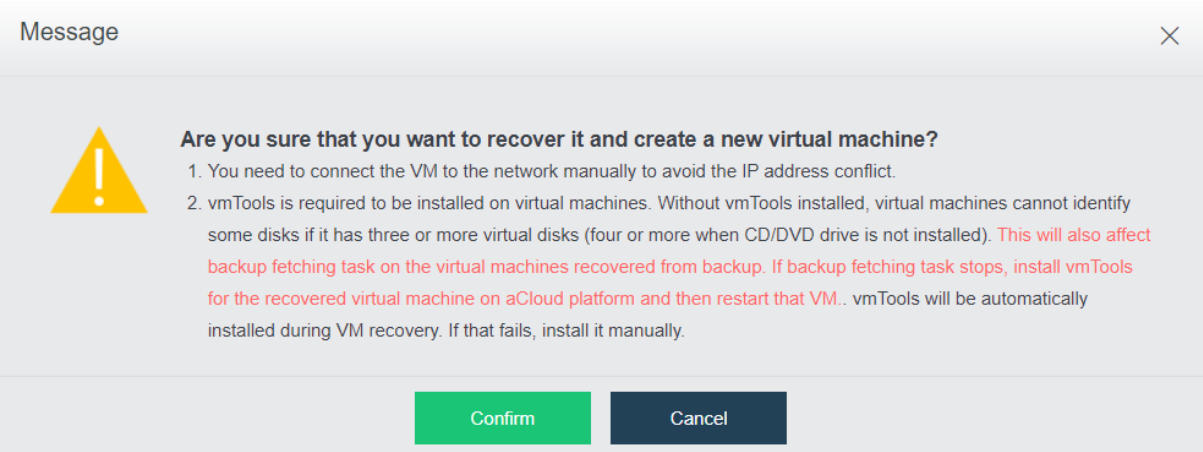
Virtual machines in VMware vCenter can be recovered on Sangfor HCI platform or recovered to VMware vCenter. Enter the name of the virtual machine and select destination location, as shown below:



To recover virtual machine to Sangfor HCI, select Sangfor HCI as **Destination Location**, as shown below:



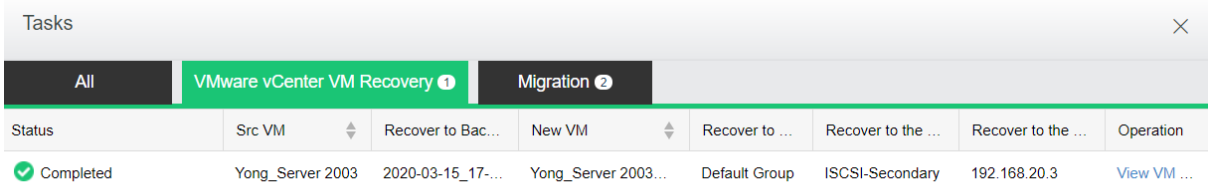
Specify **Group, Run on Node** and **Datastore,** click **OK,** and then a new virtual machine will be created.



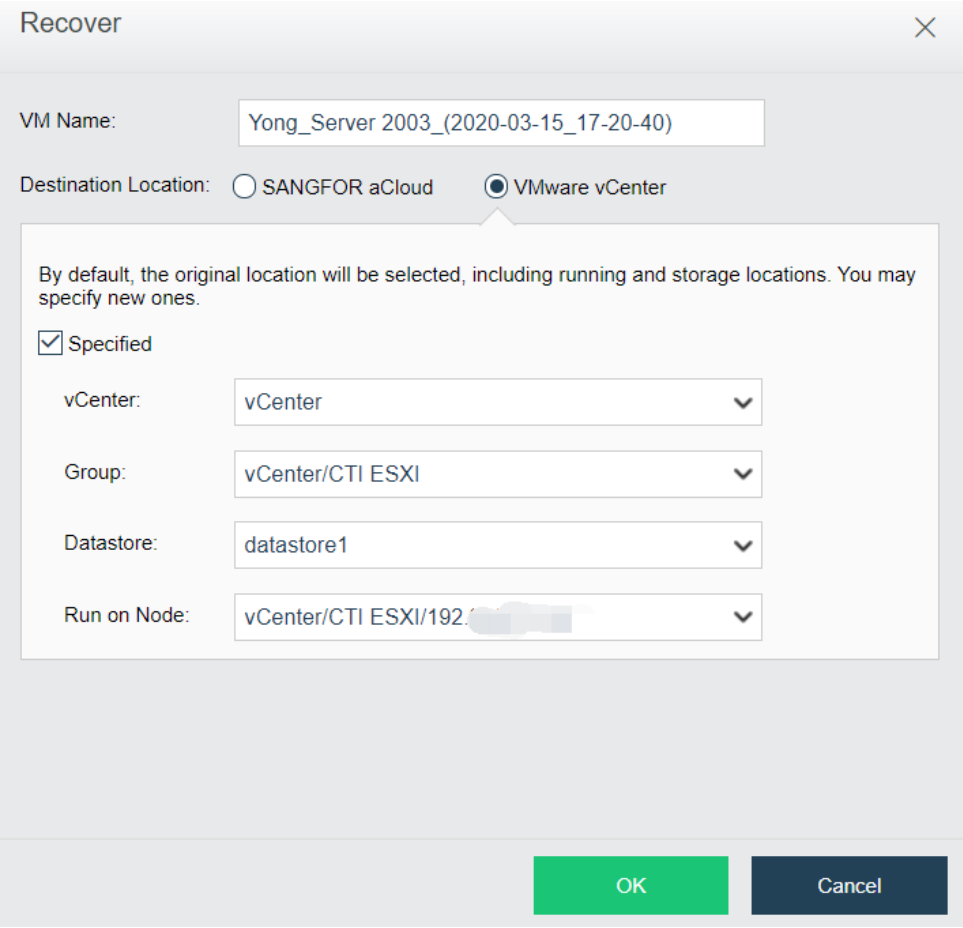
- You need to connect the VM to the network manually to avoid the IP address conflict.
- Install vmTools on the recovered virtual machine to support IP address restoration and improve performance of virtual machine, otherwise, some disks will not be identified if

virtual machine has three or more virtual disks.

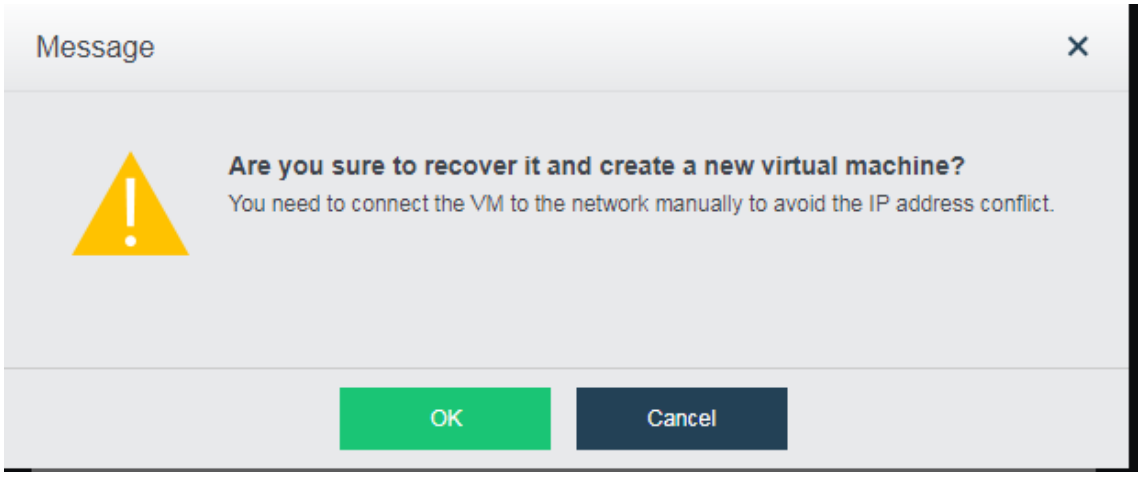
You may view recovery progress in **Tasks**.



Recover virtual machine to VMware vCenter, as shown below:



Specify **vCenter**, **Group**, **Run** on **Node** and **Datastore**, click **OK**, and then a new virtual machine will be created. You may view recovery progress in **Tasks**.

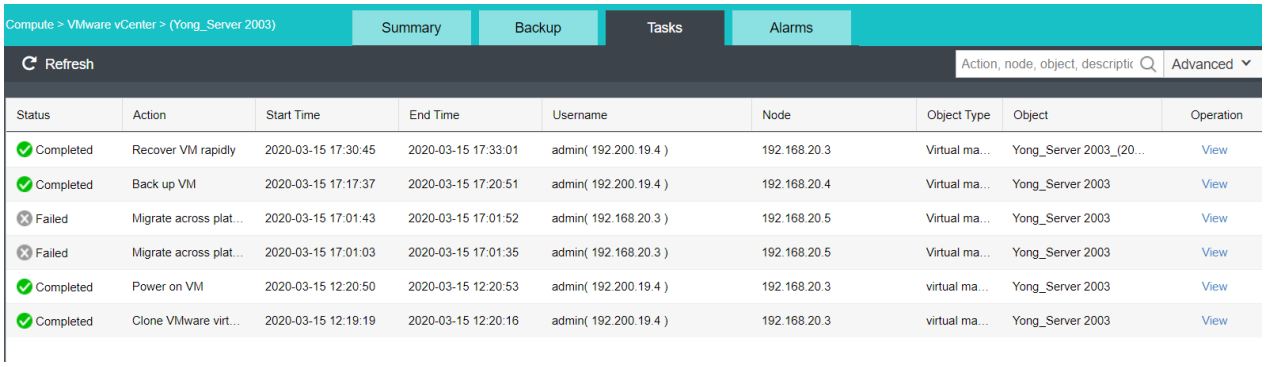


By default, the original location will be selected, including running and storage locations. You may specify new ones.

You need to connect the VM to the network manually to avoid the IP address conflict.

2.2.2.10 Viewing Tasks

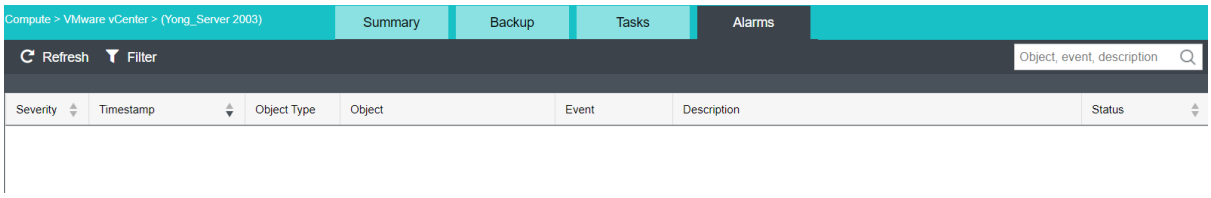
The **Tasks** page displays administrator logs about various operations performed by administrator, such as creating a virtual machine, etc. Each log contains the following information: **Status, Action, Start Time, End Time, Username, Node, Object Type, Object** and **Operation**. To view log details, click **View** in **Operation** column.



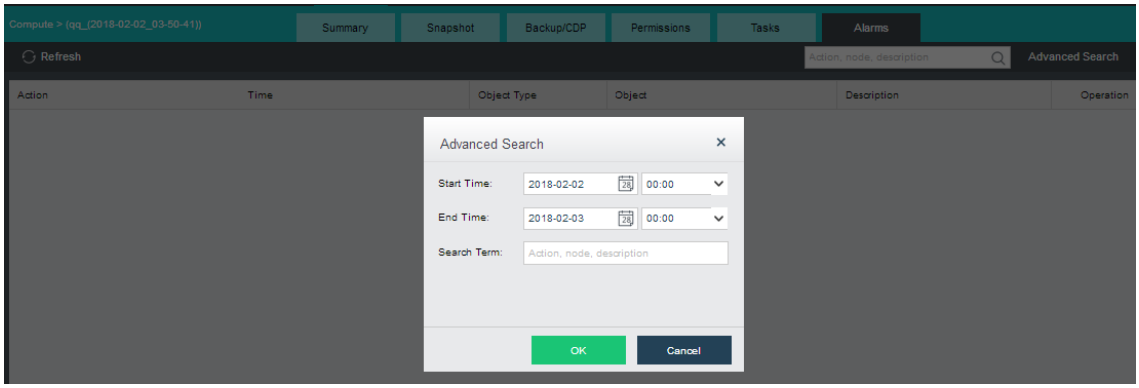
Status	Action	Start Time	End Time	Username	Node	Object Type	Object	Operation
Completed	Recover VM rapidly	2020-03-15 17:30:45	2020-03-15 17:33:01	admin(192.200.19.4)	192.168.20.3	Virtual ma...	Yong_Server 2003_(20...	View
Completed	Back up VM	2020-03-15 17:17:37	2020-03-15 17:20:51	admin(192.200.19.4)	192.168.20.4	Virtual ma...	Yong_Server 2003	View
Failed	Migrate across plat...	2020-03-15 17:01:43	2020-03-15 17:01:52	admin(192.168.20.3)	192.168.20.5	Virtual ma...	Yong_Server 2003	View
Failed	Migrate across plat...	2020-03-15 17:01:03	2020-03-15 17:01:35	admin(192.168.20.3)	192.168.20.5	Virtual ma...	Yong_Server 2003	View
Completed	Power on VM	2020-03-15 12:20:50	2020-03-15 12:20:53	admin(192.200.19.4)	192.168.20.3	virtual ma...	Yong_Server 2003	View
Completed	Clone VMware virt...	2020-03-15 12:19:19	2020-03-15 12:20:16	admin(192.200.19.4)	192.168.20.3	virtual ma...	Yong_Server 2003	View

2.2.2.11 Viewing Alerts

On the **Alarms** page, you can view alarm logs. For instance, an alarm log records that VM CPU usage is above threshold, etc. When an alarm-triggering threshold is reached, a corresponding alarm will be triggered and an alarm log will be generated. An alarm log includes the following information: **Action**, **Time**, **Object**, **Object Type**, **Description** and **Status**. To view details of an alarm log, click **View** in **Operation** column.



Alarm logs can be searched by action, node, object and description. By clicking **Filter**, you may also specify a period of time and search term to filter logs.

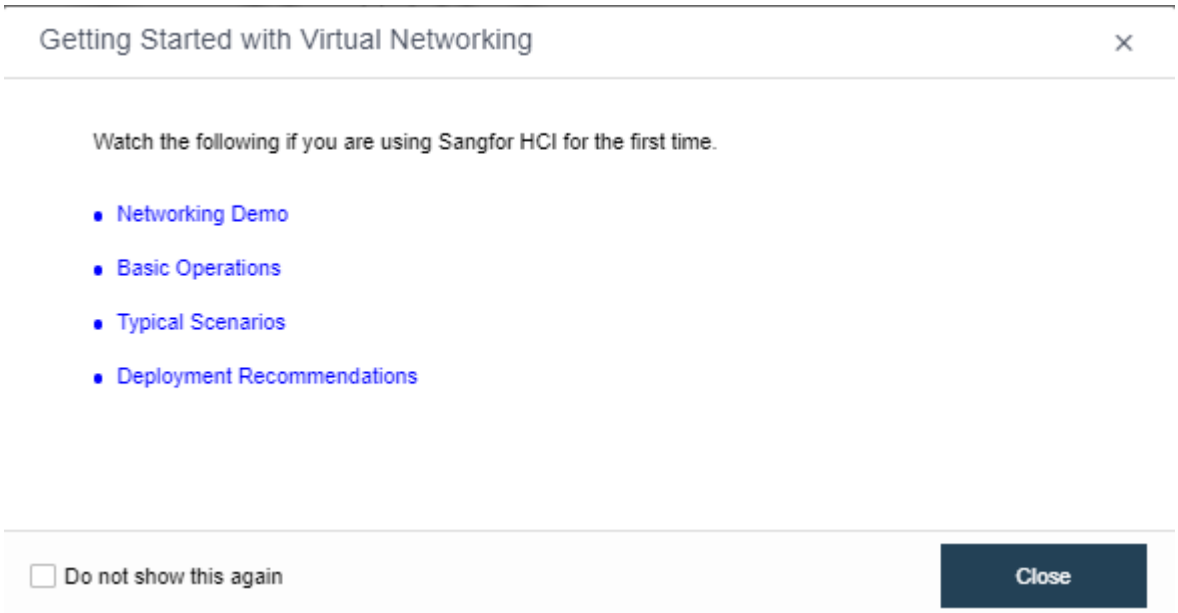


For how to configure alarm options, refer to **Alarms Options** section.

2.3 Configuring Virtual Network

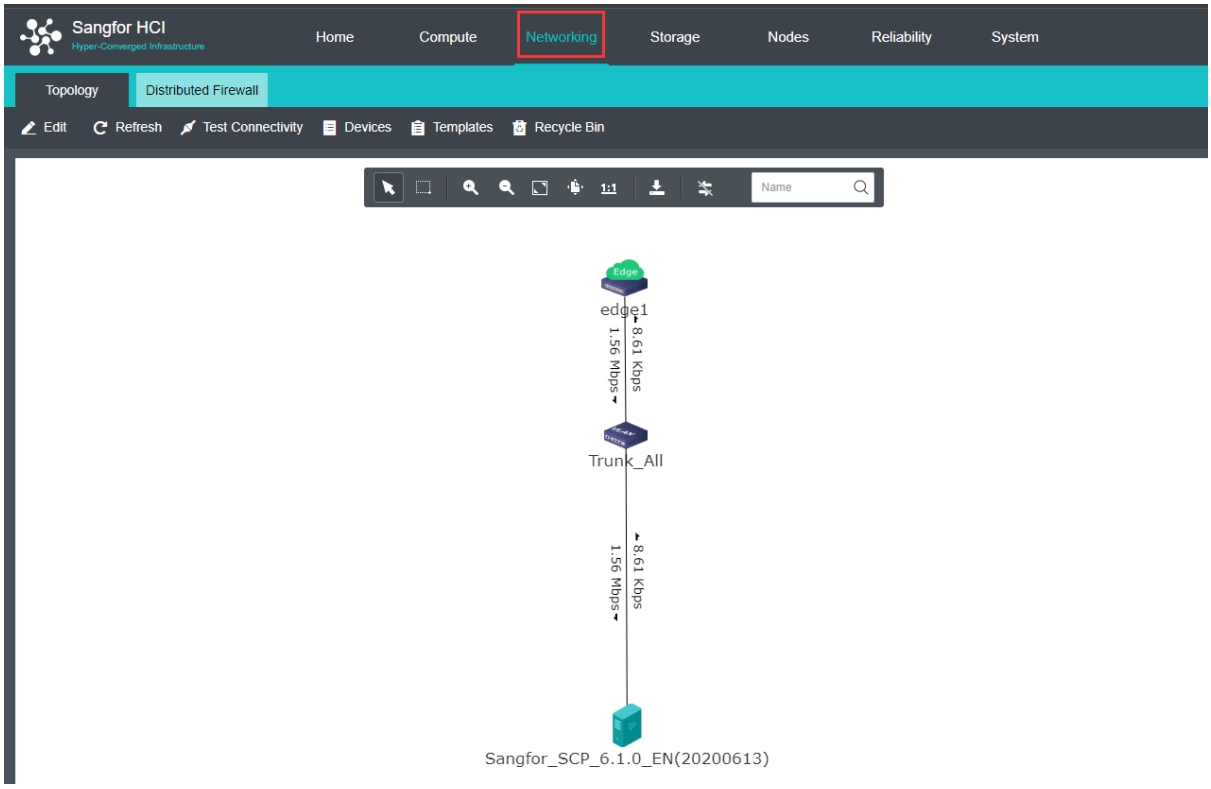
2.3.1 How To?

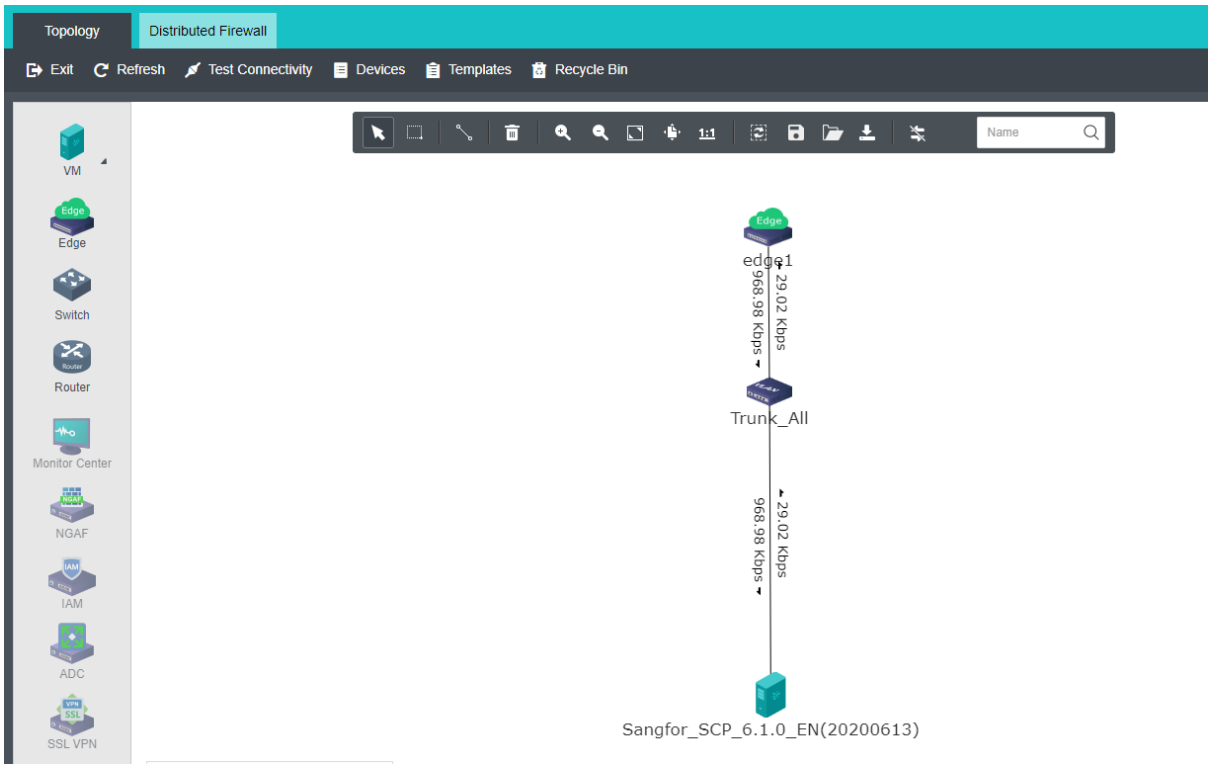
When you log in to Sangfor HCI platform for the first time, a wizard will pop up to guide you through virtual network deployment (You can also enter the wizard by clicking **How To** at the upper-right corner). The wizard contains the following information: **Networking Demo, Basic Operations, Typical Scenarios** and **Deployment Recommendations,** as shown below:



2.3.2 Deploying Network Topology

In **Networking,** you can deploy virtual network topology. To edit network topology, you must enter editing status first, otherwise, the topology can only be viewed. Click **Edit** to enter editing status, as shown below:

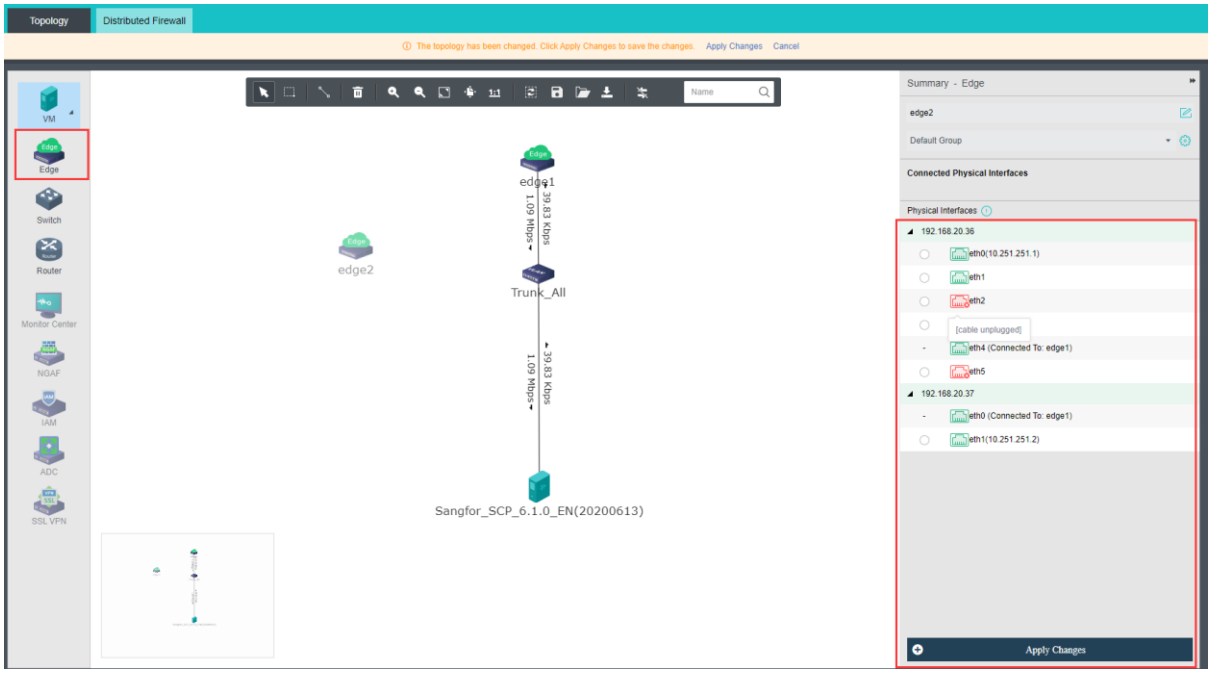




2.3.3 Configuring Edge

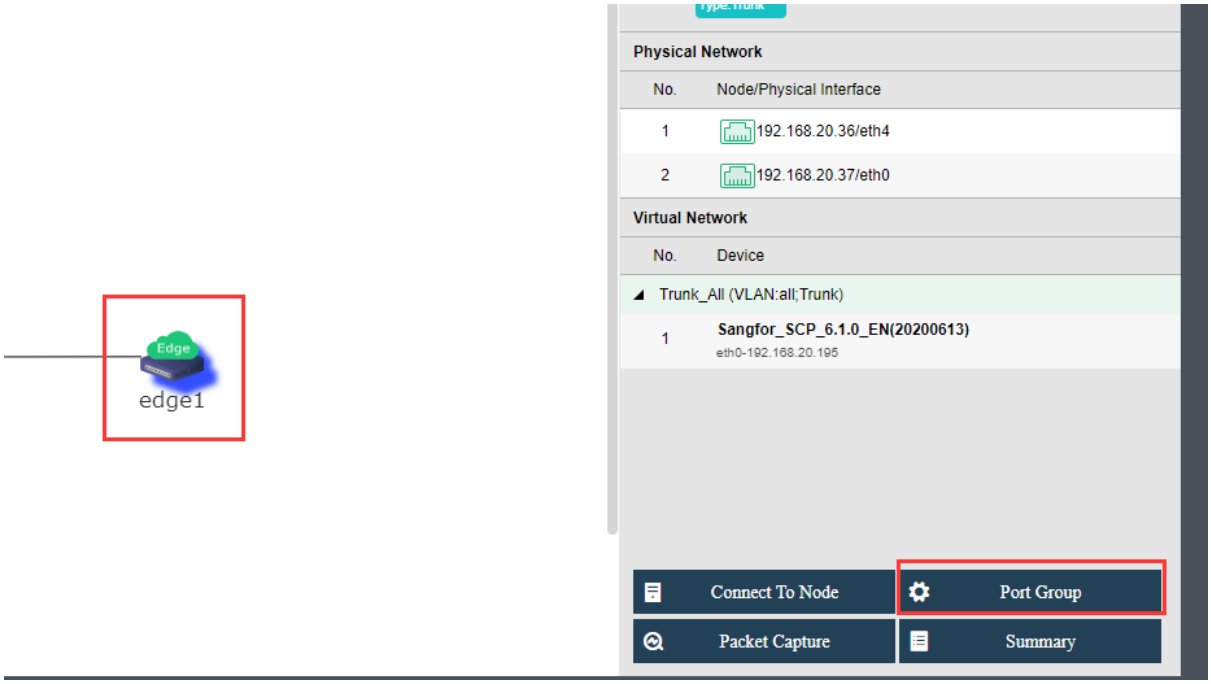
An edge connects physical network and virtual network. It uses physical interface or aggregate interface to connect to physical network in **Trunk** mode. When configuring edge, you need to specify port group. A port group consists of more than one interfaces with the same configuration(such as VLAN).

To deploy an edge, drag an edge onto the canvas from the left panel, select the physical interfaces that need to be connected and then click **Apply Changes**.



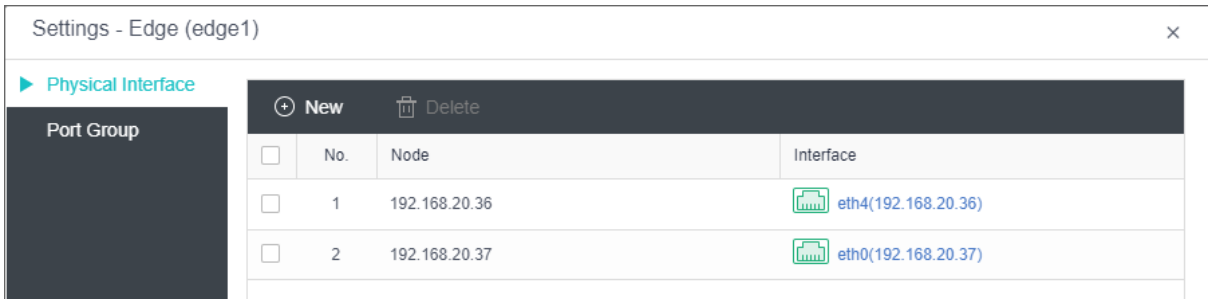
2.3.3.1 Viewing Edge Settings

Select an edge and click on **Settings** button on the right to enter edge settings page. On the **Settings** page, you can view and configure physical interface and port group.



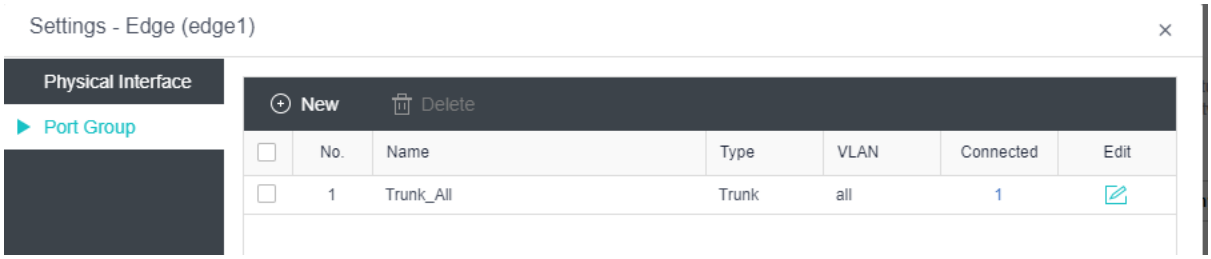
2.3.3.1.1 Configuring Physical Interface

On the **Physical Interface** tab, as shown below, you can add a new physical interface, delete or edit an existing physical interface. Each node should be specified a physical interface to be connected to a same edge, and that interface should be connected to a same L2 switch so as to ensure that virtual network traffic can go to physical network through any node. as shown below:

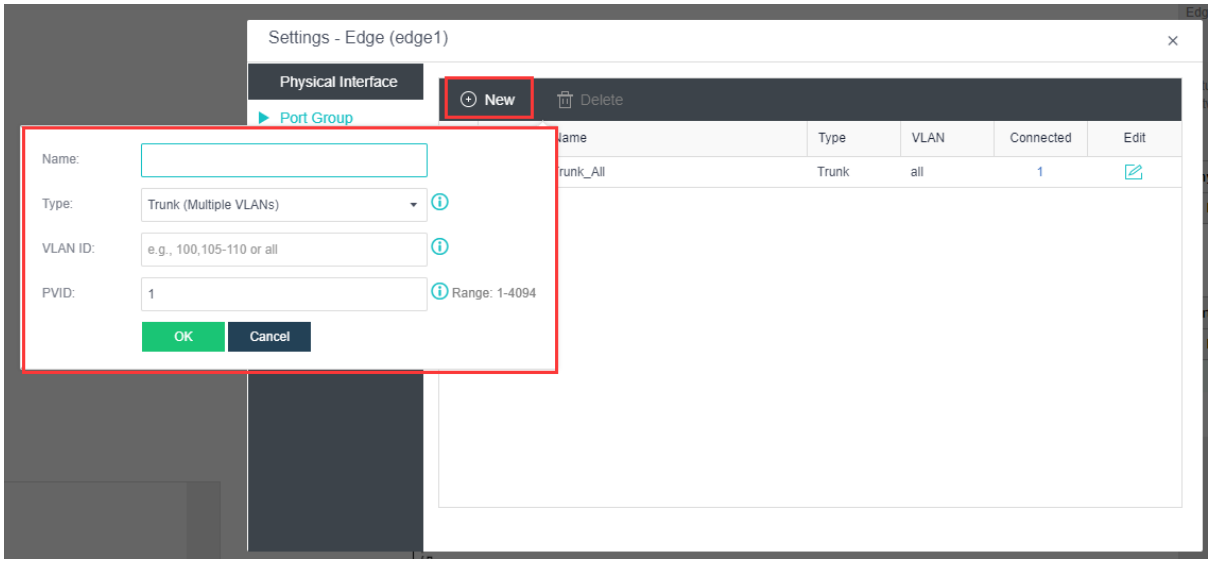


2.3.3.1.2 Configuring Port Group

On the **Port Group** tab, you can add a new port group, delete or edit an existing port group.



To add a new port group, click **Add** to enter the following page and configure related fields.



[**Name**]: Specifies a name for the port group.

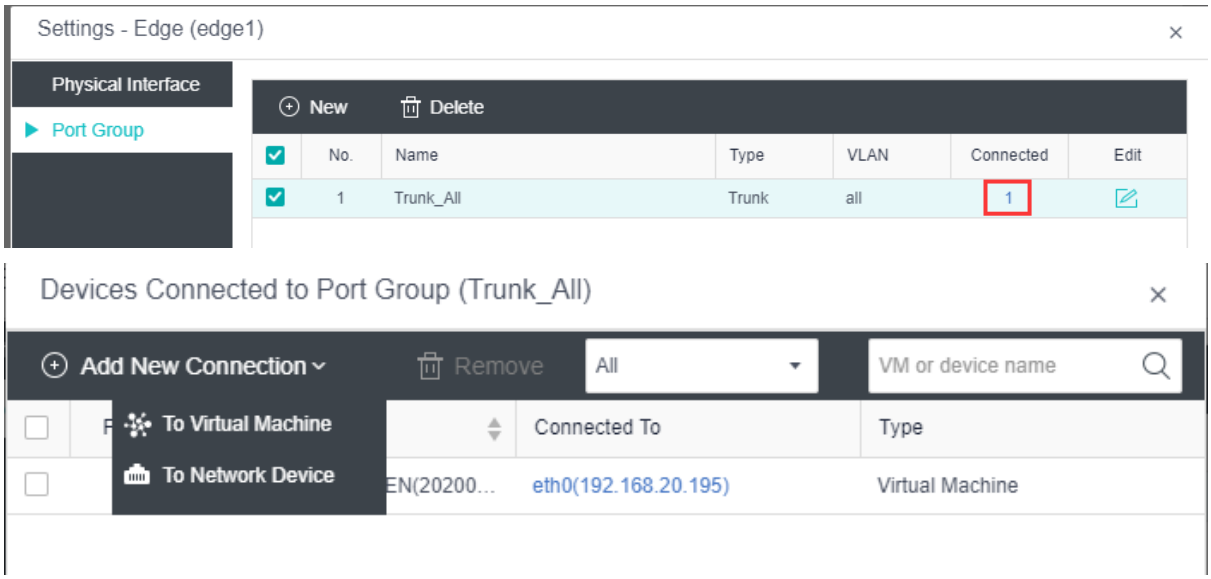
[**Type**]: Specifies the type of VLAN interface, **Trunk** or **Access**. Trunk port is used for VLAN trunking or VLAN aggregation. It allows packets that do not carry VLAN information, or carry VLAN information but VLAN ID is within specific VLAN range; if VLAN ID is not in VLAN range, packets will be rejected. The packets without VLAN information are allowed to go through this port.

Access port is used for untagged VLAN. If it receives packets without carrying VLAN information, the packets will be tagged with specific VLAN IDs, which will be removed when the packets go out of that Access port. The packets with VLAN information are not allowed to go through this port.

[**VLAN ID**]: It is required when the type is **Trunk**.

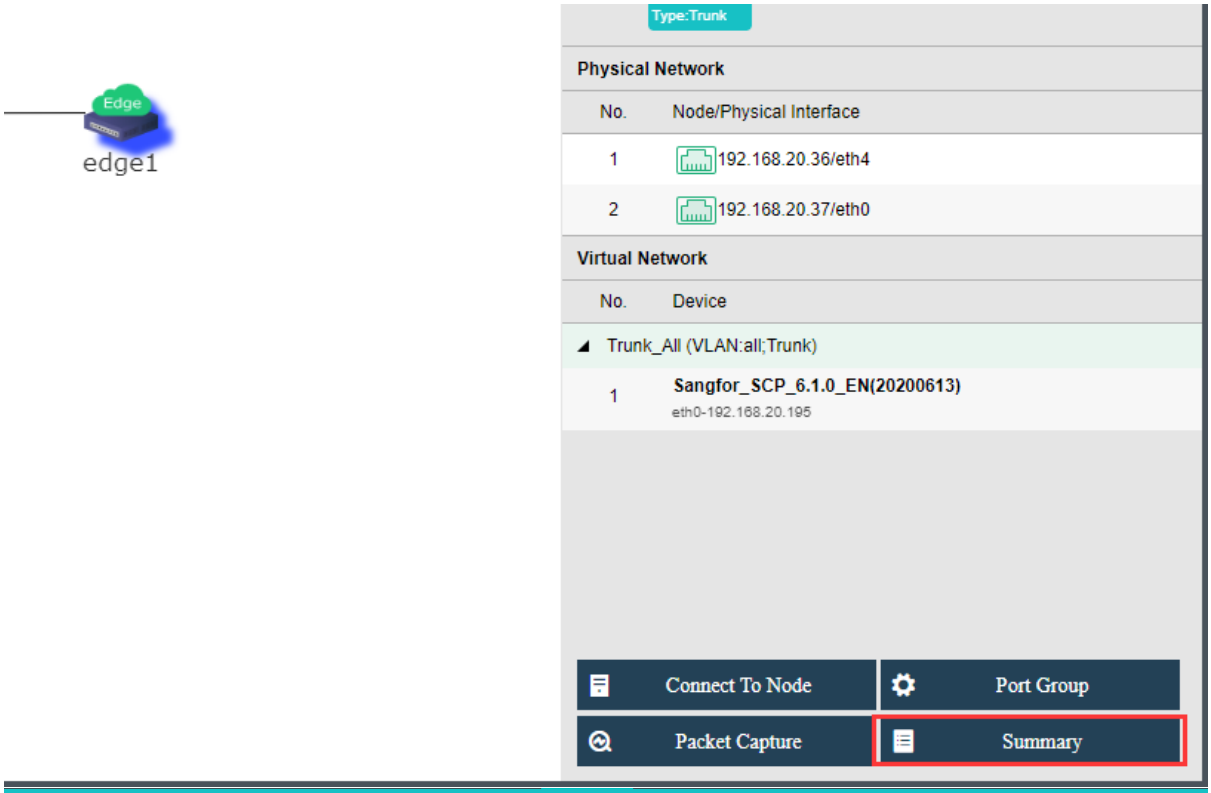
[**PVID**]: It is the default VLAN ID that will be tagged on the packets going through the switch but not carrying VLAN ID.

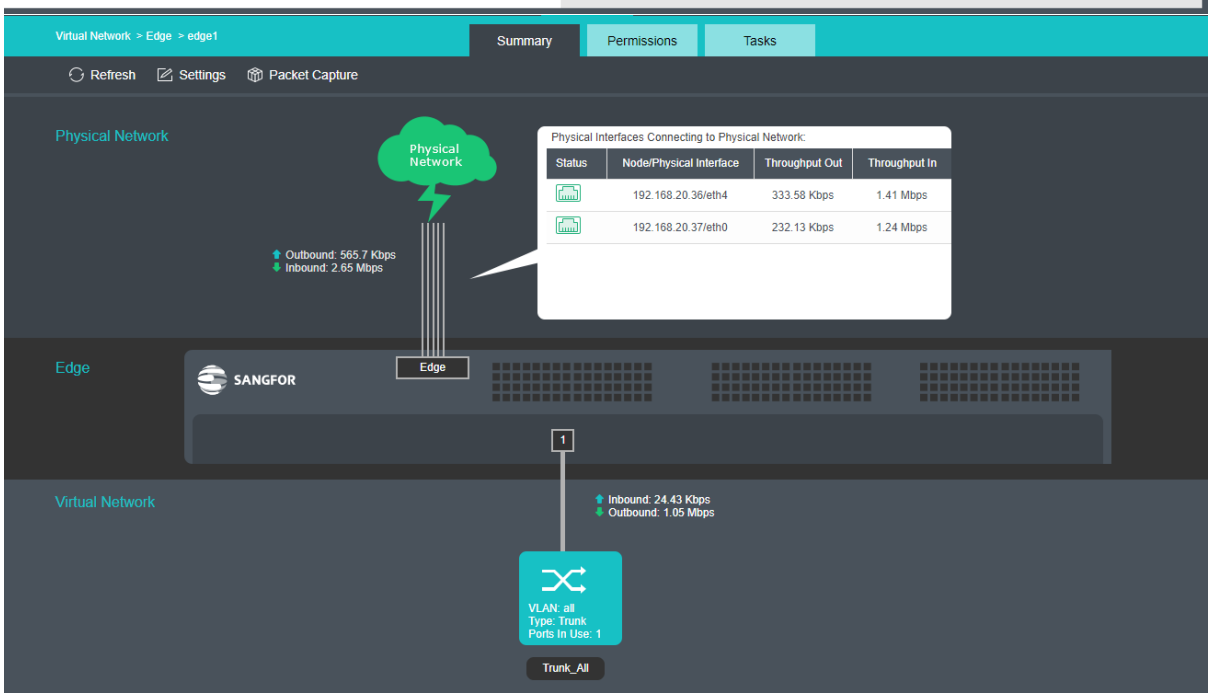
On the **Port Group** tab, you may click on the number in **Connected** column to enter the following page on which you can add connection to virtual machine, network device(including router, NGAF and ADC),



2.3.3.2 Viewing Edge Details

On the **Summary** page, you can view the basic information of the edge, and the outbound and inbound rate of the edge and port group.

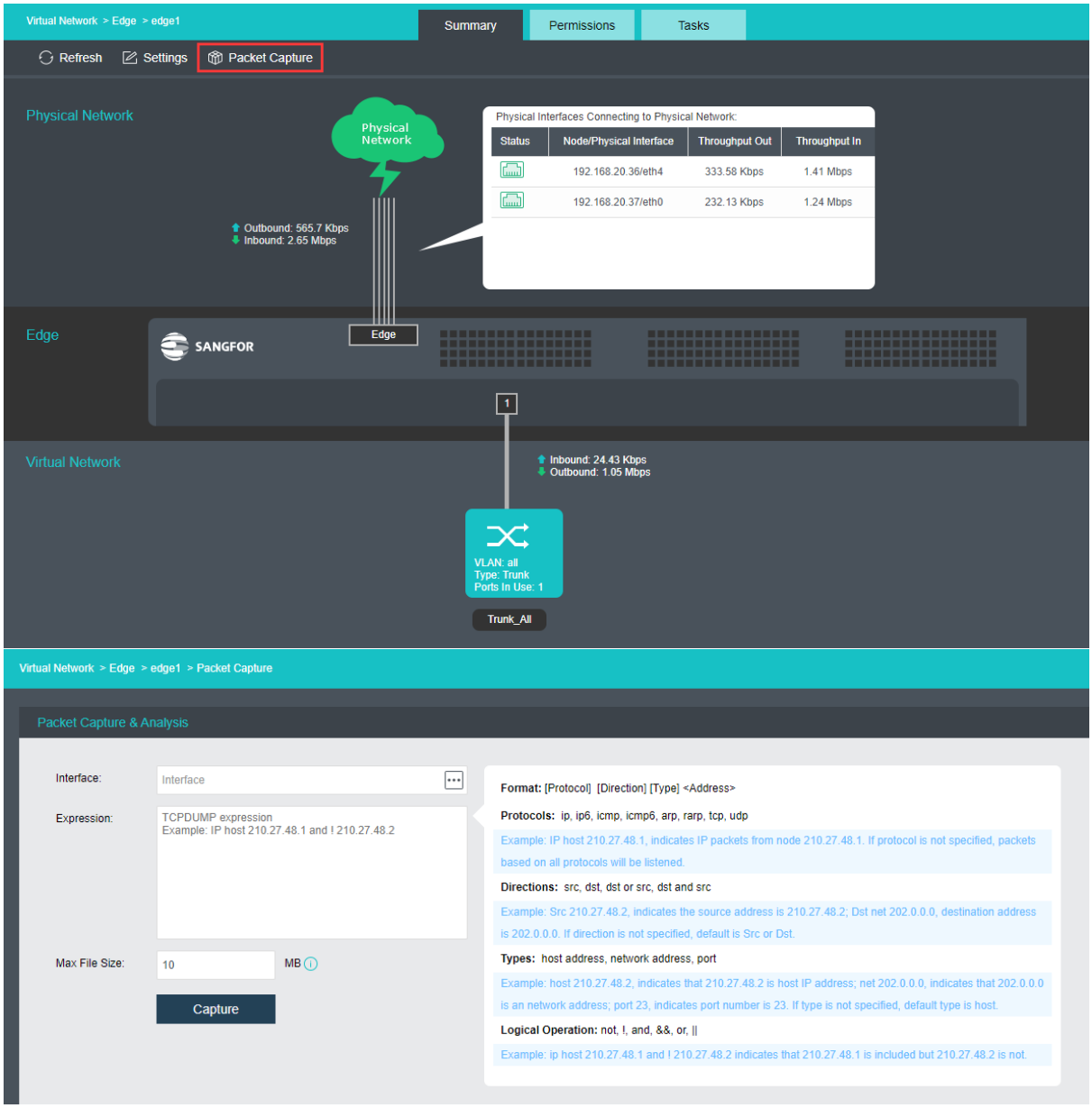




To reload the current page, click **Refresh**.

To change edge settings, click on **Settings**, and then configure physical interface and port group.

To capture and analyze packets, click **Packet Capture**, as shown below:



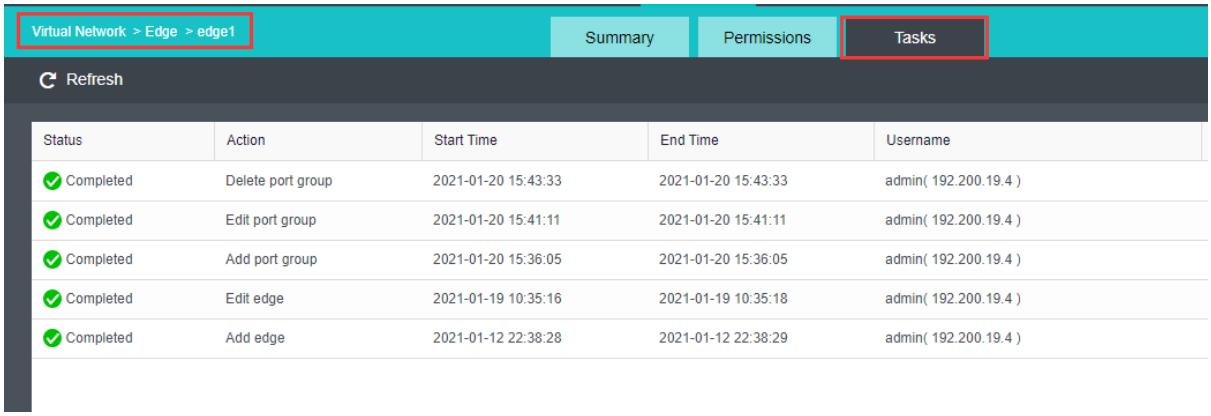
Interface: Specifies the interface. The packets passing through that interface will be captured.

Expression: Specifies expression to filter packets. On the right panel of the **Packets Capture & Analysis** page, it displays the expression formats.

Max File Size: Specifies the maximum size of the file. If a file size is larger than the maximum, capturing packet will stop.

Tasks: This section displays administrator logs, which record various operations performed

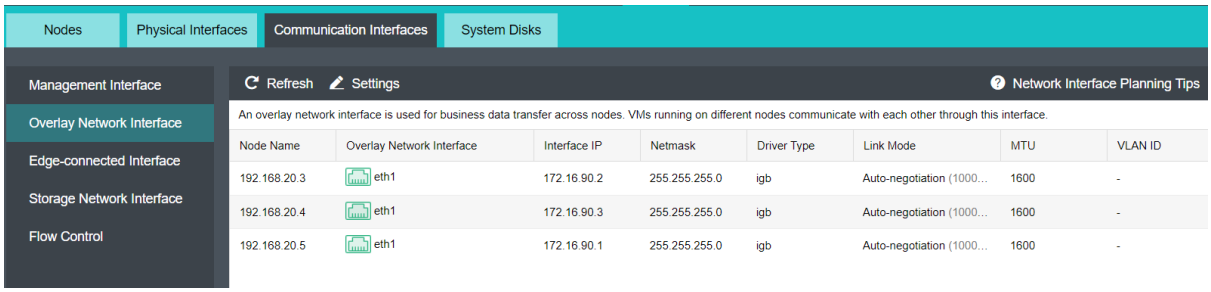
by the administrator, such as creating edge. Each log contains the following information: **Status, Action, Start Time, End Time, Username, Node, Object Type, Object** and **Operation**. To view log details, click **View** in **Operation** column.



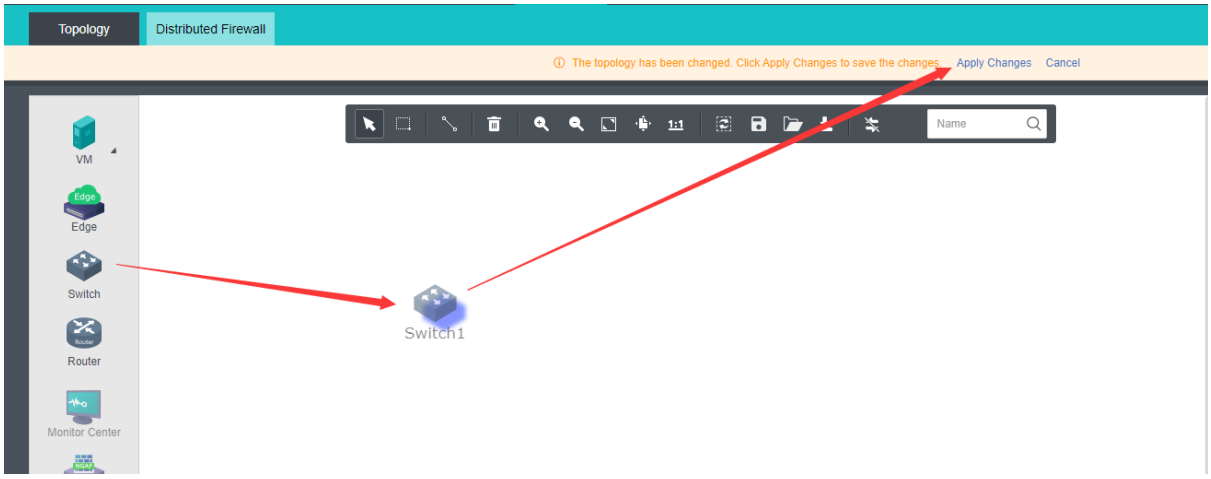
2.3.4 Configuring Virtual Switch

On a virtual switch, you can add connection, and broadcast storm prevention.

First, you need to check whether overlay network interfaces(VXLAN) of each node are configured on a same network segment. If they belong to different subnets, nodes cannot communicate with each other through a virtual switch. To check overlay network interface settings, select a node in **Nodes**, click **Communication Interface** andthen click on the **Overlay Interface** tab to enter the following page:



Navigate to **Networking** page and then drag a virtual switch onto the canvas. To make the changes take effect, click **Apply** Changes.

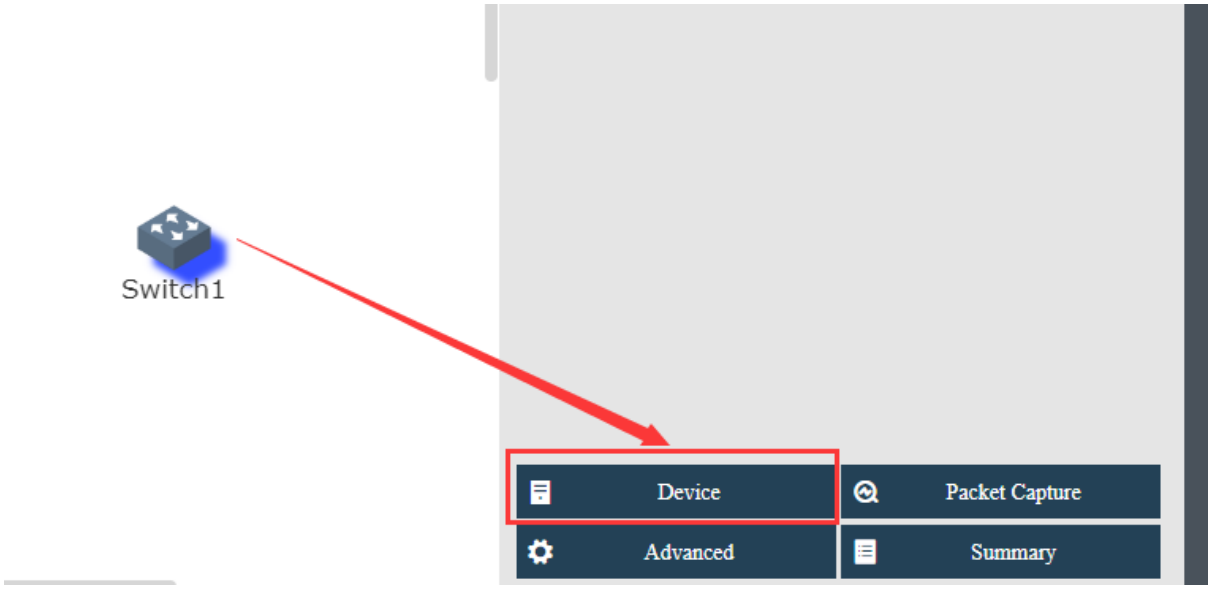


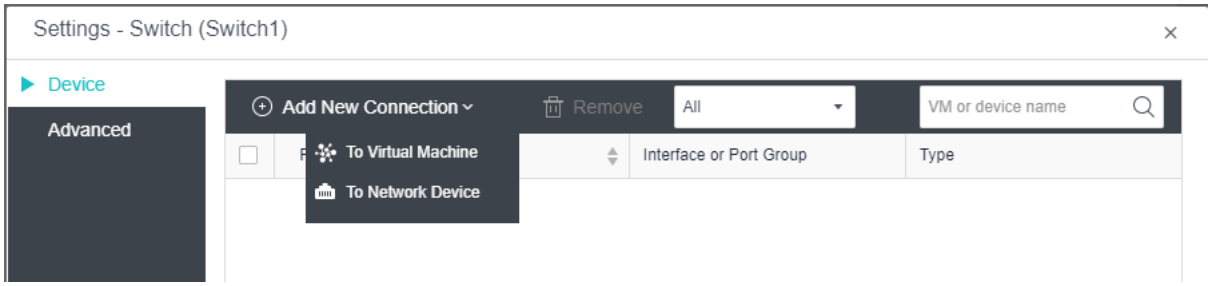
2.3.4.1 Viewing Switch Settings

Select a virtual switch, you can view its configuration on the right. To configure switch, click **Settings** button to enter **Settings** page, as shown below. On the following page, you can add connection and enable broadcast storm prevention.

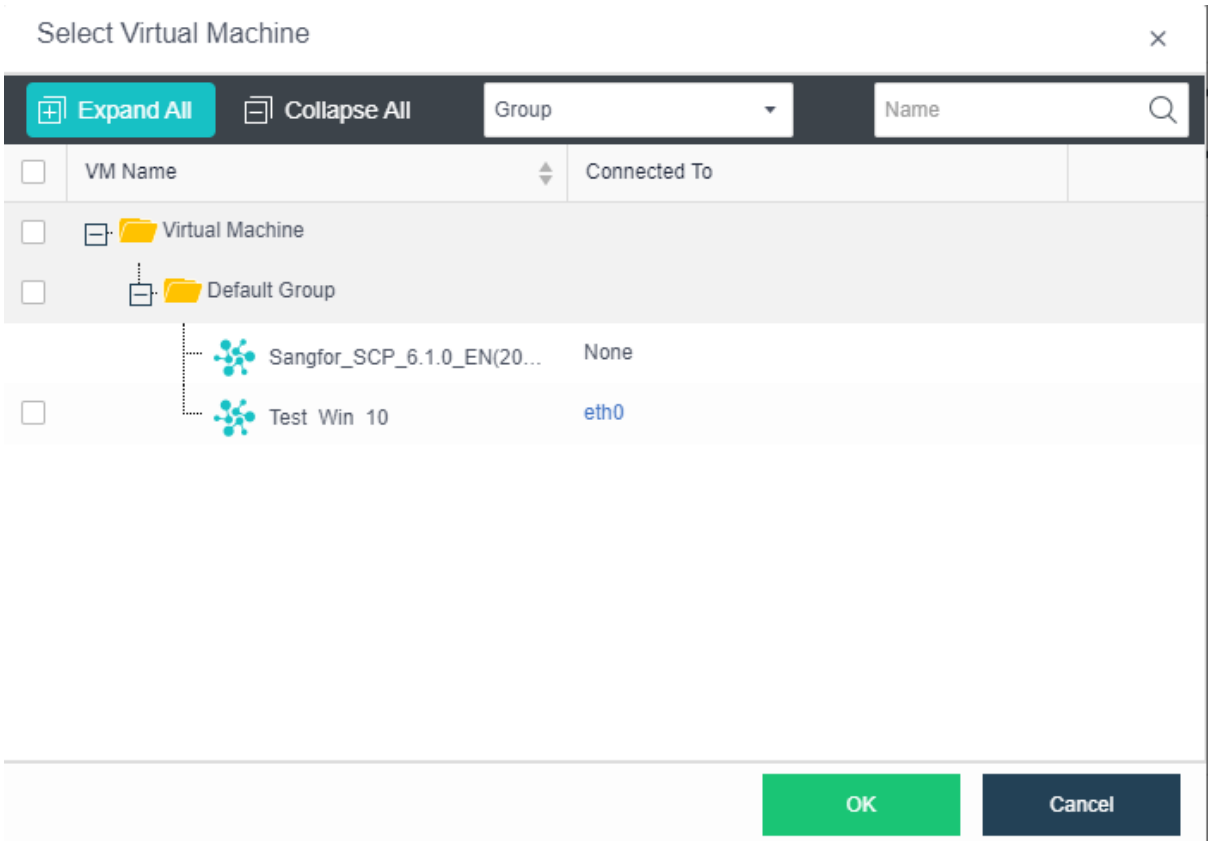
2.3.4.1.1 Adding Connection

On the **Device** tab, you can add connection to virtual machines and network devices(such as router, NGAF, ADC, IAM, WOC, and SSL VPN), as shown below:

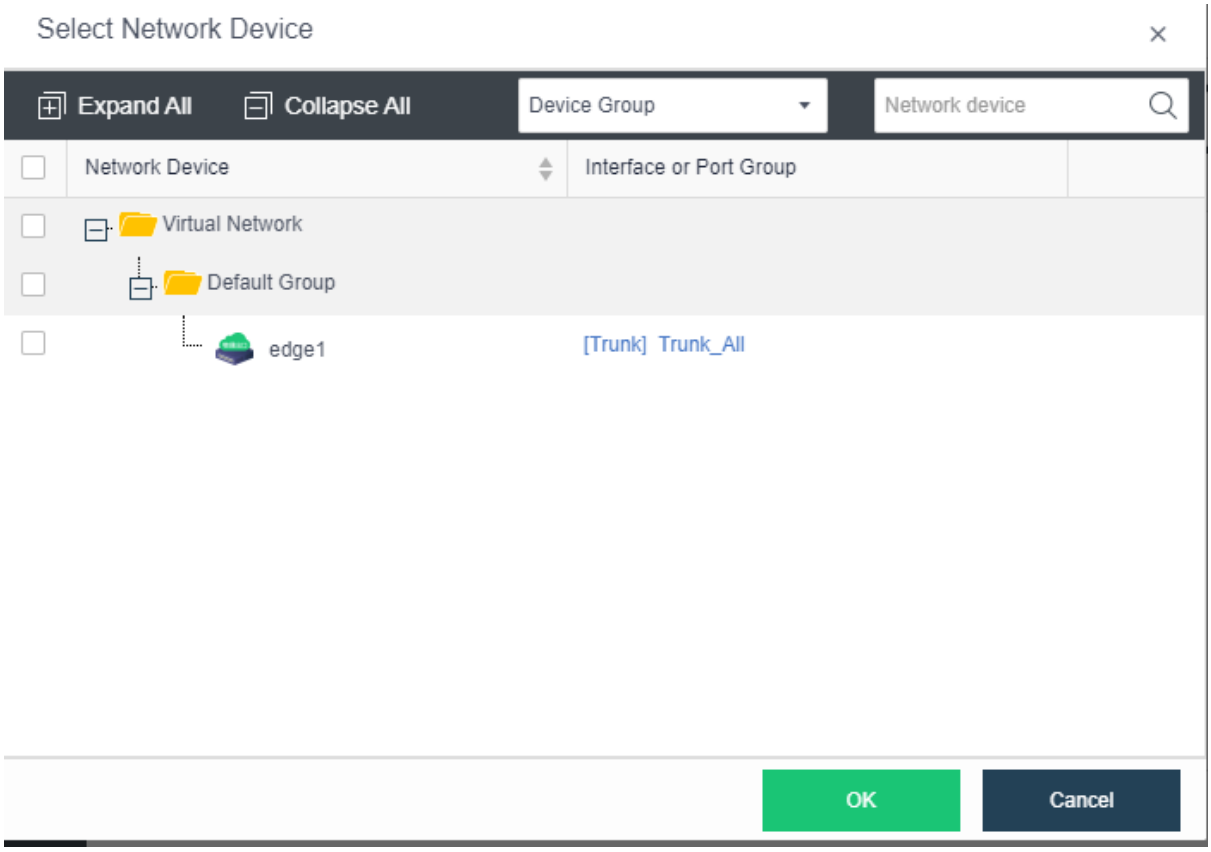




To add connection to a virtual machine, select **Add Connection > To Virtual Machine**, then select the VM that you want to connect to the switch. Click **OK** to save the settings. as shown below:

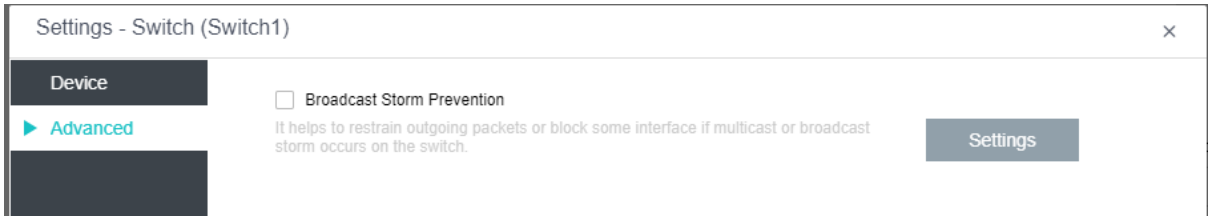


To add connection to a network device, select **Add Connection > To Network Device**, select the network device that you want to connect to the switch and then click **OK**, as shown below: as shown below:

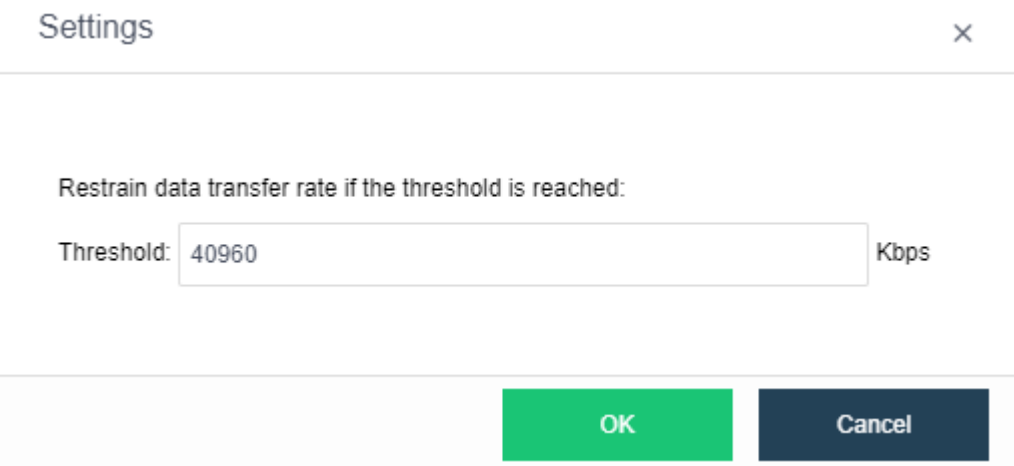


2.3.4.1.2 Configuring Advanced Settings

On the **Advanced** tab, you can enable and configure broadcast storm prevention which can help to restrain outgoing packets or block some interface if multicast or broadcast storm occurs on switch. Broadcast storm prevention is disabled by default.

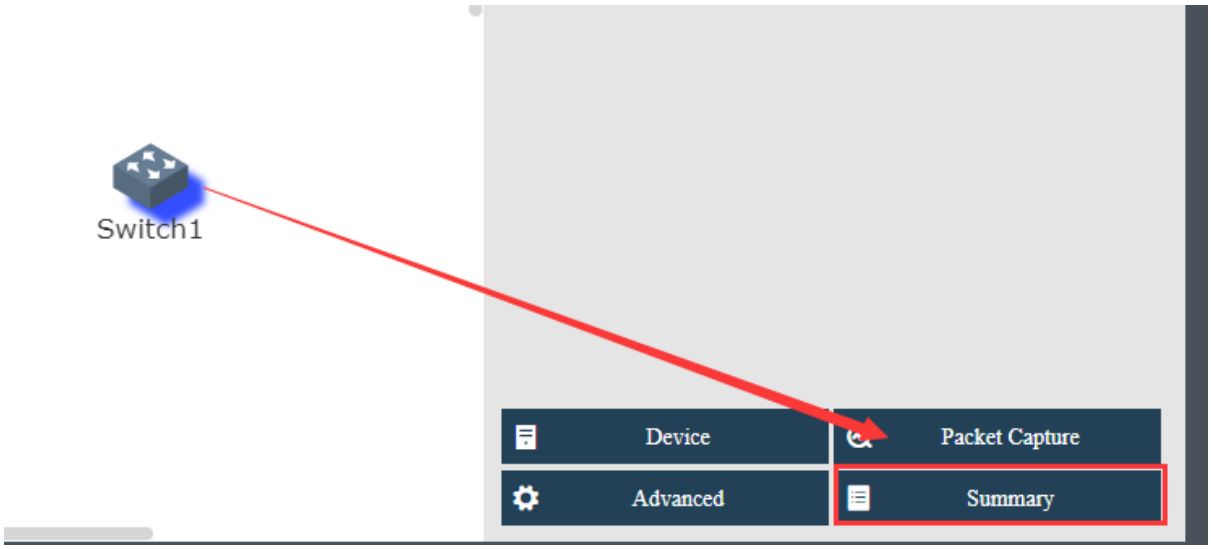


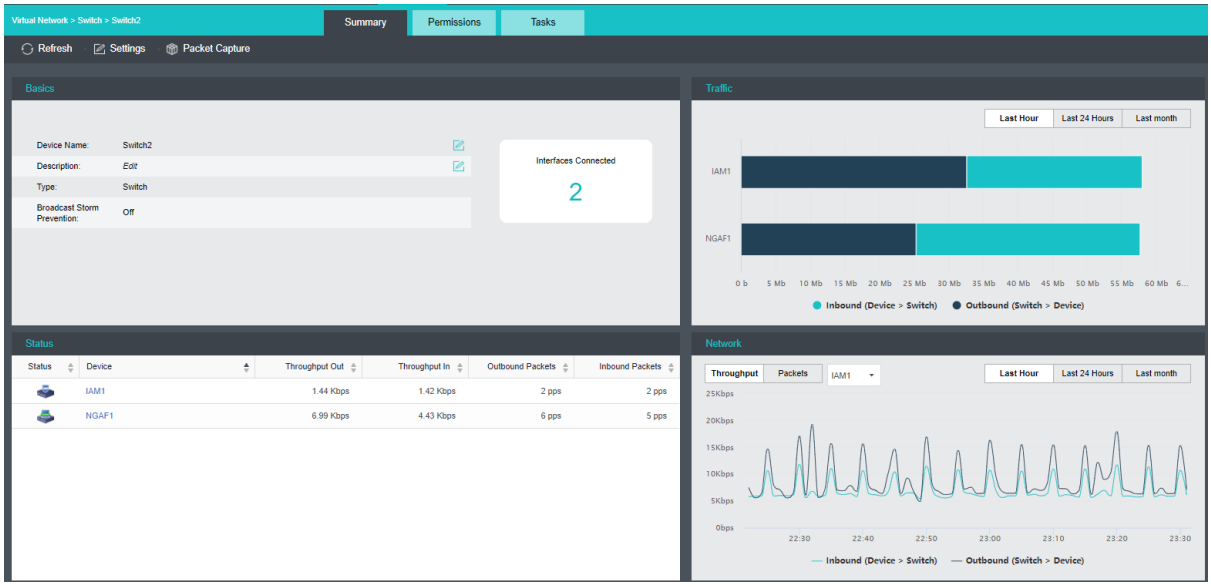
To configure broadcast storm prevention, click **Settings** to enter the following page and specify threshold.



2.3.4.2 Viewing Switch Summary

To view detailed settings of a switch, select the switch and click **Summary** button to enter switch summary page. Here you can view **Basics, Traffic, Status** and **Network**. You can also view admin logs on the **Admin Logs** tab.

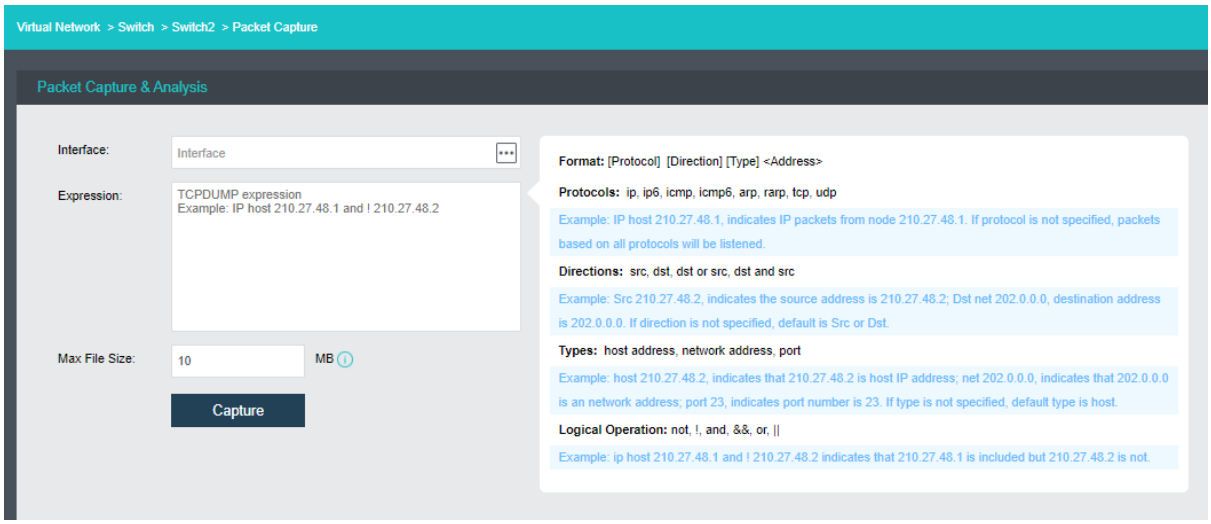




To reload the current page, click **Refresh**.

To configure the switch, click **Settings**.

To capture and analyze packets, click **Packet Capture**, as shown below:



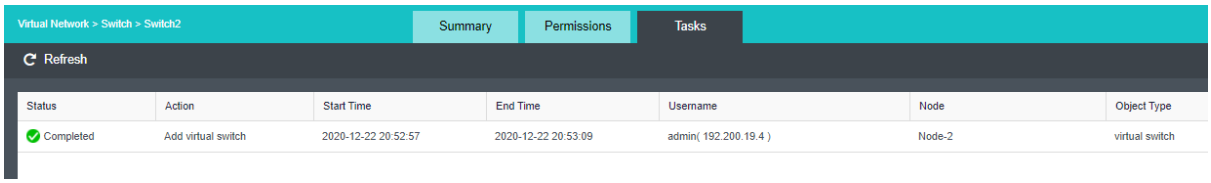
Interface: Specifies the interface. The packets passing through that interface will be captured.

Expression: Specifies expression to filter packets. On the right panel of the **Packets Capture & Analysis** page, it displays the expression formats.

Max File Size: Specifies the maximum size of the file. If a file size is larger than the maximum, capturing packet will stop.

Tasks: This section displays administrator logs, which record various operations on the switch, performed by administrator, such as adding connection. Each log contains the following information: **Status, Action, Start Time, End Time, Username, Node, Object**

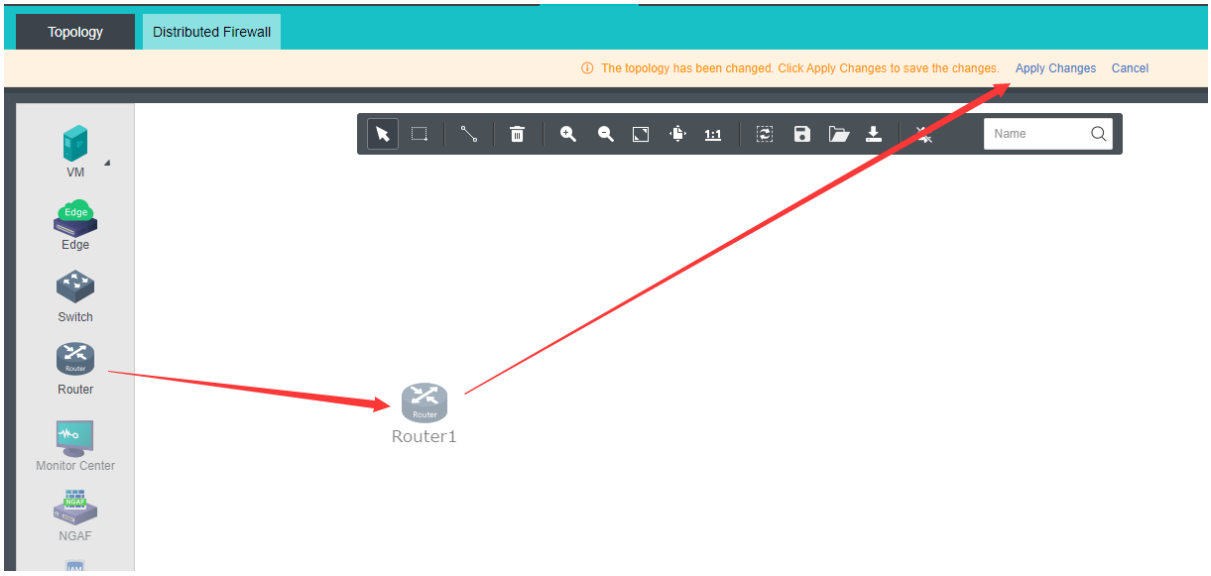
Type, **Object** and **Operation**. To view log details, click **View** in **Operation** column.



2.3.5 Configuring Virtual Router

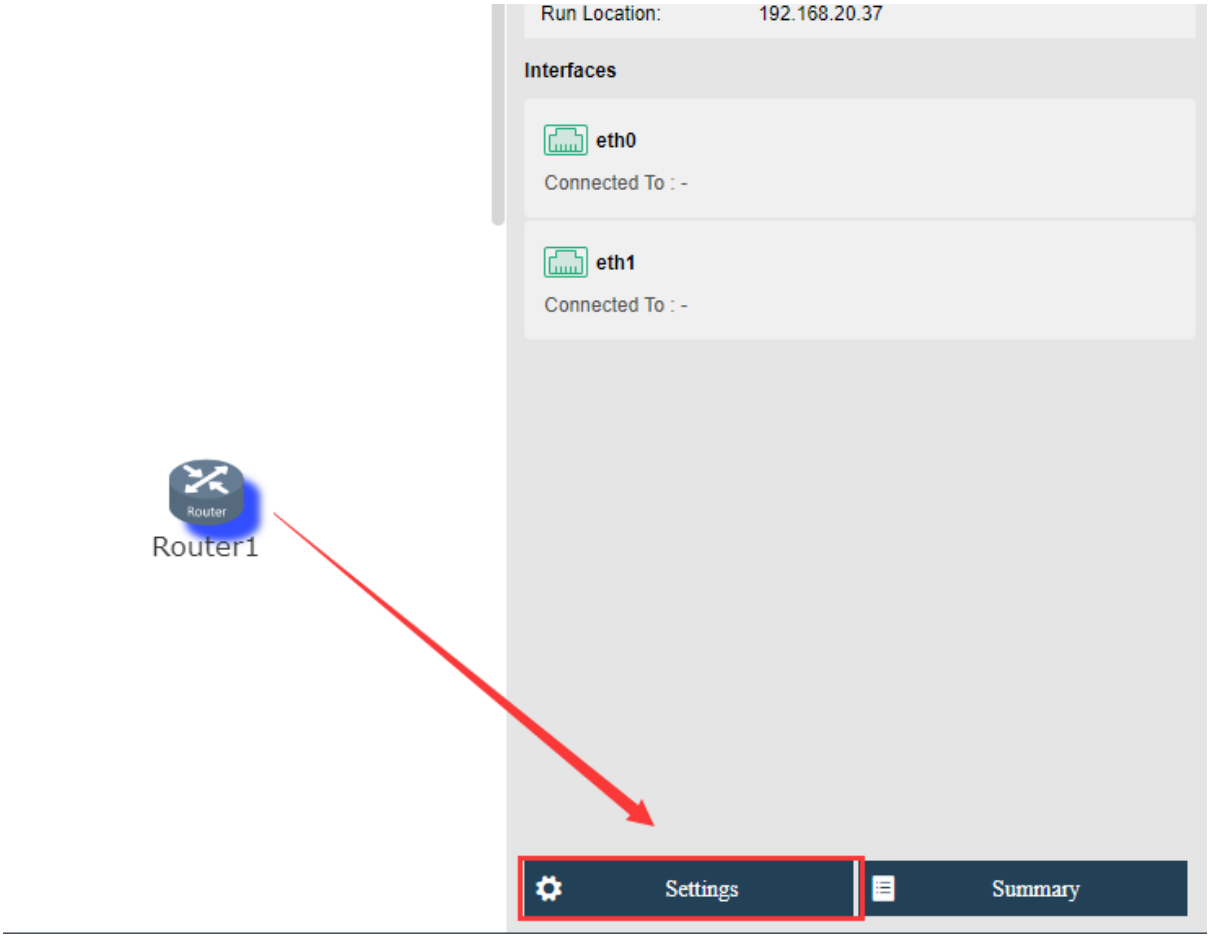
On a virtual router, you can configure interfaces, VLAN subinterface, static route, NAT, access control, DHCP, DNS and high availability(HA).

To deploy a virtual router, go to **Networking** page, enter editing status, drag a virtual router onto the canvas and then click **Apply Changes**, as shown in the following page. To edit router's name, select the router and edit its name on the right panel.



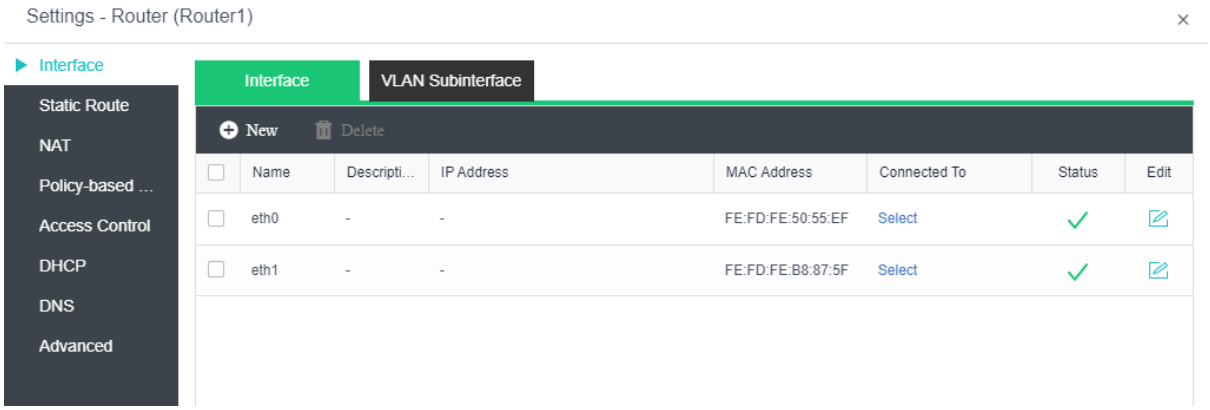
2.3.5.1 Viewing Router Settings

You can configure a virtual router by clicking **Settings** button to enter the **Settings** page. On that page, you can configure interface and VLAN subinterface, static route, NAT, access control policy, DHCP, DNS and high availability(HA).

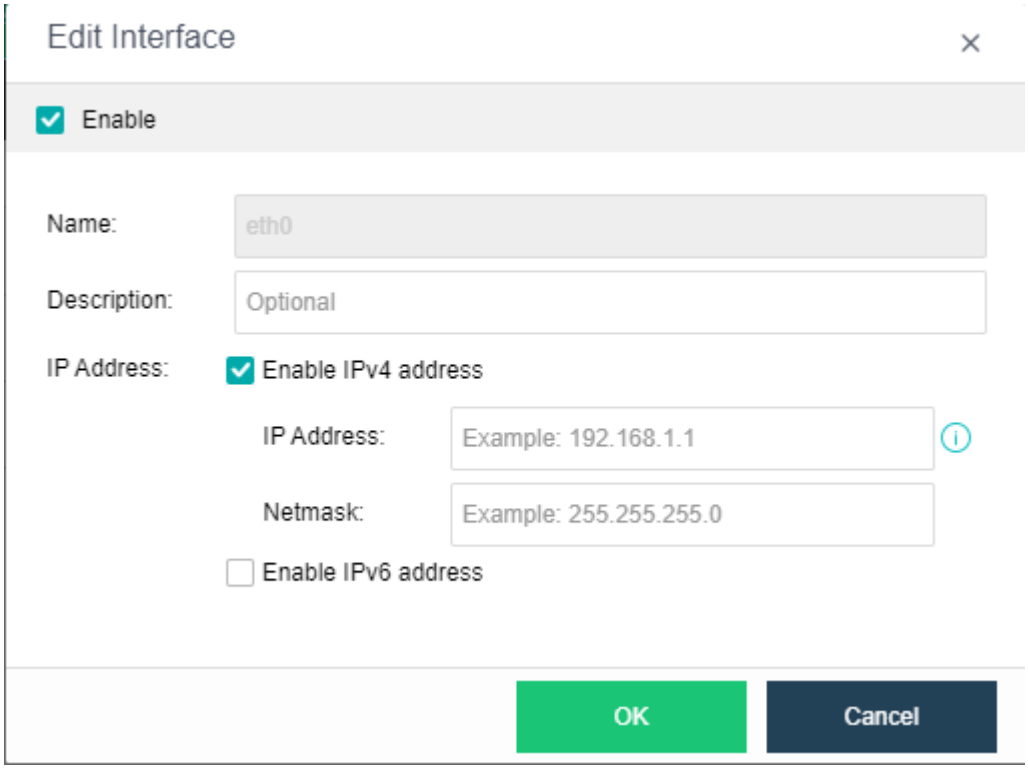


2.3.5.1.1 Configuring Interface

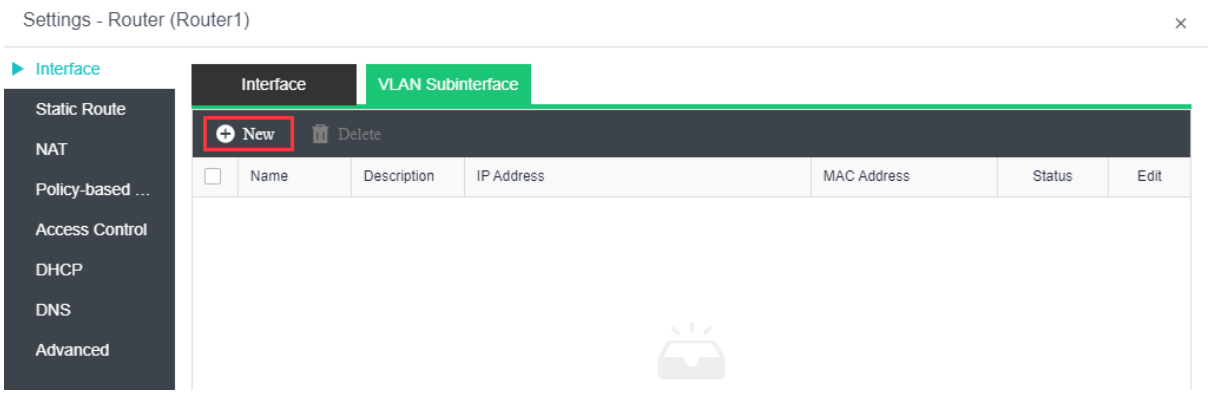
On the **Interface** tab, you can configure the router's network interface and the corresponding VLAN subinterface.

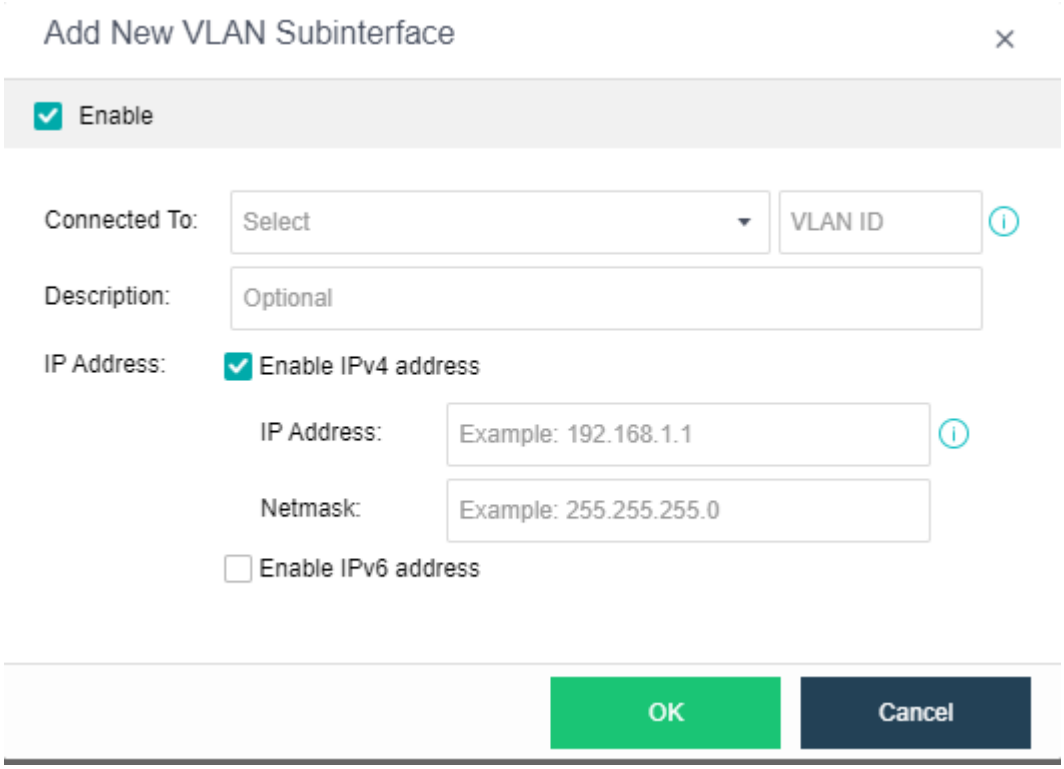


To add interface(s), click **Add** and specify the number of interfaces that you want to add.



Support to enable Ipv4 and Ipv6 address in the interface.

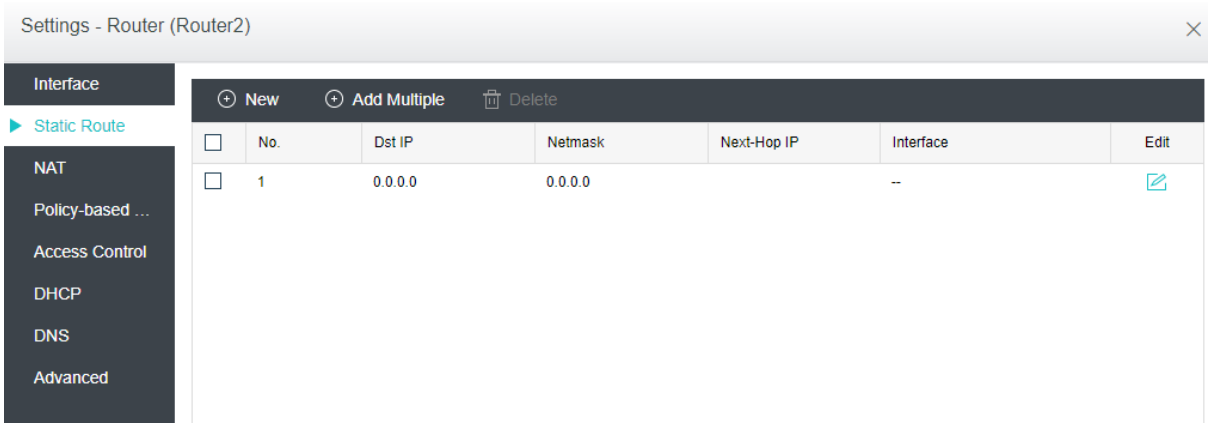




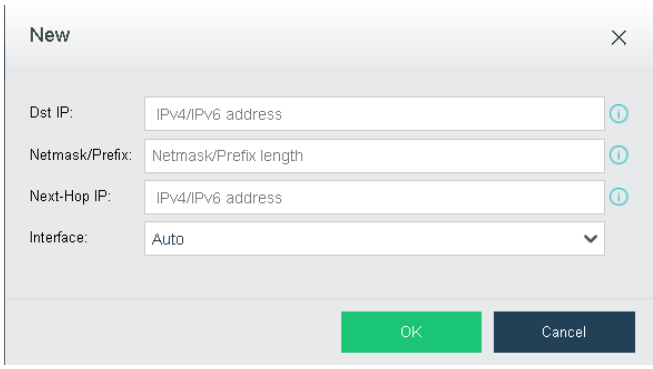
Support to enable IPv4 and IPv6 address.

2.3.5.1.2 Configuring Static Route

On the **Route** tab, you can configure a static route, or multiple static routes at a time. Static route works when the router needs to send packets to various subnets. You may add one static route at a time or multiple static routes at a time.



To add a static route, click **Add Static Route** and configure related fields on the following page:



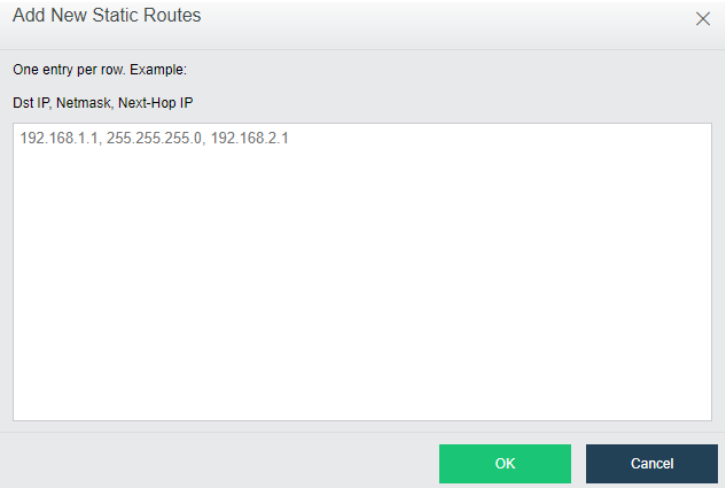
Dst IP: Specifies **the destination Ipv4 or Ipv6 address.**

Netmask: Specifies netmask **corresponding to the destination IP address.**

Next-Hop IP: Specifies **the next-hop Ipv4 or Ipv6 address.**

Interface: Specifies **the interface through which data is forwarded.**

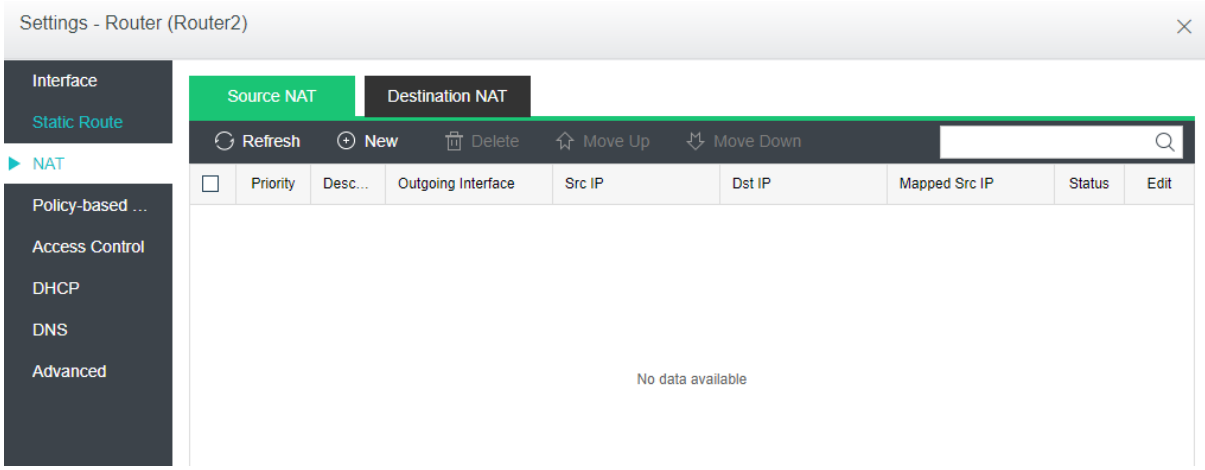
To add multiple static routes, click **Add Multiple** to enter the following page:



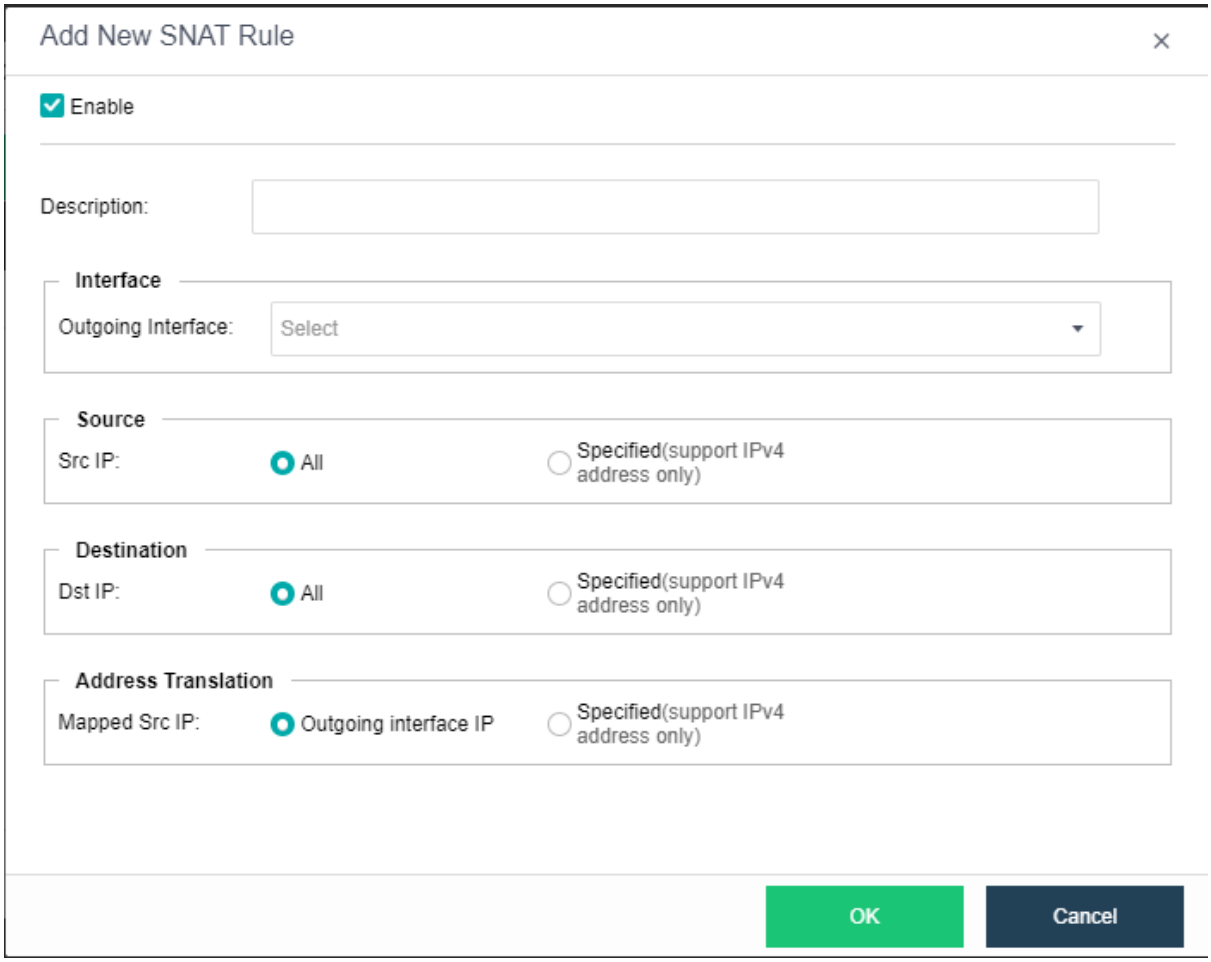
One static route per row. Example: destination IP address, netmask, next-hop IP address.

2.3.5.1.3 Configuring NAT Rule

On the **NAT** tab, you can configure SNAT and DNAT rules. SNAT is used to translate source IP address of a data packet, while DNAT is used to translate destination IP address of a data packet and commonly used to publish an internal service on a publicly accessible IP address.



To add a source NAT rule, click **Add** on the **Source NAT** tab and configure the fields on the following page:



[**Enabled**]: Select this option to **enable** the SNAT rule.

[**Description**]: Specifies description for **the** SNAT rule.

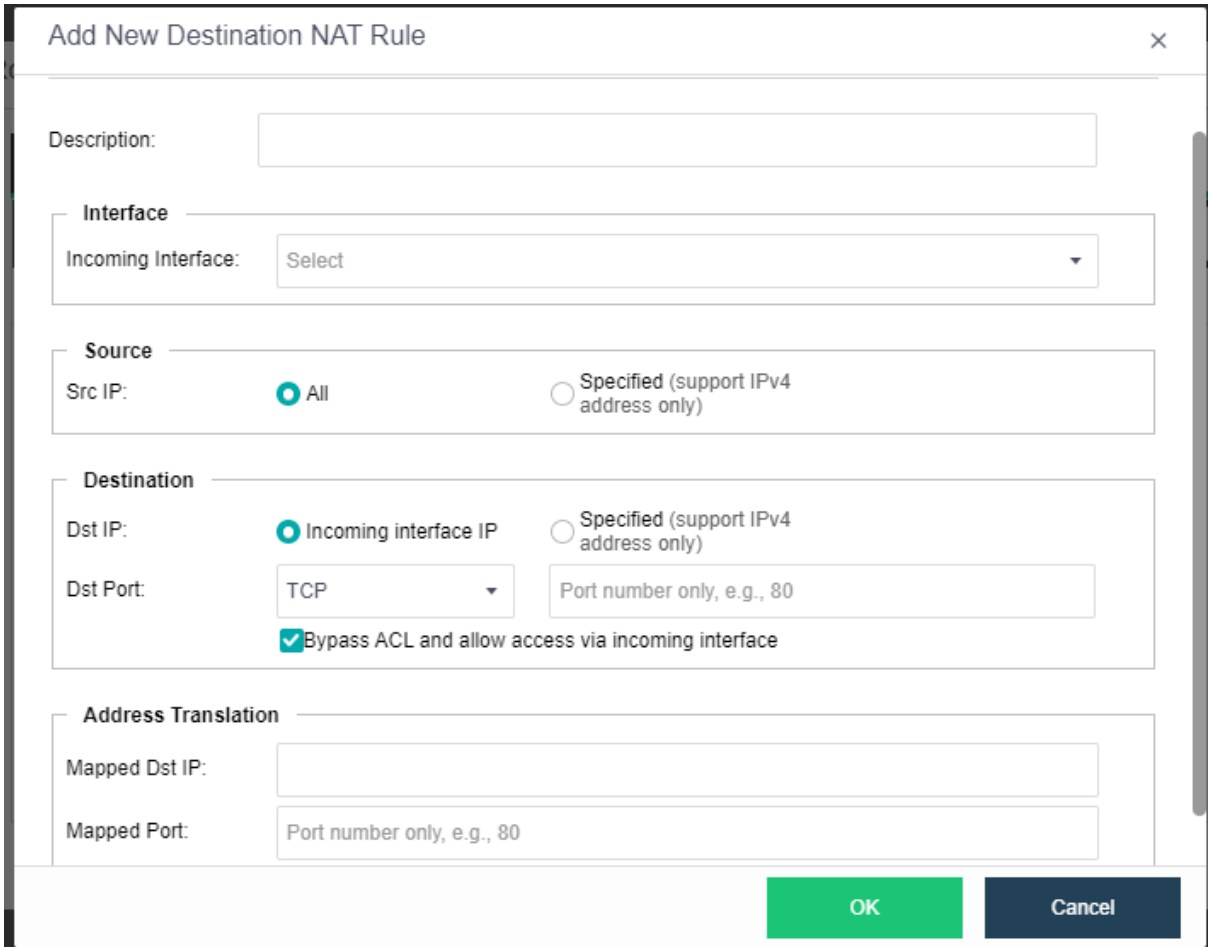
[**Interface**]: Specifies outgoing interface through which data is forwarded.

[**Source**]: Specifies source IP address. Options are **All** and **Specified**. If **Specified** is selected, only the IP addresses **within** the specified IP range will be translated

[**Destination**]: Specifies destination IP address. Options are **All** and **Specified**. If **Specified** is selected, only the source IP addresses of the packets routed to the specified destination IP address will be translated.

[**Address Translation**]: Specifies mapped source IP address. If **Outgoing interface IP** is selected, source IP address will be translated to the IP address of specified outgoing interface. If **Specified** is selected, source IP address will be translated to the specified IP address.

To add a DNAT rule, click **Add** on the **Destination NAT** tab, as shown below:



[**Enabled**]: Select this option to enable the DNAT rule.

[**Description**]: Specifies description for the DNAT rule.

[**Interface**]: Specifies the incoming interface through which inbound traffic flows into intranet.

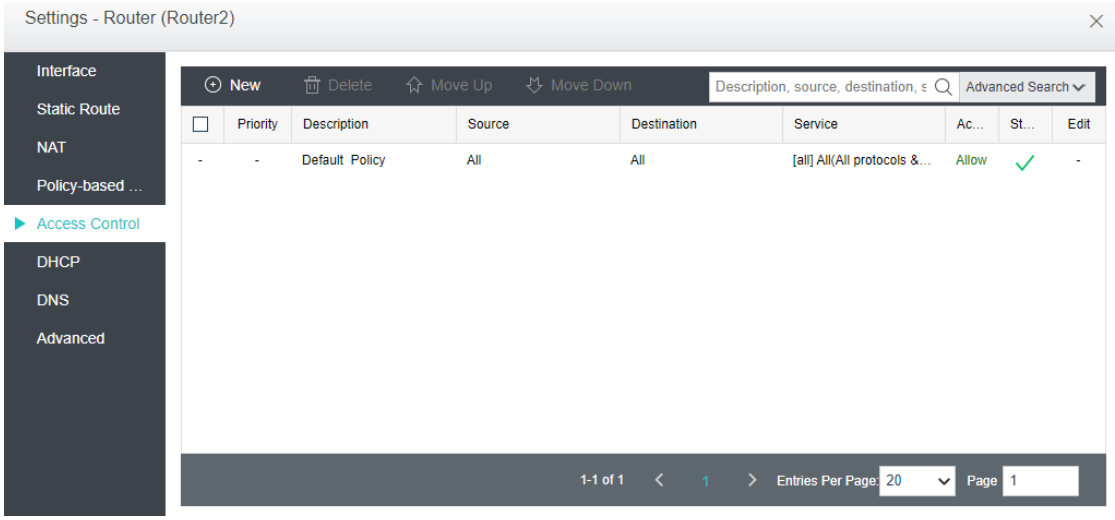
[**Source**]: Specifies source IP address.

[**Destination**]:Specifies destination IP address and port. Destination IP address can be incoming interface address or a specified IP address. If **Incoming interface IP** is selected, the destination IP address will be translated to specified IP address only when the dst address is matching with the specified incoming interface address. To translate a destination port, you need to specify protocol, port number and mapped port. To bypass ACL and allow access via incoming interface, select the option **Bypass ACL and allow access via incoming interface**.

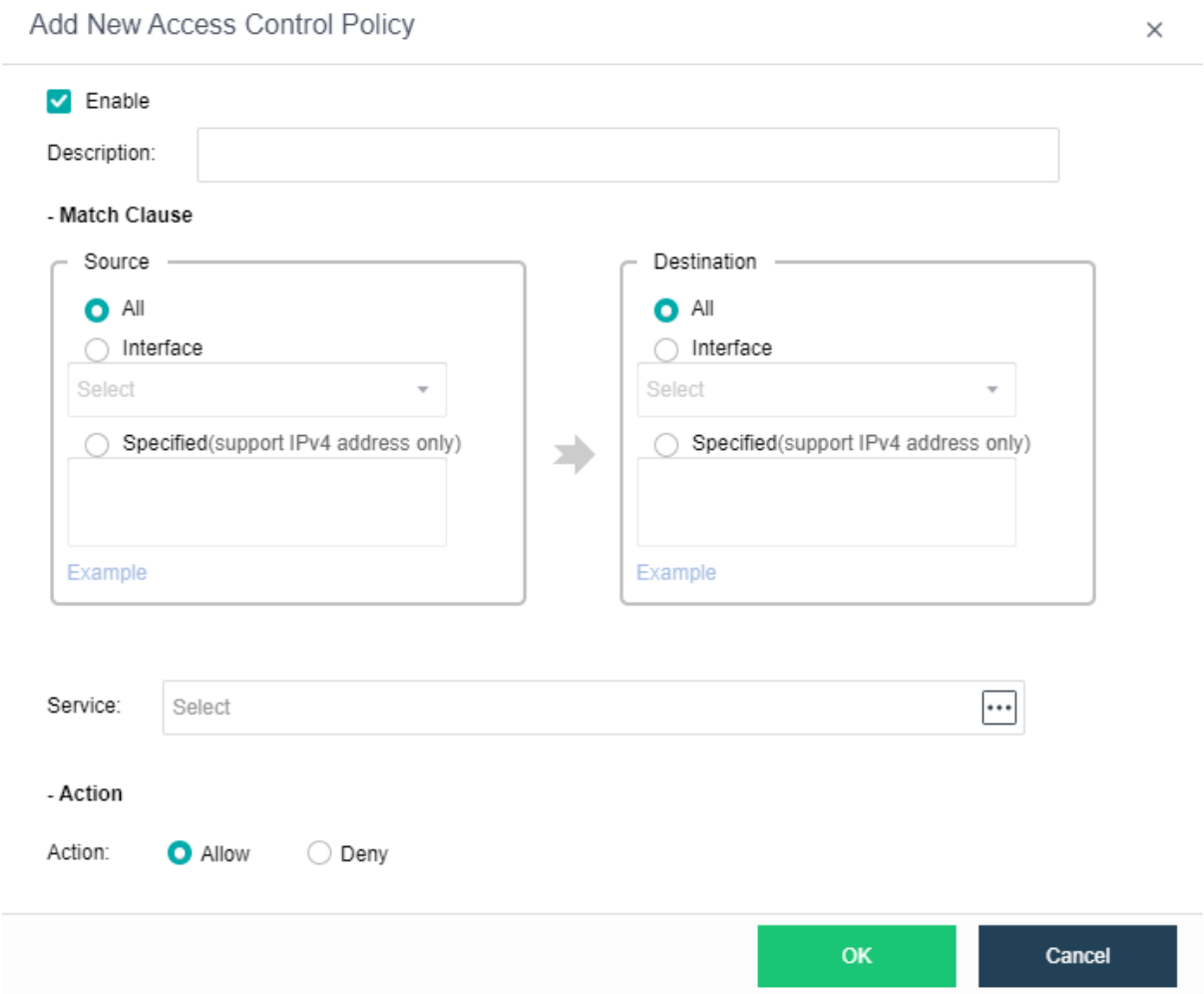
[Address Translation]: Specifies mapped destination IP address and mapped port.

2.3.5.1.4 Configuring Access Control Policy

On the **Access Control** tab, you can add an access control policy. There is a default access control policy which can be enabled or disabled but not deleted.



To add an access control policy, click **Add** to enter the following page:



Enabled: Select this option to enable the policy.

Description: Descriptive information of the policy.

Filter: Specifies **Source** and **Destination**.

All: Indicates any source or destination IP address.

Interface: Specifies source or destination interface.

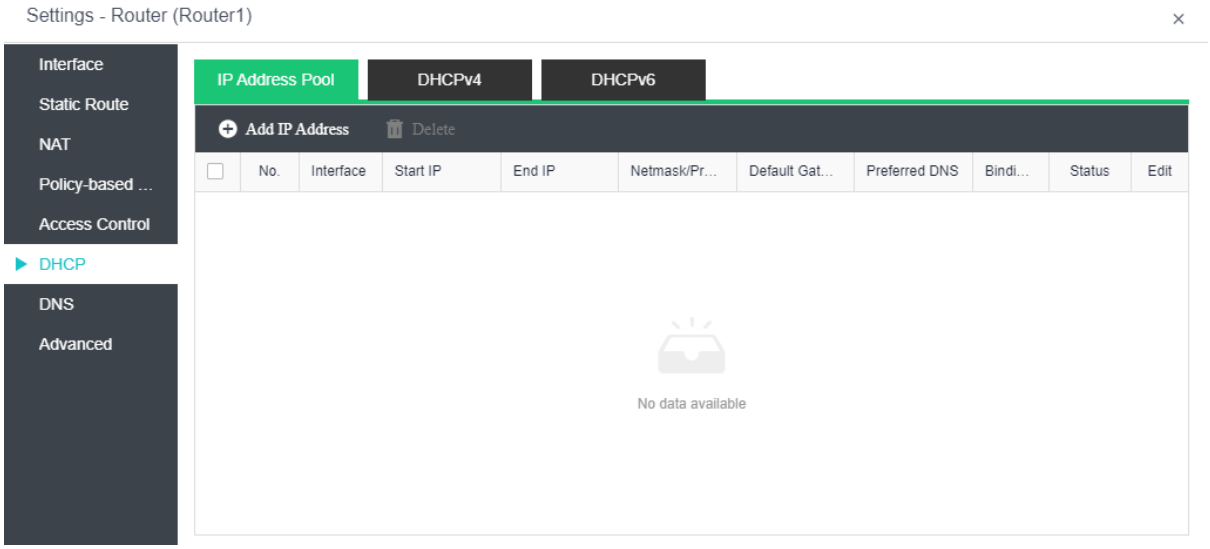
Specified: Specifies specific source or destination IP address.

Service: Specifies service, such as WEB, DNS and other services.

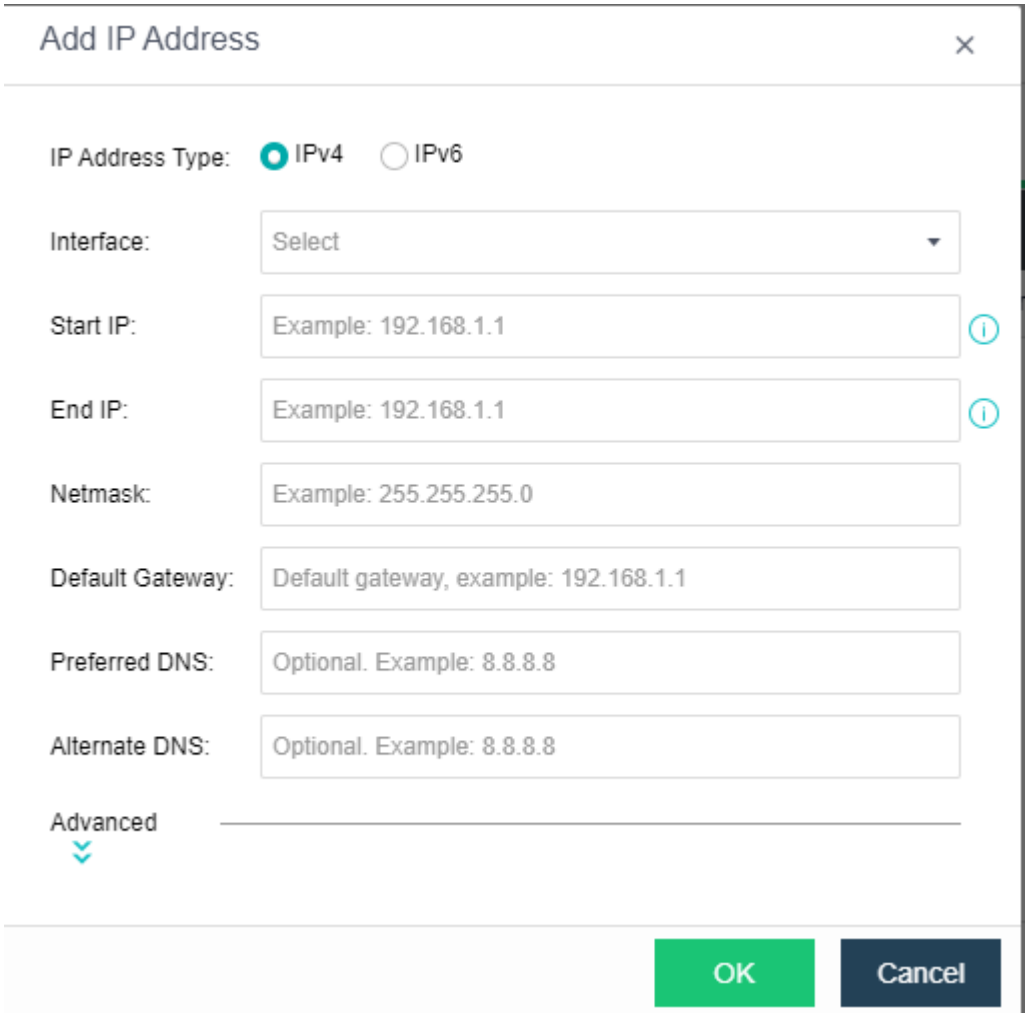
Action: Specifies action against matching packets. To allow the packets, select **Allow**. To reject packets, select **Reject**.

2.3.5.1.5 Configuring DHCP

DHCP is used to automatically assign IP addresses to virtual machines. You can configure DHCP address pool on the **IP Address** Pool tab and view status of assigned IP addresses on the **Status** tab.



To add IP address pool, click **Add IP Address** on the **IP Address Pool** tab.

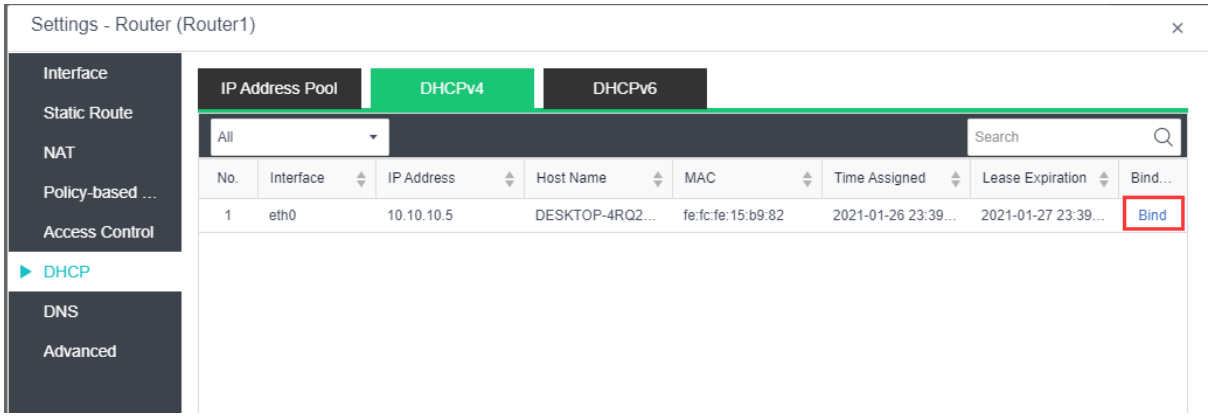


On the above page, specify **IP Address Type, Interface, Start IP, End IP, Netmask, Default Gateway, Preferred DNS** and **Alternate DNS**.

Advanced: You can specify **Preferred WINS, Alternate WINS,** and **Lease**. As for **Lease,** it specifies the period that allocated IP addresses can be used, as shown below:

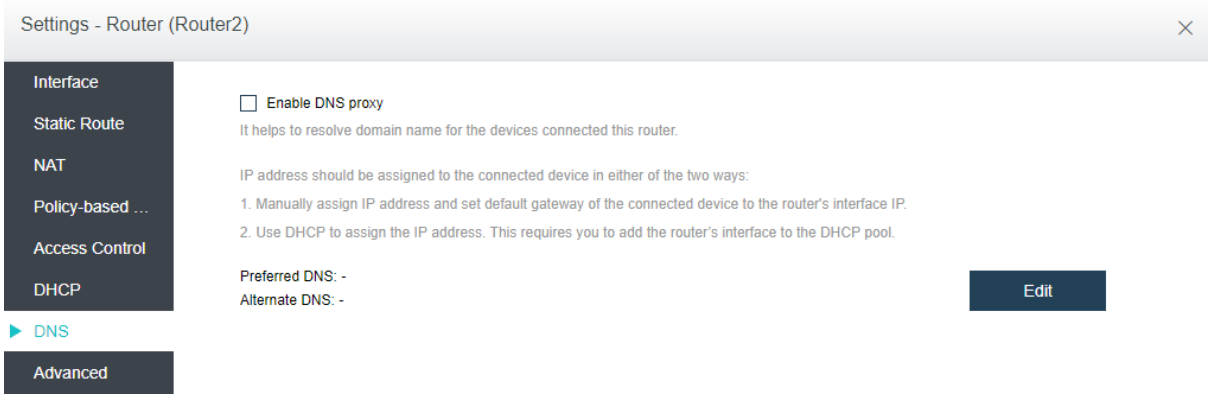
On the **DHCPv4/DHCPv6** tab, it displays the following information: **Interface, IP Address,**

Host Name, MAC, Time Assigned, Lease Expiration and **Bindings**. To bind IP address with a corresponding host, click **Bind** and specify MAC address. Thus, the IP address will be only assigned to the host with the specified MAC address.



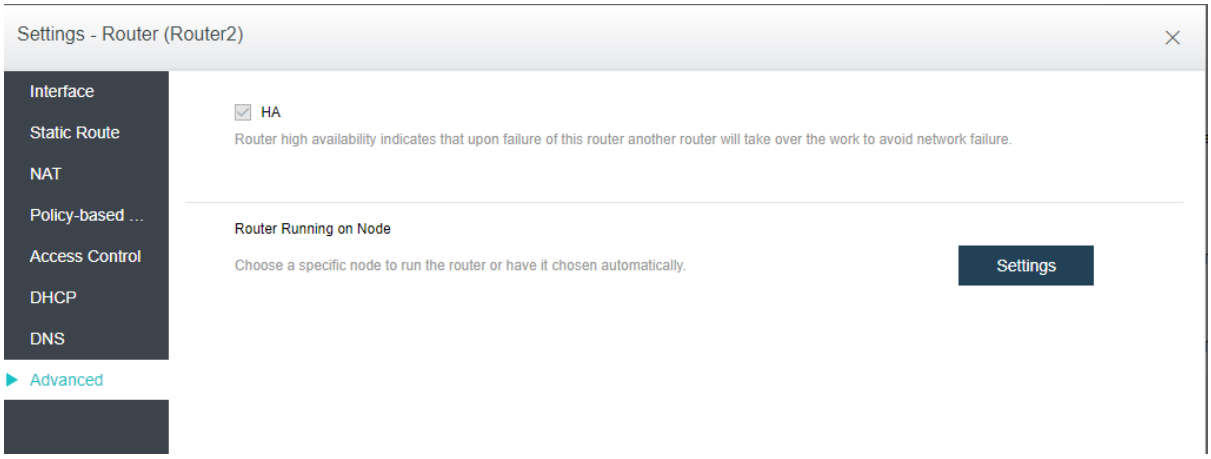
2.3.5.1.6 Configuring DNS

DNS proxy can help to resolve domain names for the devices connected to the virtual router. To edit DNS server, click **Edit**.



2.3.5.1.7 Configuring Advanced Settings

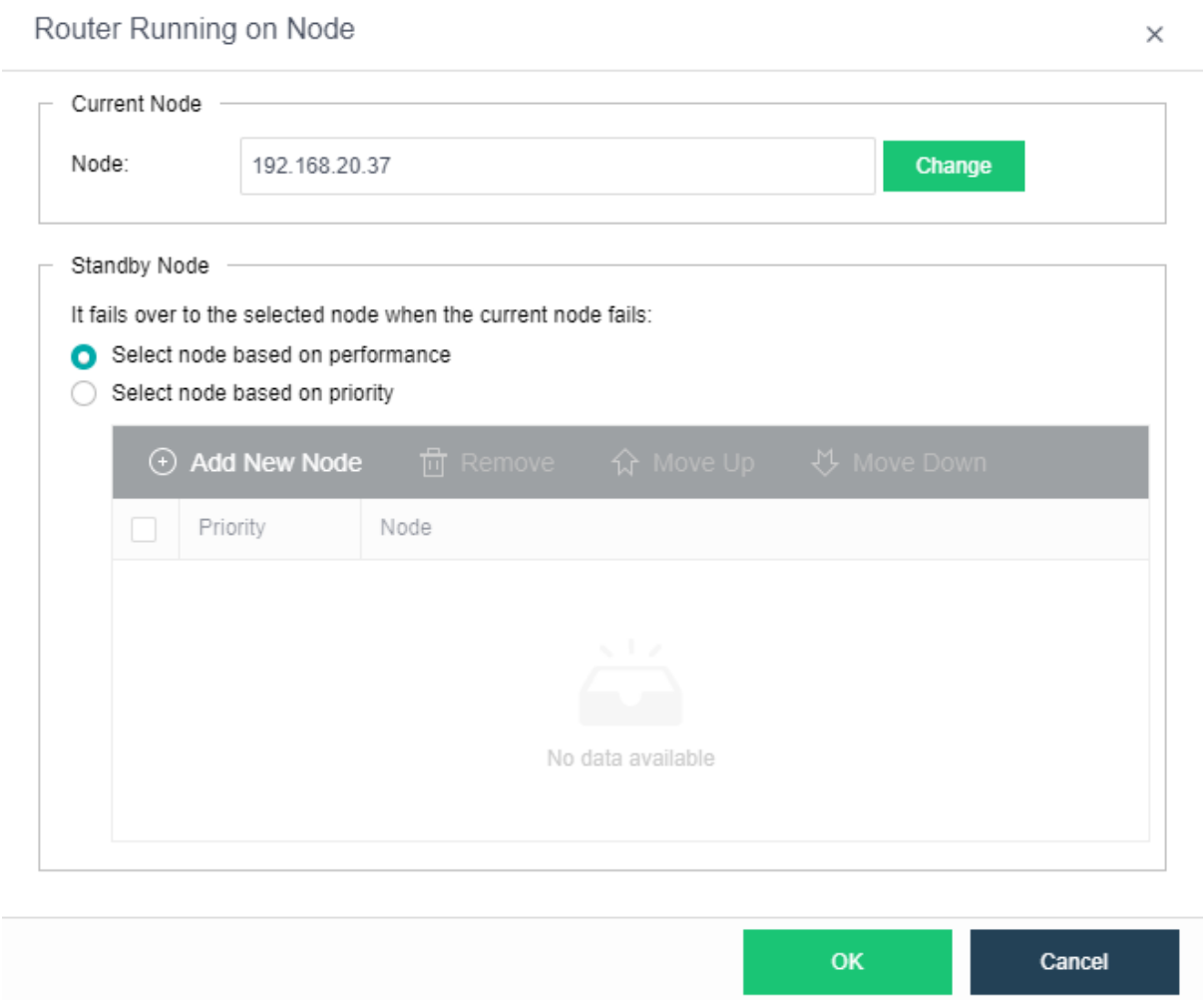
On the **Advanced** tab, you can enable high availability (HA) and specify a node to run the virtual router.



To enable HA, select the option HA. If HA is enabled, a second router will be built on another node and synchronize data in real time. If one node fails, the second router will take over seamlessly. However, synchronizing data between the two routers will consume extra network bandwidth.

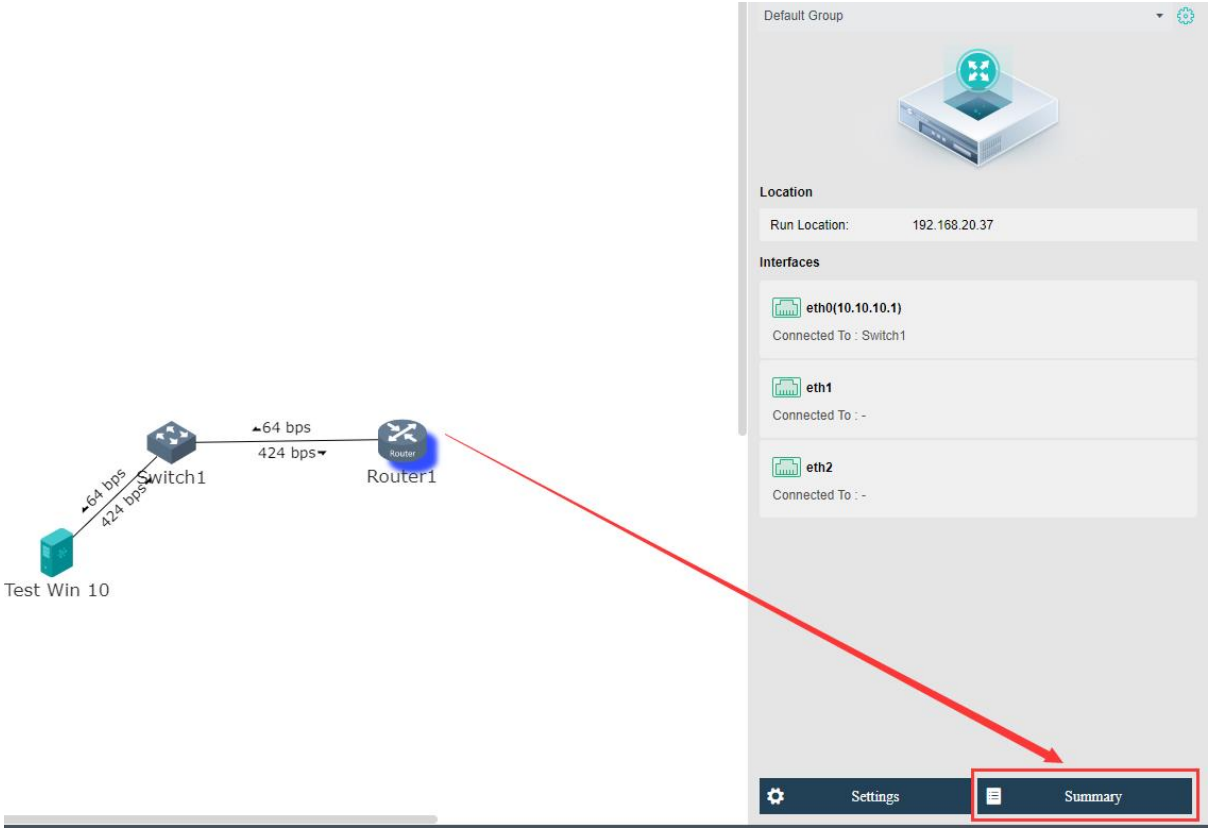
Without high availability enabled, the router will still recover to a second node, but it will take longer to get up and running.

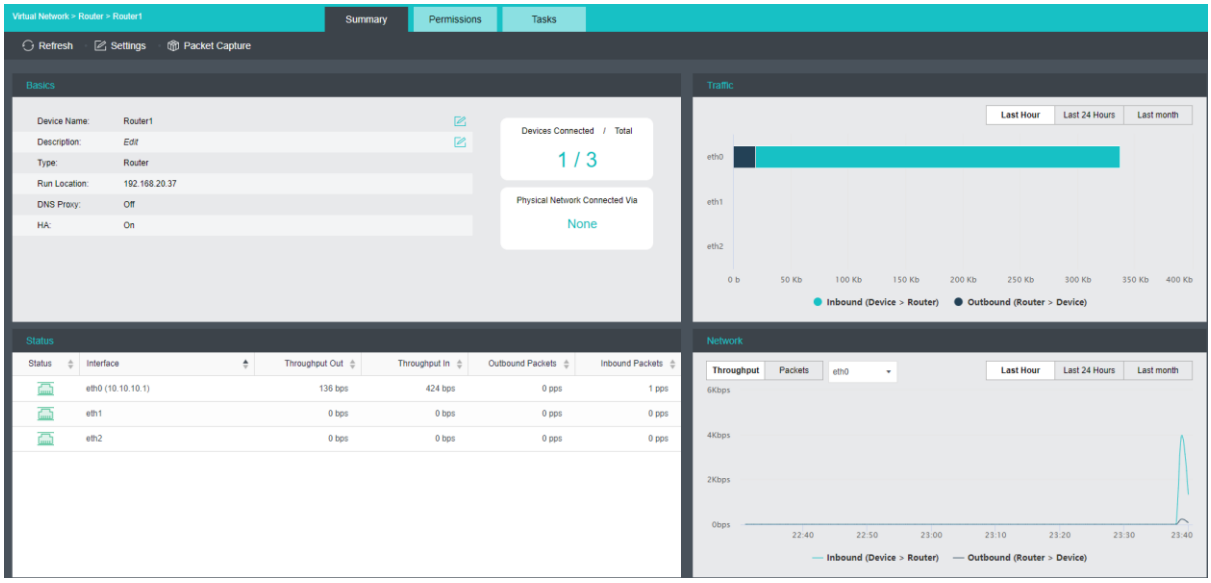
[**Router Running on Node**]: By default, the node where the router runs is automatically selected according to the settings on the following page. You can change the current node running the router as per your need.



2.3.5.2 Viewing Router Summary

You can view detailed information of a virtual router by selecting the router and clicking **Summary** button. On the **Summary** page, it displays **Basics, Traffic, Status** and **Network**. On the **Admin Logs** page, it displays administrator logs.

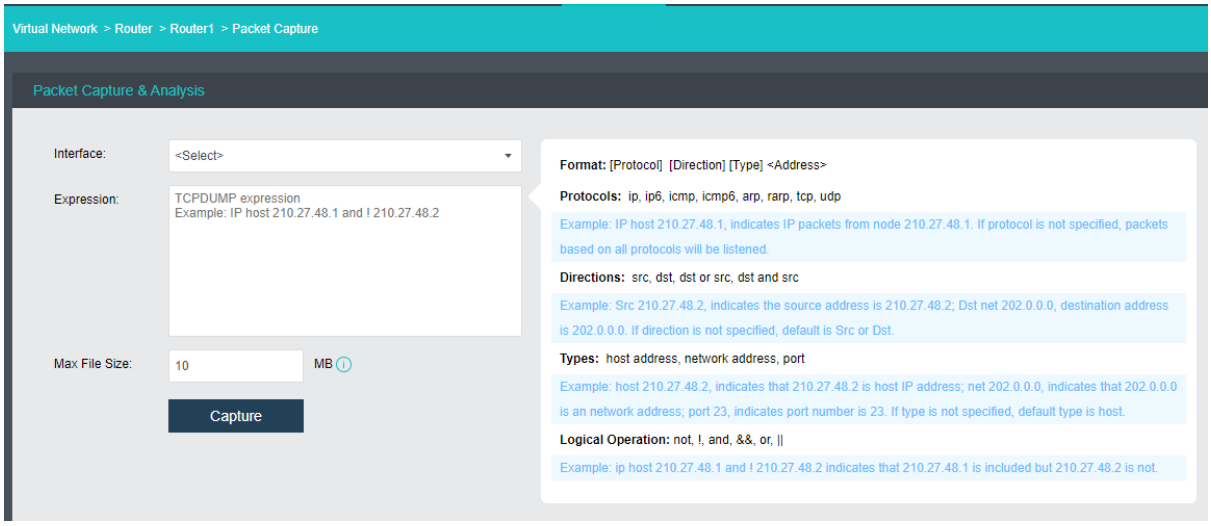




To reload the current page, click **Refresh**.

To configure the virtual router, click **Settings**.

To capture and analyze packets, click **Packet Capture**, as shown below:

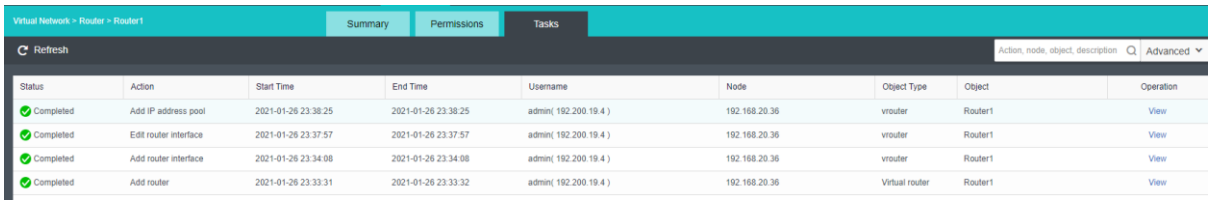


Interface: Specifies the interface. The packets passing through that interface will be captured.

Expression: Specifies expression to filter packets. On the right panel of the **Packet Capture & Analysis** page, it displays the expression formats.

Max File Size: Specifies the maximum size of the file. If a file size is larger than the maximum, capturing packet will stop.

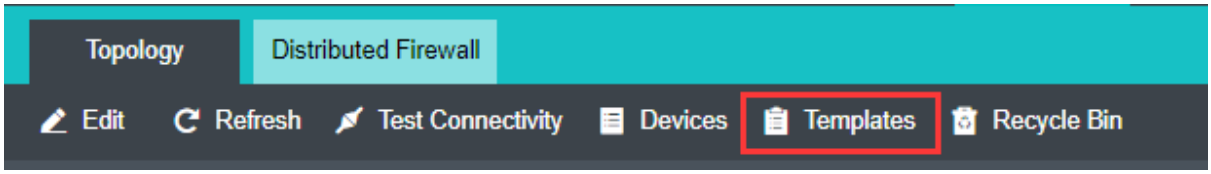
Tasks: This section displays administrator logs, which record various operations on the router, performed by administrator, such as adding an interface. Each log contains the following information: **Status, Action, Start Time, End Time, Username, Node, Object Type, Object** and **Operation**. To view log details, click **View** in **Operation** column.



2.3.6 Configuring Virtual Network Device

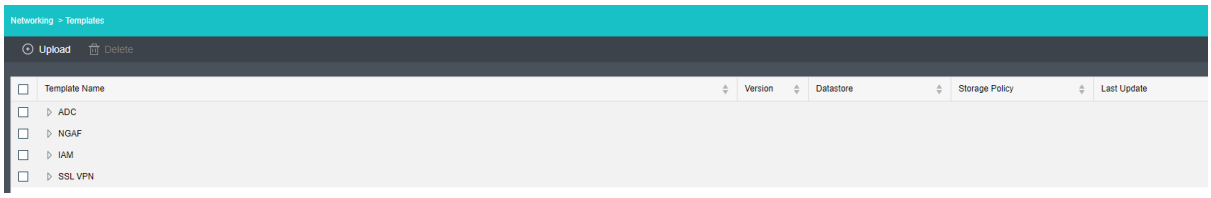
Currently, the virtual network devices(NGAF, ADC, IAM, SSL VPN and WOC) could be deployed into virtual network in **Networking**.

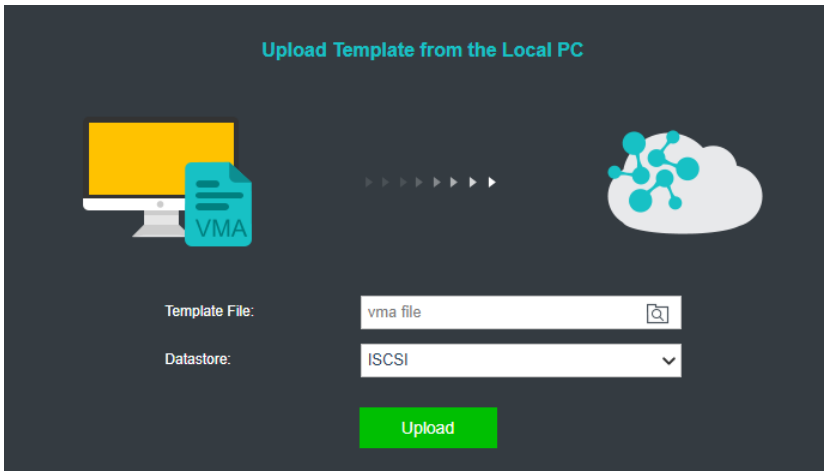
Navigate to **Networking** and click **Templates**, as shown below:



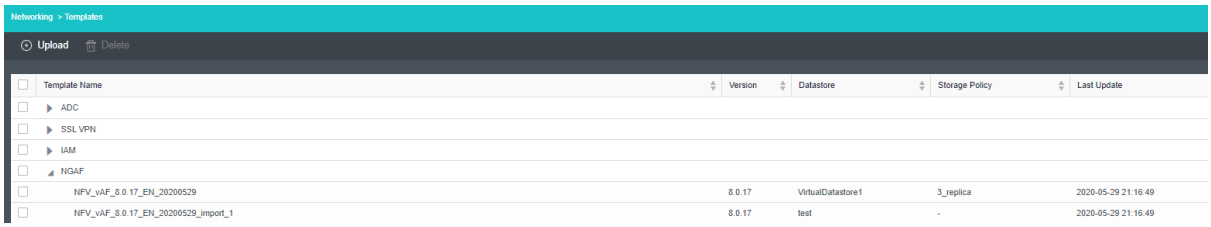
2.3.6.1 Uploading Template

In **Networking > Templates**, you can upload the .vma file of a virtual network device. To upload a template file, click **Upload**, select the **vma** file that you want to upload, and specify datastore. Then click **Upload** to start upload.

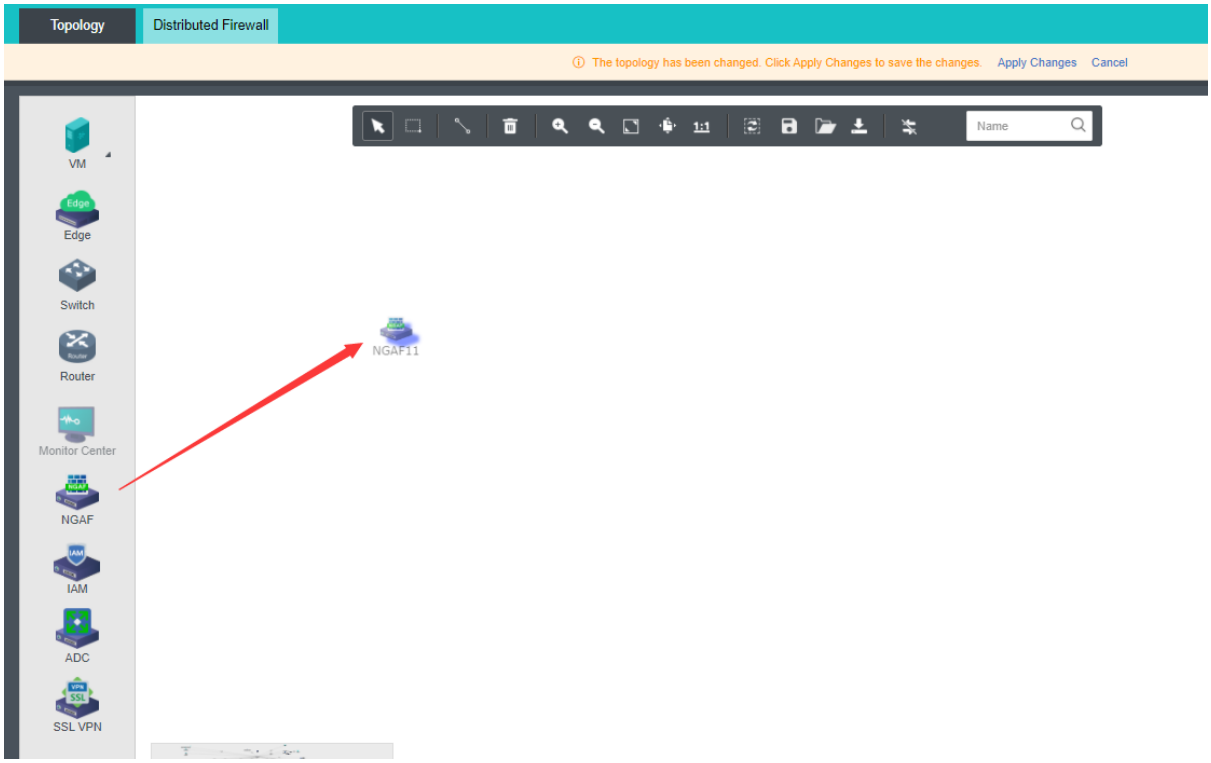


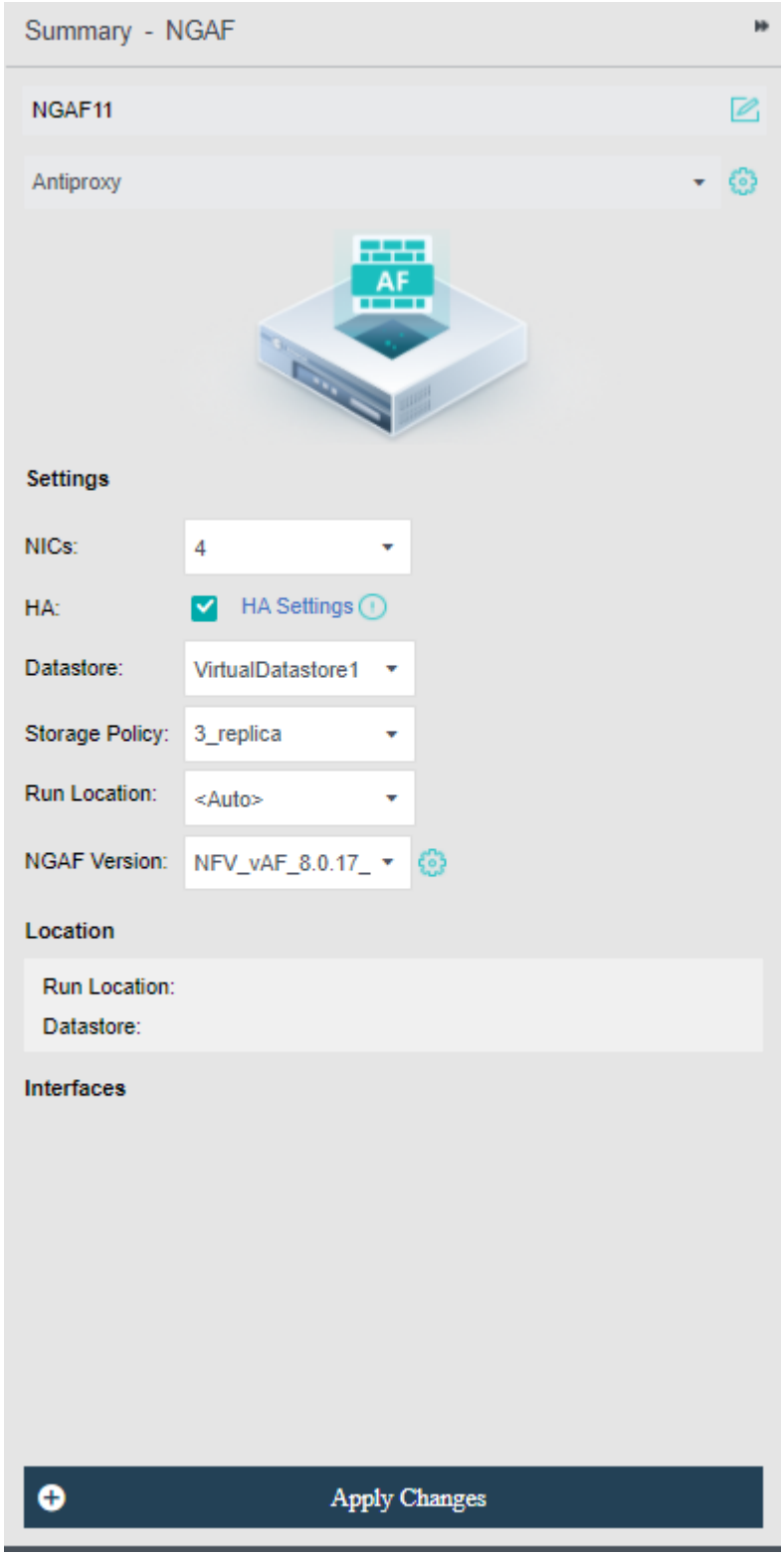


If the template file is uploaded successfully, you will see its information in the template list, as shown below:



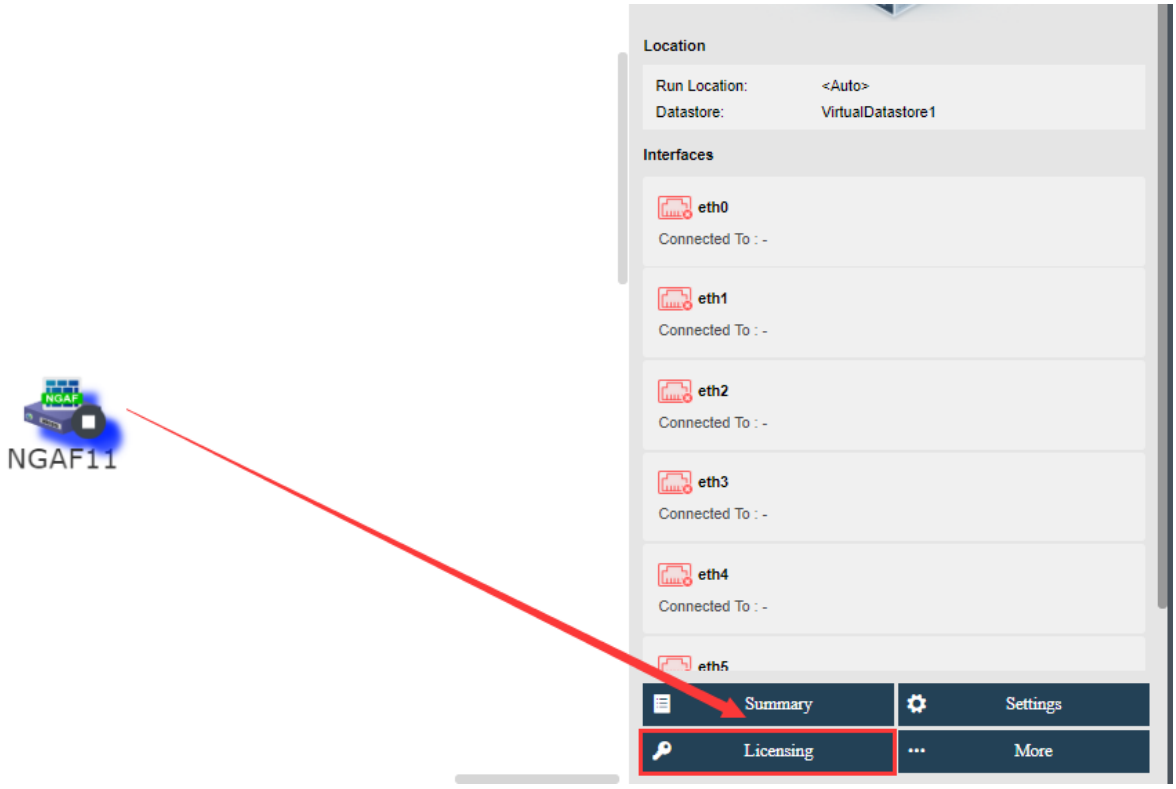
To create a virtual network device, drag the virtual network device onto the canvas and configure the basic information, **then** click **Apply Changes**.


Topology
Distributed Firewall
The topology has been changed. Click Apply Changes to save the changes.
Apply Changes
Cancel
Name
VM
Edge
Switch
Router
Monitor Center
NGAF
IAM
ADC
SSL VPN
NGAF11

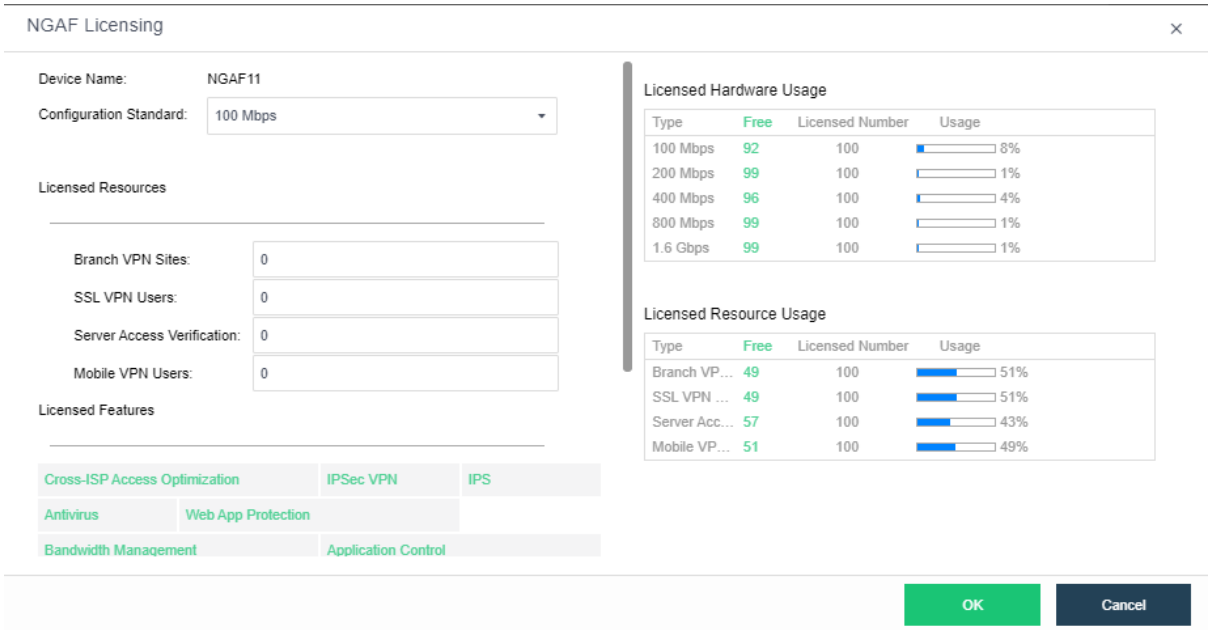


2.3.6.2 Licensing Virtual Network Device

After a virtual network device is **created**, you need to license it before using it.



To license virtual network device, click **Licensing** button, as shown below:



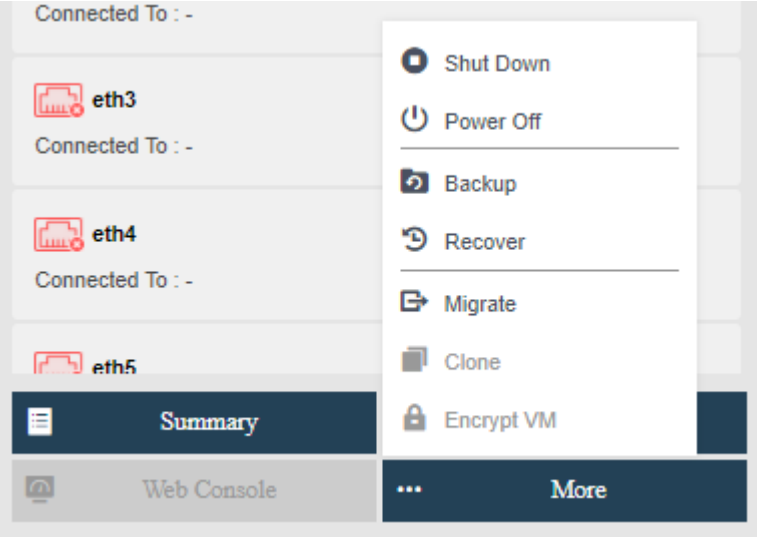
Device Name: Displays the name of the virtual network device.

Configuration Standard: Specifies bandwidth for the virtual network device.

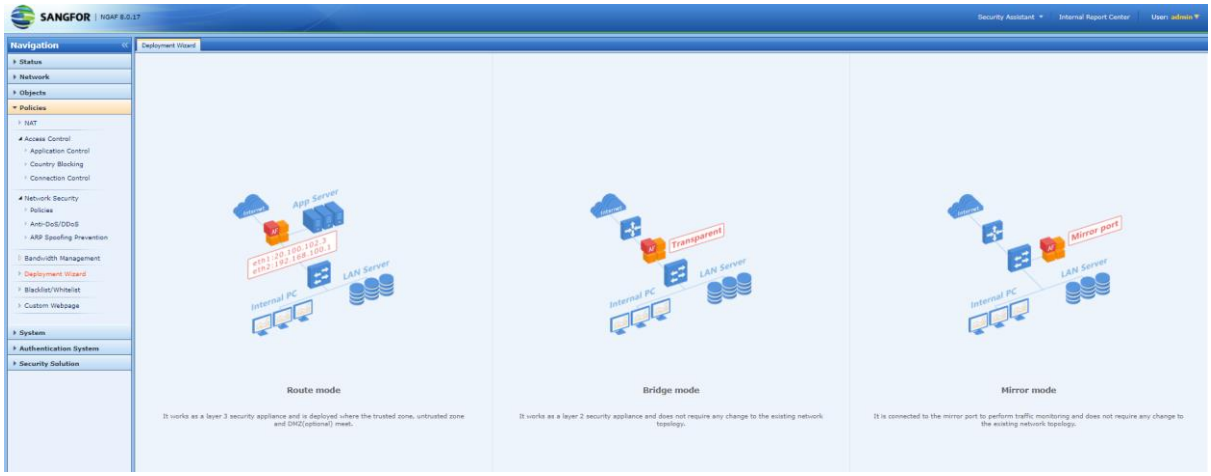
Licensed Resources: Specifies licensed resources of the virtual network device.

Licensed Features: Displays licensed functions.

When the virtual network device is successfully licensed, it will be automatically restarted and then you will **see** the **Web Console** and **More** buttons on the right panel in **Networking**. To perform more operations against the virtual network device, click **More,** and select an operation, such a**s Shut Down, Power Off, Backup, Recover, Migrate ,Clone,** and **Encrypt VM**.



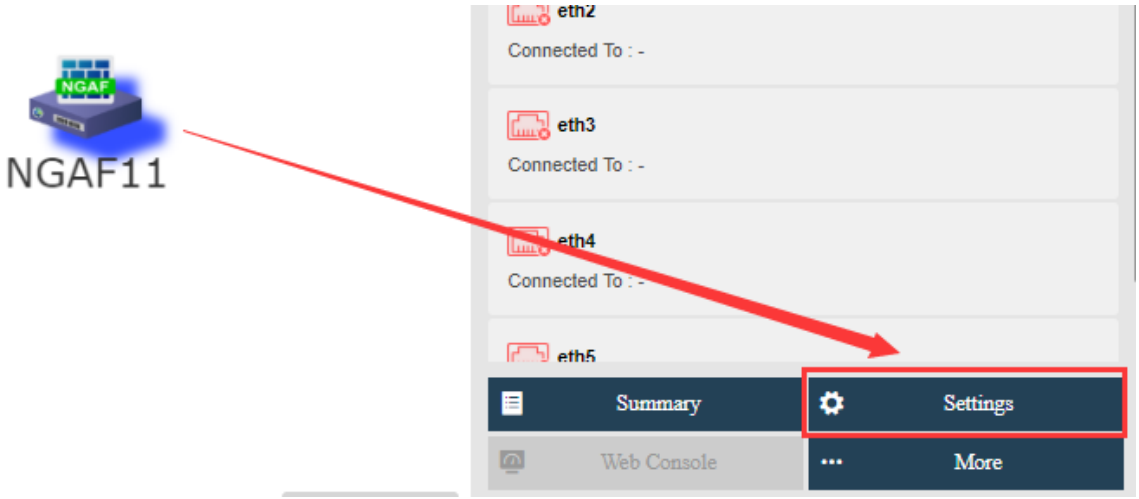
To enter Web admin console of virtual network device, click **Web Console**.



2.3.6.3 Configuring Virtual Network Device

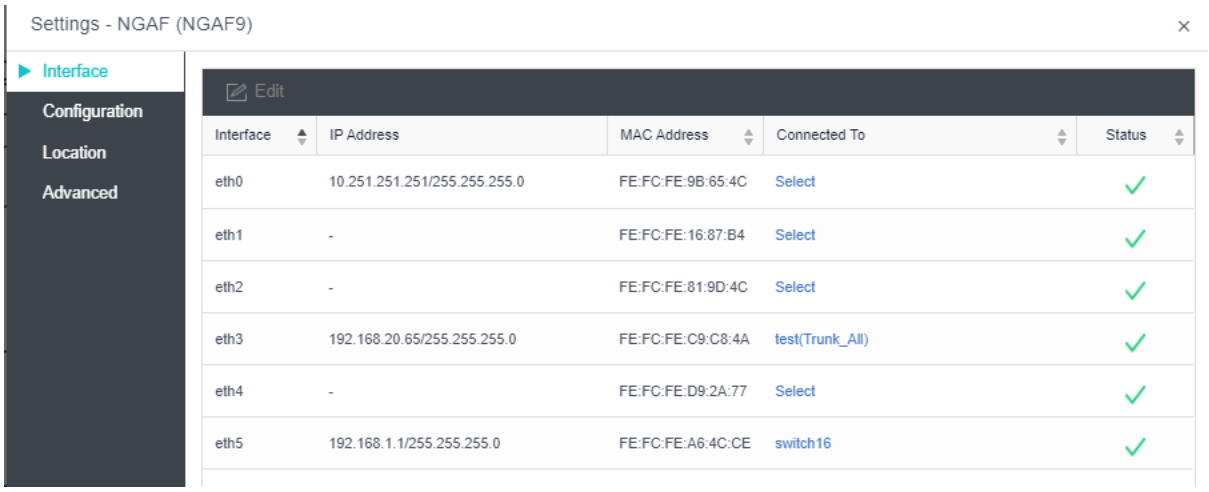
To configure a virtual network device, select it and click on **Settings** button to enter settings

page, as shown below:

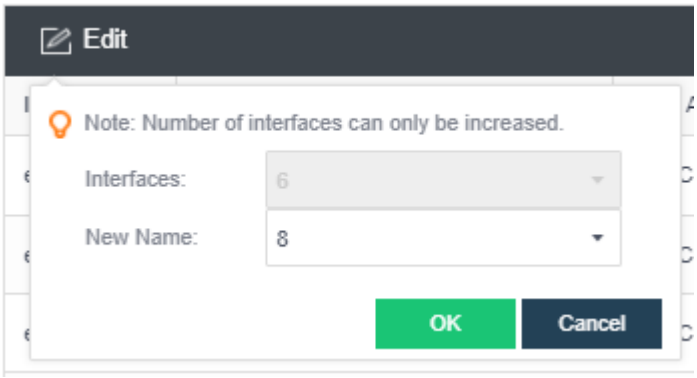


2.3.6.3.1 Configuring Interface

On the **Interface** tab, it displays the following information: **Interface, IP Address, Netmask, MAC Address, Connected To** and **Status**. To change number of interfaces, click **Edit**.



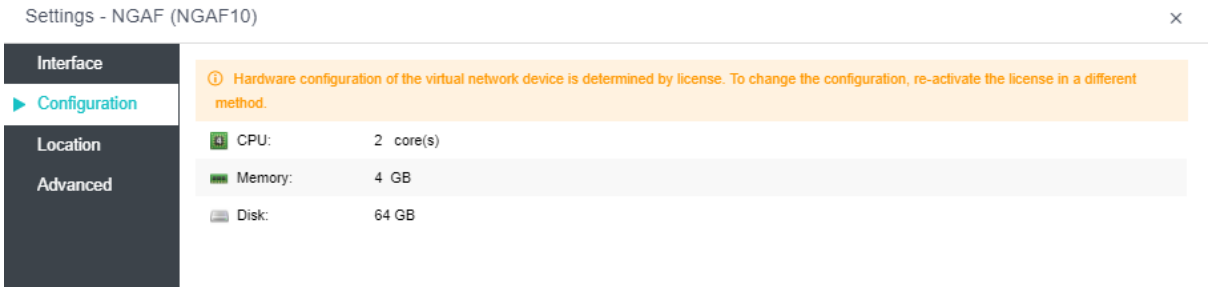
Interface	IP Address	MAC Address	Connected To	Status
eth0	10.251.251.251/255.255.255.0	FE:FC:FE:9B:65:4C	Select	✓
eth1	-	FE:FC:FE:16:87:B4	Select	✓
eth2	-	FE:FC:FE:81:9D:4C	Select	✓
eth3	192.168.20.65/255.255.255.0	FE:FC:FE:C9:C8:4A	test(Trunk_All)	✓
eth4	-	FE:FC:FE:D9:2A:77	Select	✓
eth5	192.168.1.1/255.255.255.0	FE:FC:FE:A6:4C:CE	switch16	✓



To enable an **interface**, click on the icon. To disable an interface, click on the icon.

2.3.6.3.2 Modifying Configuration

Hardware configuration is displayed on the **Configuration** tab, including CPU, memory and disk. Re-licensing is required in order to change the hardware configuration of the Virtual Network Device.

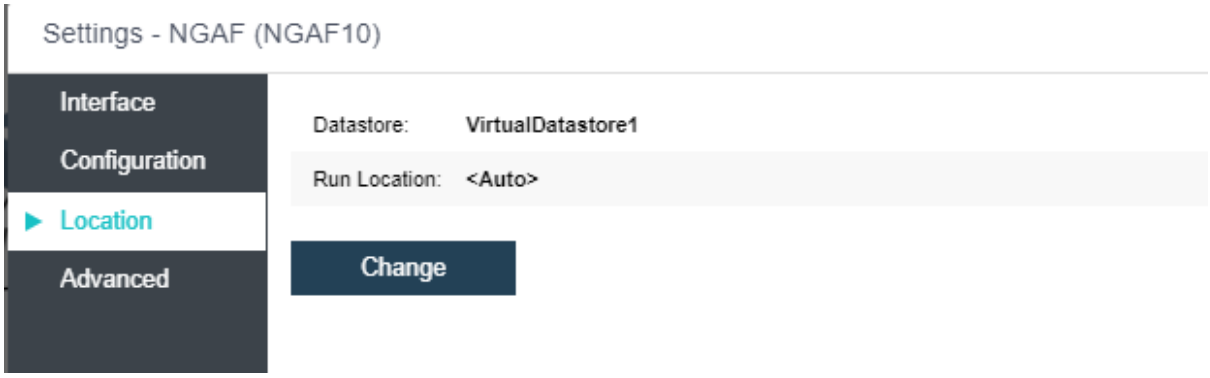


On the above page, you can modify hardware configuration on the right.

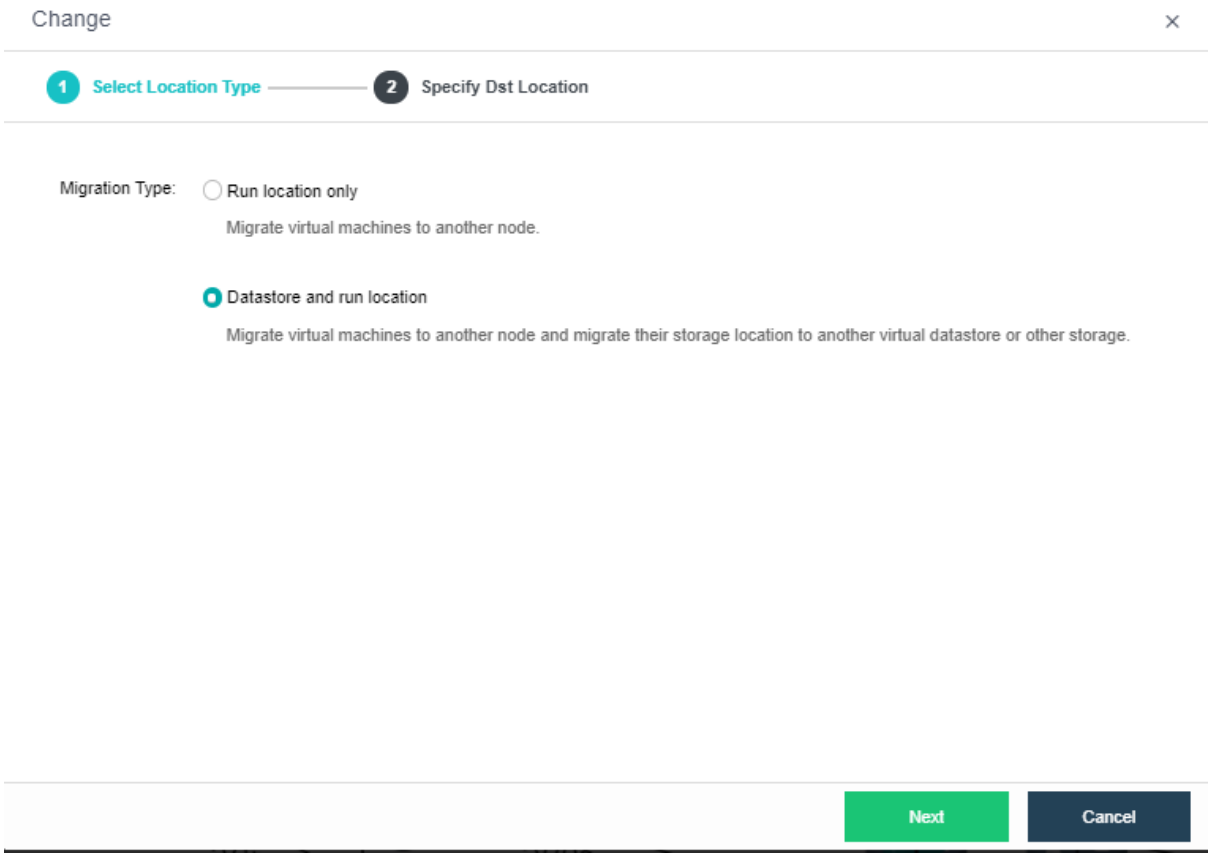
Hardware configuration can only be set higher.

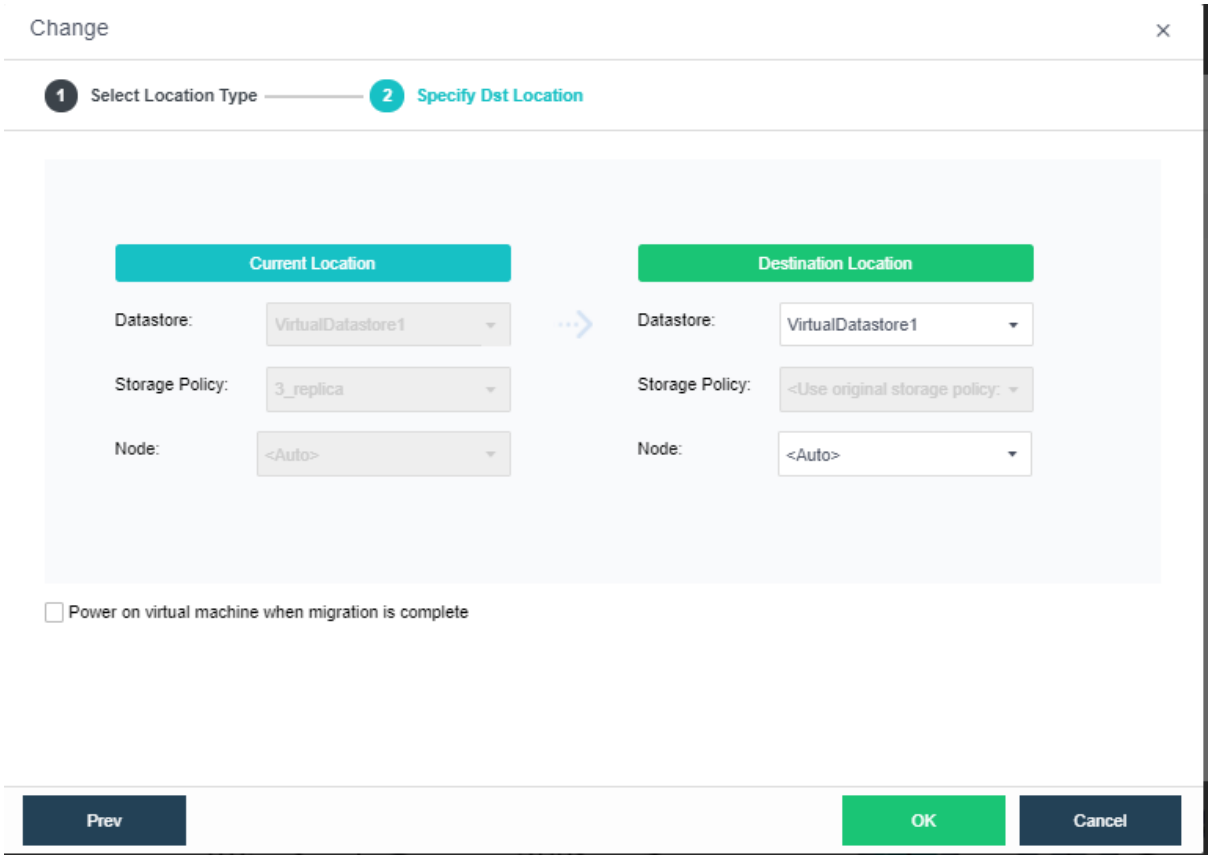
2.3.6.3.3 Changing Location

On the **Location** tab, it displays the datastore where the virtual network device is stored and the current node running the virtual network device.



To change the current location, click on the **Change** button to enter the following page and specify destination location.



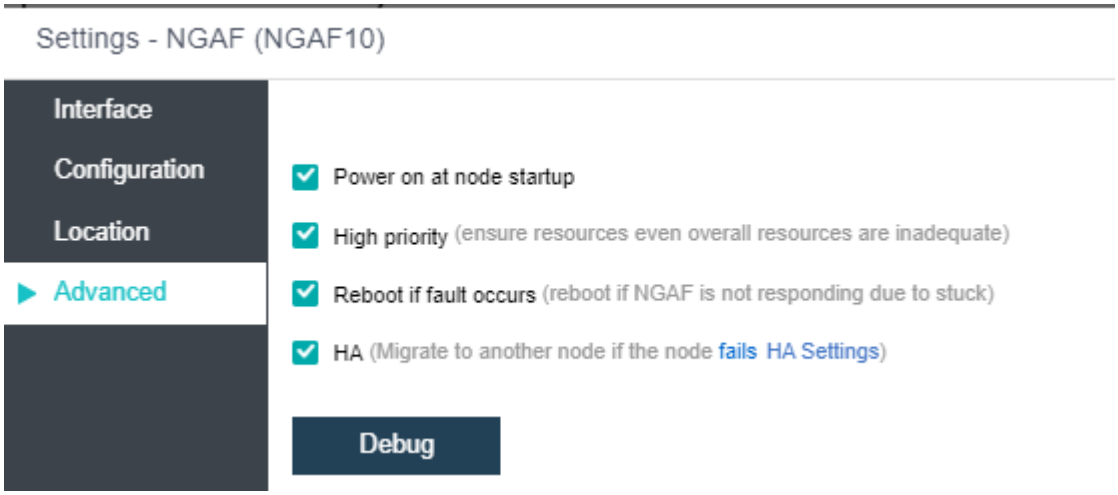


As shown above, the current location is displayed on the left side and the destination location can be specified on the right side.

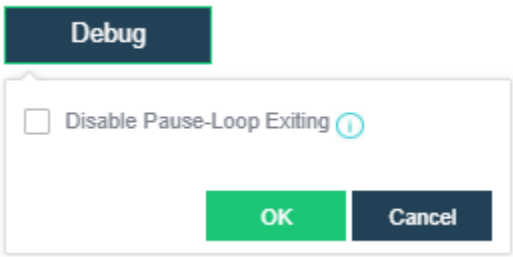
If the destination datastore is not shared, HA will not be supported.

2.3.6.3.4 Configuring Advanced Options

To have the virtual network device power on upon node startup, select **Power on at node startup**. High priority can ensure that the virtual network device has enough resources even when overall resources are inadequate. **Reboot if error occurs** enables virtual device to restart automatically when it is not responding due to stuck. **HA** enables virtual network device to be migrated to another node when the working node fails.

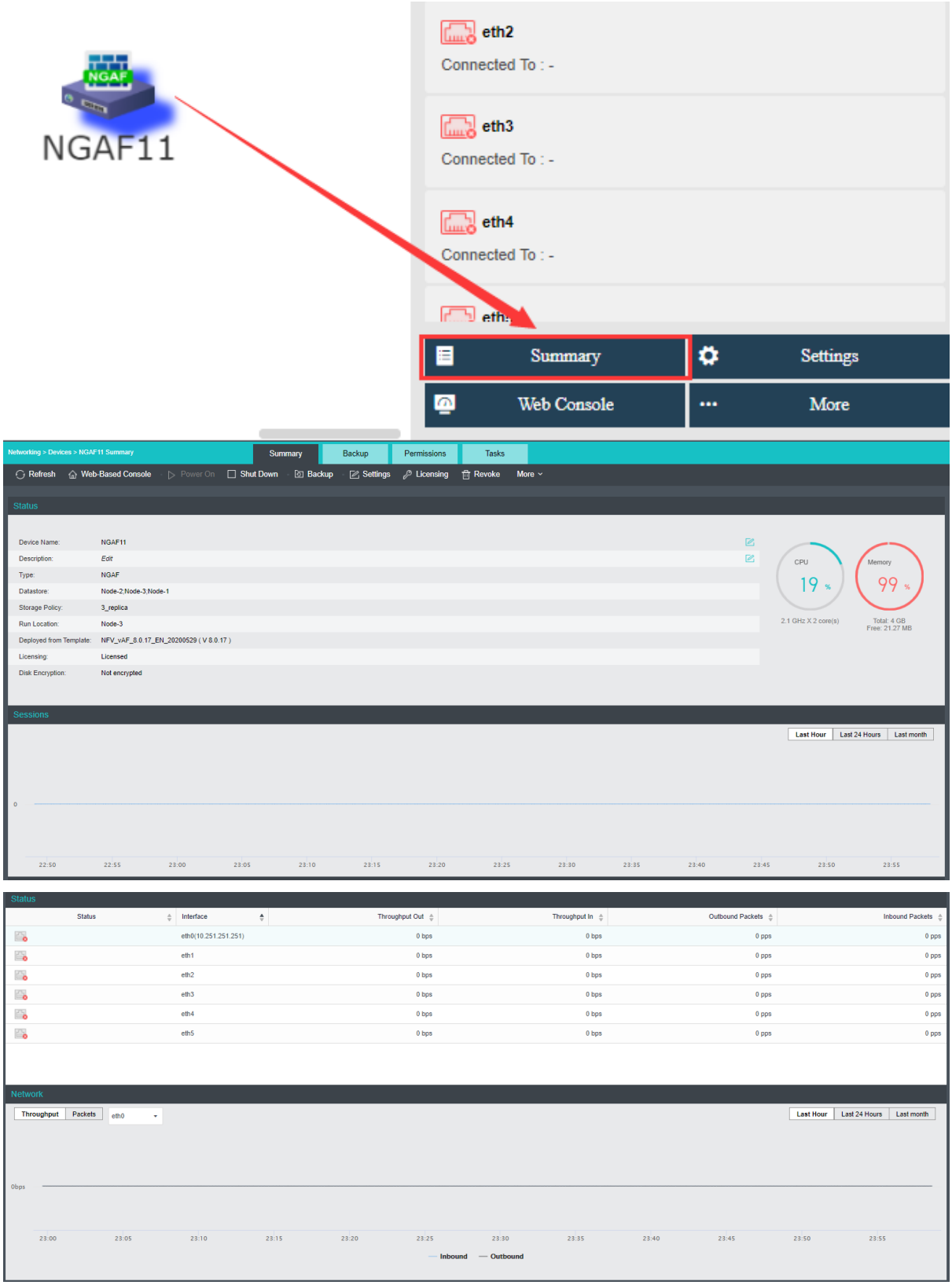


To configure debugging options, click **Debug** to enter the following page. On that page, you may select **Disk write caching**, which enables files on disks to be loaded to memory so as to improve disk IO performance.



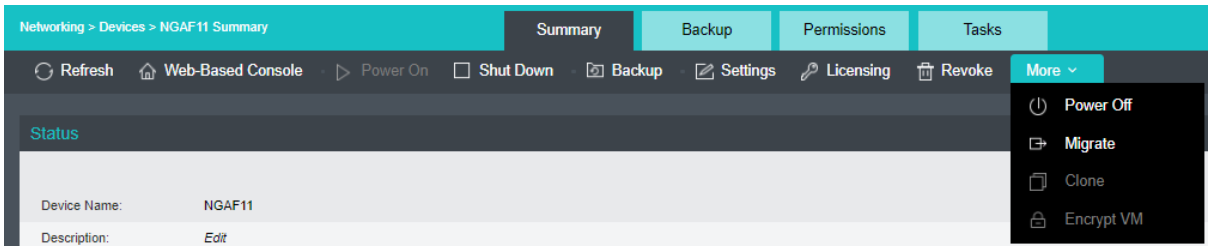
2.3.6.4Viewing Virtual Network Device Summary

You may view detailed information of virtual network device by selecting that device and clicking **Summary** button. The following information are displayed on the **Summary** page: device status, sessions, connection status, and inbound and outbound rate. On the **Admin Logs** page, you can view detailed operation logs.



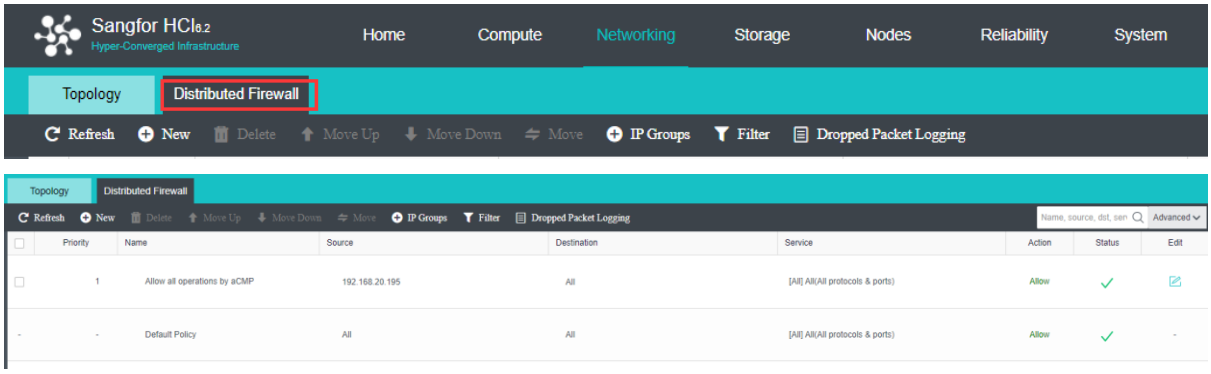
On the above page, you can perform the following operations: **Refresh, Web-based Console, Power On, Shut Down, Backup, Settings, Licensing,** and **Revoke**. Click **More** to perform

more operations, such as **Power Off**, **Migrate**, **Clone,** and **Encrypt VM**.

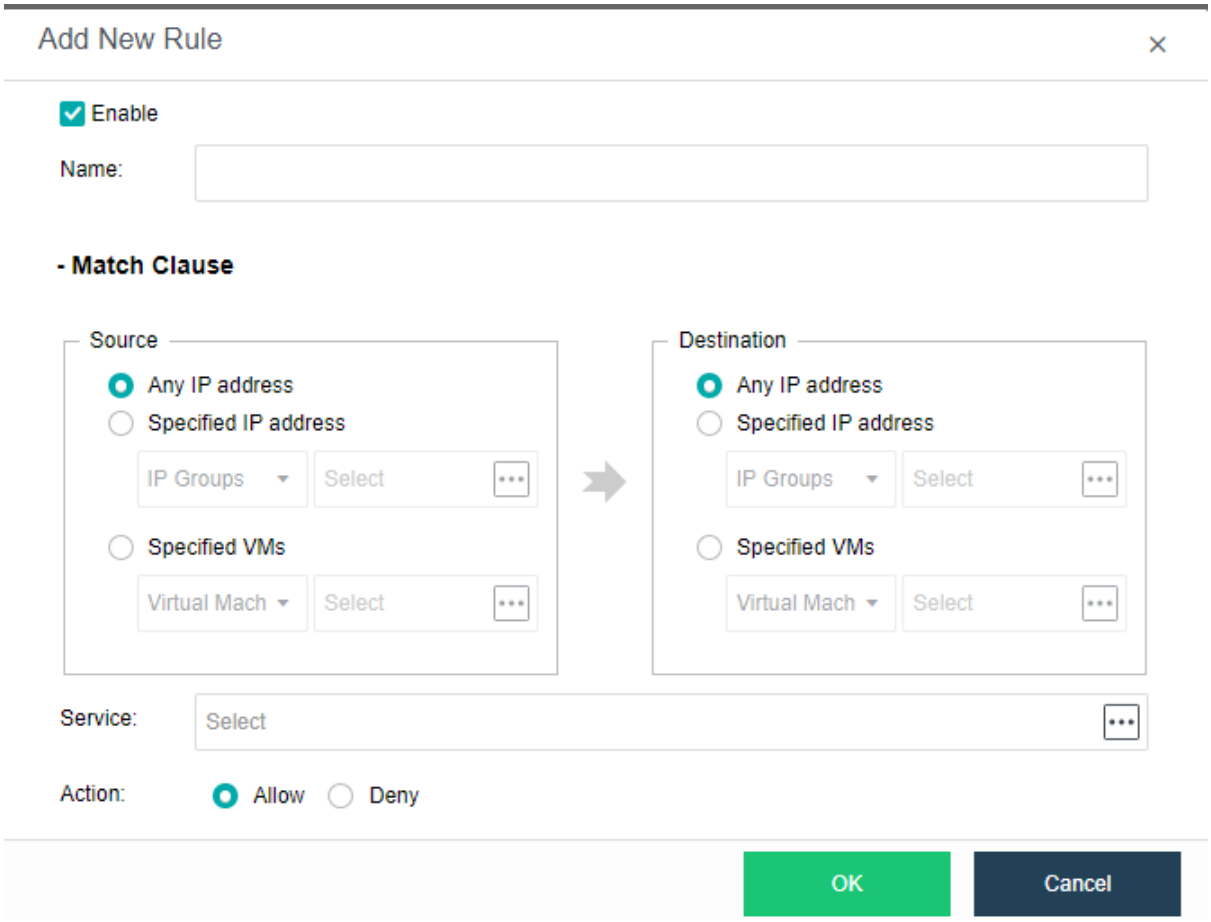


2.3.7 Distributed Firewall

Distributed firewall is supported starting from Sangor HCI 5.2 version, which can achieve control over access to any node based on virtual machine IP address, virtual machine, VM group or VM tag.



To configure a firewall rule, click **Distributed Firewall** in **Networking** and then click **New** to enter the following page.



To enable firewall rule, select **Enabled**.

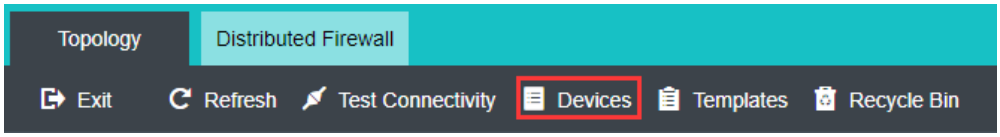
Name: Specifies a distinguishable name for the firewall rule.

Match Clause: For **Source** and **Destination**, options are **Any IP address**, **Specified IP address**, **Specified virtual machine**. If **Specified IP address** is selected, you may select **IP Groups** or **IP Addresses**. If **Specified virtual machine** is selected, you may select **Virtual Machine**, **VM Group**, or **Tags**.

Service: Specifies service(s) to which the firewall rule applies.

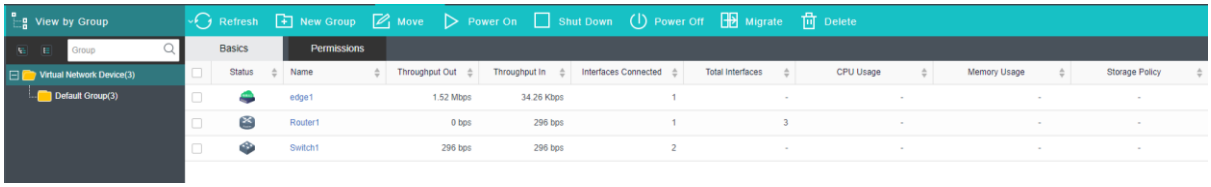
Action: Specifies action to matching service, **Allow** or **Deny**.

2.3.8 Viewing Virtual Network Devices



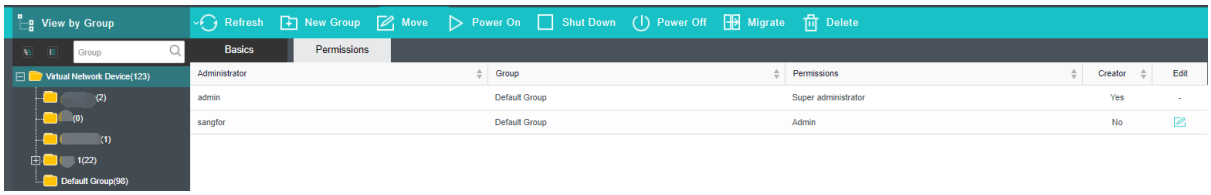
In **Networking > Devices**, there lists the following virtual network devices: virtual switches,

edge, virtual routers, NGAF, IAM, vADC. The **Basics** tab displays the following information: **Status**, **Name**, **Outbound**, **Inbound**, Interfaces, **Total Interfaces**, **CPU Usage**, **Memory Usage**, **Storage Policy**.



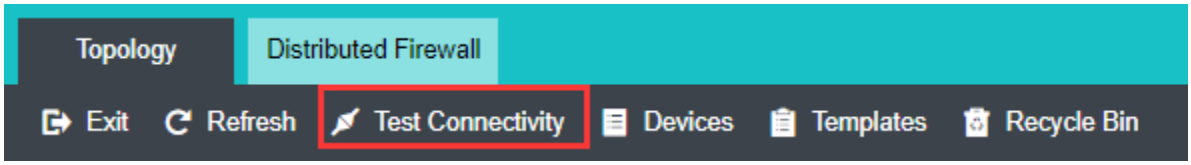
Virtual network devices can be created and added to different groups so that they can be managed by sub-administrators with different permissions.

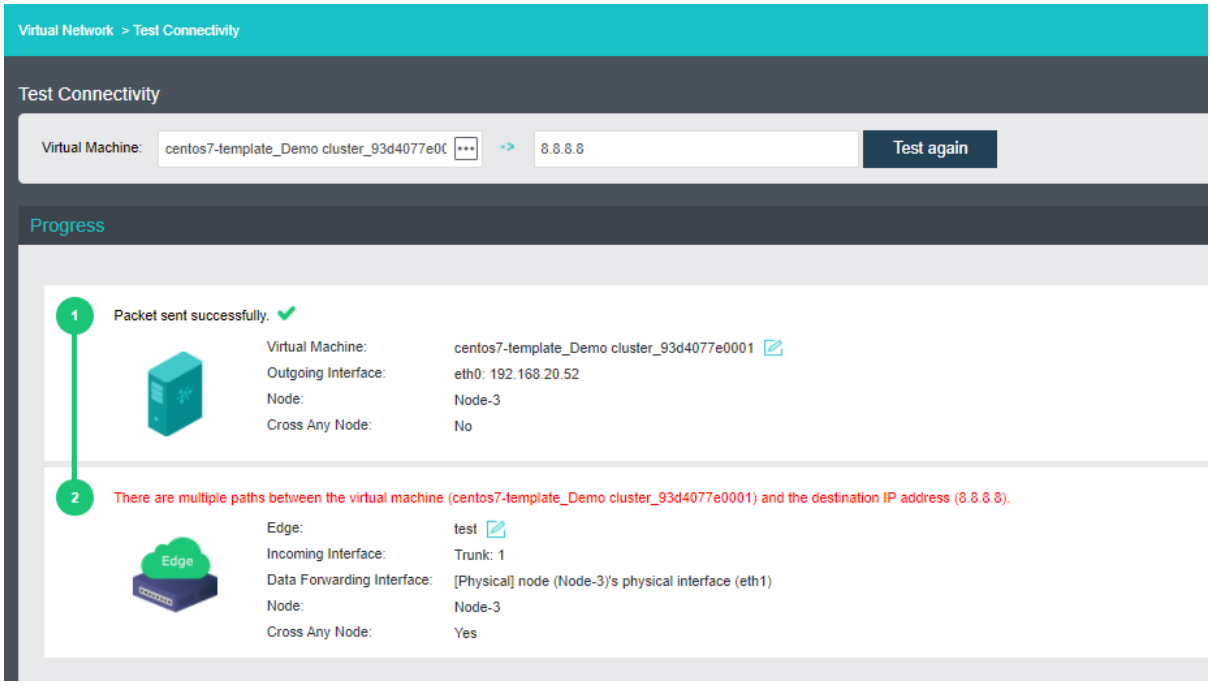
On the **Permissions** page, you can edit permissions of virtual network devices.



2.3.9 Testing Connectivity

Test Connectivity tool helps administrator to quickly and easily troubleshoot network issues, which just requires administrator to specify source and destination addresses. To test connectivity, specify a source virtual machine and destination IP address, then click Start, as shown below:

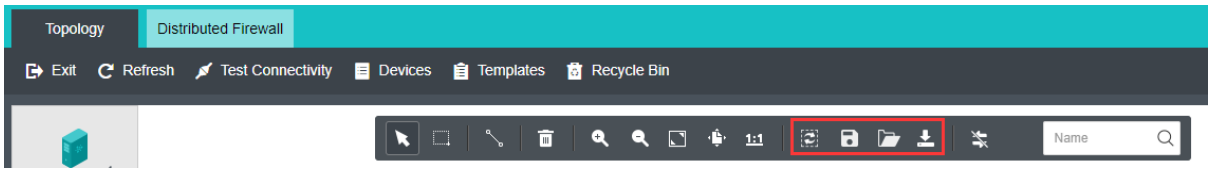




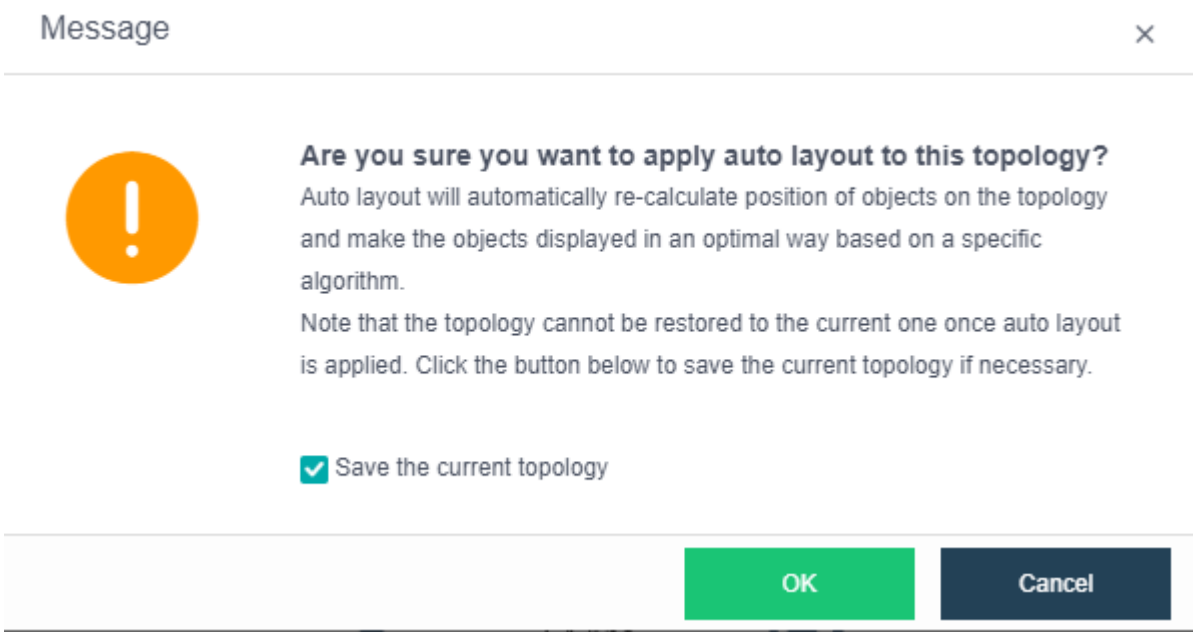
To test connectivity from a virtual machine, that virtual machine must be powered on and installed vmTools.

2.3.10 Virtual Network Topology

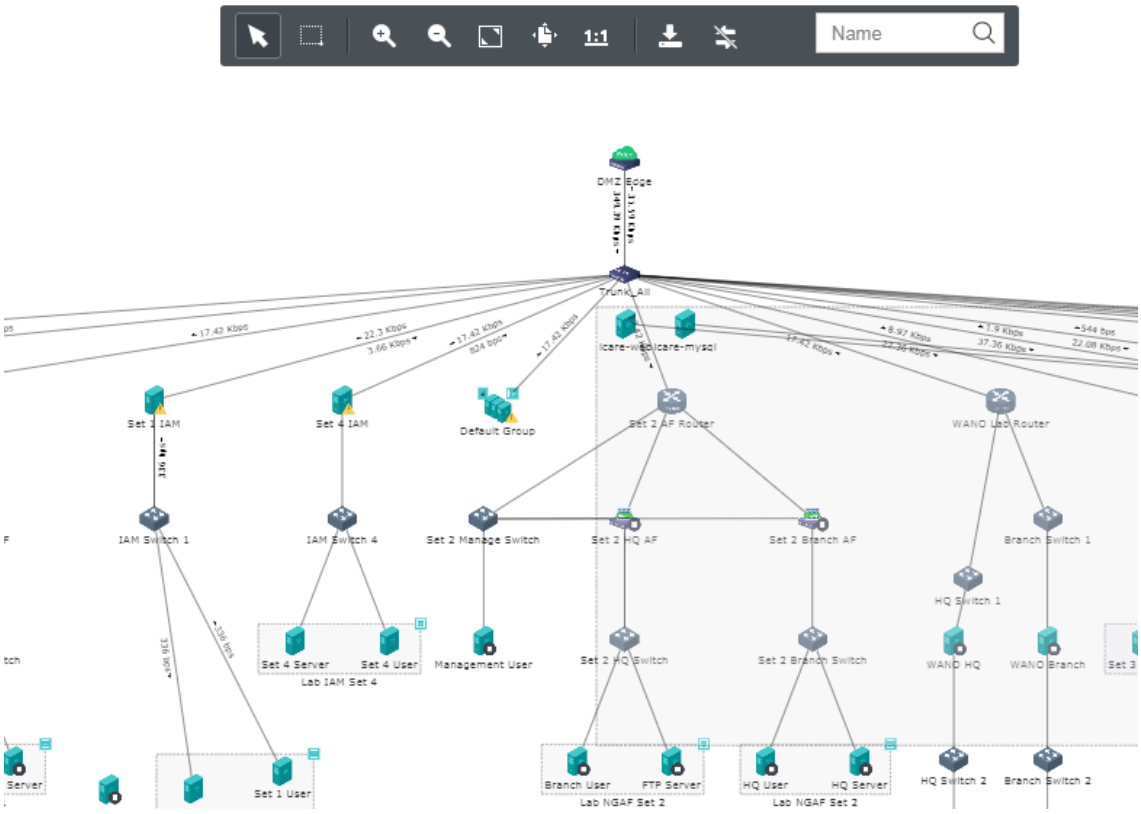
In HCI6.2.0 version, it supports auto layout, saving layout changes, restoring and exporting topology, and selecting all pages.



 : Auto layout enables objects on the topology to be displayed in an optimal way based on specific algorithms.



Before applying auto layout, you may save the current topology and then click **OK** to start applying auto layout.



Topology can be saved, restored and exported.

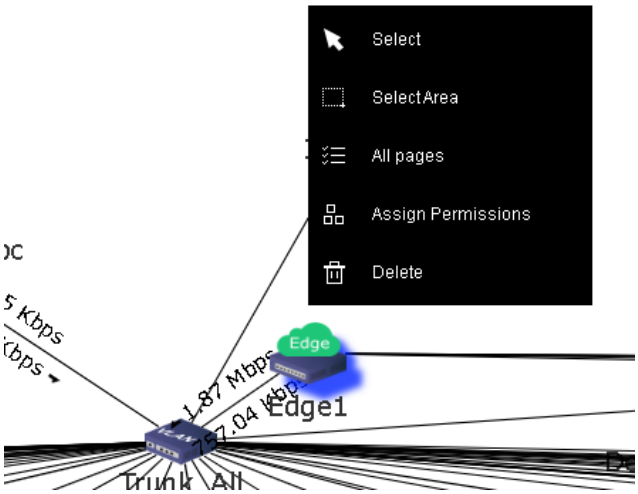
To save layout changes, you may click on  .

To view topologies, you may click on  .

To export the current topology, you may click on  .

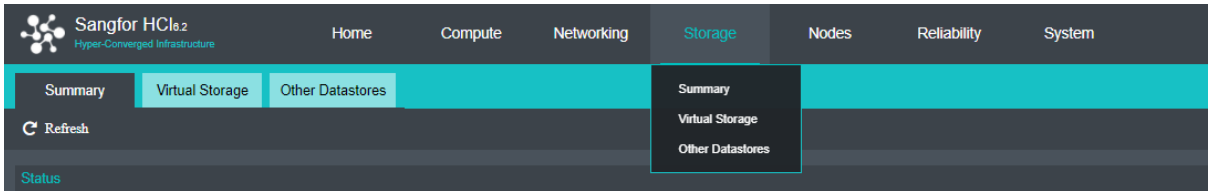
Connections cannot be restored once deleted.

To select all object that are connected to edge, select **All pages**,as shown below.



2.4 Storage

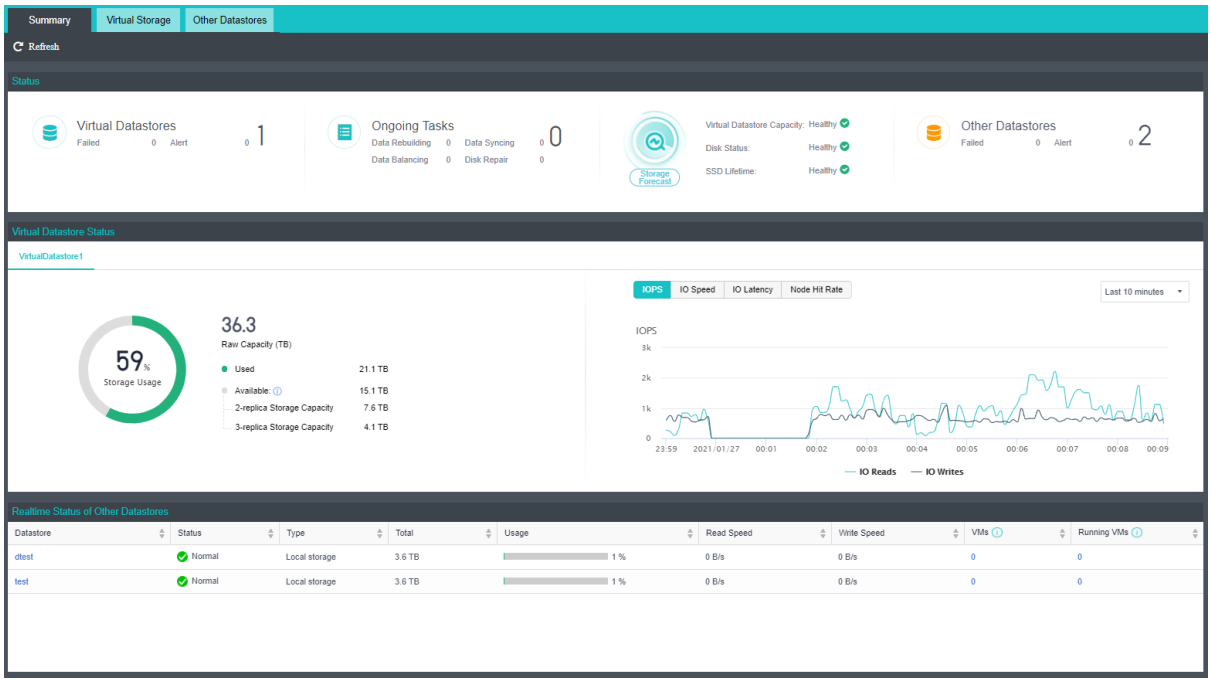
In **Storage**, there are three pages: **Summary, Virtual Storage** and **Other Datastore**.



2.4.1 Storage Summary

2.4.1.1 Storage Status

On the **Summary** page, it displays the following sections, **Status, Storage Usage, Realtime Status, Performance of Virtual Storage, Unread Alarms** and **Task Status**.

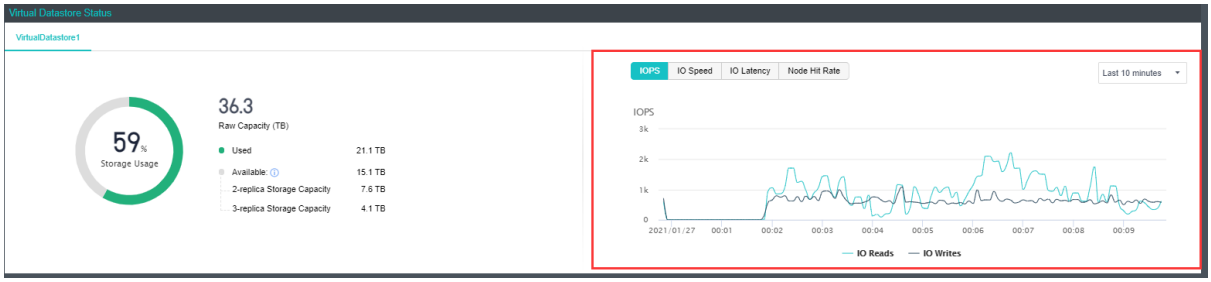


Status: This section displays the number of virtual datastores and other datastores, the status of those datastores, the number of unread alarms, and the number of ongoing tasks, as shown below:

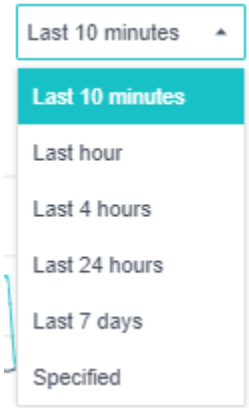
Virtual Storage Usage: This section displays the storage usage of the entire HCI, including

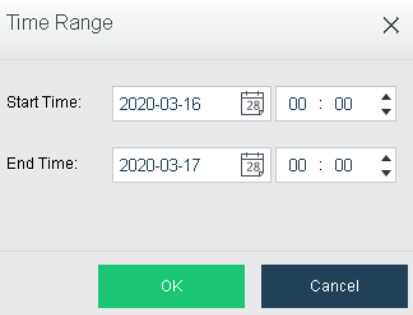
the total number of storage, the quantity already used, and the unused quantity. as shown below:

This section also displays IOPS, IO speed, IO latency, storage usage, cache hit rate, and node hit rate of the specified virtual datastore in different period, as shown below. On the following graph, you may view **IOPS, IO Throughput, IO Latency, and Node Hit Rate**.



To specify **Period**, you can choose **Last 10 minutes**, **Last hour**, **Last 4 hours**, **Last 24 hours**, **Last 7 days**, or **Specified** to customize a new period, as shown below:

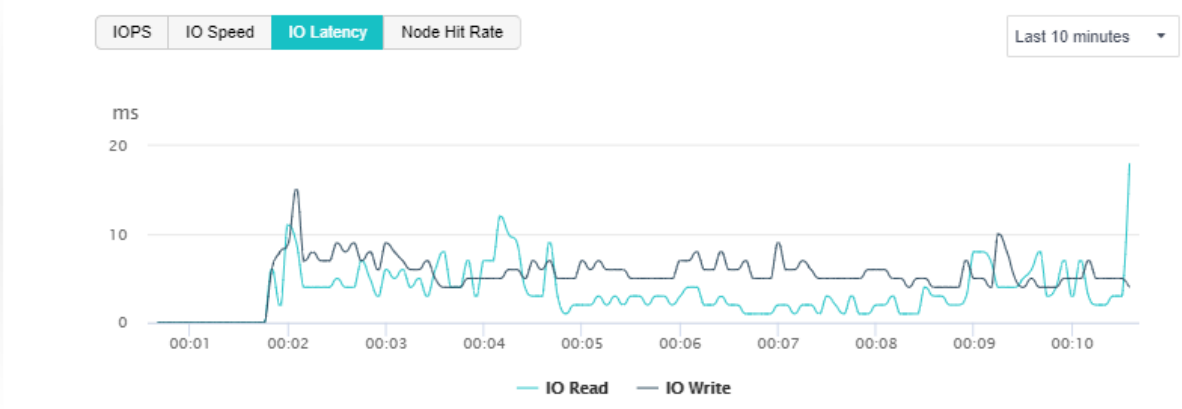




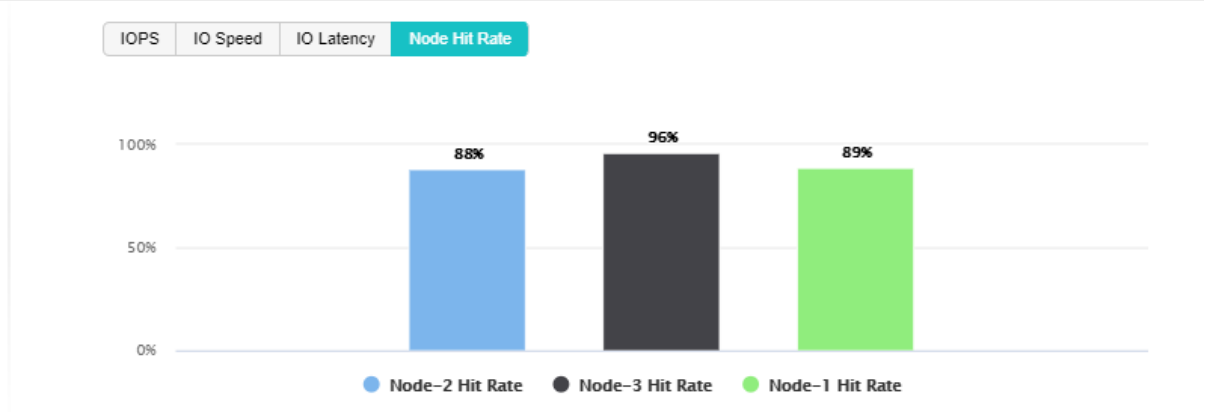
IOPS: Indicates virtual storage input/output operations per second, which represents IO performance of virtual storage.

IO Speed: Indicates bytes read or written by virtual storage per second, which represents IO throughput of virtual storage.

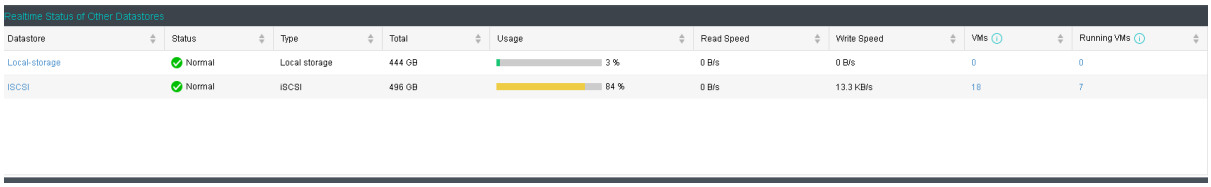
IO Latency: Indicates how long it takes for virtual storage to perform each write/read operation. Through IO latency trending graph, you may know storage IO load. If IO latency increases, it indicates that IO request is in queue and IO performance becomes poorer. Generally, it indicates that IO load is low if the average IO latency is less than 30ms and that IO load is normal if the average IO latency is less than 60ms.



Bar graph of **Node Hit Rate** shows the average hit rate of different nodes.

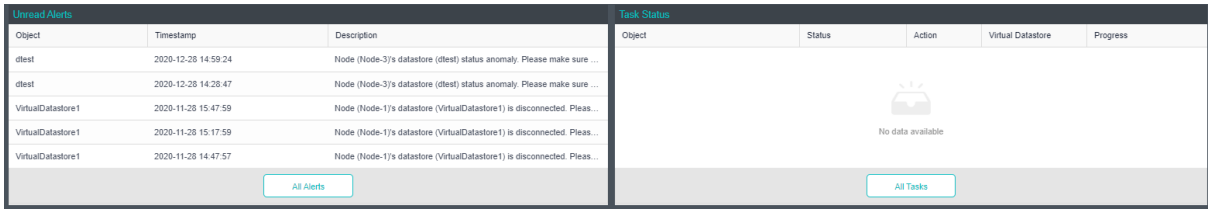


Realtime Status of Other Storage: This section displays the name of datastore, storage type, datastore capacity and usage, read and write speed, the number of virtual machines stored on the datastore, and the number of running virtual machines, as shown below:



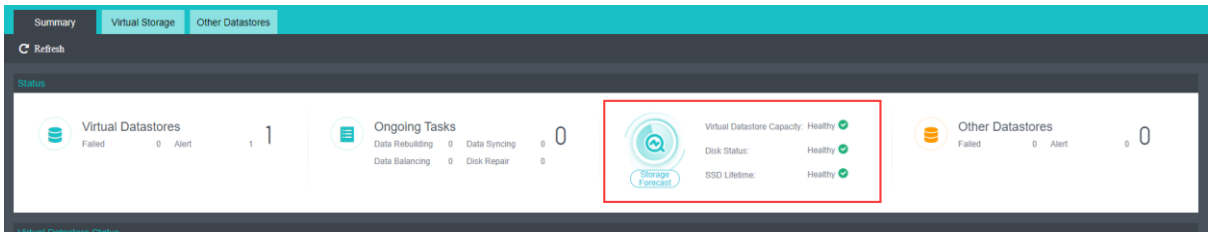
Unread Alerts: This section displays unread alarms, and you can click **All Alarms** to view those alarms in details.

Task Status: This section displays the ongoing data sync and data balancing tasks, and you can click **All Tasks** to view details.



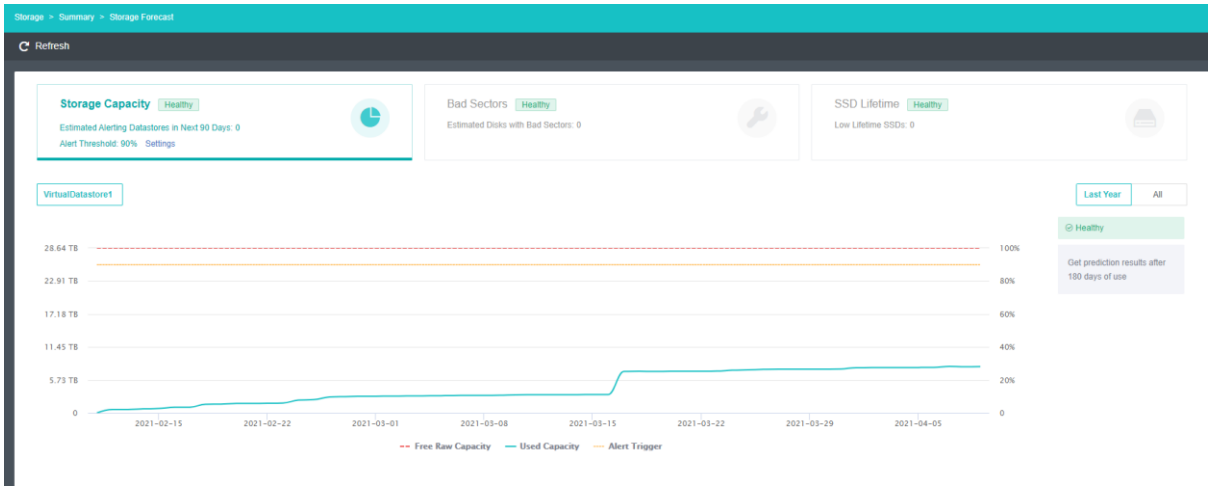
2.4.1.2 Storage Forecast

aSAN analyzes a large amount of real business scenario data, the underlying algorithm library integrates a variety of machine learning and deep learning algorithms, and independently developed the storage forecasting module, including bad sector prediction, capacity prediction and SSD life prediction functions.



1. Storage Capacity

   aSAN can dynamically predict the capacity growth trend in the next 90 days based on the capacity usage of customer clusters. In the capacity forecast interface, users can switch to view the bare capacity of different storage volumes, the actual capacity used and the dynamic forecast curve, and the user is prompted in the section surface that the capacity used is expected to reach the capacity alarm threshold (90%) in xx days.

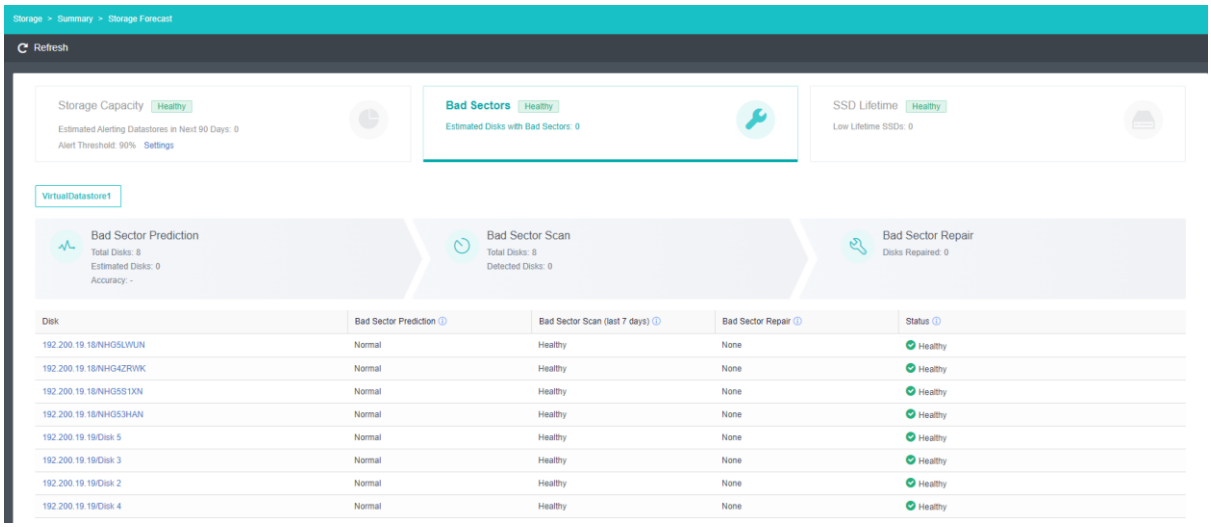


2. Bad Sectors

   By collecting and analyzing the SMART data, performance parameters and hard disk log information of a large number of customers' real use scenarios, combined with advanced algorithm training models, Sangfor has independently developed a highly accurate bad sector forecasting function, and the aSAN bad sector forecasting

accuracy rate is up to 95% or more through a large number of different business scenarios.

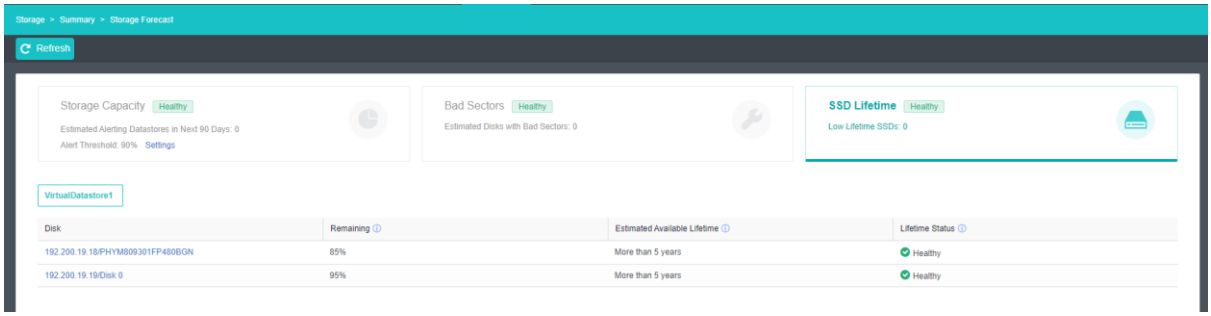
aSAN can dynamically sense which hard disks in the cluster are most likely to have bad sectors according to the upper business pressure and cluster hard disk usage, and prioritize them for bad sector scanning, which can shorten the actual window for hard disk bad sectors to be found from a week or even a month to a day, and combine aSAN bad sector scanning and repair to form a closed-loop processing of hard disk bad sectors, which greatly shortens the risk period of data being in "single copy" due to hard disk bad sectors.



In the **Bad Sectors** interface, users can see the hard disk bad sectors forecast results, actual scan results and bad sector repair, and at the same time will also be based on the number of hard disk bad sector risk assessment of the hard disk, for the history of a high number of bad sector hard disk alarm, prompting users to replace the hard disk as soon as possible to prevent data loss due to excessive number of bad channels resulting in hard disk damage.

3. SSD Lifetime

aSAN collects and analyzes the SSD hard disk IO data in the cluster, calculates the remaining life of SSD hard disk, and displays the expected remaining available time of SSD in combination with the upper business pressure, and divides the three life levels of "healthy", "risk" and "high risk" according to the prediction result, prompting users to replace the SSD hard disk in the cluster with critical life in time.



High Risk: Remaining life <= 10%

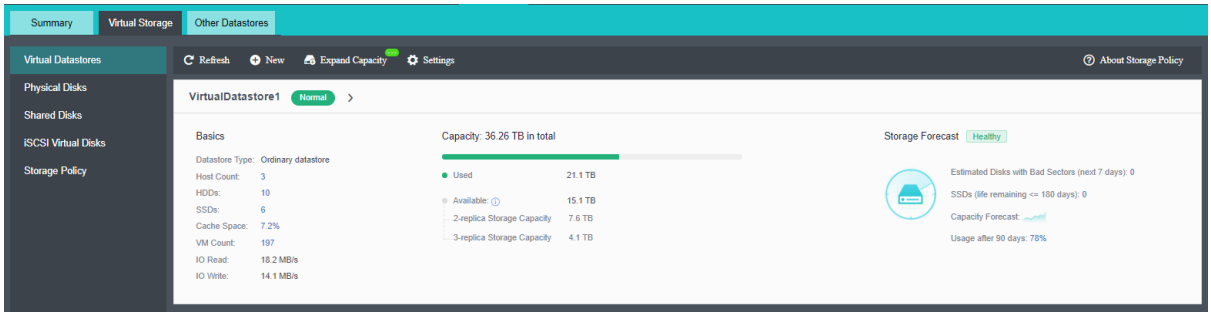
Medium Risk: Remaining life <= 15%

Healthy: Remaining life > 15%

2.4.2 Virtual Storage

Sangfor virtual storage (later renamed Sangfor aSAN)) is storage virtualization software developed based on distributed file system, to adapt to the trend of storage virtualization. Currently, aSAN software is embedded into Virtualization Management Platform (VMP), through which all hard disks (except for system disk) on the physical machines in a cluster are managed together.

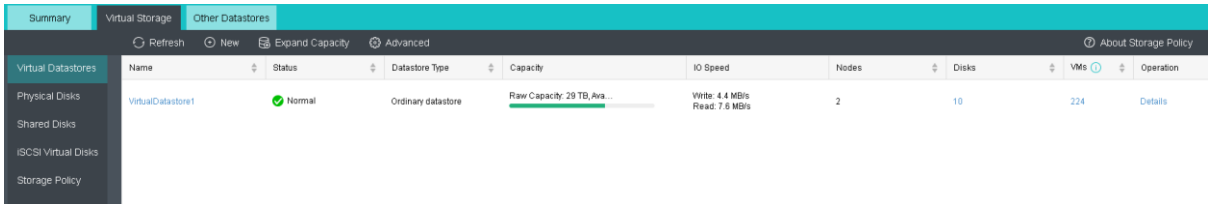
On the **Virtual Storage** page, there are five tabs: **Virtual Datastores**, **Physical Disks**, **Shared Disks**, **iSCSI Virtual Disks** and **Storage Policy**, as shown below.



2.4.3 Virtual Datastores

In 6.2.0, for cluster with 3 nodes and above can be divided into different virtual datastores, so as to meet requirements for IO data and performance segregation for different businesses. Each resource pool is a virtual datastore.

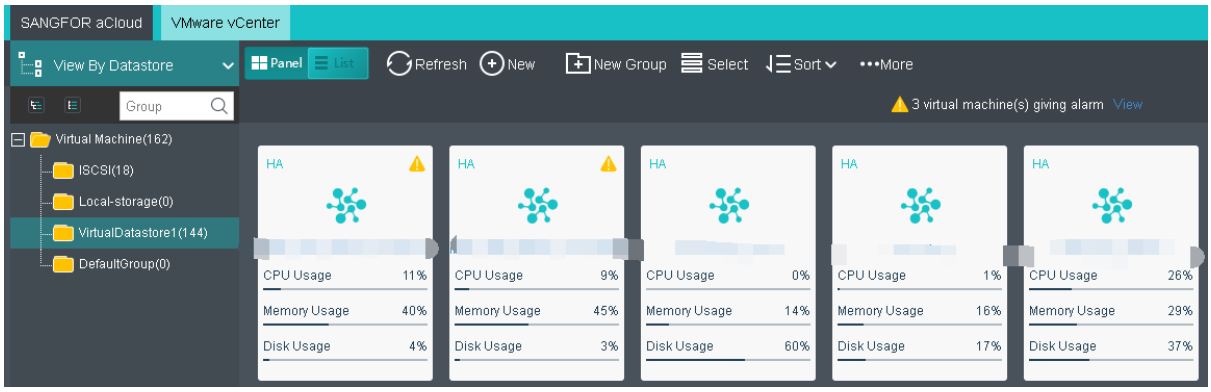
On the **Virtual Datastores** tab, it displays name, status, total capacity, usage, read and write speed, number of replicas, nodes, disks and virtual machines, as shown below:



To view detailed information of a virtual datastore, you may click on the name of the virtual datastore. For details, you may refer to the **Error! Reference source not found.**.

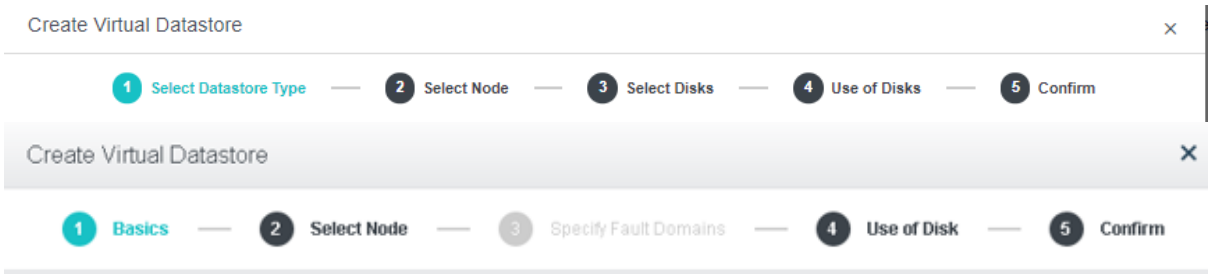
To view disks in detail and manage disks, you may click on the number under **Disks**. For details, you may refer to the Error! Reference source not found. section.

To view details of the virtual machines, you may click on the number under **VMs**, as shown below:



2.4.3.1 Creating Virtual Datastore

To create a second virtual datastore, there must be at least three nodes in the cluster. There are four steps to create a new virtual datastore: 1) Specify Datastore Type 2) Select node(s) 3)Specify use of disk 4)Confirm configurations. The following illustrates the creation process in details:

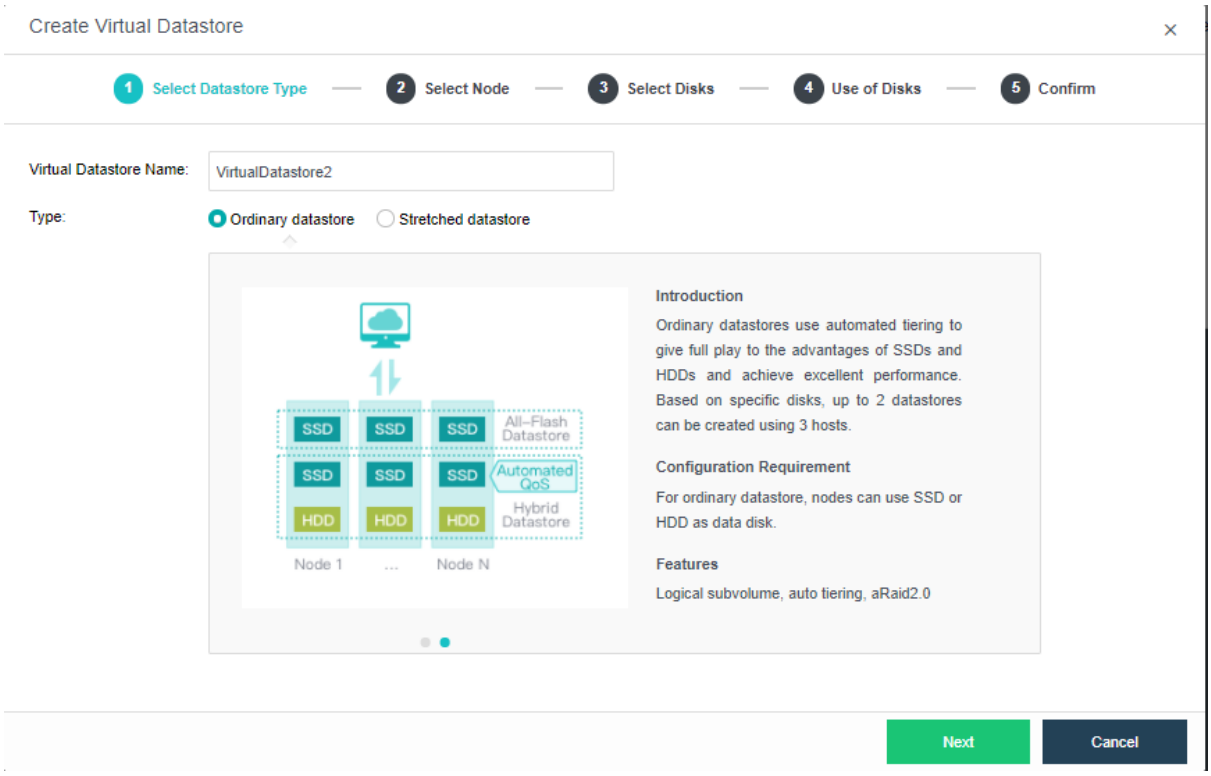


1. Specify basic information for the virtual datastore. You should specify virtual datastore **Name** and **Type** whether it is Ordinary Datastore or Stretched Datastore.

   Ordinary datastore: Ordinary datastore use automated tiering to give full play to the

advantages of SSDs and HDDs to achieve excellent performance. 2 datastores can be created using 3 nodes/hosts.

Stretched datastore: Stretched datastore used to build an active-active data center. Host comprising a stretched datastore are deployed in 2 server rooms which function as primary and secondary fault domain. Multiple replicas will be written into the 2 fault domains respectively to achieve zero RPO.



2. Select node(s) that you want to add to the virtual datastore.

   First, select the Method where it will be **Use disks on new hosts** or **Use unused disks added to existing datastores**.

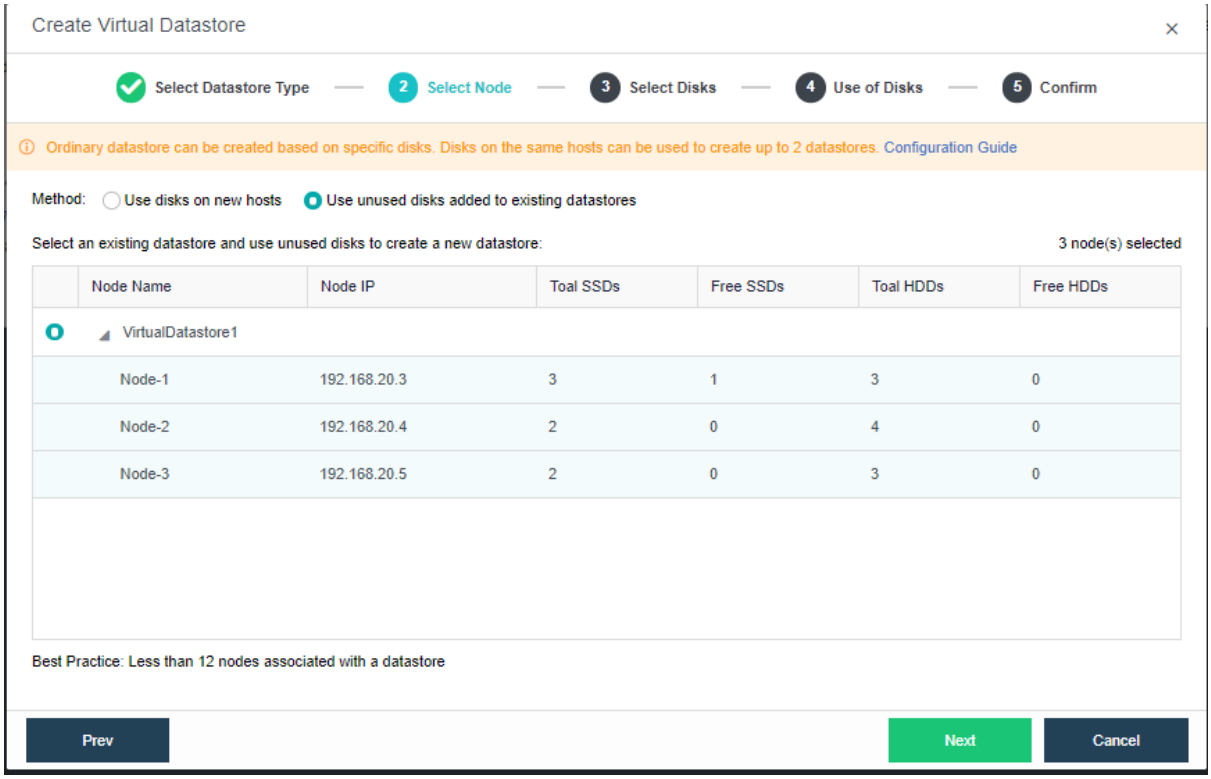
   Use disks on new hosts: Create virtual datastore based on nodes. Every first virtual datastore of the cluster must select this option.

   Use unused disk added to existing datastores: Create new virtual datastore based on disk available on the nodes created with the "Use disks on new hosts".

   Prerequisites of adding VS with [**Use unused disk added to existing datastores**]:

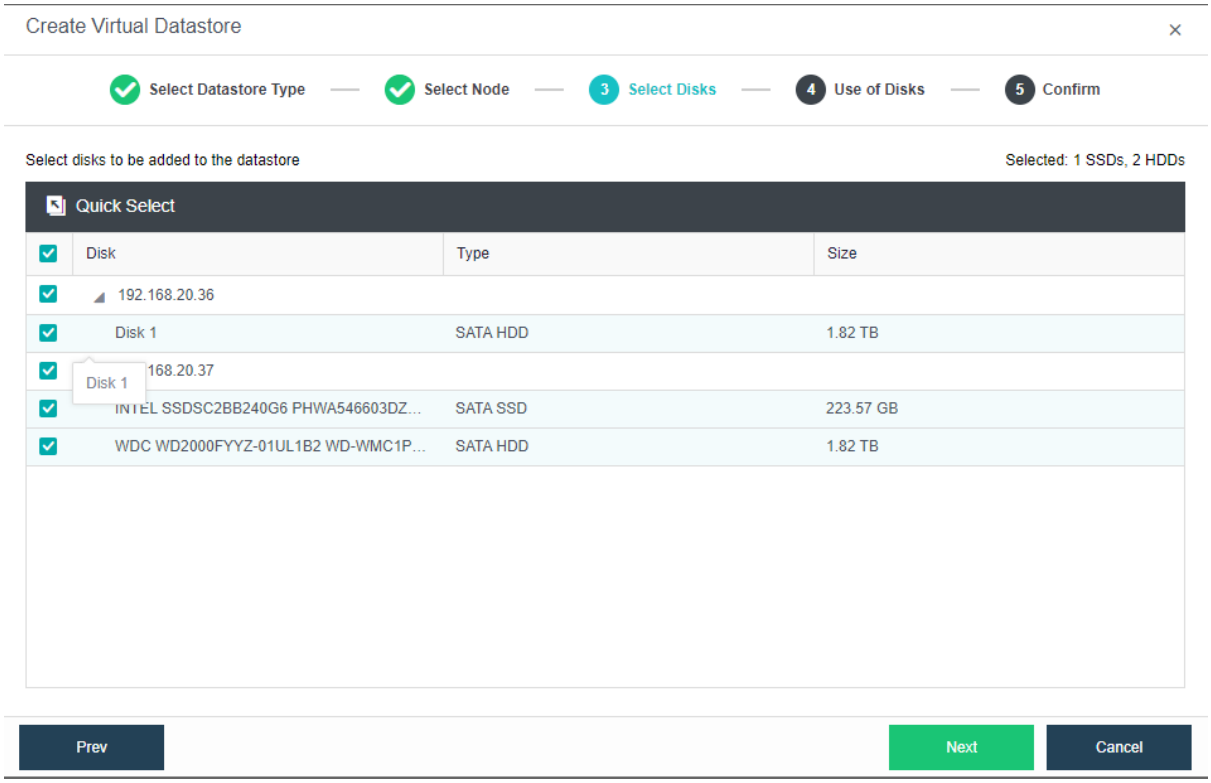
   1. Version 6.2.0 and above
   2. There are existing virtual datastore which created based on nodes.
   3. Required at least 3 nodes in the cluster.

There is a list displaying node information such as node name, node IP, total SSDs and HDDs. You should select the node(s) from that list that you want to add to virtual datastore. Note that at least three nodes are required to create a second virtual datastore.



3. Select disk

   There is a list displaying all disk available in the selected nodes. Select the disks from the list that you want to add to the virtual datastore.



4. Specify use of disk.

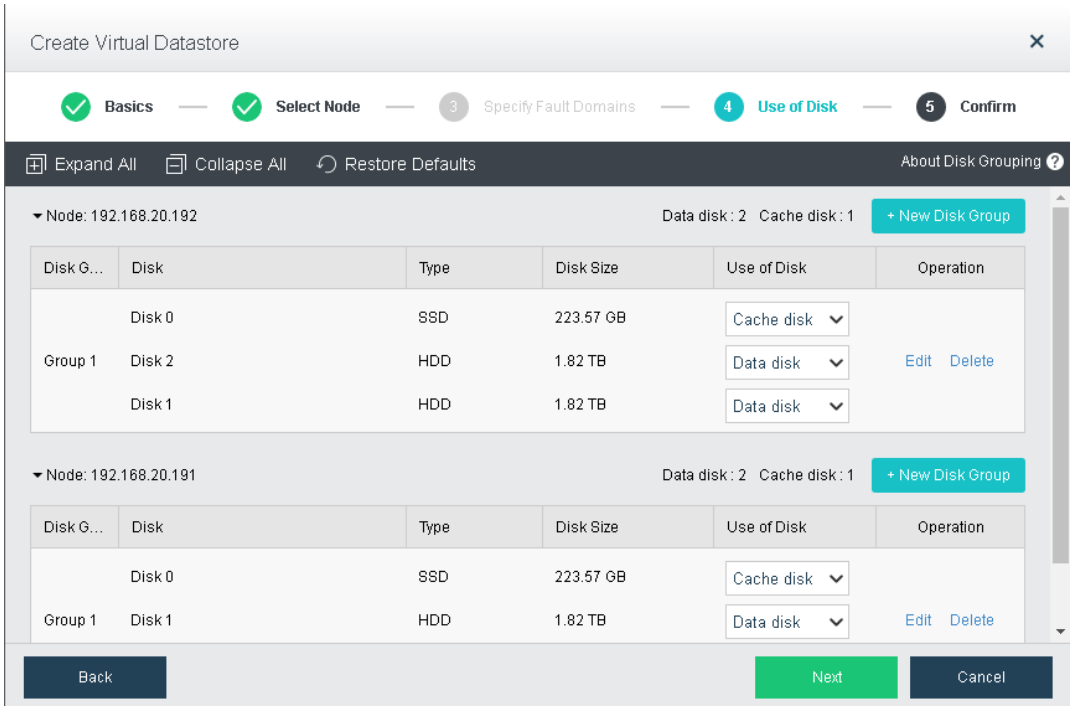
   In this step, you will see the following information of discovered disks(system disk is not listed): disk name, disk type, disk size and use of disk. Then, you should specify use of those disks. Disks that are added to virtual storage can be used as data disk, cache disk or spare disk.

   Data disk: It is used to store disk data files of virtual machine and create virtual disk. Its capacity should be greater than or equal to 200GB.

   Cache disk: It is used for caching, to improve performance of virtual storage. SSD is often used as cache disk. Its capacity should be greater than or equal to 100GB. Since version HCI5.3, SSD cannot be used as cache disk to add to virtual datastore if it is not an SSD for data center, and storage performance may be affected without cache disk.

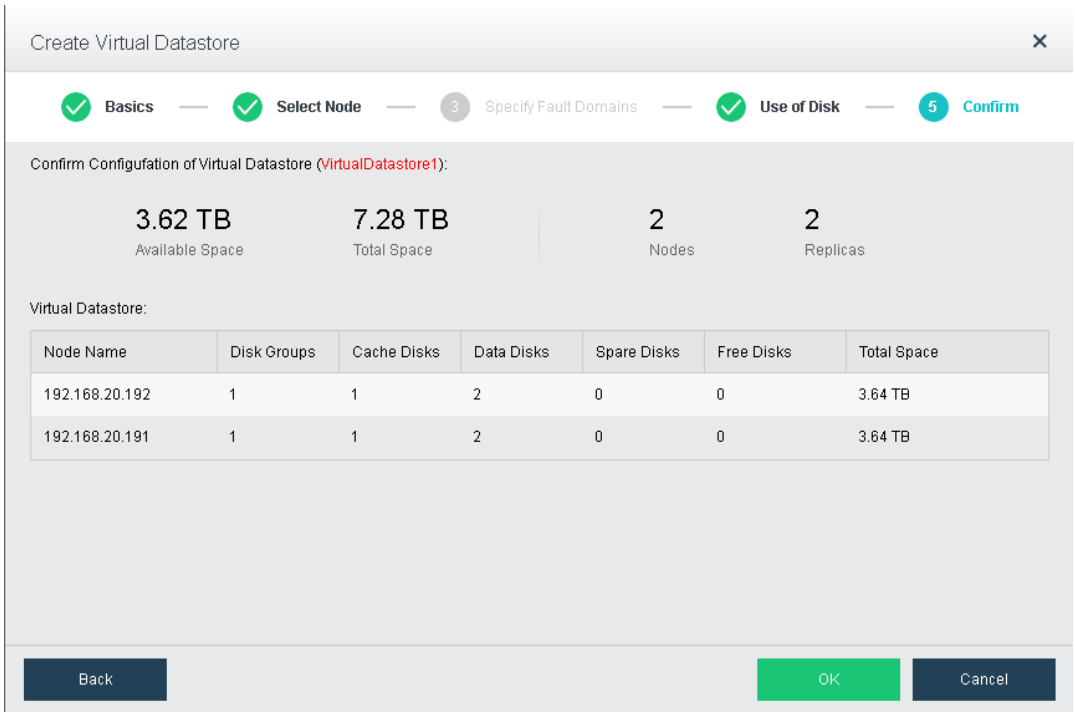
   Spare disk: It acts as backup of data disk on virtual storage, and is always ready to replace the data disk when it fails. Once the failed disk recovers, it returns to spare disk. Its capacity should be greater than or equal to 200GB.

   If none of the above uses is selected for disk, it may not associate with virtual storage.



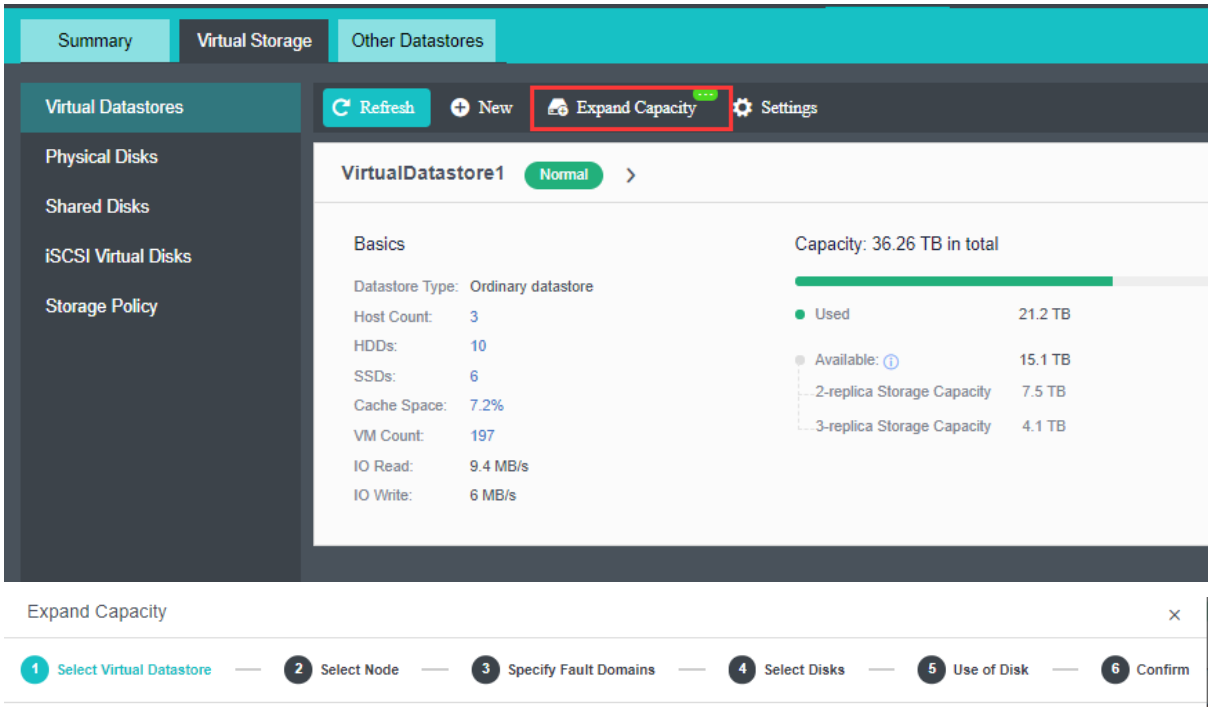
5. Confirm configuration.

   After configuring use of disk, you need to type admin password to confirm the operation of creating virtual datastore.



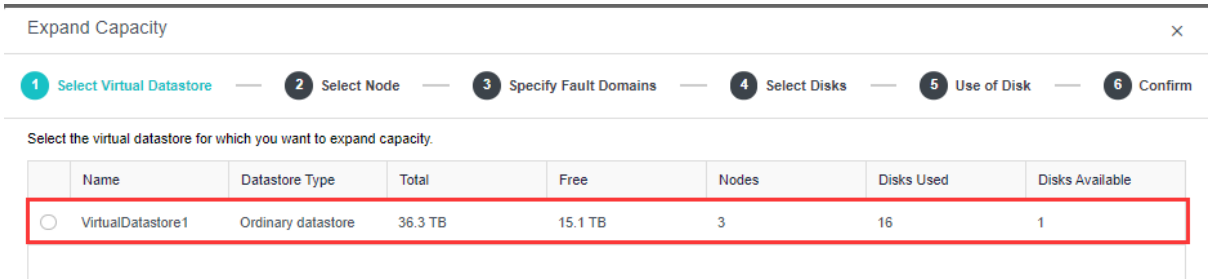
2.4.3.2 Expanding Capacity

Capacity of a virtual datastore can be expanded by adding more nodes or disks to it. Before expanding capacity via node, storage network interface of the new node should be specified. Steps of capacity expansion include the followings: 1) Select virtual datastore for which you want to expand capacity 2) Select a type to expand capacity 3) Specify use of disks 4)Confirm configurations.

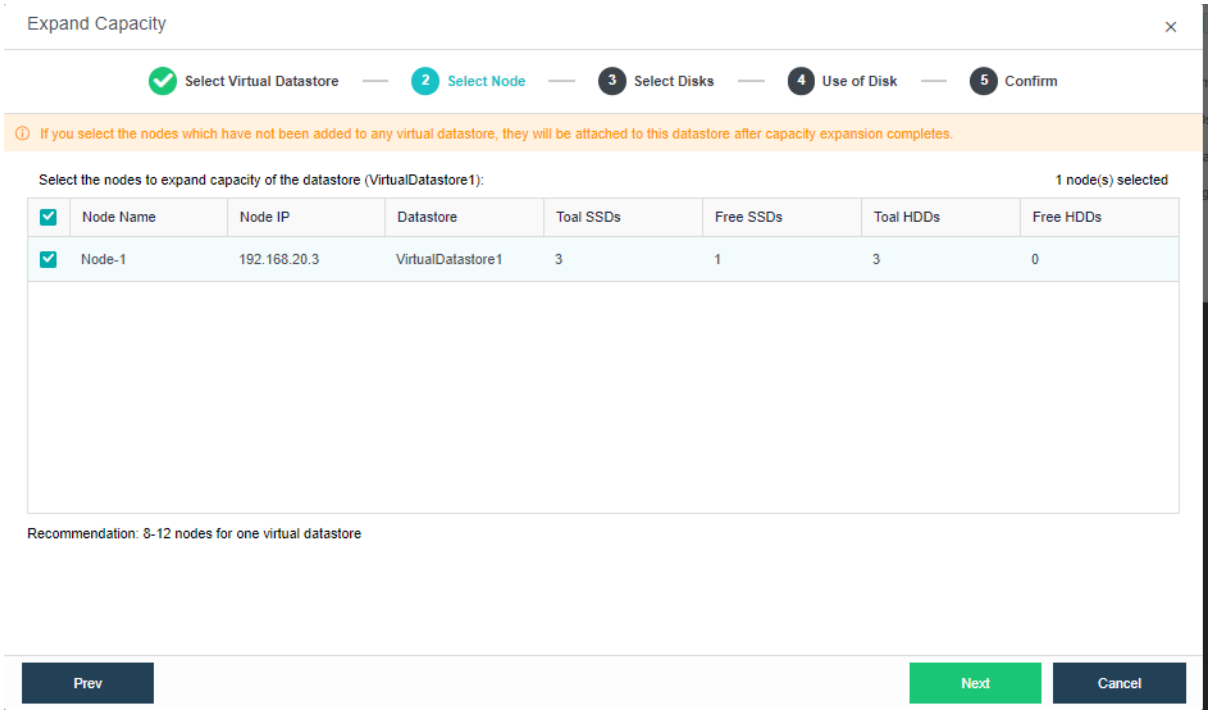


1. Select virtual datastore.

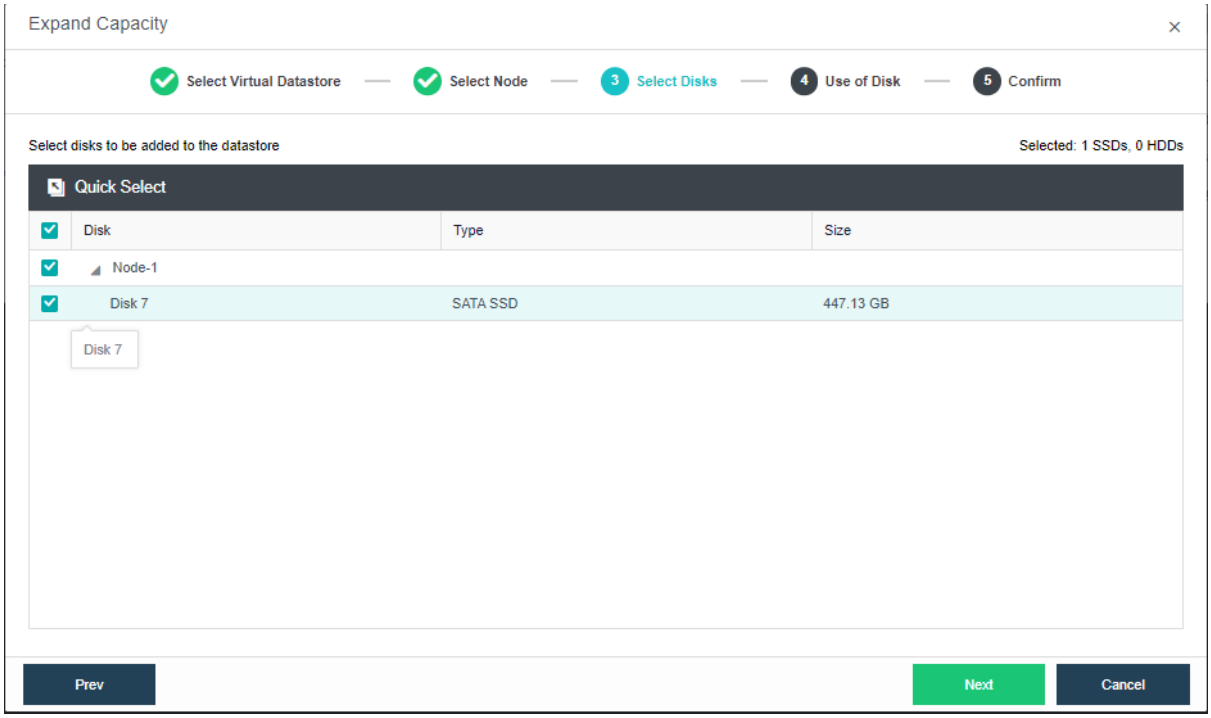
   There is a list displaying information of virtual datastore: datastore name, datastore tpye, total capacity, free space, the number of nodes, the number of disks that have been used and the number of free disks. From the list, select the datastore for which you want to expand capacity.



2. Select the to expand capacity. You may select **Expand capacity via node** or **Expand capacity via disk**. If **Expand capacity via node** is selected, the following page will be shown:



3. Select Disks



4. Configure use of disk.

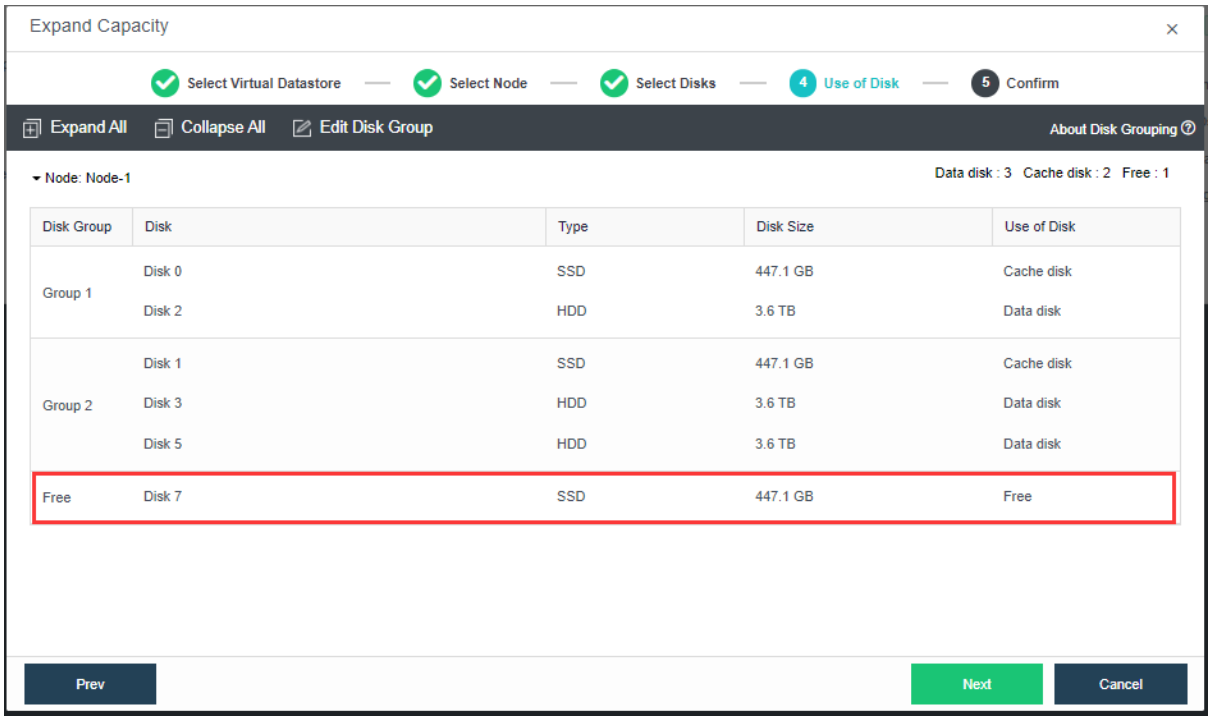
In this step, you will see the following information of available disks(system disk is not

listed): disk name, disk type, disk size and use of disk. Then, you should specify use of those disks. Disks that are added to virtual storage can be used as data disk, cache disk or spare disk.

Data disk: It is used to store disk data files of virtual machine and create virtual disk. Its capacity should be greater than or equal to 200GB. **The number of data disks should be multiple of the data replicas, or else some data disks cannot be added to virtual datastore.**

Cache disk: It is used for caching, to improve performance of virtual storage. SSD is often used as cache disk. Its capacity should be greater than or equal to 100GB. Since version HCI5.3, SSD cannot be used as cache disk to add to virtual datastore if the SSD is not an SSD for data center, and storage performance may be affected without the cache disk.

Spare disk: It acts as backup of data disk on virtual storage, and is always ready to replace the data disk when it fails. Once the failed disk recovers, it returns to spare disk. Its capacity should be greater than or equal to 200GB.

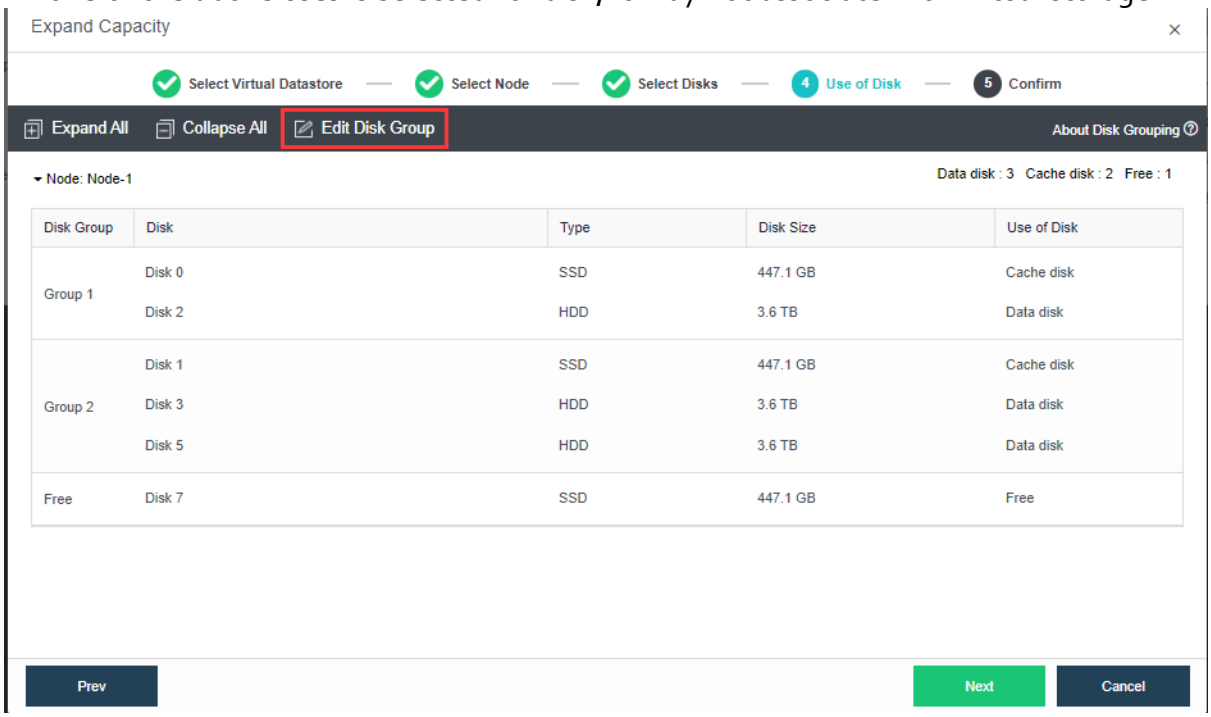


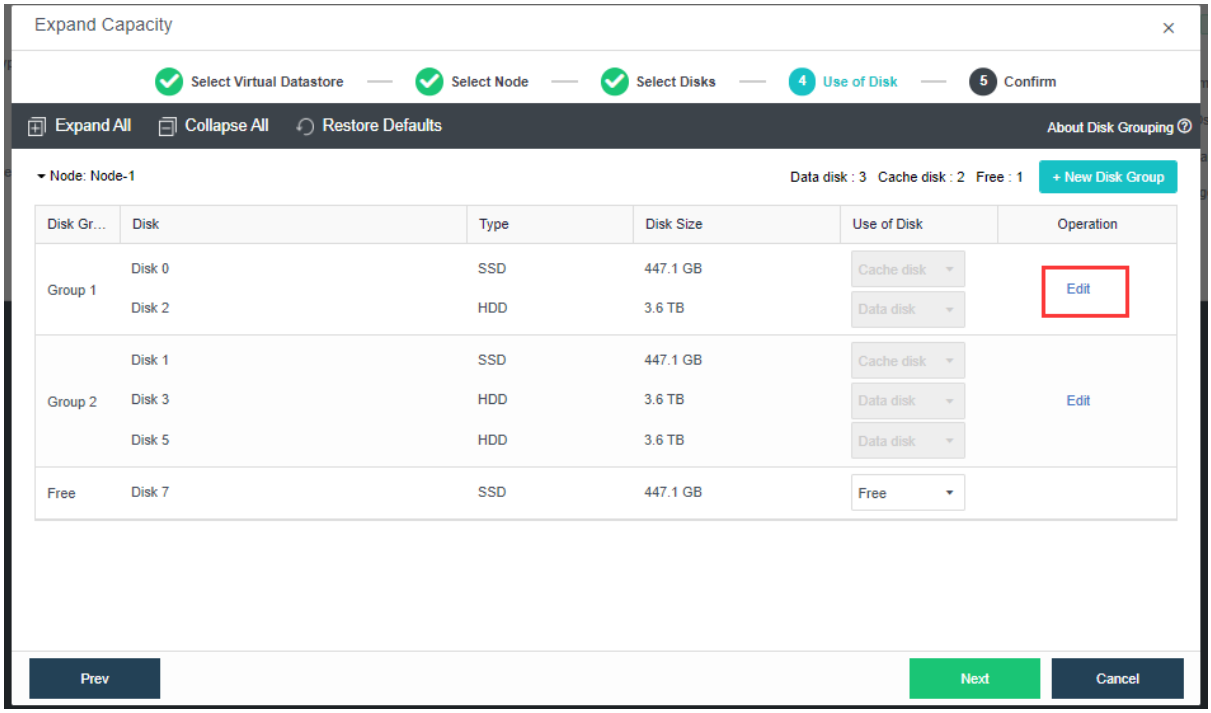
Edit Disk Group: Allow to edi the existing disk group by adding or removing disk from the disk group. When trying to expand the datastore with new disks, you may need to edit the disk group manually to add the disk normally.

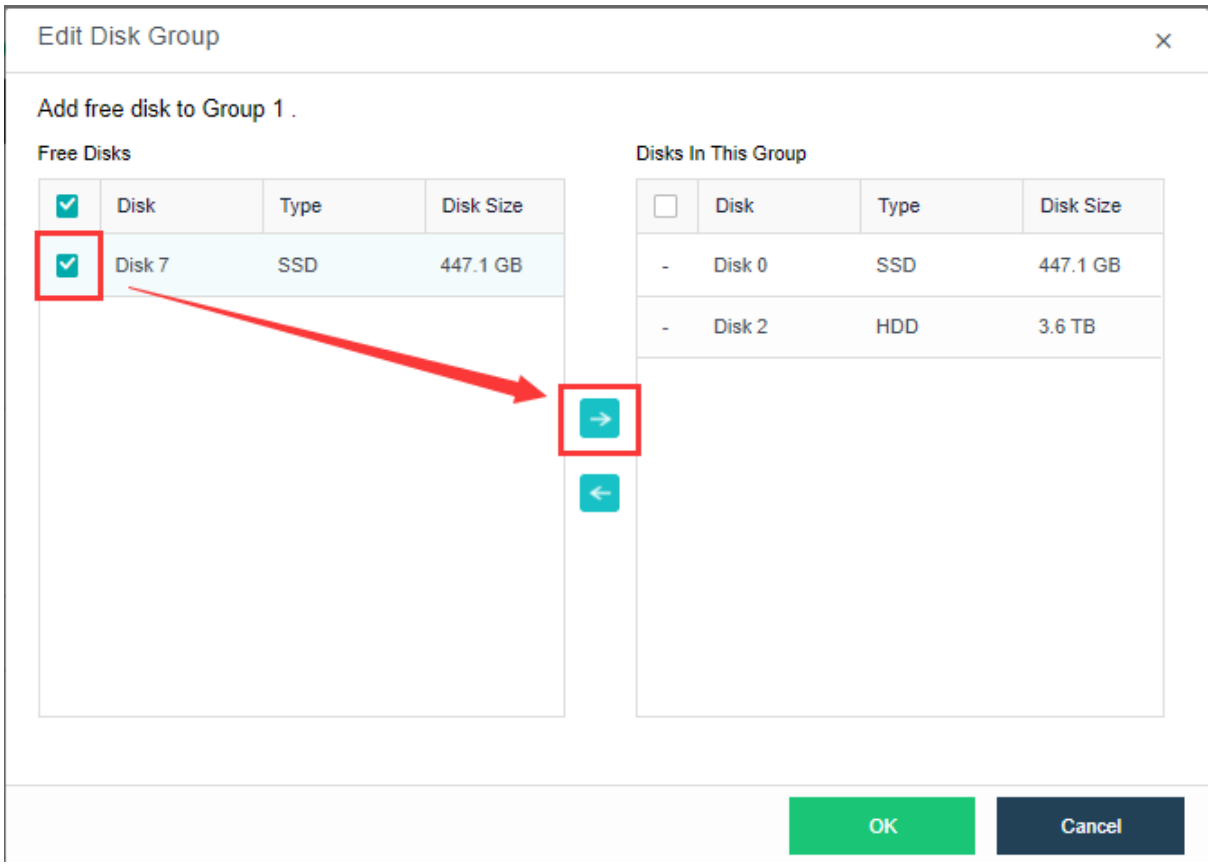
If none of the above uses is selected for disk, it may not associate with virtual storage.

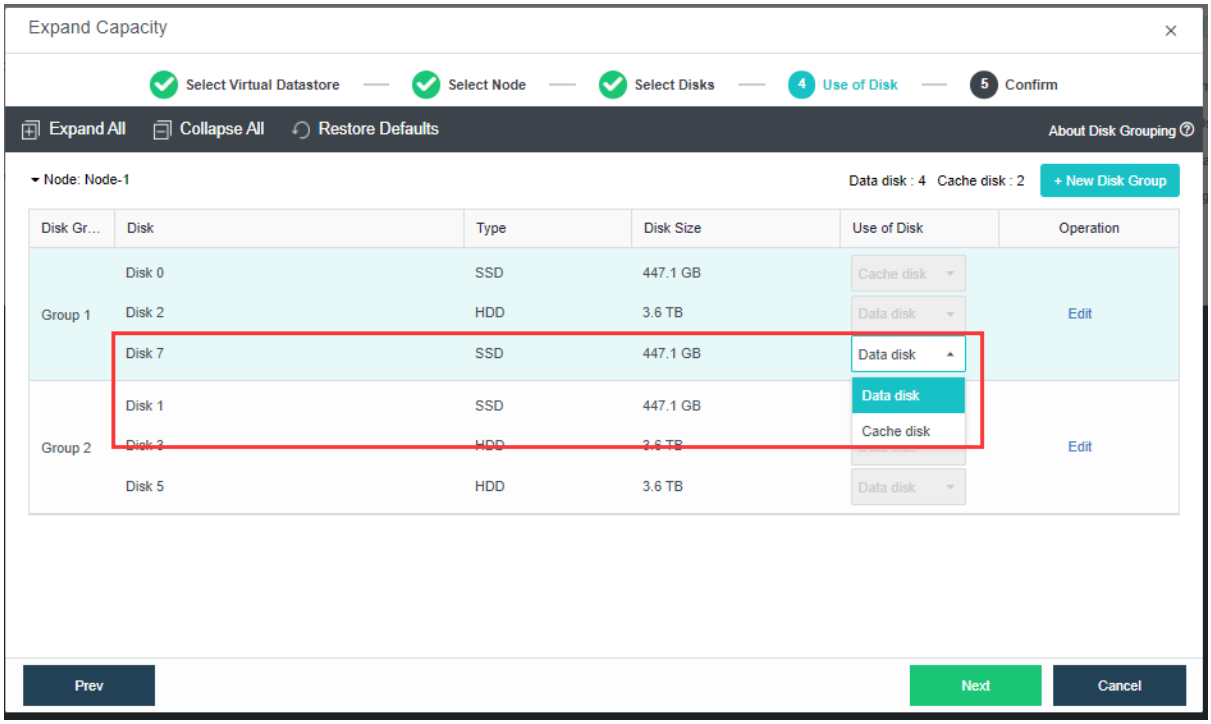
Edit Disk Group: Allow to edi the existing disk group by adding or removing disk from the disk group. When trying to expand the datastore with new disks, you may need to edit the disk group manually to add the disk normally.

If none of the above uses is selected for disk, it may not associate with virtual storage.




Expand Capacity
Select Virtual Datastore
Select Node
Select Disks
4 Use of Disk
5 Confirm
Expand All
Collapse All
Restore Defaults
About Disk Grouping
Node: Node-1
Data disk : 3 Cache disk : 2 Free : 1
+ New Disk Group
Disk Gr...
Disk
Type
Disk Size
Use of Disk
Operation
Group 1
Disk 0
SSD
447.1 GB
Cache disk
Disk 2
HDD
3.6 TB
Data disk
Edit
Group 2
Disk 1
SSD
447.1 GB
Cache disk
Disk 3
HDD
3.6 TB
Data disk
Edit
Disk 5
HDD
3.6 TB
Data disk
Free
Disk 7
SSD
447.1 GB
Free
Prev
Next
Cancel

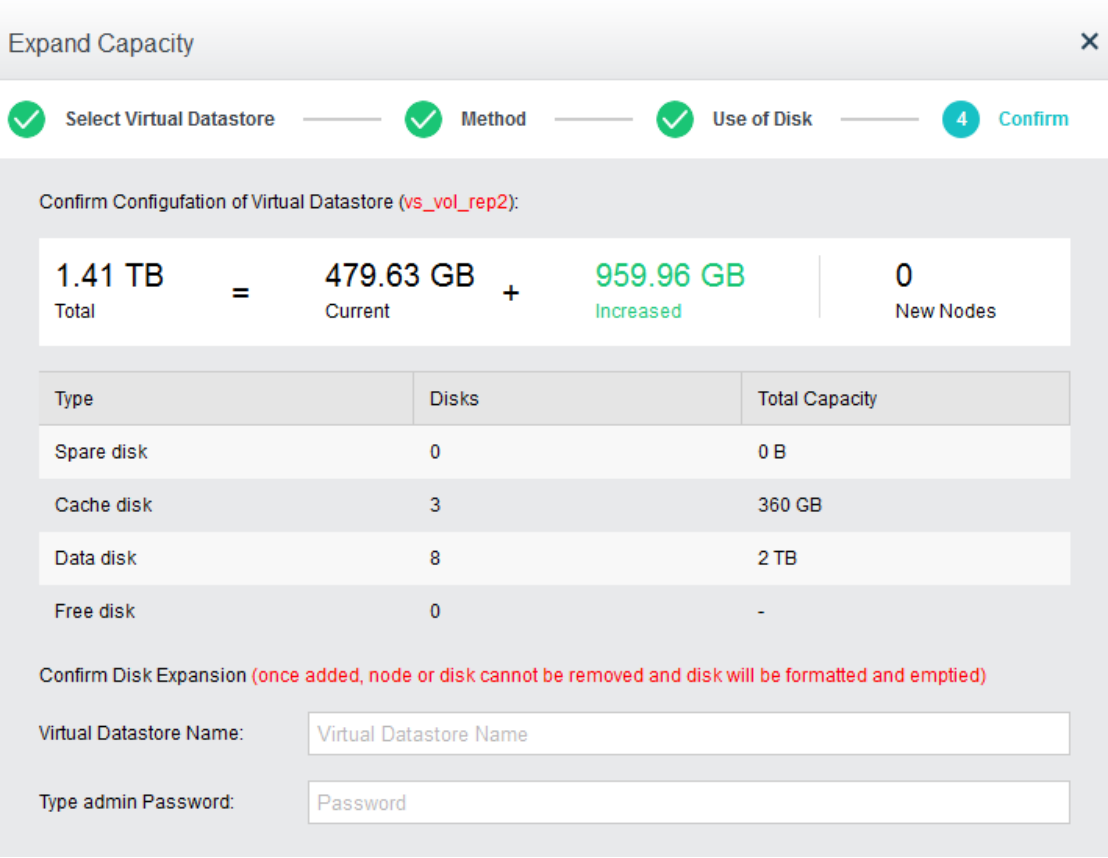

Edit Disk Group
Add free disk to Group 1 .
Free Disks
Disk
Type
Disk Size
Disk 7
SSD
447.1 GB
Disks In This Group
Disk
Type
Disk Size
Disk 0
SSD
447.1 GB
Disk 2
HDD
3.6 TB
OK
Cancel



5. Confirm configuration.

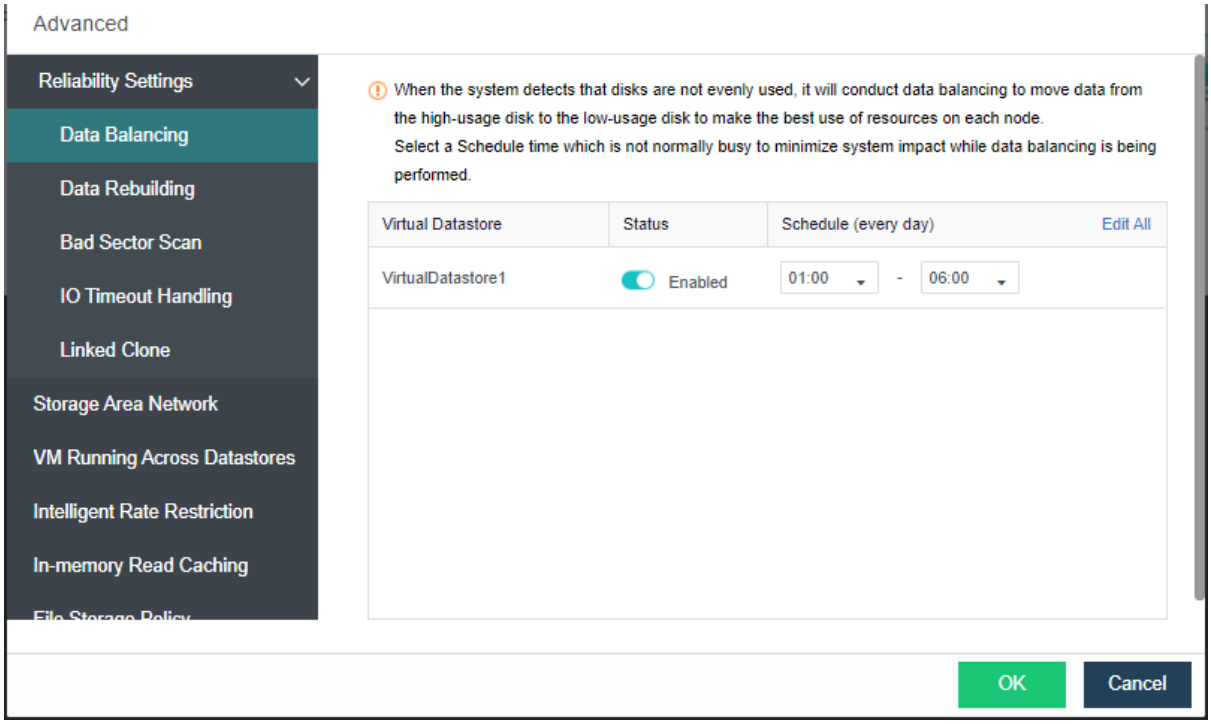
   After configuring use of disk, type virtual datastore name and admin password to confirm capacity expansion operation.

Note that node or disk that has been added to virtual datastore cannot be removed, and disk will be formatted and emptied once the capacity expansion operation is confirmed.

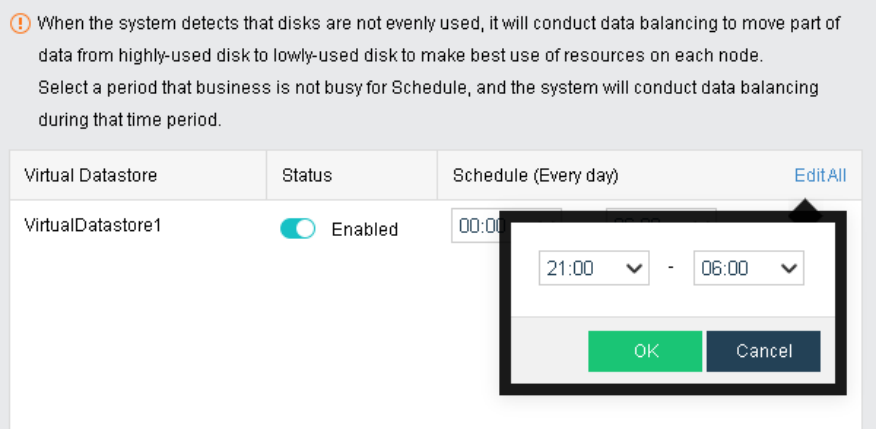


2.4.3.3 Configuring Advanced Settings

In **Storage > Virtual Storage > Virtual Datastore**, you may click **Advanced** to configure more. On the **Advanced** page, there are **Data Balancing, Data Rebuilding ,Storage Area Network , VM Running Across Datastores** and **Intelligent Rate Restriction,** as shown below:



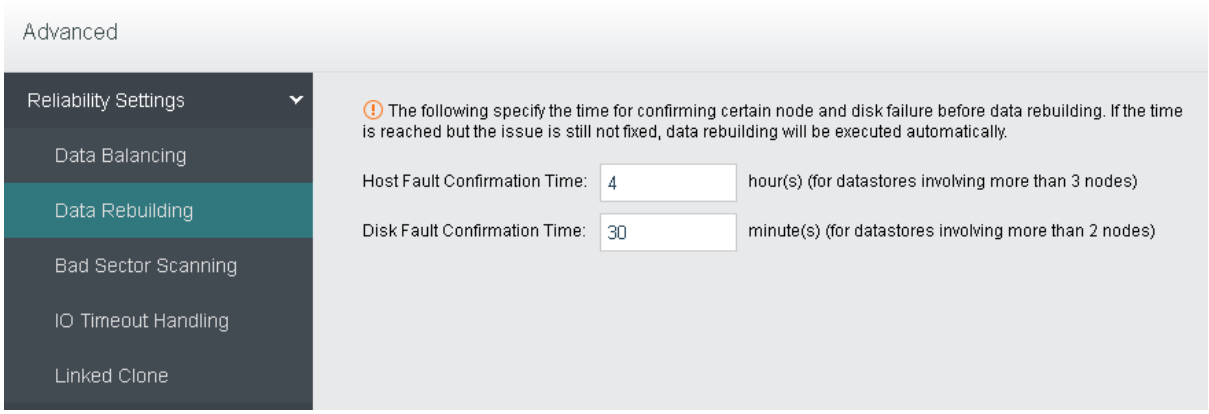
Data Balancing: You can create data balancing task for different virtual datastores. After the task is created, available storage space of each node will be restricted within a certain range. If the remaining storage space is below a certain range, the data balancing task will be executed automatically to have VM files stored on the node short of resources moved to another node. Data that have been migrated will be evenly written into each disk so as to keep disk usage balanced.



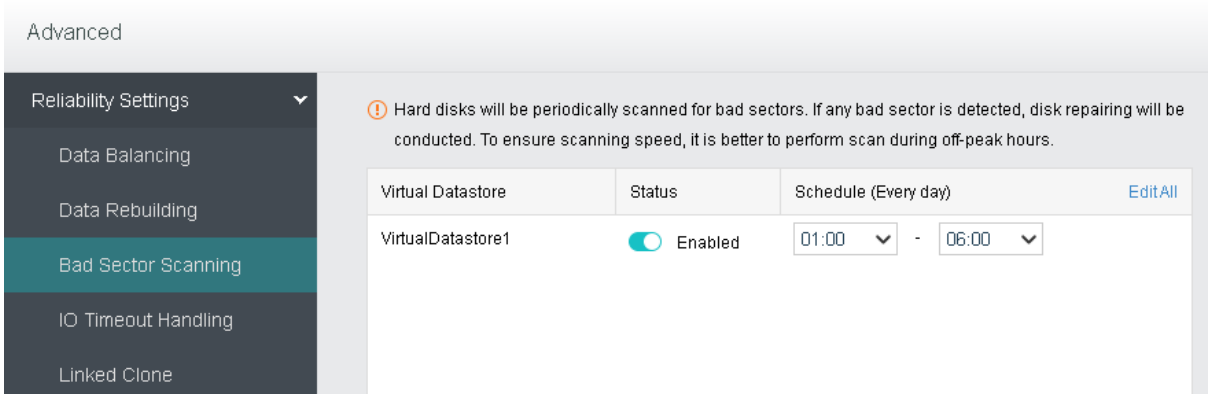
Since performance of virtual machine will be affected during data balancing,virtual machines of high priority will not chosen to perform data balancing. Virtual machines will not be migrated back immediately after migration.

Data Rebuilding: Taking data with two-copy policy as the example, when components (disk or host) in storage volume suffer physical fault, the other copy of the data of faulted component is stored on other components to ensure normal reading and writing of virtual machine, but meanwhile the redundancy of storage volume is reduced, which will lead to data loss if the component storing the other copy also breaks down.With data reconstruction, when component breaks down, the other copy of the data on faulted component will be used as the recovery source to reconstruct a new copy on the target component in fragments to recover completeness of the copy and realize system self-recovery.

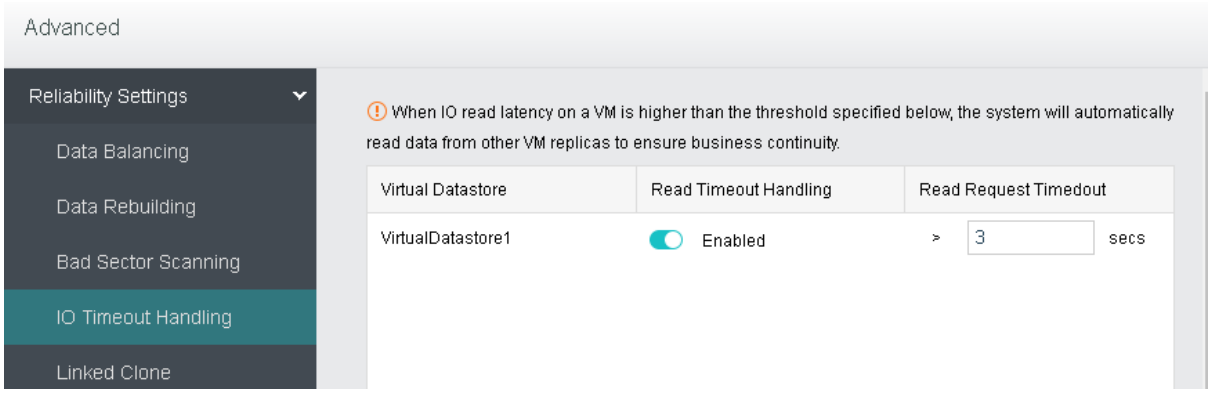
you can specifie the time for confirming certain node or disk failure before data rebuilding.if the time is reached but the issue is still not fixed,data rebuilding will be executed automatically,as shown below:



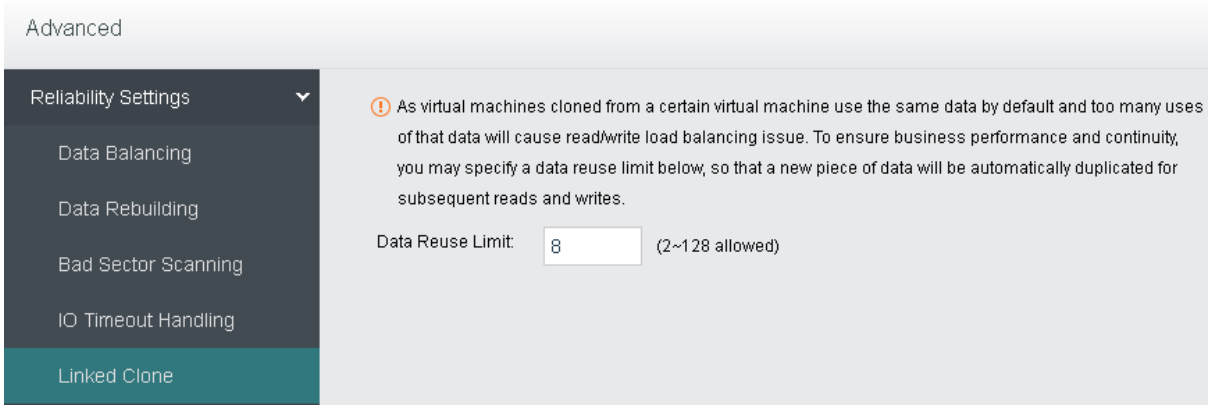
Bad Sector Scanning: Hard disk will be periodically scanned for bad sectors. If any bad sector is detected, disk repairing will be conducted. To ensure scanning speed, it is better to perform scan during off-peak hours.



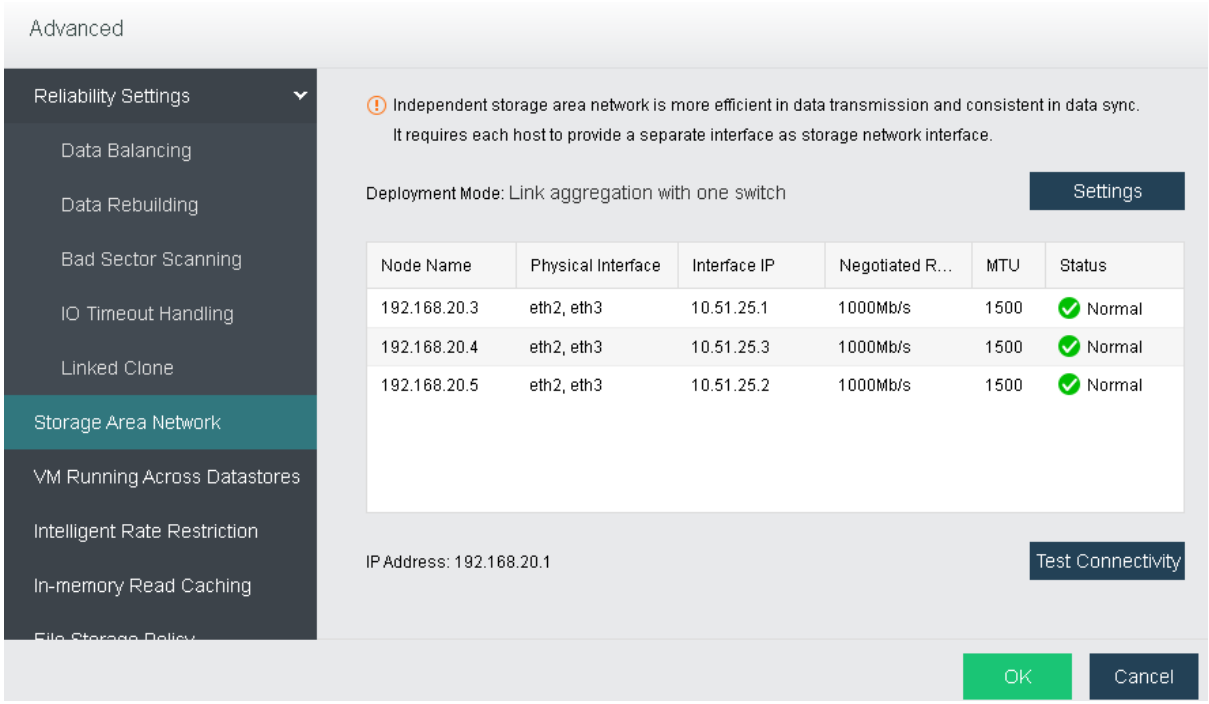
IO Timeout Handling: When IO read latency on a VM is higher than the threshold specified below, the system will automatically read data from other VM replicas to ensure business continuity.



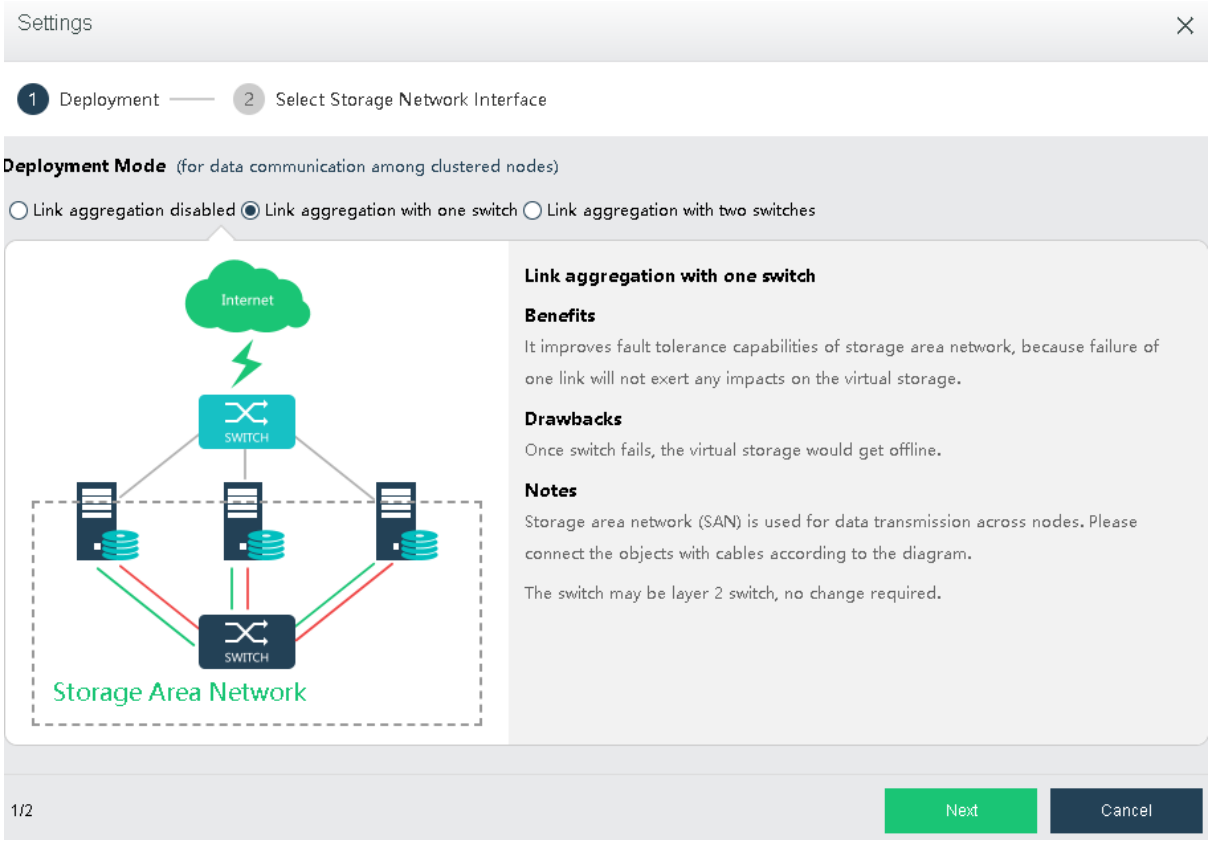
Linked Clone: As virtual machines cloned from a certain virtual machine use the same data by default and too many uses of that data will cause read/write load balancing issue. To ensure business performance and continuity, you may specify a data reuse limit below, so that a new piece of data will be automatically duplicated for subsequent reads and writes.



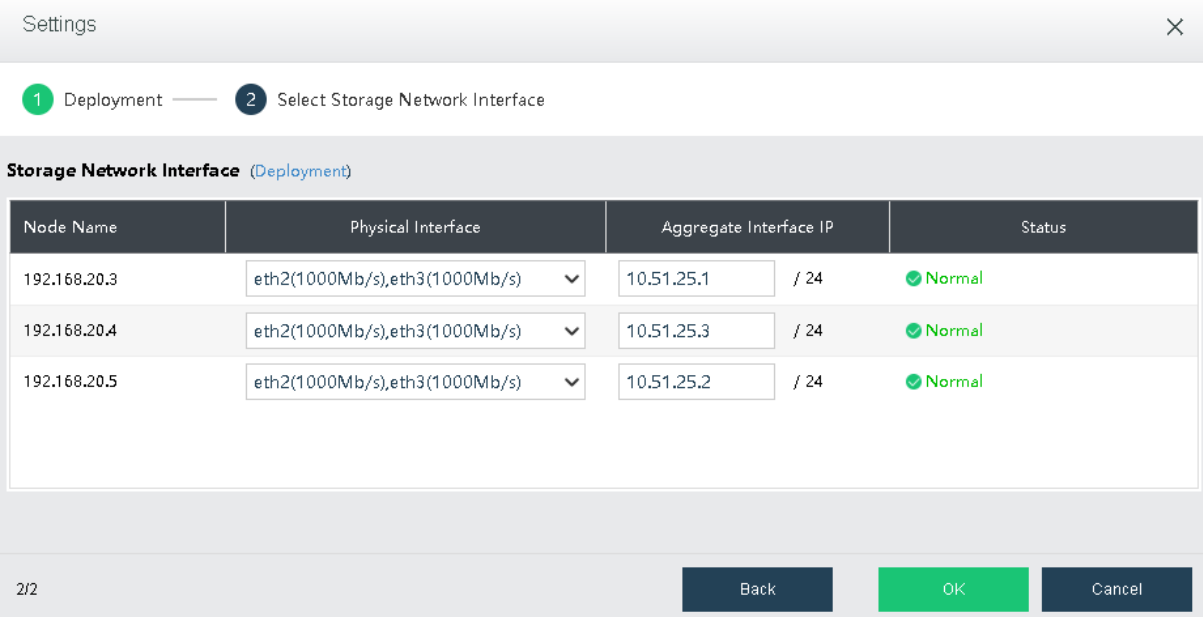
Storage Area Network: You can change deployment mode(**Link aggregation disabled, Link aggregation with one switch, Link aggregation with two switches**) in **Settings,**as shown below:



Take changing deployment mode to **Link aggregation with one switch** for example, select the option **Link aggregation with one switch(Recommended)** first, as shown below:

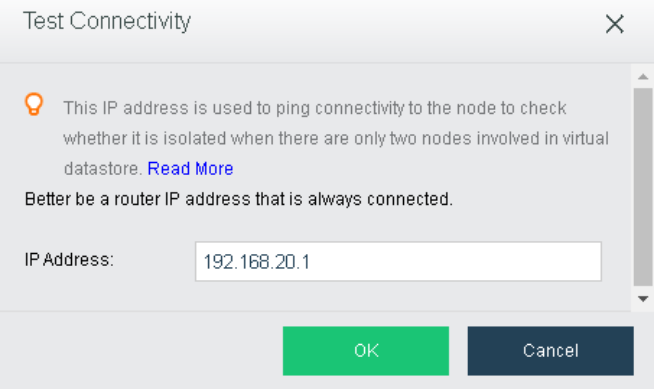


Click **Next** to configure storage network interface, and then click **Finish**.



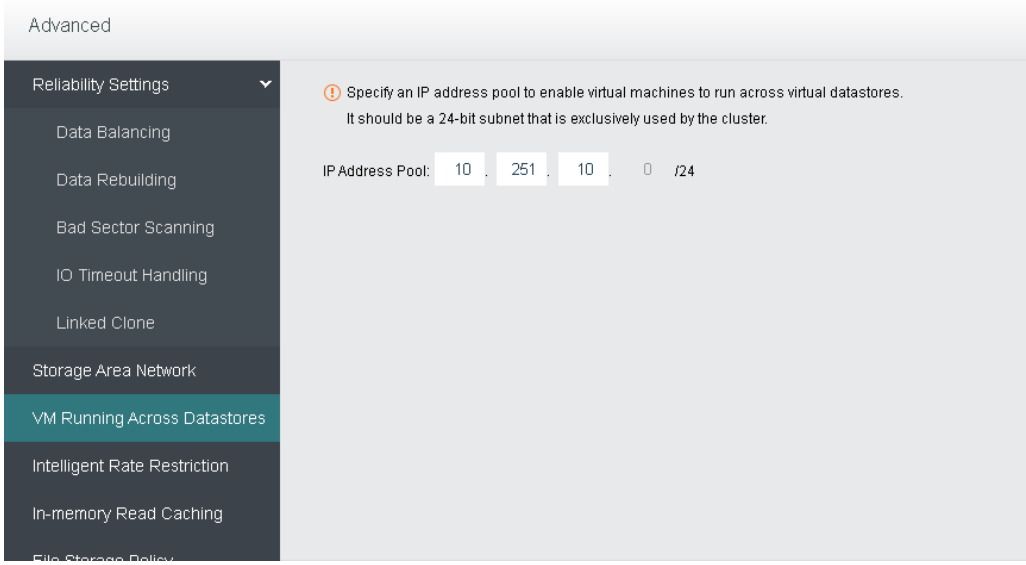
Independent storage area network is more efficient in data transmission and consistent in data sync. Furthermore, independent storage area network helps to reduce data sync risk caused by network connection error, since virtual storage contains crucial business data. The drawback is that additional interface must be provided on the node for the storage to communicate across nodes

Test Connectivity: It is used to test whether the node is offline. First, you need to specify an IP address which should better be router IP address.

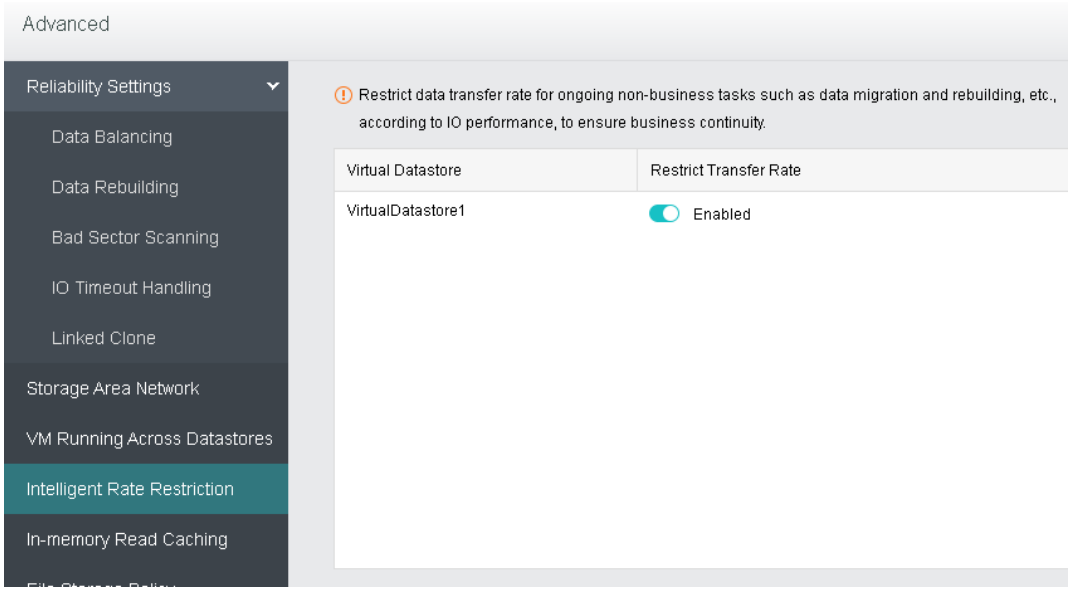


In case that the working node gets offline, virtual machines running on it may be recovered on another clustered node, which may lead to two instances for one virtual machine when the failed virtual machine recovers and interrupts the service. For that reason, we need to stop the instance on the offline node to ensure business continuity.

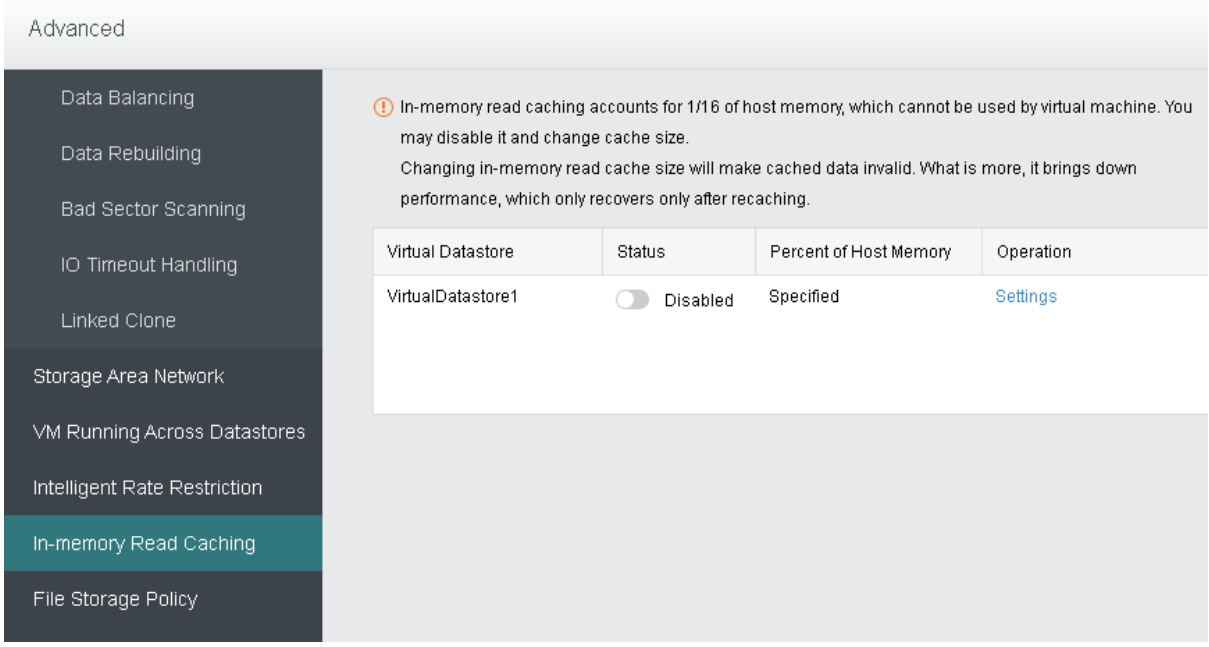
VM Running Across Datastores: This enables virtual machines to run across virtual datastores. It should be configured only when the number of virtual datastores is greater than or equal to 2. IP addresses in the pool should be in a 24-bit subnet that is exclusively used by the cluster.



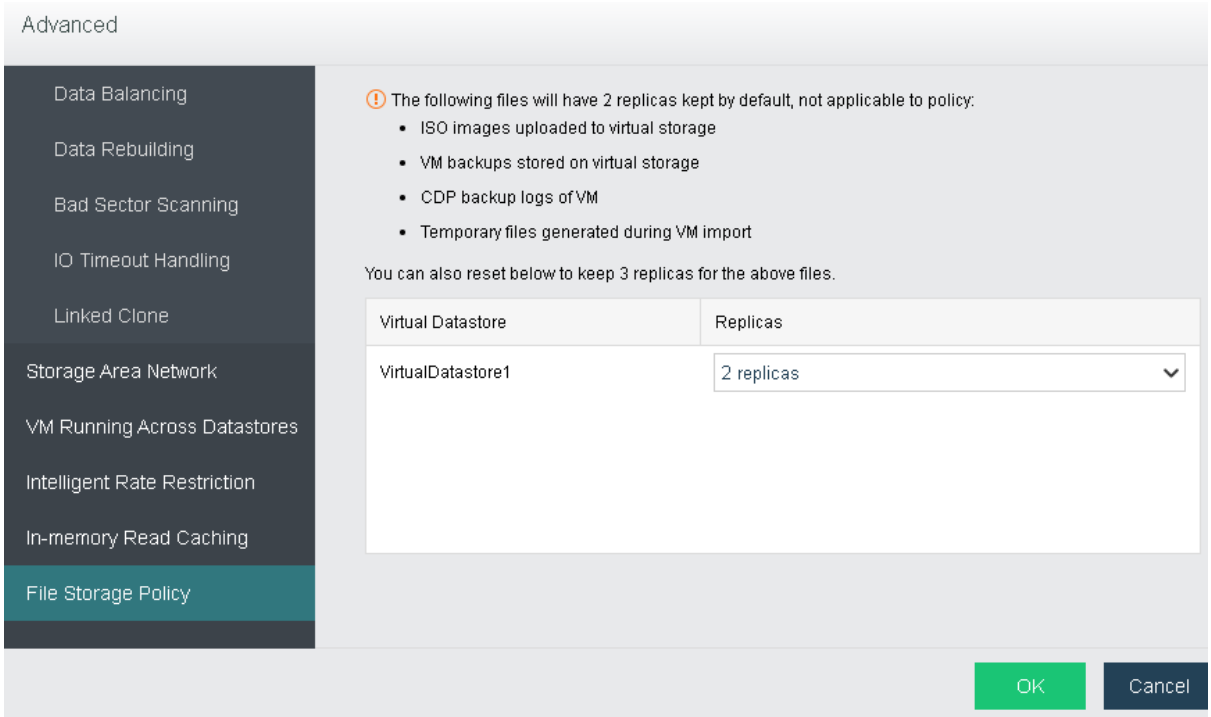
Intelligent Rate Restriction: Restrict data transfer rate for ongoing non-business tasks such as data migration and reconstruction , etc,accordiing to IO performance,to ensure business continuity.



In-memory Read Caching: In-memory read caching accounts for 1/16 of host memory, which cannot be used by virtual machine. You may disable it and change to cache size.

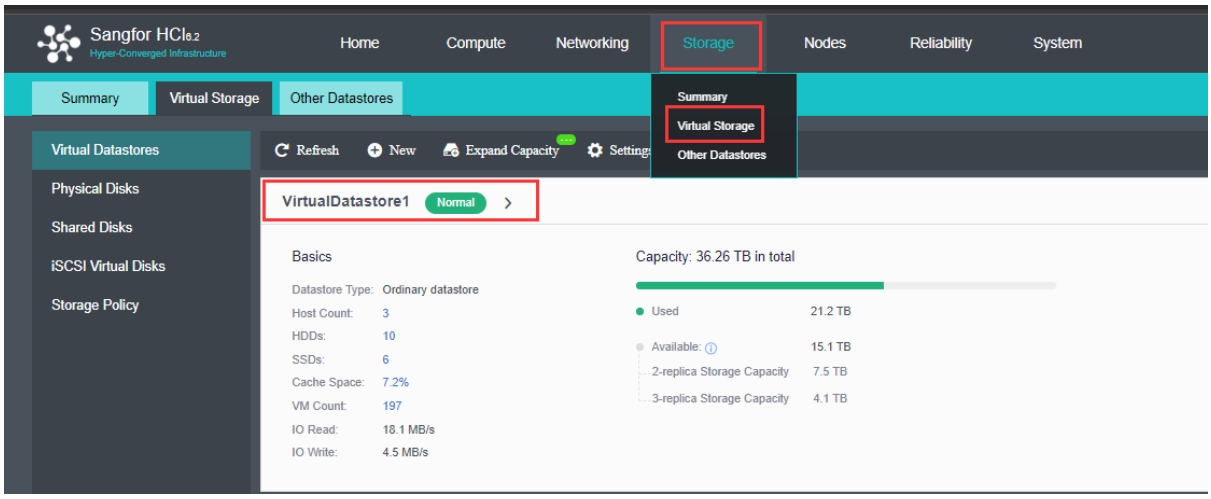


File storage Policy: To specifies number of replication which the ISO images, VM backups, CDP backup and the temporary file generated during import which stored in virtual storage.



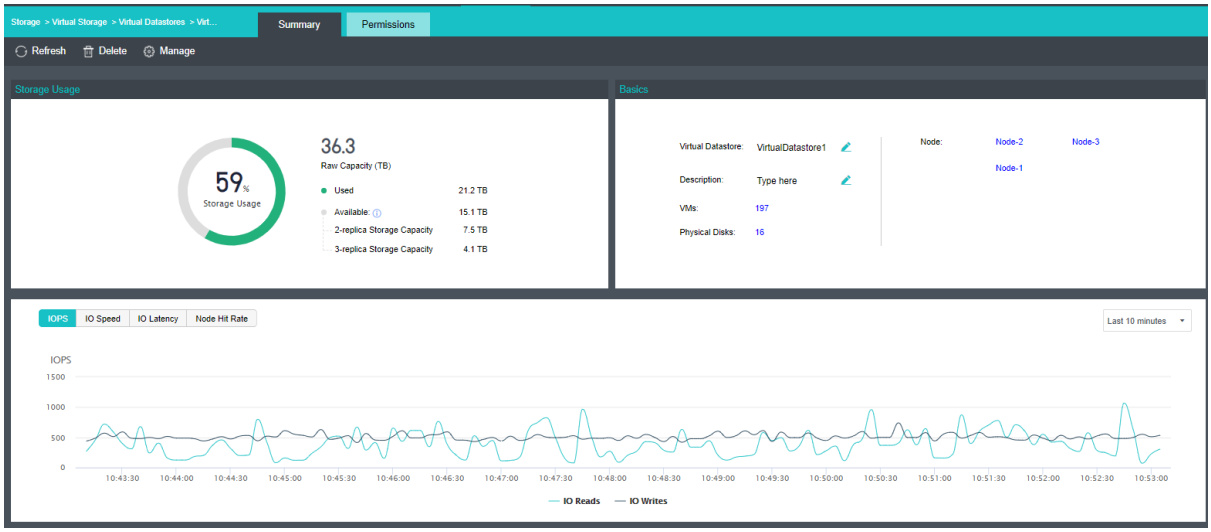
2.4.3.4 Viewing Virtual Datastore Details

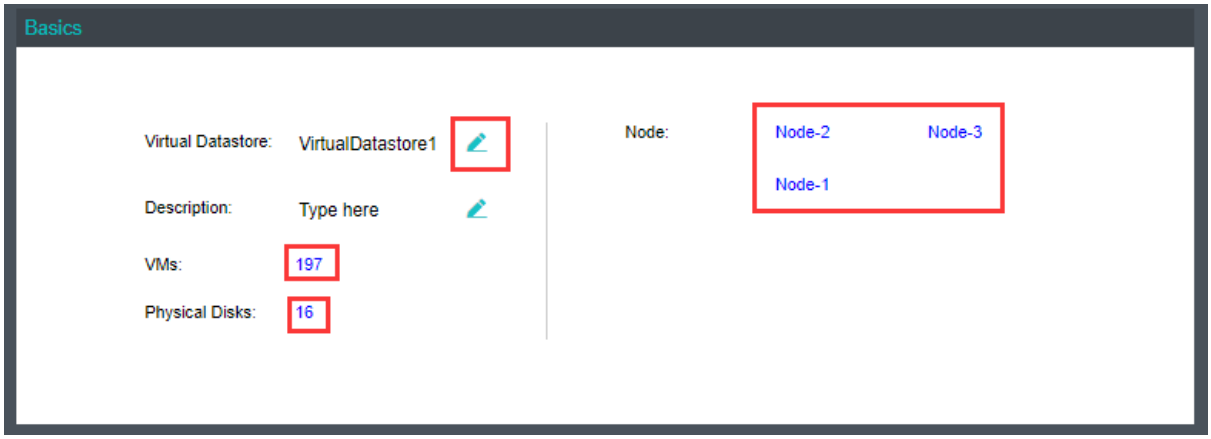
Navigate to **Storage > Virtual Storage > Virtual Datastores a**nd click on datastore's name to enter the following page. Here you may view detailed information about a virtual datastore. There are two tabs: **Summary** or **Permissions**.



2.4.3.4.1 Viewing Virtual Datastore Summary

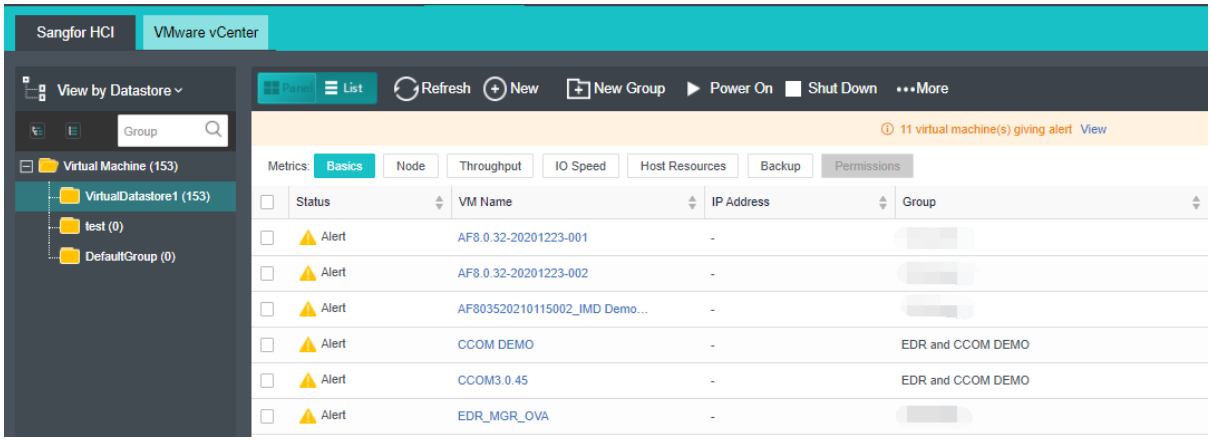
On the **Summary** page, you may view virtual datastore capacity, basic information, status, etc.



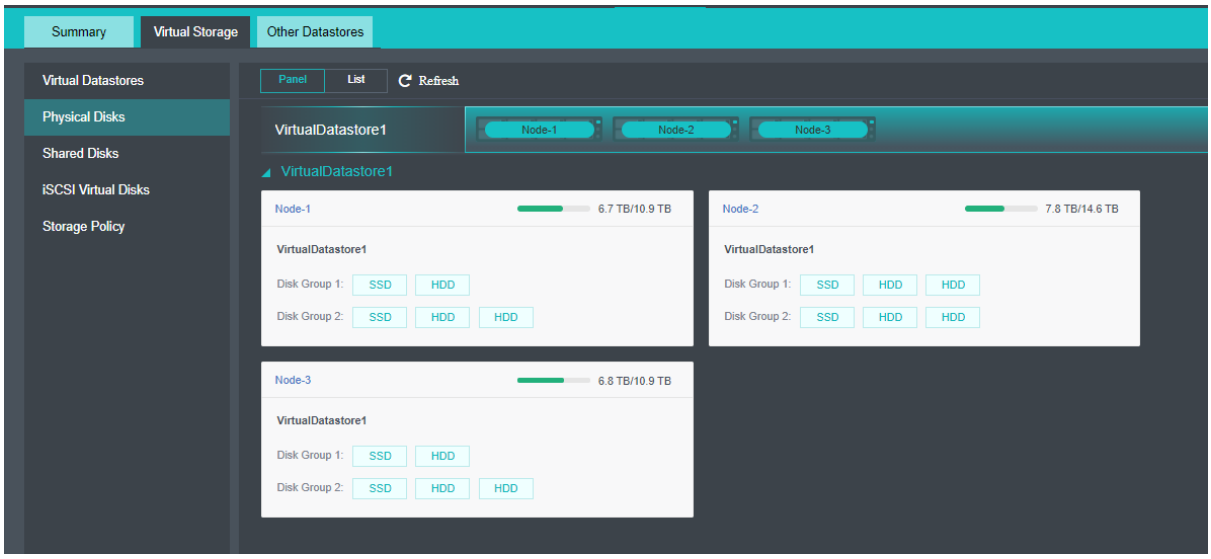


To change virtual datastore name and description, click .

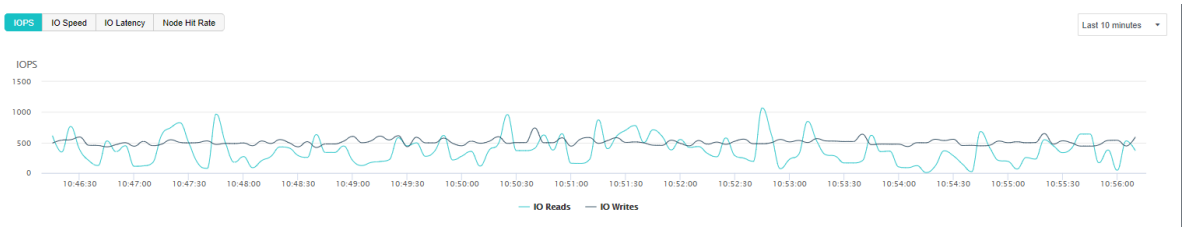
To view virtual machines in the virtual datastore, click on the number beside **VMs**.



To view disks in the virtual datastore, click on the number beside **Physical Disks**.

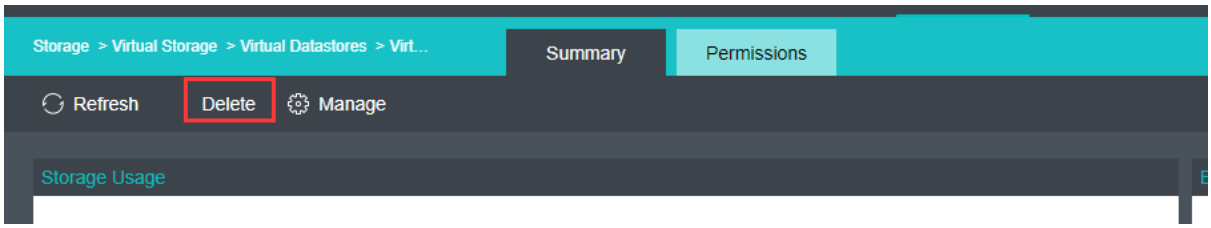


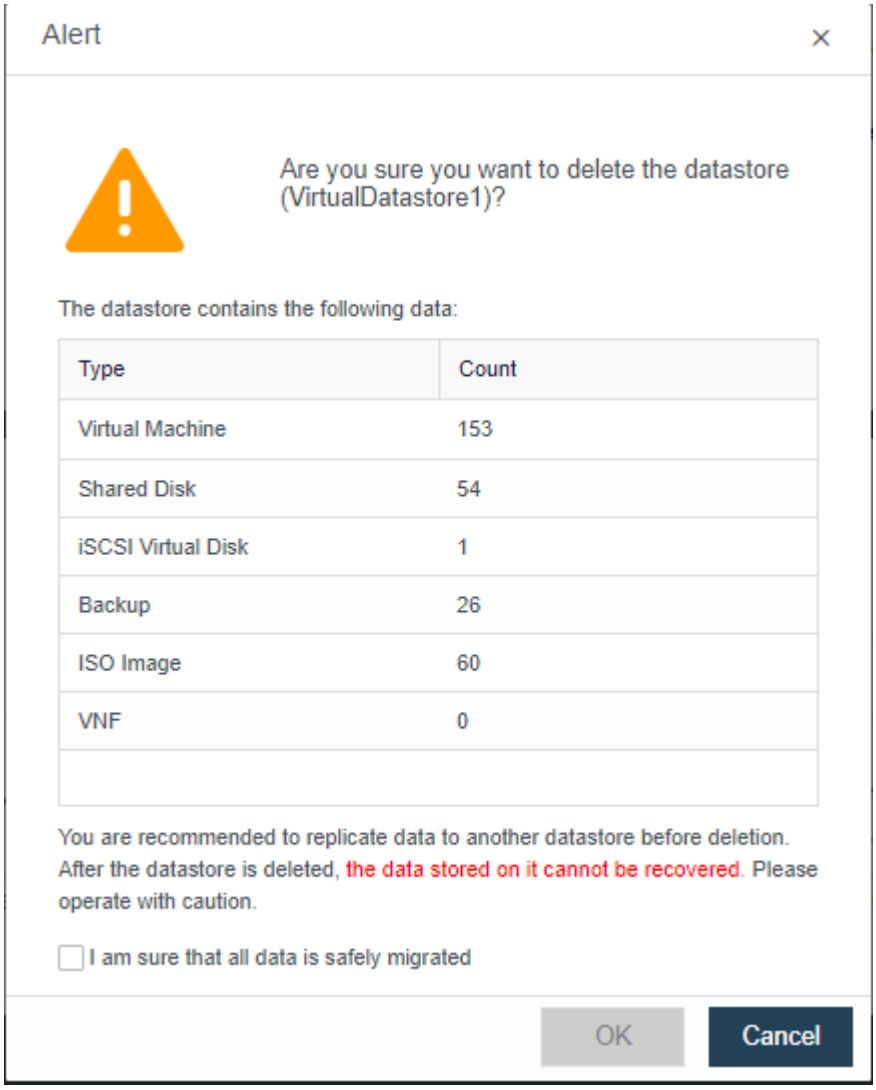
For storage operating details, you may refer to the **2.4.1 Storage** Summarysection.



2.4.3.4.2 Deleting Virtual Datastore

On the **Summary** page of a virtual datastore, click **Delete** to delete the datastore and the following dialog will pop up. Note that all the data will be deleted permanently and cannot be restored once the virtual datastore is deleted.





Before performing deletion operation, do the following:

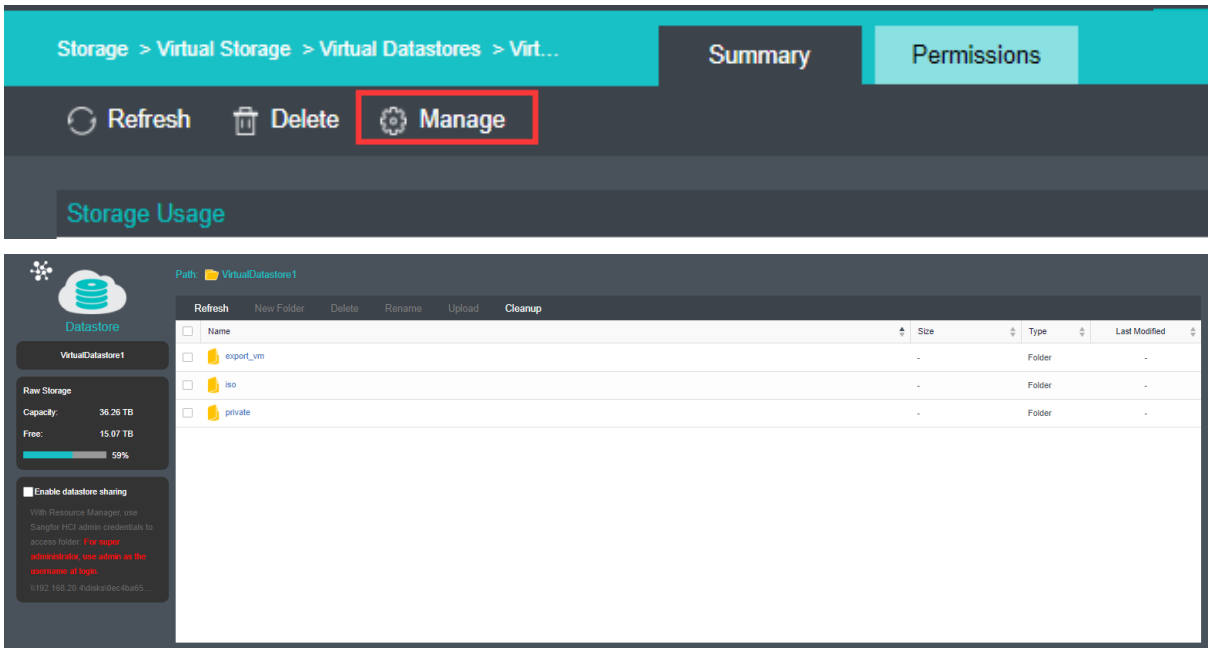
1. Make sure that all the virtual machines running in this virtual datastore are shut down.
2. Make sure that the virtual machines running in another virtual datastore but stored in this one are shut down.
3. If the iSCSI virtual disks provided by this virtual datastore are not to be used any more, end all the iSCSI connections to it.

Type admin password to confirm the deletion operation.

Once the virtual datastore is deleted, nodes added to the virtual datastore will be removed from the cluster.

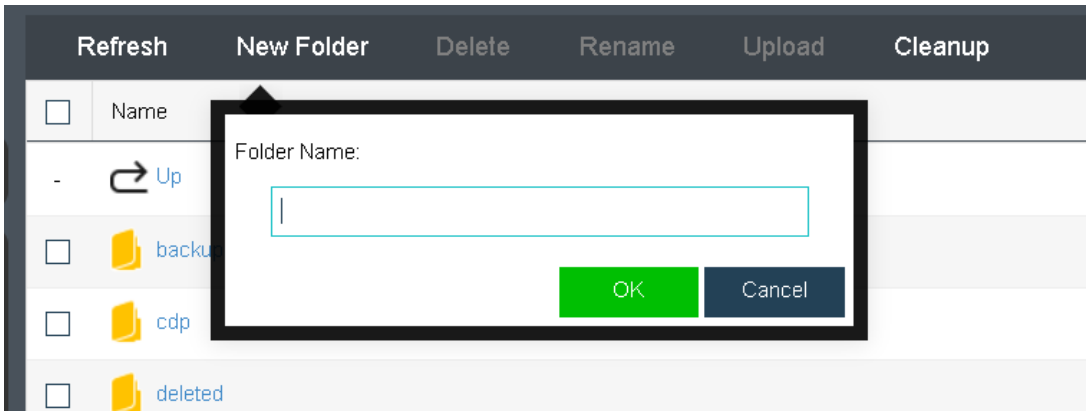
2.4.3.4.3 Managing Datastore

On the **Summay** page of a virtual datastore, you may click **Manage** to enter the following page. Here you can manage the datastore and folders on it.



Enable datastore sharing: If this option is selected, you can access virtual datastore through the directory displayed under that option.

To add a new folder, click **New Folder** and then enter a folder name.



Delete: To delete a file or folder, select the file or folder that you want to delete and then click **Delete**.

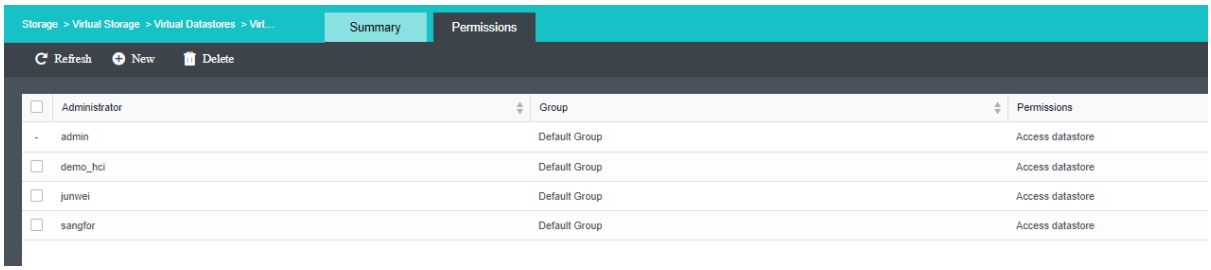
Rename: To rename a file or folder, select the file or folder that you want to rename and click **Rename**.

Upload: To upload a file, select a folder and click **Upload** to upload a file to that folder. For

example, upload an ISO image file to ISO folder for the purpose of creating virtual machines.

2.4.3.4.4 Permissions

Permissions of virtual datastore is used to assign to sub-administrator to manage datastore. To add permission of virtual datastore on the **Permissions** page, you need to add the permission of accessing datastore in **System > System Administrators and Permissions** first.

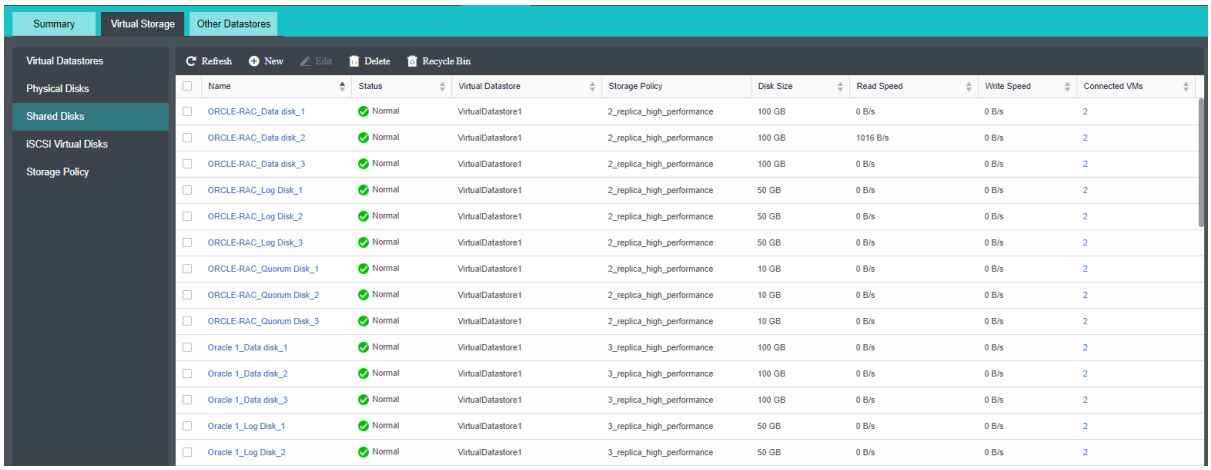


2.4.4 Managing Physical Disks

2.4.5 Shared Disks

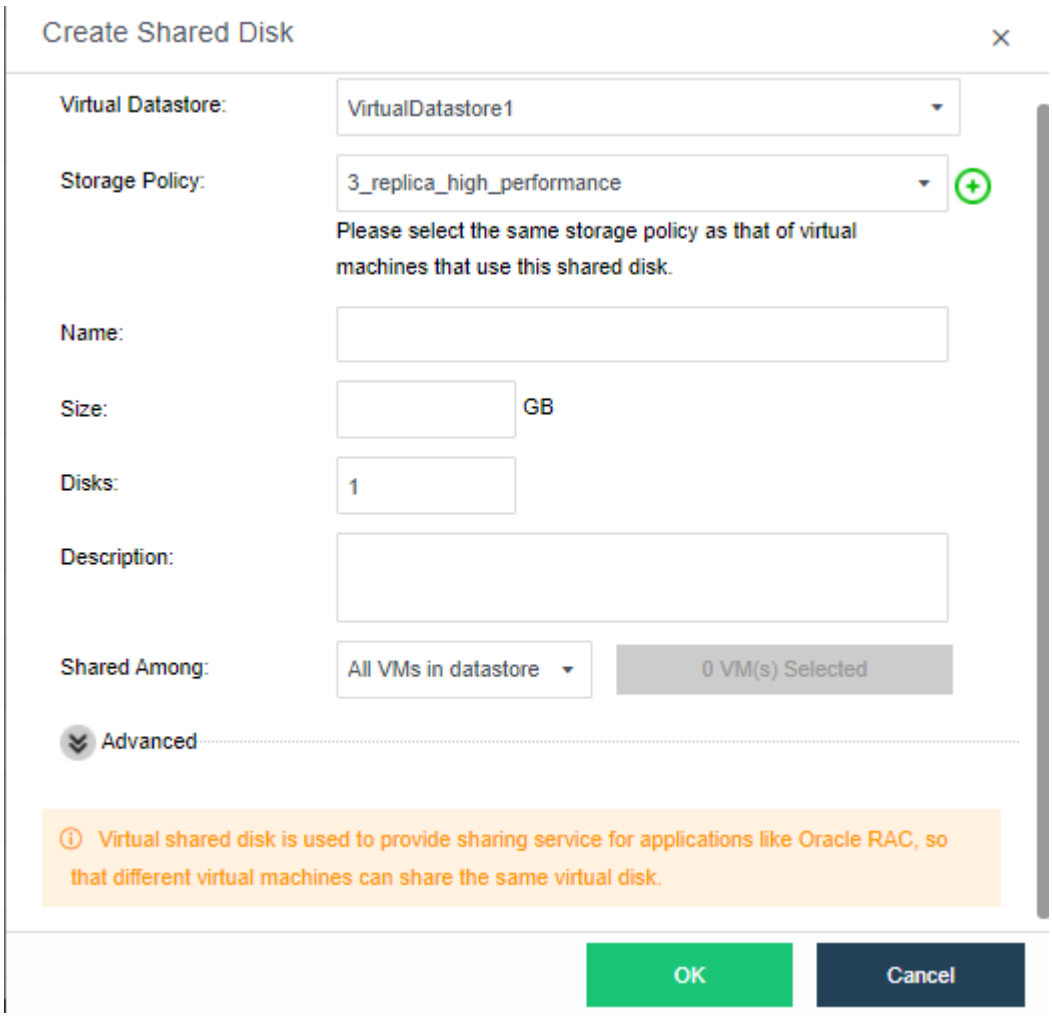
A shared disk can be mapped and used by more than one virtual machines that run compatible applications. Note that if the disk is shared by virtual machines running different applications that do not support disk sharing, disk data may get damaged. However, that is not a problem for Oracle RAC database environment, which supports disk sharing among nodes in RAC (Real Application Clusters)

On the **Shared Disks** tab shown below, it displays the following information: **Name, Status, Virtual Datastore, Disk Size, Write Speed, Read Speed,** and **Connected Virtual Machines**.



2.4.5.1Creating Shared Disk

To create a shared disk, you may click **New** in **Storage > Virtual Storage > Shared Disks** and configure the related fields on the pop-up page, as shown below:



Virtual Datastore: Specifies where the shared disk is stored.

Name: Specifies a distinguishable name of the shared disk. It can only contain Chinese characters, digits, letters, space and the following special characters: ()[]{} （）【】{} @|._-+

Storage Policy: Select the number of replication for the disk.

Disks: Specifies the number of shared disks.

Description: It is optional.

Size: Specifies size of shared disk. The maximum is 1TB(1024GB).

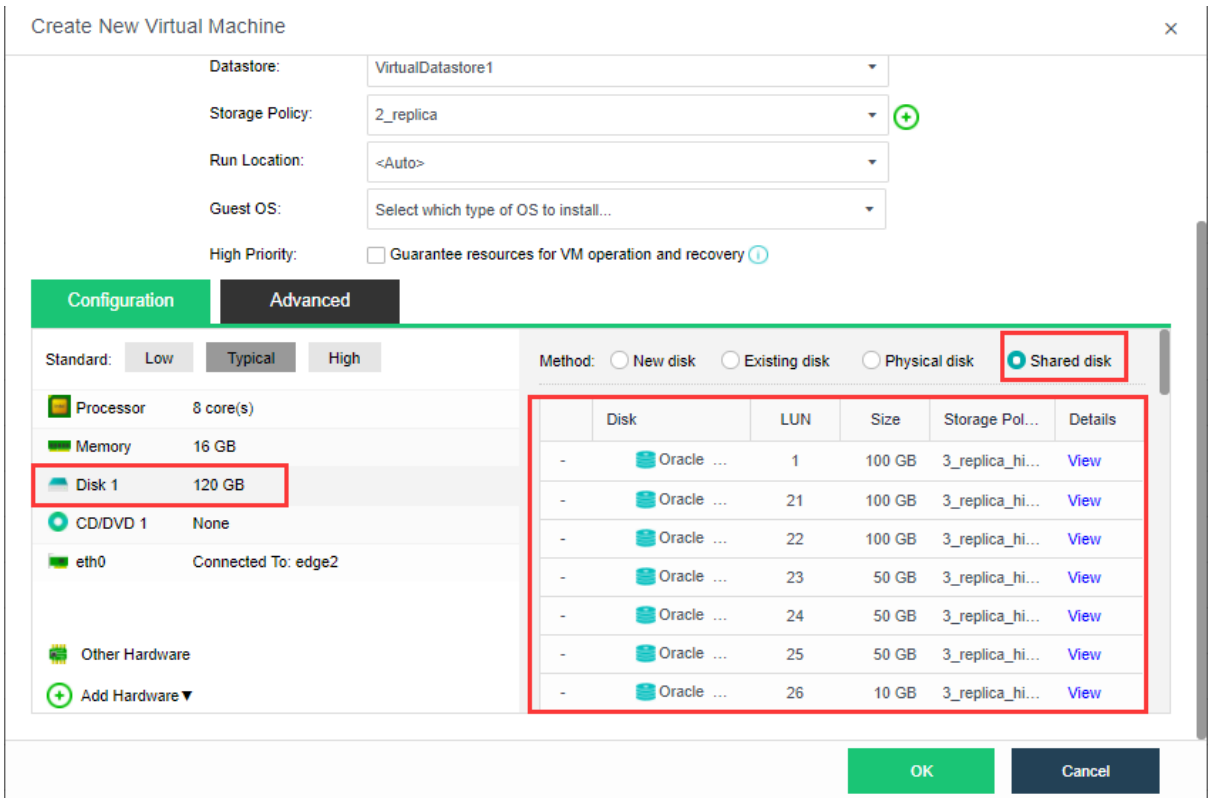
Shared Among: You may select **Any virtual machine in this virtual datastore** or **Specified virtual machines**.

Any virtual machine in this virtual machine: If it is selected, it indicates that shared disk can be accessed by any virtual machine in the specified virtual datastore.

Specified virtual machines: If it is selected, you need to specify virtual machines. Only the selected virtual machines can access shared disk.

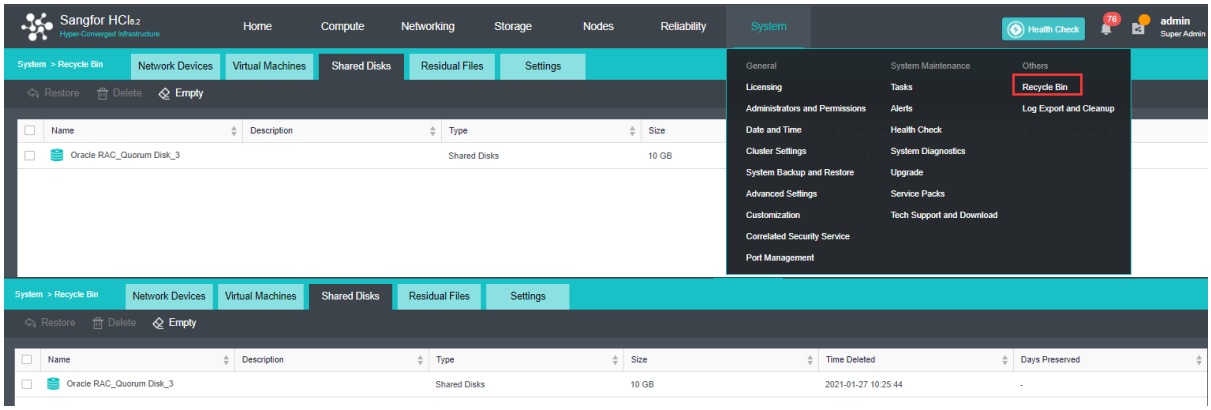
2.4.5.2 Allocating Shared Disk

To assign a shared disk to a virtual machine, first edit that virtual machine. Then, on the **Edit Virtual Machine** page, select **Add Hardware** > **Disk** and choose **Shared disk**, as shown below:



2.4.5.3Restoring Shared Disk

A shared disk can be deleted. After deletion, it will go to **Recycle Bin**. In **Recycle Bin**, you may restore it or delete it permanently.



2.4.6 Storage Policy

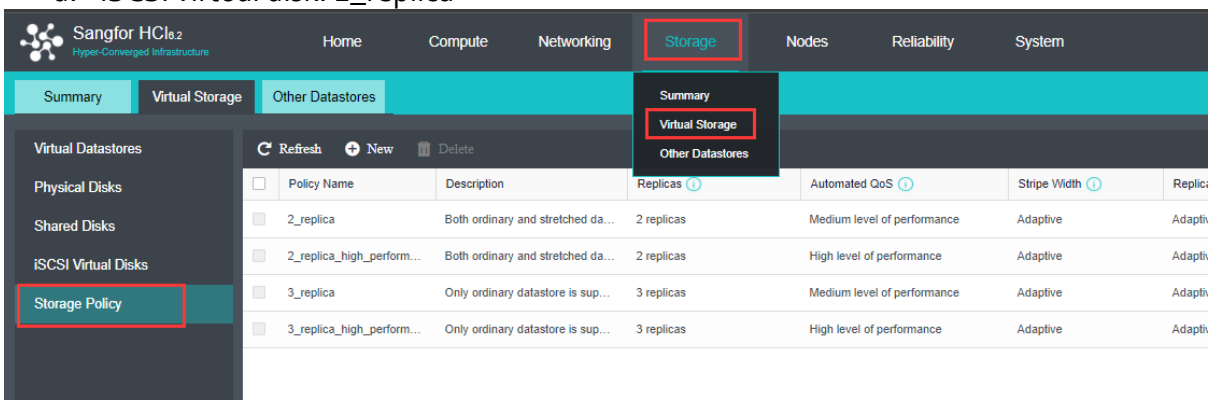
In version 6.0.1, Storage Policy had been implemented for virtual machine and virtual disk. This allow user to separate the VM based on the priority of the business.

HCI will create the storage policy automatically after the virtual storage had been created.

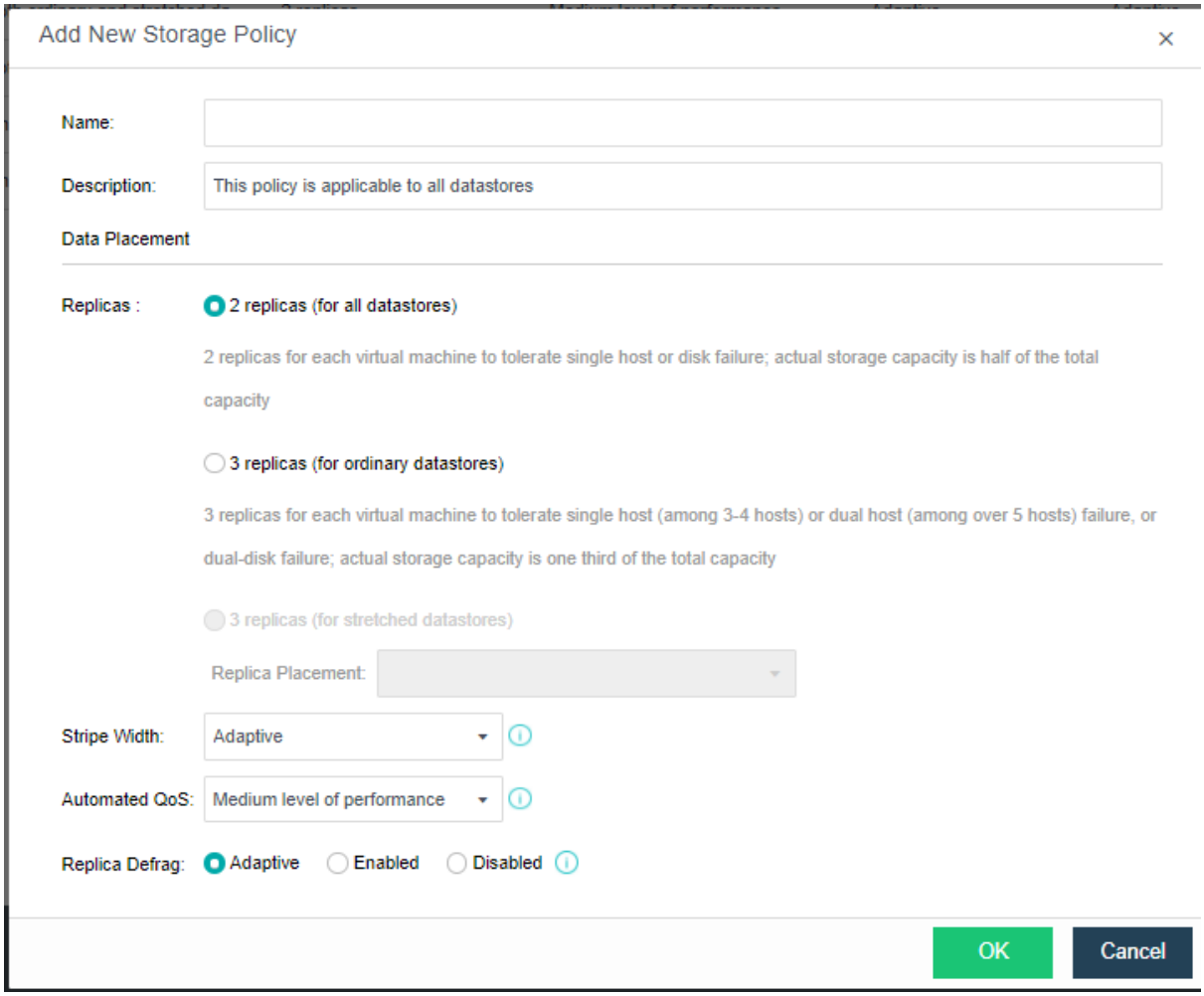
Navigate to **Storage** > **Virtual Storage** > **Storage Policy** to view the current available Storage Policy.

Below is the default storage policy for different scenario.

a. Normal VM : 2_replica
b. SQL Server/ Oracle Database: 3_replica_high_performance
c. Shared disk: 3_replica_high_performance
d. iSCSI virtual disk: 2_replica



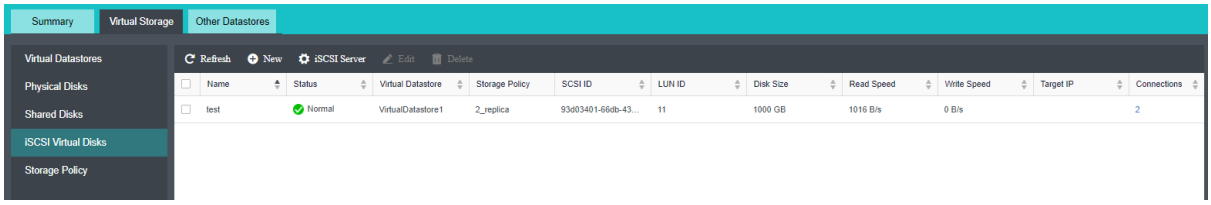
Creating new storage policy allow to customize in terms of Replicas, Auto Tiering QoS, Stripe Width and Replica Defrag.



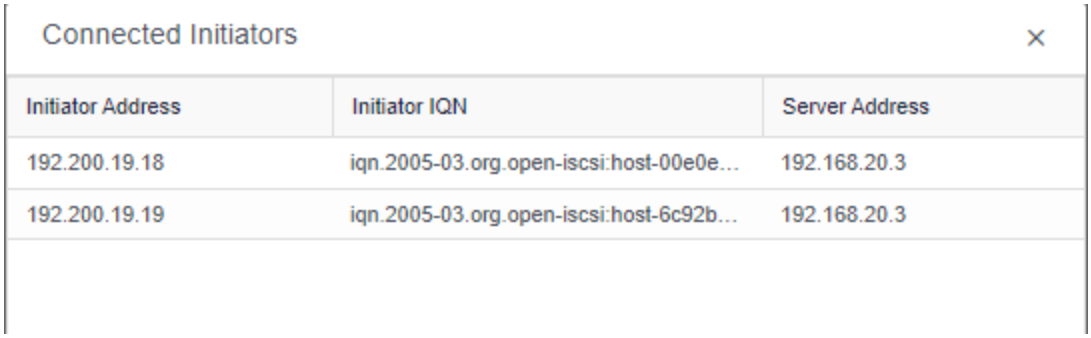
2.4.7 iSCSI Virtual Disks

Virtual storage can be configured to be an iSCSI sever so that part of virtual storage can be preallocated as iSCSI disks which can be accessed by iSCSI initiators.

Navigate to **Storage > Virtual Storage > iSCSI Virtual Disks** and you will see the following information: **Name, Status, Virtual Datastore, LUN ID, Disk Size, Write Speed, Read Speed, Target IP Address,** and **VMs**.

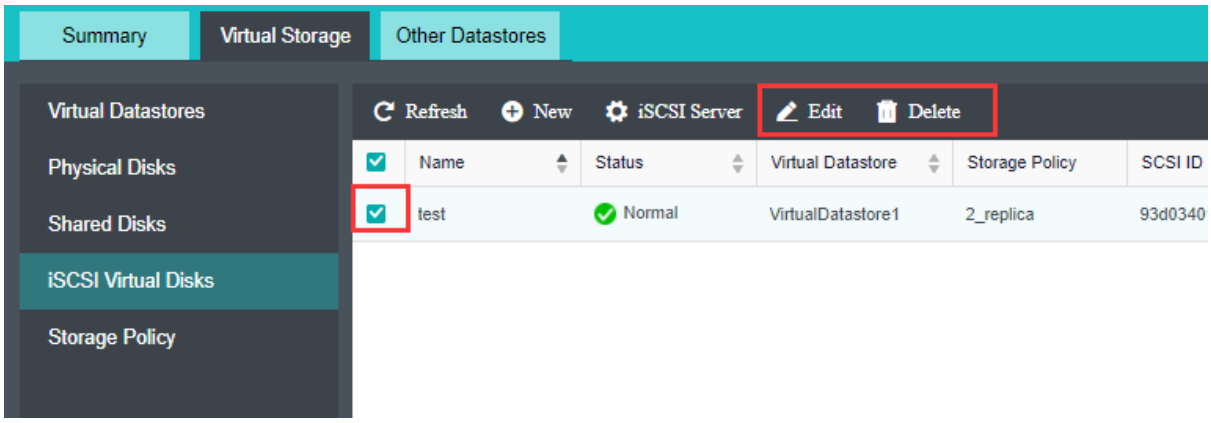


To view connected iSCSI initiators, click on the number under the **Connected** column.



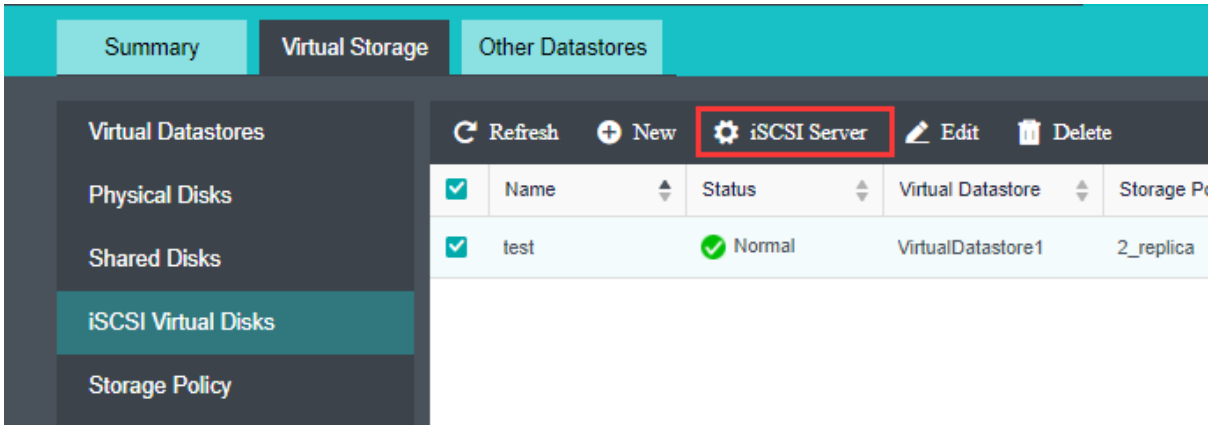
To edit an iSCSI virtual disk, you may select the disk that you want to edit and then click .**Edit**

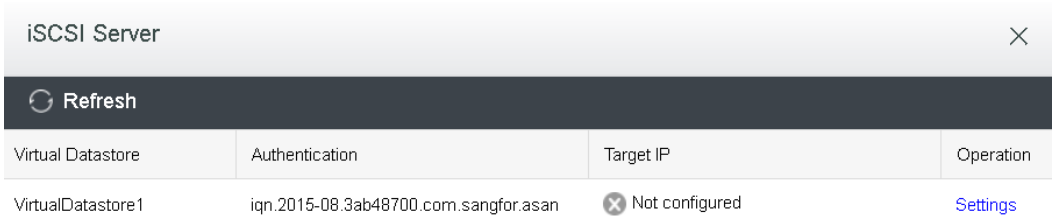
To delete an iSCSI virtual disk, you may select the disk that you want to delete and then click **Delete**



2.4.6.1Configuring iSCSI Server

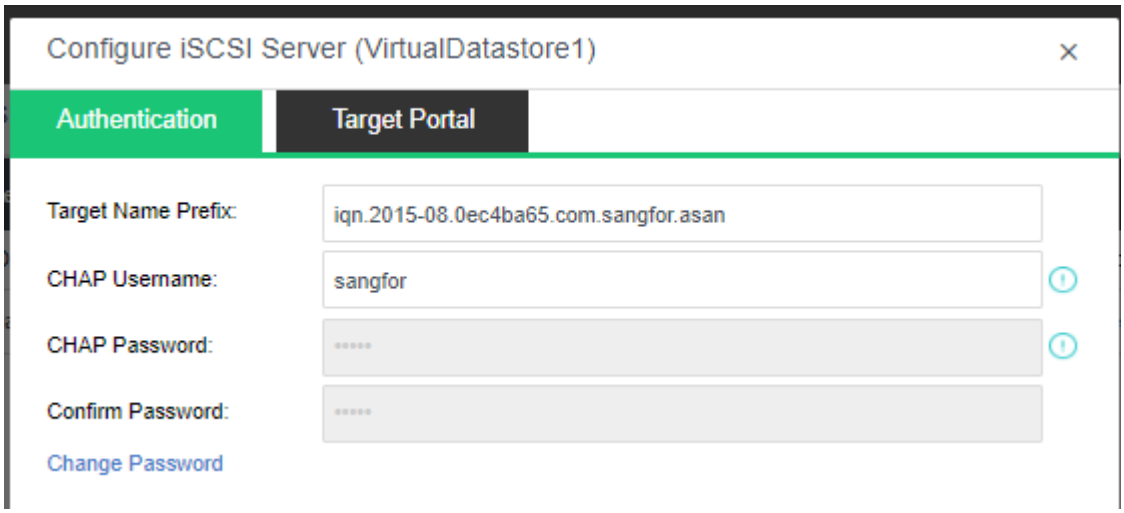
An iSCSI server should be configured before you create iSCSI virtual disk. You con configure iSCSI server for different virtual datastores. The configuration process involves configuring iSCSI authentication and target portal(only available for cluster with 3 nodes and above).





2.4.6.1.1 Configuring iSCSI Server Authentication

Target Name Prefix, CHAP Username, CHAP Password, and Retype Password fields should be specified, as shown below:



Target Name Prefix: Specifies prefix of target name. Default format is iqn.date.com.sangfor.asan. The default is recommended.

CHAP Username: Specifies CHAP username used by iSCSI initiator to connect to iSCSI server.

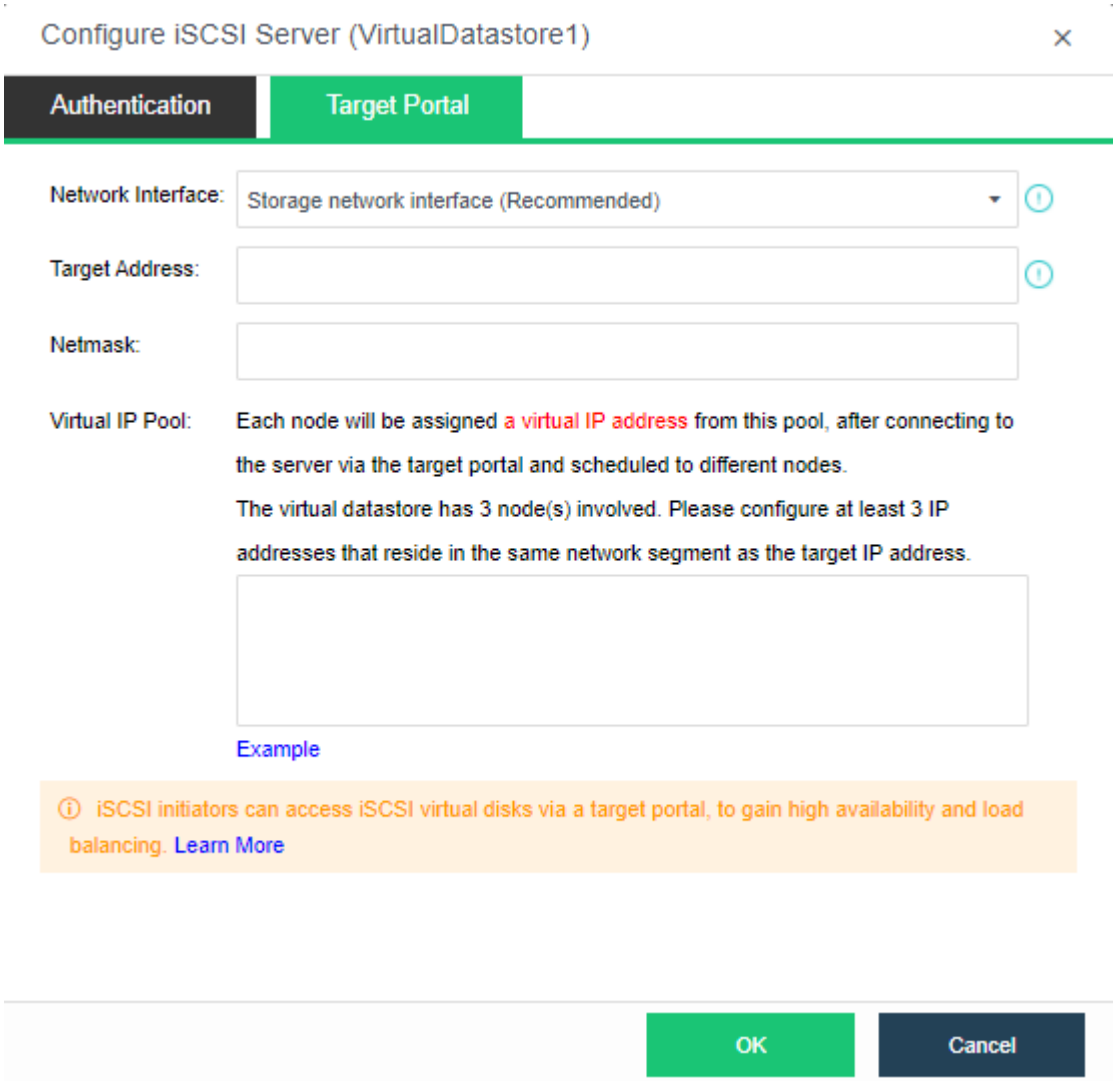
CHAP Password: Specifies CHAP password used by iSCSI initiator to connect to iSCSI server.

Retype Password: Retype the CHAP password.

Change Password: To change password, click **Change Password**.

2.4.6.1.2 Configuring Target Portal

On the **Target Portal** tab, configure the following fields: **Network Interface, Target IP Address, Netmask** and **Virtual IP Pool** :



Network Interface: Specifies the interface for iSCSI initiator to access iSCSI server. Options are **Storage Network Interface** and **Management Interface**. Management interface cannot be used in the following situations: 1) It is reused as overlay network interface; 2) It is reused as the edge; 3) It applies link aggregation.

Target IP Address: Specifies target IP address. iSCSI initiator connects to iSCSI server through this IP address. Make sure that the target IP address is reachable for iSCSI initiators.

Netmask: Specifies the netmask of the target IP address.

Virtual IP Pool: Each clustered node will be assigned an IP address from virtual IP pool. Thus, initiators will be scheduled to to different nodes after connecting to iSCSI server.

iSCSI initiators can access virtual iSCSI disk via target IP address, to gain high availability

and load balancing. Each clustered node will be assigned an IP address from virtual IP pool. Thus, initiator connections to a specified target IP address will be scheduled to different nodes. This has the following strengths:

Click **OK** to save the changes. Changes to target portal should also be made at iSCSI initiator side, and if there is any change made to network interface, the iSCSI network should be reconfigured correspondingly.

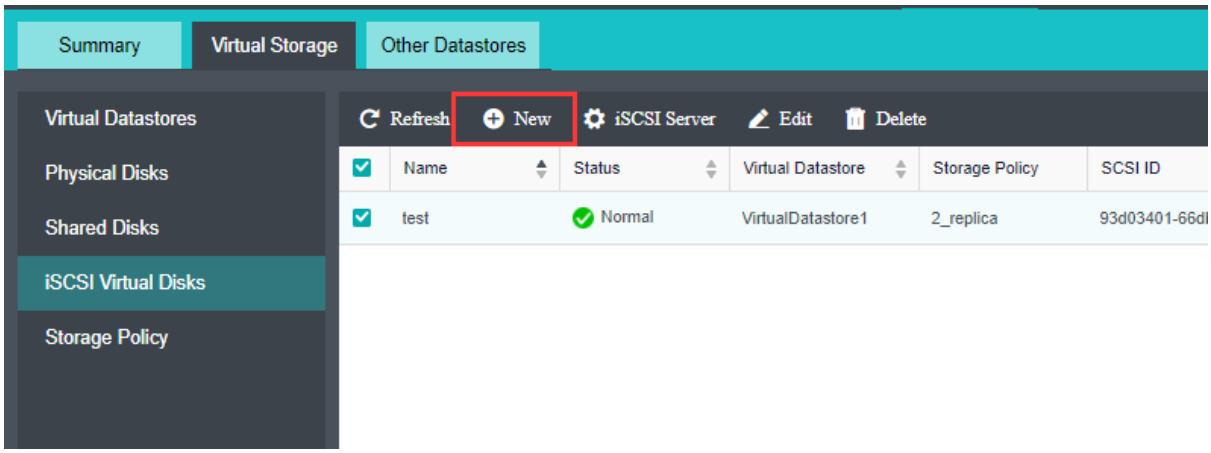
2.4.6.1.3 Load Balancing

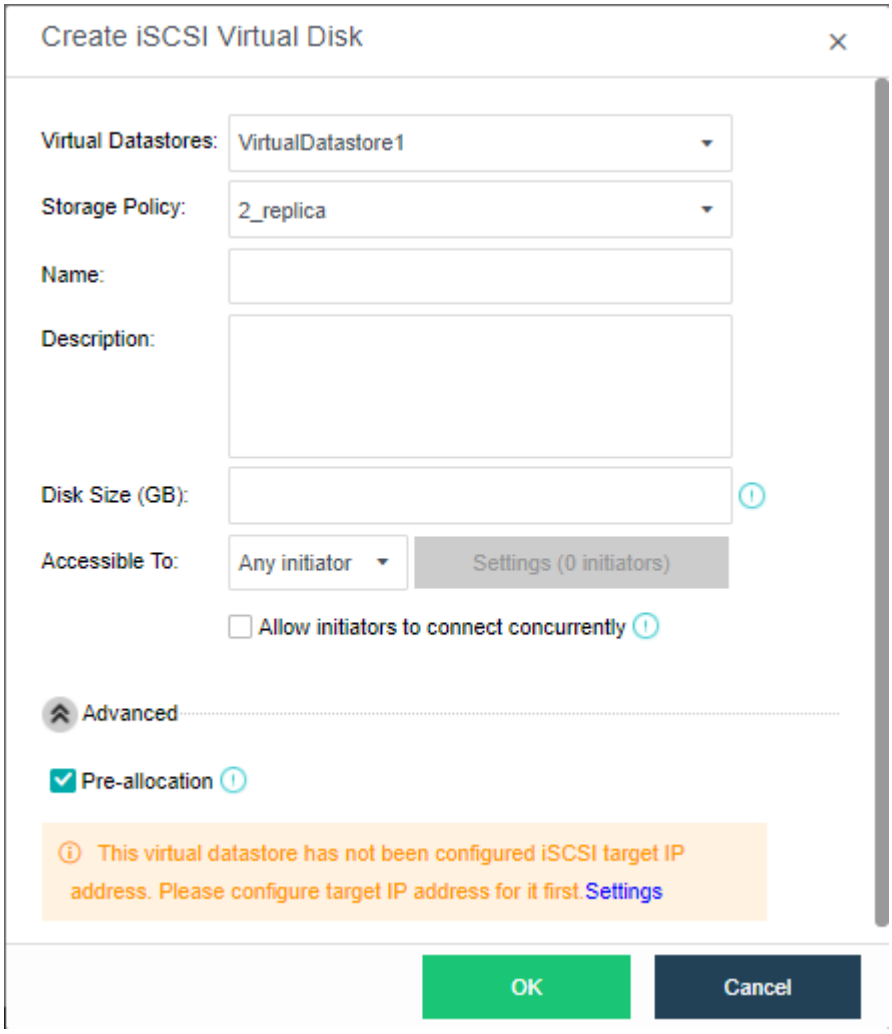
If the iSCSI connections to nodes are not balanced, click **Perform Again** to re-schedule initiator connections to different nodes so as to ensure iSCSI connections evenly assigned to each clustered node. iSCSI connections will be preferentially scheduled to the node which has LUN replicas, which helps to enhance IO performance and reduce network load.

Rebalancing load will make some iSCSI connections disconnected and requires administrator to enter password of the username to confirm operation.

2.4.6.2 Creating iSCSI Virtual Disk

After iSCSI server has been configured, you can create iSCSI virtual disk by click **New** in **Storage > Virtual Storage > iSCSI Virtual Disks**, as shown below:





Virtual Datastore: Specifies a datastore for creating iSCSI virtual disk.

Name: It can contain digits, letters, dots and colons only. iSCSI disk name consists of the name specified here and target name prefix which is specified when configuring iSCSI server.

Description: Specifies description for the new virtual disk. It is optional.

Disk Size: Specifies size of the iSCSI disk. The maximum is 48TB(49152GB) and cannot exceed the available storage capacity.

Accessible To: You may select **Any initiator** or **Specified initiator**.

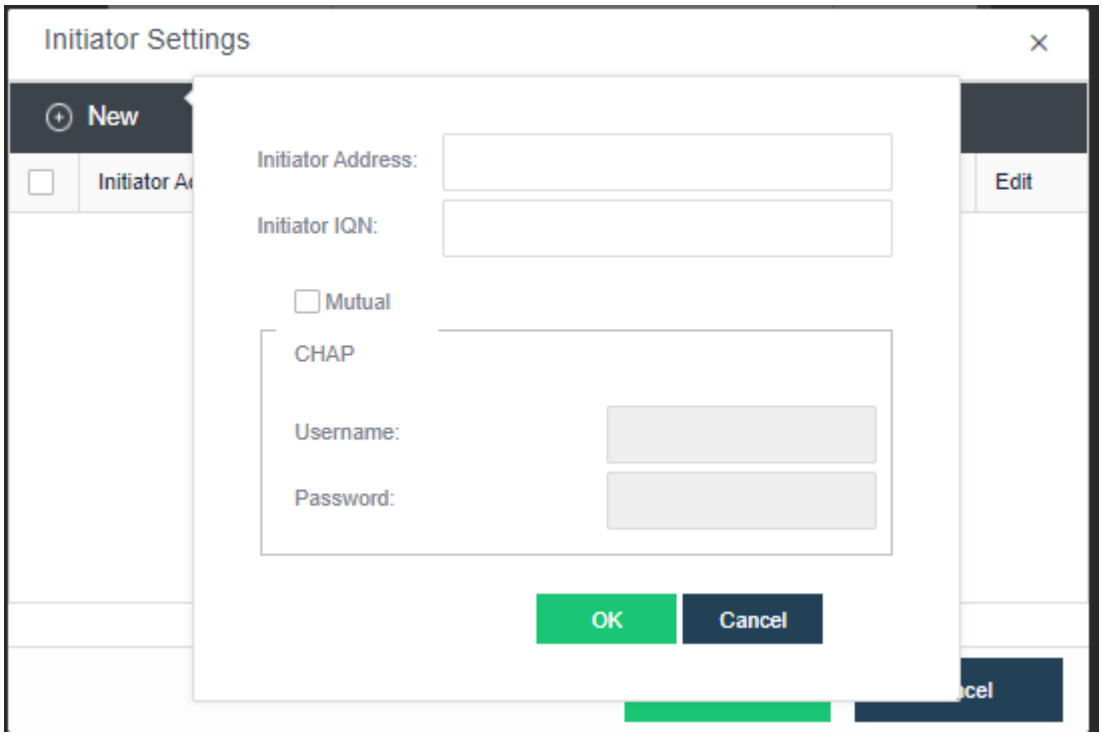
Any Initiator: If it is selected, the iSCSI disk can be accessed by any initiator as long as cluster IP address or node IP address, and CHAP username and password are provided correctly.

Specified Initiator: If it is selected, click the **Settings (o initiators)** button to configure iSCSI initiator. To add an iSCSI initiator, click **Add** on the **Initiator Settings** page to enter the following page.

To enable iSCSI disk to be accessed by multiple initiators concurrently, select the option **Allow initiators to connect concurrently**: For the sake of data security, that option is

deselected by default. Enable this to allow an entire cluster to access, for example, VMware vSphere cluster.

Pre-allocation: It will pre-allocate the iSCSI virtual disk for better performance. However, it will consume more storage space.



Initiator Address: Specifies management interface address of initiator or cluster IP address.

Initiator IQN: Indicates the device name of iSCSI initiator.

Mutual CHAP: If it is selected, **Username**,and **Password** fields are required. This option is optional. If mutual CHAP has not been configured on iSCSI initiator, keep this option deselected. iSCSI disk cannot be accessed by iSCSI initiator if the correct CHAP username and password are not provided in case that mutual CHAP has been configured on that iSCSI initiator and that initiator is required to be authenticated by iSCSI server,

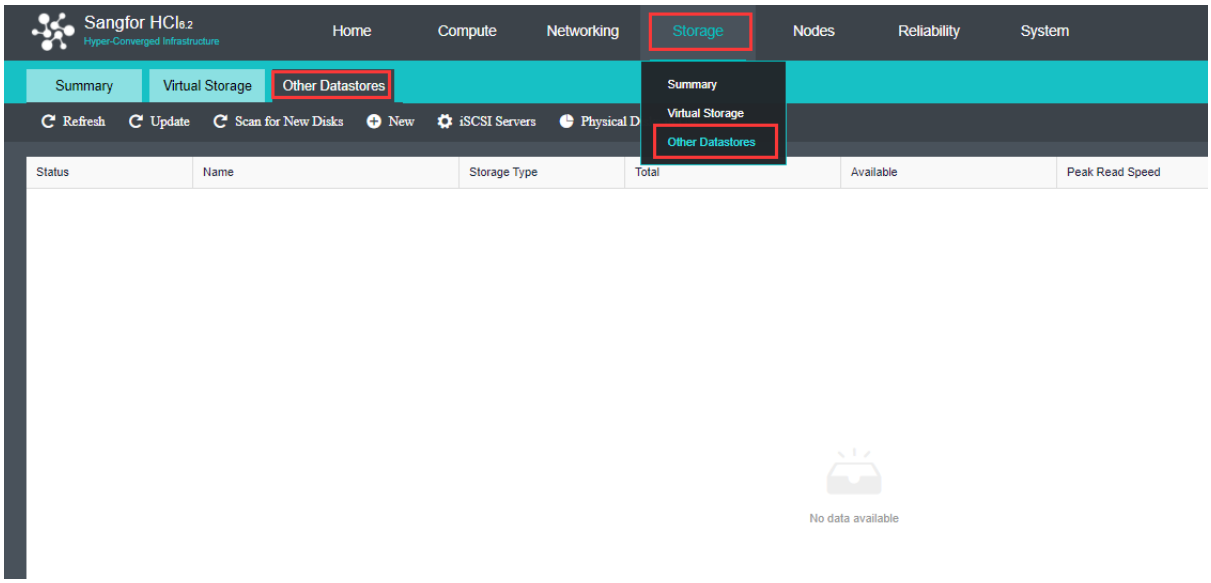
One of the two fields is required at least.

2.4.8 Other Datastores

Storage falls into the following tyeps: FC, iSCSI, NFS and local storage. Sangfor HCI virtualizes storage and makes hardware-related storage settings hidden. Storage space of a host relies on physical disk size but can be expanded by using external storage. Local storage is provided by physical disk of the host installed Sangfor HCI software and can only be

accessed by the host where that storage resides but not accessed by other hosts.

On the **Other Datastore** page, status, name, storage type, total capacity, available space, peak read speed, peak write speed, and connected nodes are displayed as follows:

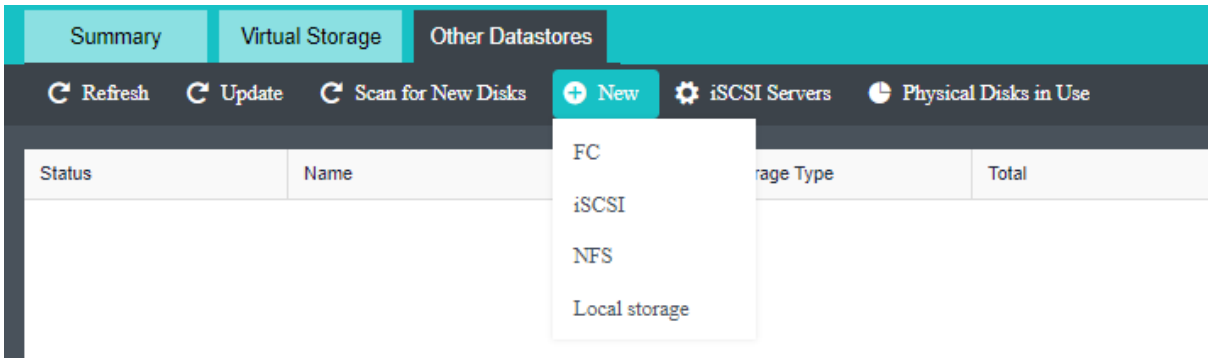


To view detailed information of virtual datastore, click on the name of the virtual datastore. For details, refer to the Error! Reference source not found.section.

To perform more operations, you may click on the icon  beside datastore name and will see the following operations: **Edit, Summary, Manage, Delete, Format** and **Cleanup**.

2.4.7.1 Adding New Datastore

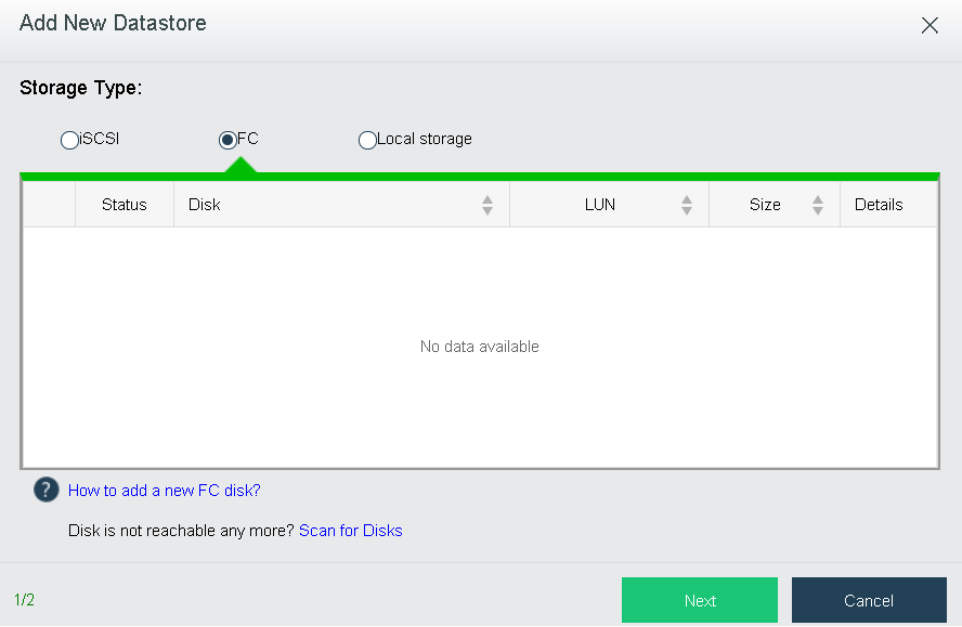
You can add the following types of datastores: iSCSI, FC, NFS or local storage by clicking **New** in **Storage > Other Datastore.**



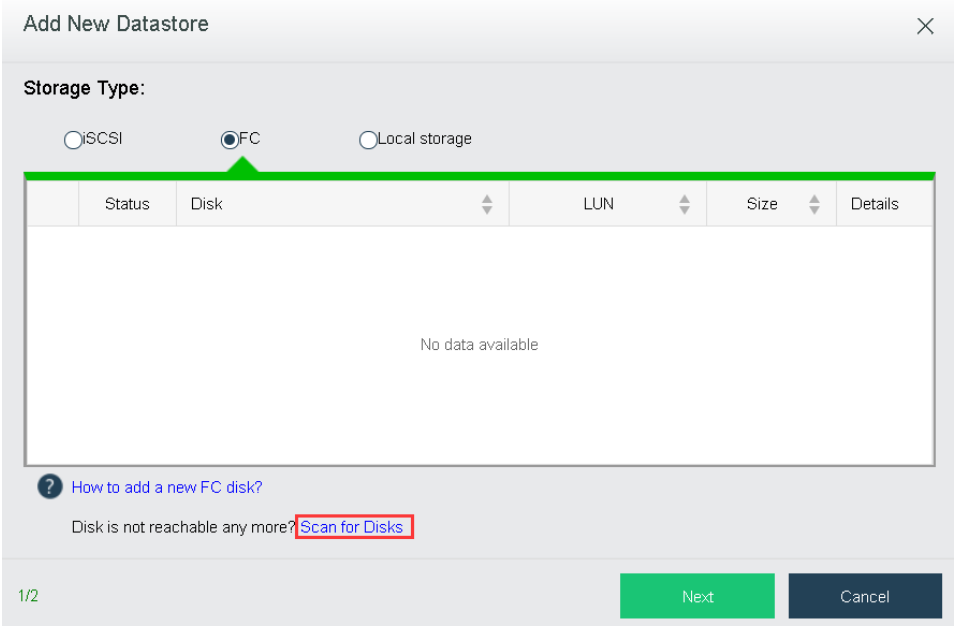
2.4.7.1.1 Adding FC Type of Datastore

Fiber channel(FC) adopts Fiber Channel over IP (FCIP) to connect storage devices in TCP/IP network. FCIP transmits Fiber Channel data by establishing a tunnel between two peers. Generally, it builds storage area network through DWDM and dark fiber.

FC storage connected to hosts will be automatically discovered by Sangfor HCI but needs to be added to virtual storage before being used.



If there is any FC disk that has not been found, you can click **Scan for Disks**.



Datastore: Specifies a distinguishable name for the datastore. Datastore name should

contain 2-16 characters consisting of digits, letters.

Connect To Node: Displays the node that the new local disk belongs to.

If any virtual machines is stored on the datastore, you can select the option **Recover existing virtual machines on this datastore as well** to recover existing virtual machines.

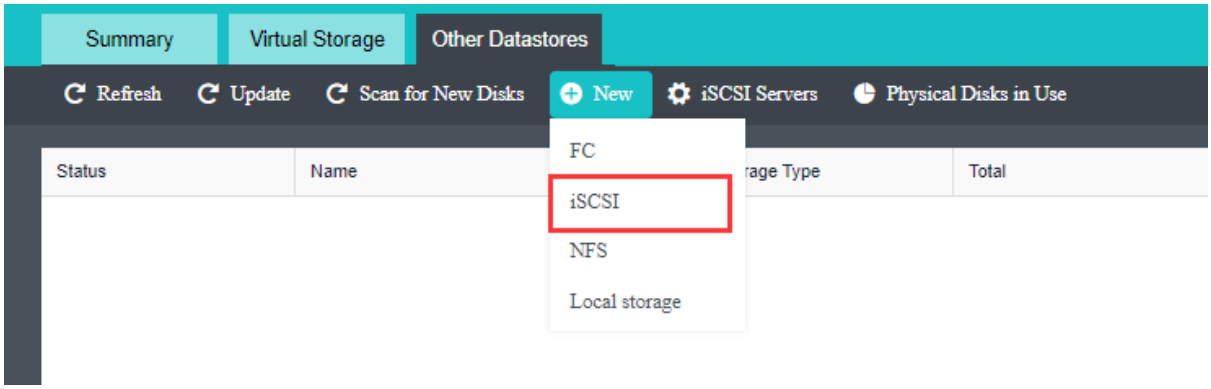
Then, click **OK** to save settings or click **Cancel** to give up the changes.

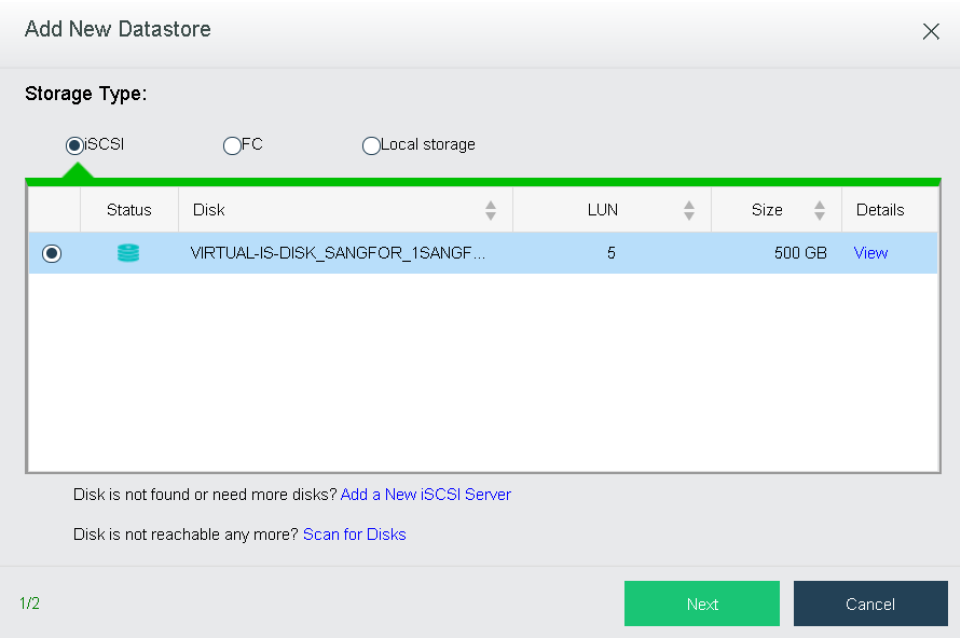
If there is virtual machine stored on the datastore, but the option Recover existing virtual machines on this datastore as well is not selected, the virtual machine will not be deleted. You should perform format operation so as to delete the virtual machine in the virtual datastore. If you'd like to recover virtual machine to HCI platform, you can add the datastore again and select the option Recover existing virtual machines on this datastore as well.

2.4.7.1.2 Adding iSCSI Type of Datastore

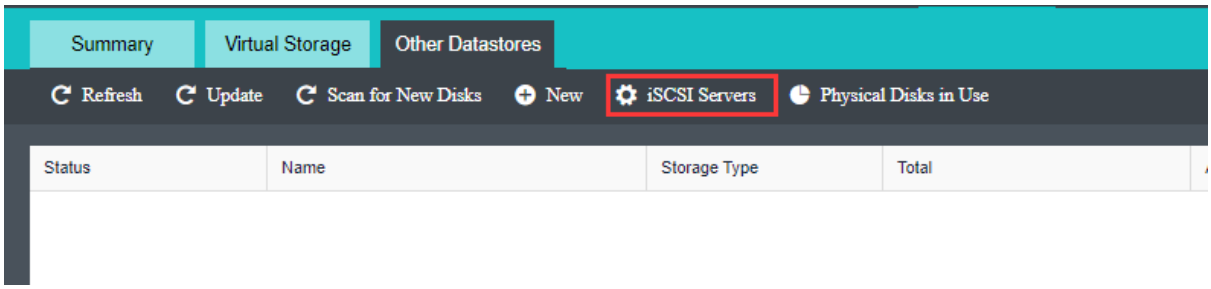
iSCSI is a P2P protocol and used to transmit storage IO data blocks over Internet Protocol(IP) network. It defines the rule and method of sending and receiving block-level storage data over TCP/IP network. More specifically, iSCSI commands and data should be encapsulated into TCP/IP packets before being forwarded.

To add iSCSI type of datastore, click **New** in **Storage > Other Datastore**, select **iSCSI** as **Storage Type** and then choose a disk.

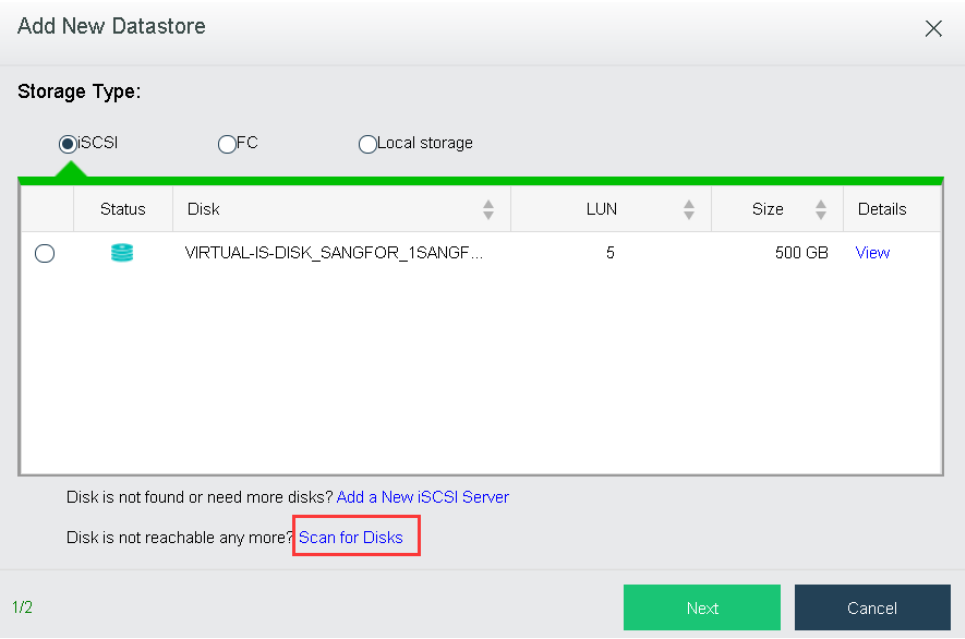




Before adding iSCSI type of datastore, you need to add iSCSI server in **Storage > Other Datastore**> **iSCSI Server**. iSCSI disks will be automatically discovered when iSCSI server settings are saved.



If any new iSCSI disk has been added but not listed here, you may click **Scan for Disks** to find new iSCSI disks.



Datastore: Specifies a distinguishable name for the datastore. Datastore name should contain 2-16 characters consisting of digits, letters, underscores, dots and hyphens only, and begin and end with letter or digit.

Connect To Node: Only the selected nodes have access to the datastore being added.

If any virtual machines is stored on the datastore, you can select the option **Recover existing virtual machines on this datastore as well** to recover existing virtual machines.

Add this datastore to VM backup repositories as well: Once this option is selected, datastore will be added to VM backup repositories.

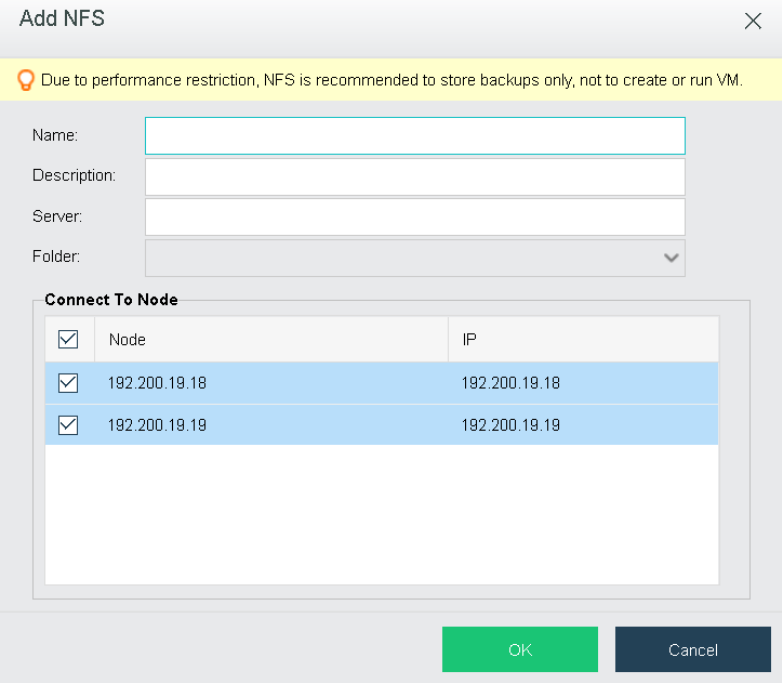
Select nodes and then click **OK** to save the settings or click **Cancel** to give up the changes.

If there are virtual machines on the datastore, and the option Recover existing virtual machines on this datastore as well is not selected, the existing virtual machines will not be cleaned up. You may try formating the datastore if you want to clean up the existing virtual machines on that datastore. If you want to recover virtual machines on the datastore, you can delete the datastore and add it again and select that option.

2.4.7.1.3 Adding NFS Type of Datastore

NFS is network file system, one type of file system supported by FreeBSD. It enables computers to share resources across TCP/IP network. NFS client can have access to files on

remote NFS server, just like accessing local files.



Name: Specifies name of the NFS type of datastore. Name can only contain 2 to 16 characters consisting of digits, letters, underscores, dots, and hyphens only, and should begin and end with letter or digit.

Description: Optional, specifies description for the NFS datastore.

Server: Specifies IP address of NFS server.

Folder: Specifies the shared folder on NFS server.

Connect to Node: Specifies node that can have access to NFS datastore.

Due to low performance of NFS datastore, it can only be used to store virtual machine backups only, not to create or run virtual machine, etc.

2.4.7.1.4 Adding Local Storage

Local storage is provided by local disks on the node installed Sangfor HCI software and can only be accessed by the host where that storage resides but not accessed by other hosts.

If there is any new disk that has been added on the node, you can add it to virtual storage by adding local storage.

Select a disk that you want to add and then click **Next** to enter the following page.

Datastore: Specifies a distinguishable name for the datastore. Datastore name should contain 2-16 characters consisting of digits, letters, underscores, dots and hyphens only, and begin and end with a letter or a digit.

Connect To Node: Displays the node that the new local disk belongs to.

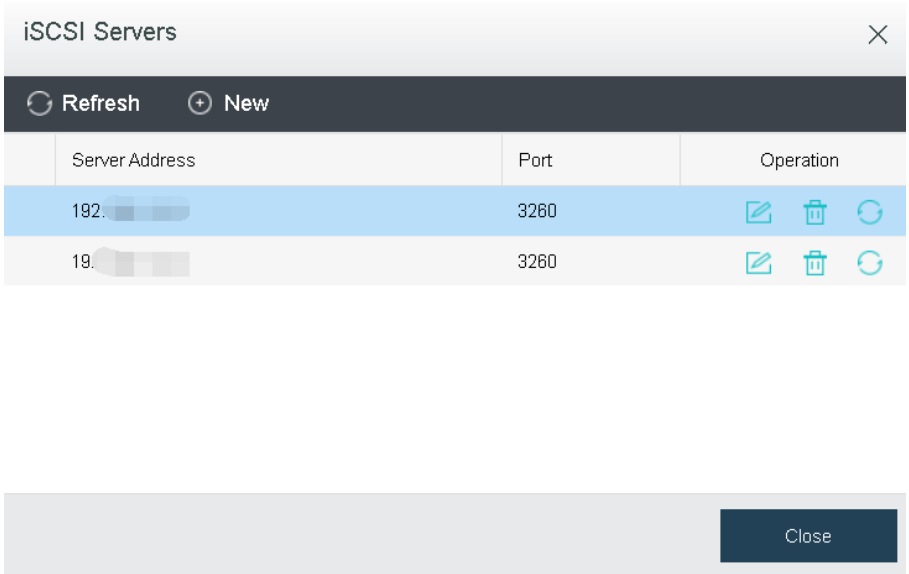
If any virtual machines is stored on the datastore, you can select the option **Recover existing virtual machines on this datastore as well** to recover existing virtual machines.

Then, click **OK** to save settings or click **Cancel** to give up the changes.

If the new disk being added has not been formatted, you will be prompted to format it when adding it into local storage. Note that formatted data cannot be restored any more.

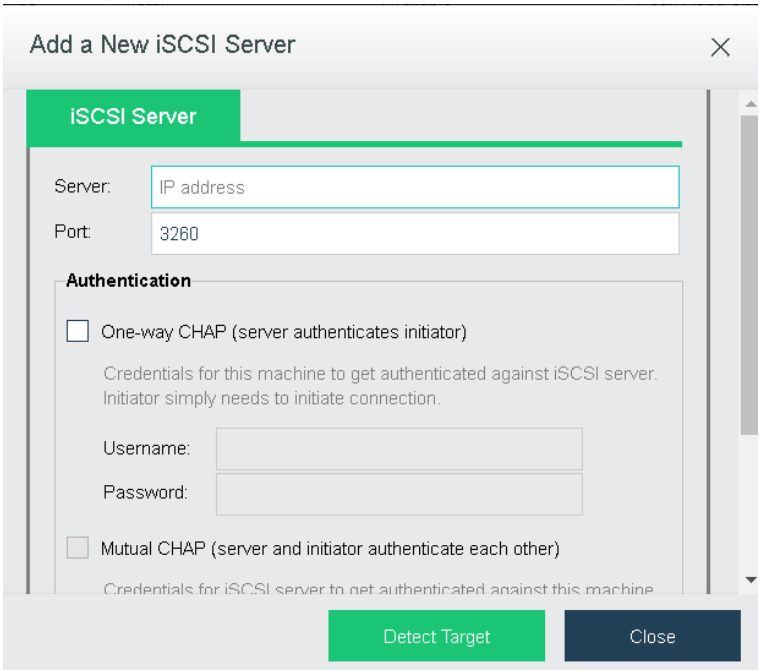
2.4.7.2 Configuring iSCSI Server

You need to configure **iSCSI Servers** in **Storage** > **Other Datastore > ISCSI server** before adding iSCSI type of datastore. Then, click **New**. iSCSI disks will be automatically discovered when iSCSI server settings are saved.



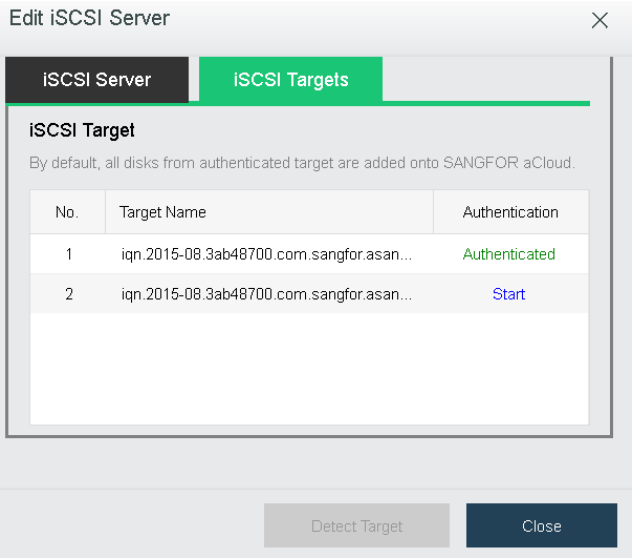
On the **Add New iSCSI Server** page, you need to specify IP address and port of iSCSI server.

If iSCSI server needs to authenticate initiator, you need to select **One-way CHAP,** and specify the corresponding **Username** and **Password**. iSCSI uses CHAP authentication, including one-way CHAP and mutual-way CHAP authentication, which depends on authentication settings on iSCSI server.



After username and password are specified, click **Detect Target**. On the **iSCSI Targets** tab, click **Start** to start authentication.

In some environment, iSCSI server may require each iSCSI disk to perform different authentication. In this case, you need to provide the corresponding credentials after clicking **Start**.



CHAP authentication method configured for iSCSI target should be the same as iSCSI server, **One-way CHAP** or **Mutual-way CHAP**.

After saving authentication information on **Target Authentication** page, you can view the authentication result on the following page. **Authenticated** indicates that authentication is successful.

Then iSCSI disks will be automatically discovered and listed on **Add Datastore** page so that you can add them to become a datastore.

2.5 Nodes

Navigate to **Nodes** and you will see the following page:

2.5.1 Managing Nodes

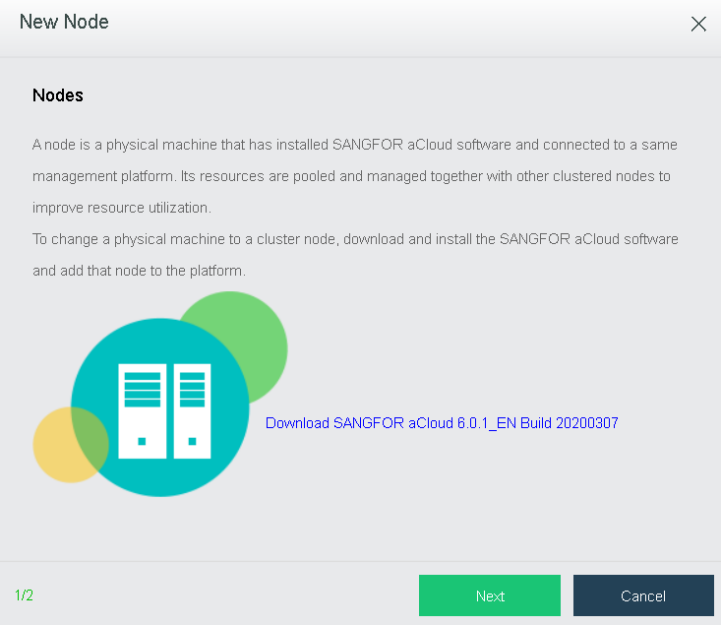
All nodes are listed on the **Nodes** page. You can view basic node information, such as node name, node IP address, CPU usage, Physical memory usage, and memory usage.

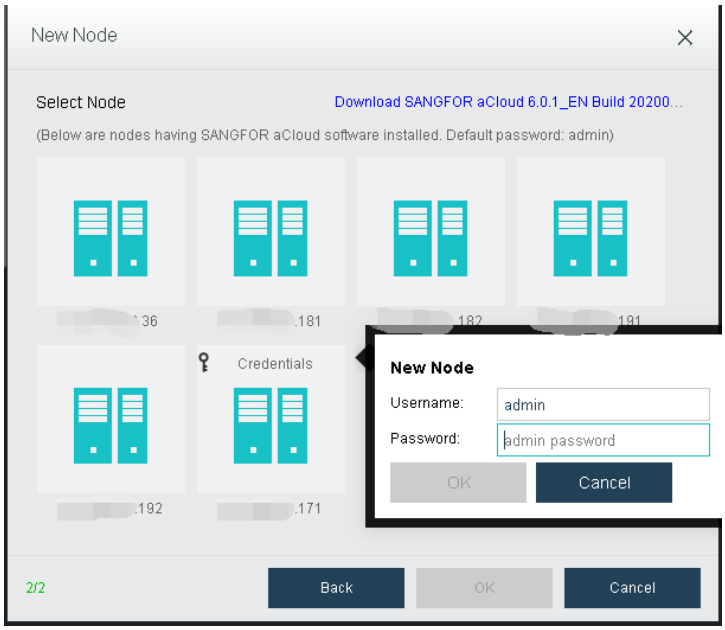
On the **Nodes** page, you can perform the following operations: **Refresh**, **Add Node, Sort** by **Name**, **CPU Usage**, and **Memory Usage**.

2.5.1.1 Adding Node

A node is a physical machine that has installed Sangfor HCI software and connected to Sangfor HCI platform. Its resources are pooled and managed together with other clustered nodes to improve resource utilization.

To add a node, click **Add New Node** to enter the following page. To change a physical machine to a node managed via Sangfor HCI platform, download and install the Sangfor HCI software and add that node to the Sangfor HCI platform. Then click **Next**.





IP Address: Specifies the IP address of the node which has installed Sangfor HCI software.

Username: Specifies administrator's username of that node.

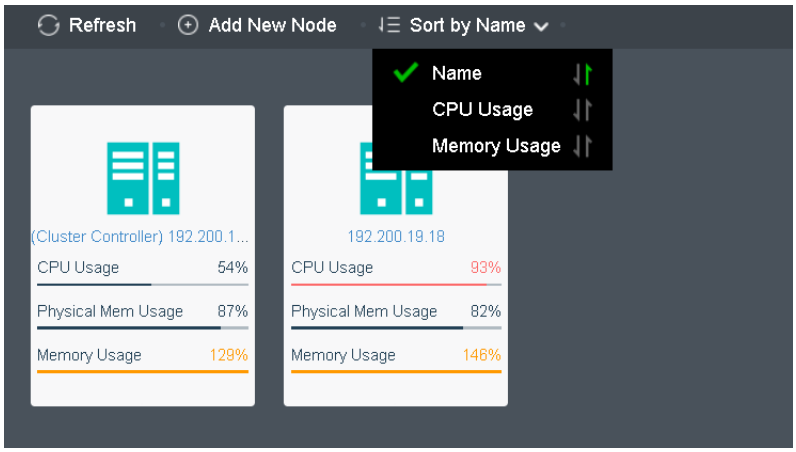
Password: Specifies administrator's password of that node.

Finally, click **OK**.

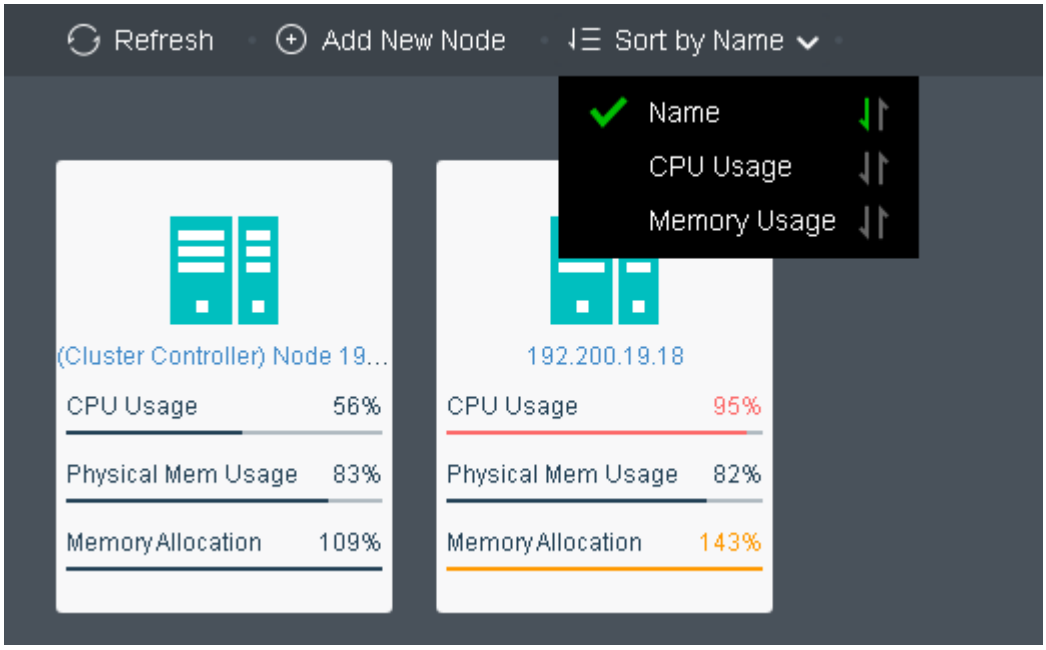
- A node can be added to one cluster only. If a node has been added to a cluster and you want to add it to another cluster, it must be removed from that cluster first.
- Versions of Sangfor HCI software installed on the nodes to be added to a same cluster must be consistent.
- Management interface IP addresses of the nodes to be added to a same cluster must reside on a same network segment.
- On the **New Node** page, it lists the automatically-discovered nodes which reside on a same subnet but have not been added to the cluster.
- You may add a new node by clicking the 〖+〗 icon and then input the its IP address, username and password.
- If a node with default password admin is selected, there is no need to specify password again.
- If a node whose password is not admin is selected, you need to specify its password.

2.5.1.2 Sorting Nodes

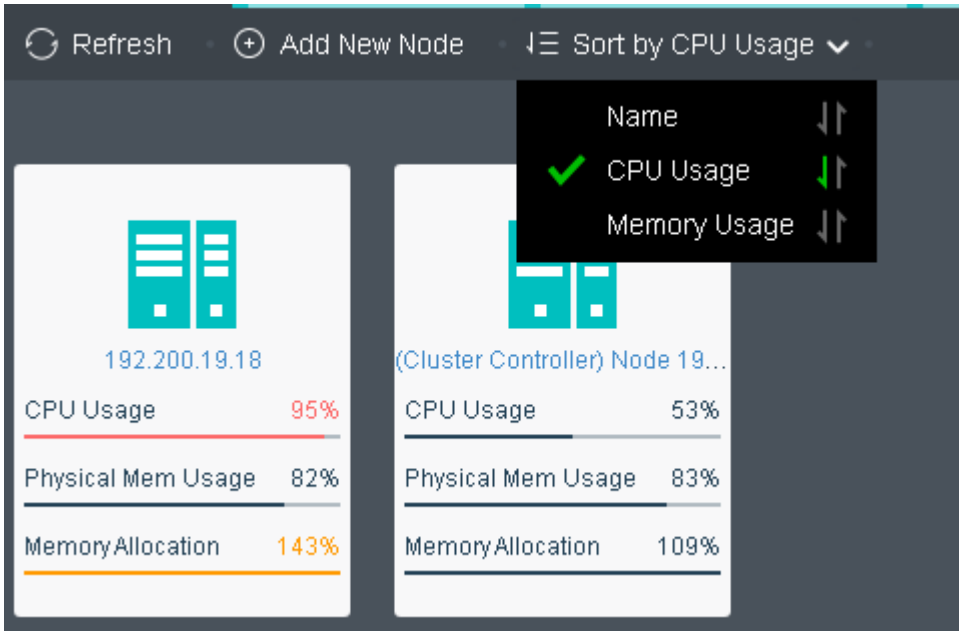
Nodes can be sorted by name, CPU usage, or memory usage.



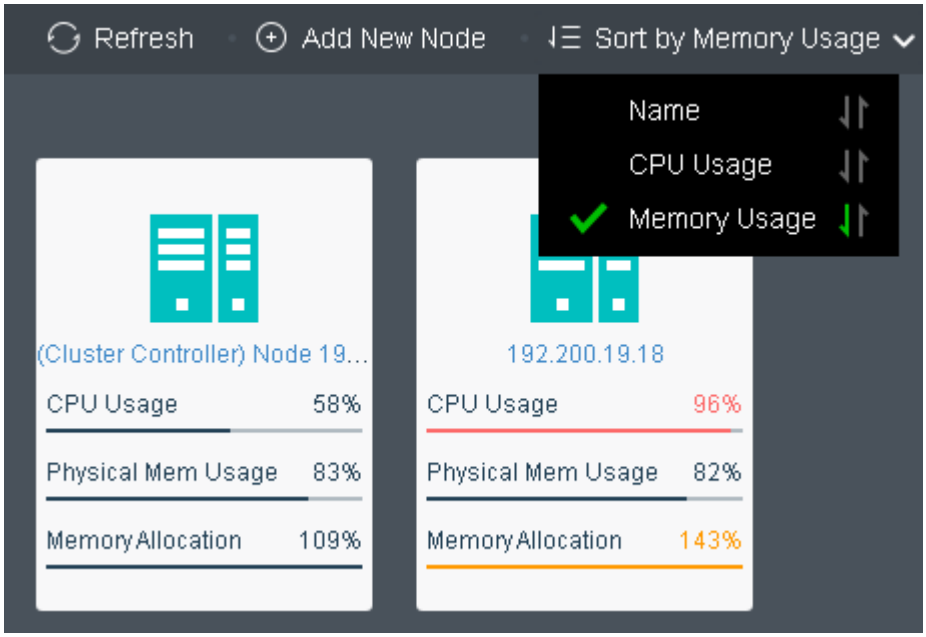
To sort nodes by name, select **Sort by Name**. Additionally, by clicking on the arrow, nodes can be sorted in ascending order or descending order.



To sort virtual machines by CPU usage, select **Sort > CPU Usage** inNodes. By clicking on that arrow, virtual machines can be sorted based on CPU usage in ascending order or descending order. The following figure shows that the virtual machines are sorted by CPU usage in a descending order.

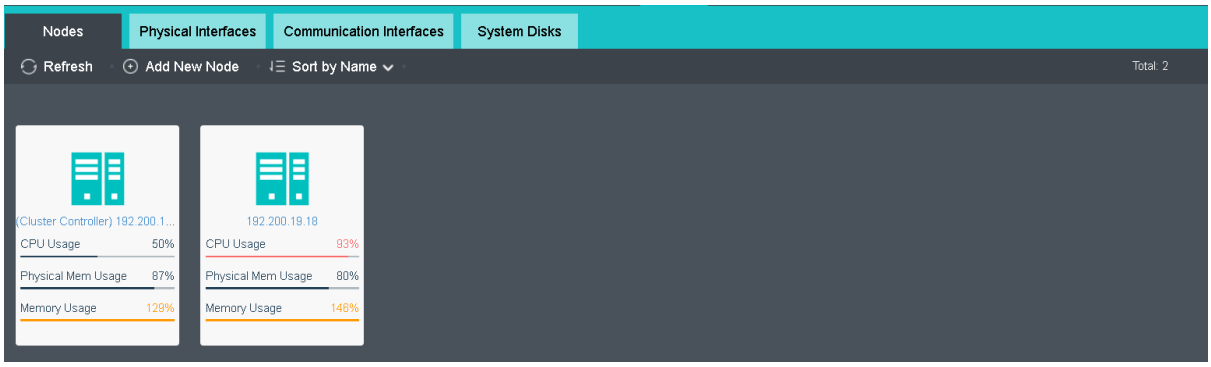


To sort nodes by memory usage, select **Sort > Memory Usage**. By clicking on that arrow, node can be sorted by memory usage in ascending order or descending order. The following figure shows that the virtual machines are sorted by memory usage in a descending order.



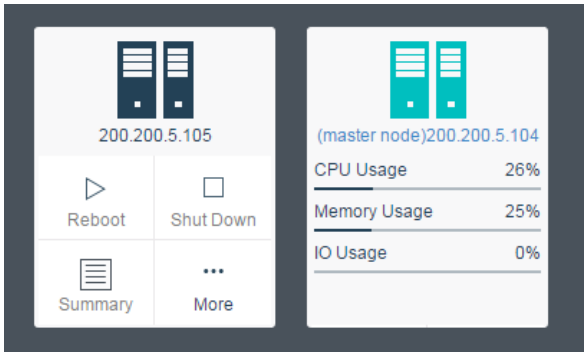
2.5.2 Viewing Node Status

The **Nodes** page is shown below:

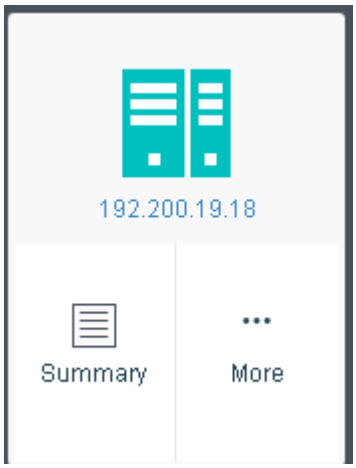


On the upper-right corner of the **Nodes** page, you may see the total number of nodes.

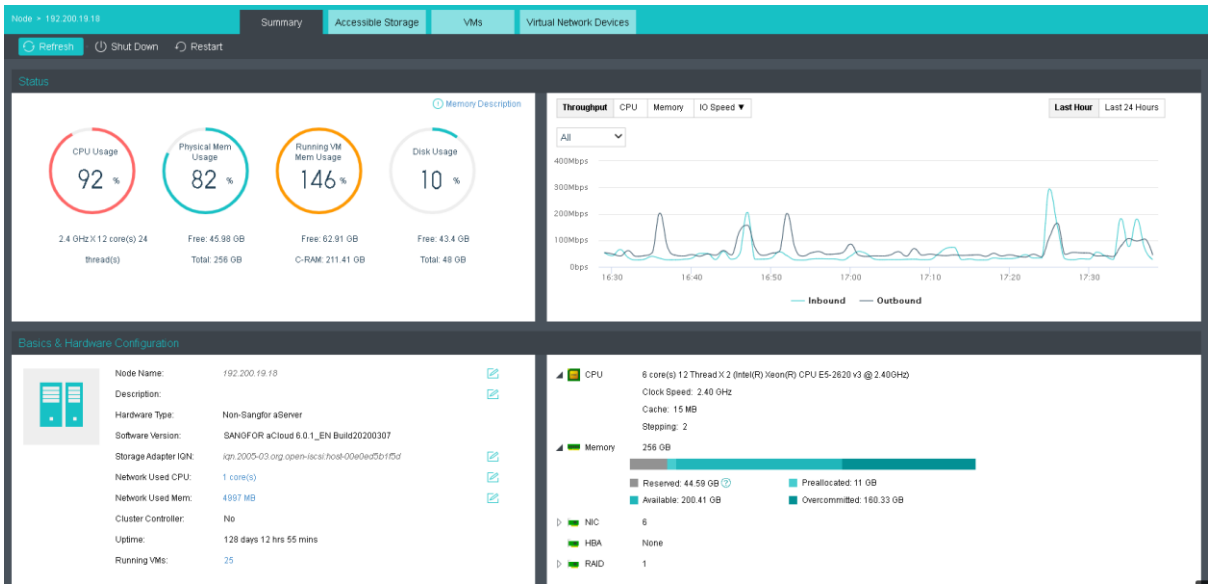
The color of node panel indicates node status. Grey indicates the node is powered off, while blue indicates the node is powered on and red indicates the node is giving alarm. Additionally, there are more information on the node panel, such as CPU usage, memory usage and IO usage, etc.

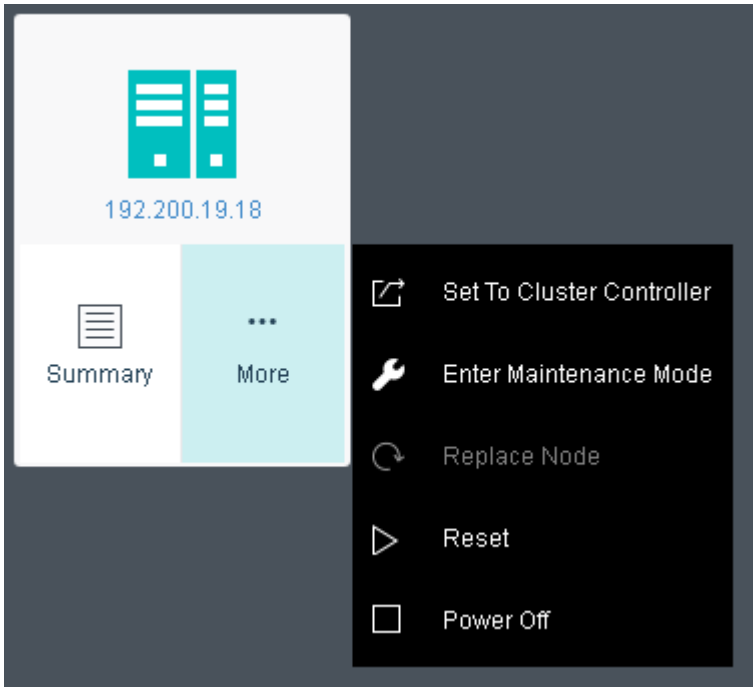


Move your cursor on the node panel and you will see the following buttons: **Summary** and **More,** as shown below:



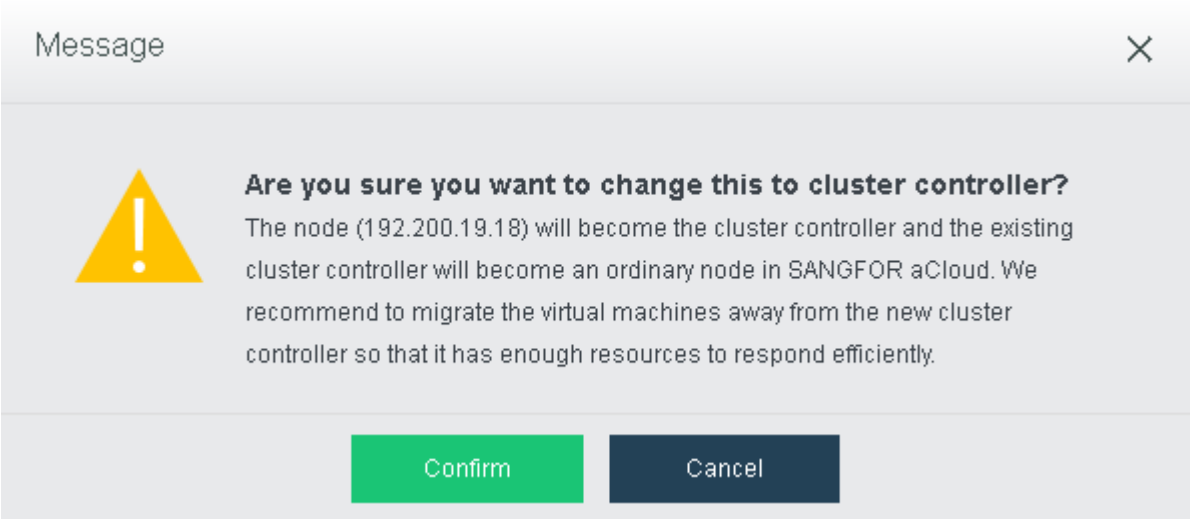
To enter node summary page, you may click on node name or **Nodes** > **Summary**.



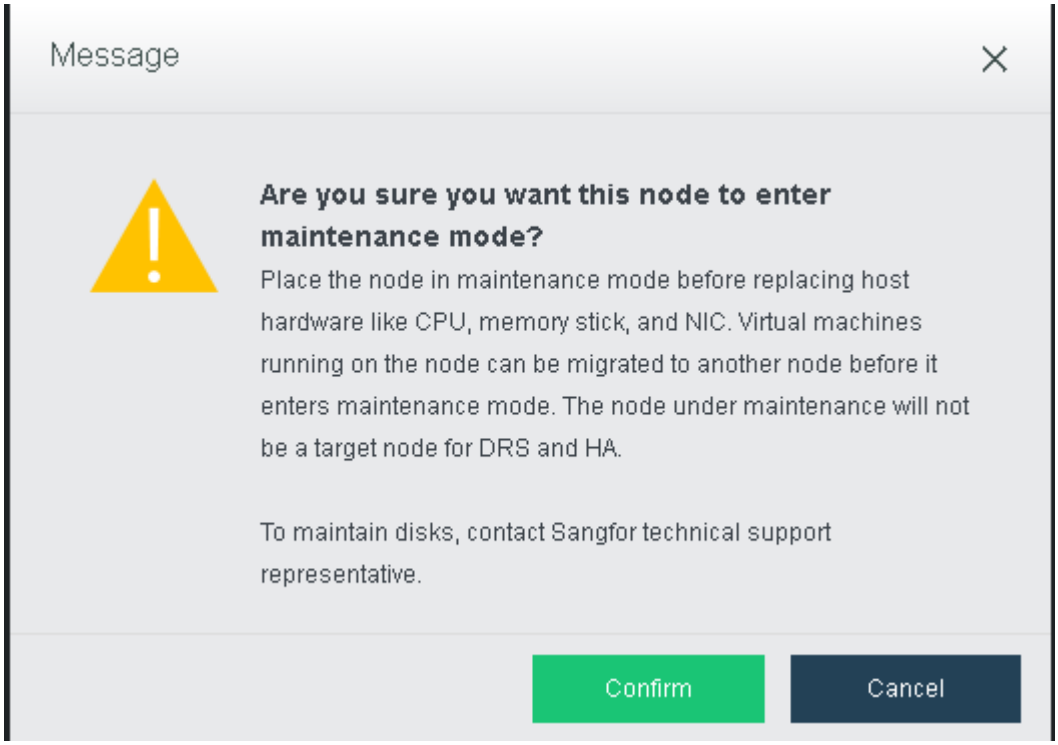


There are few more options under More which are:

a. **Set To Cluster Controller**: Set the selected node as the cluster controller node. This option is only available for non-controller node.

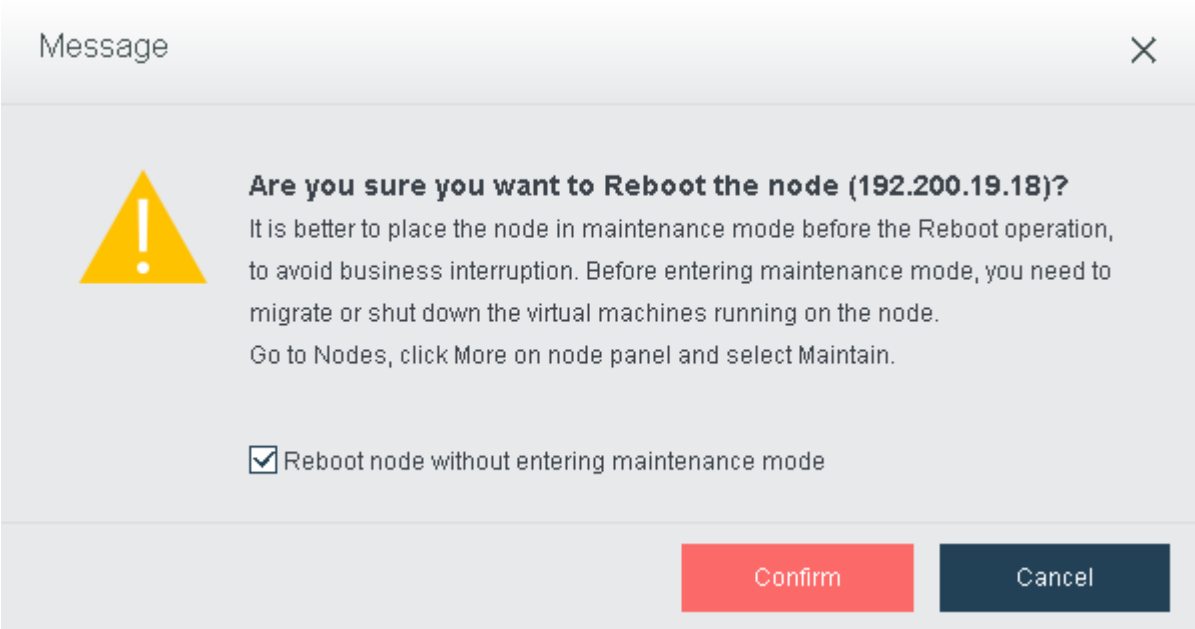


b. **Enter Maintenance Mode**: Enable to allow the selected node to enter the maintenance node for hardware maintenance such as memory replacement.



c. **Replace Node**: Allow to replace node when the node facing failure. Only available when the nodes is offline.

d. **Reset**: Reboot the selectd node.

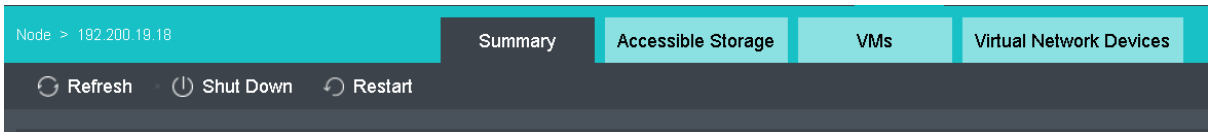


e. **Power off**: Power off the node.

Notes: Besides, A clustered node can be removed from cluster by clicking **Delete** if its disk is not added to virtual storage.

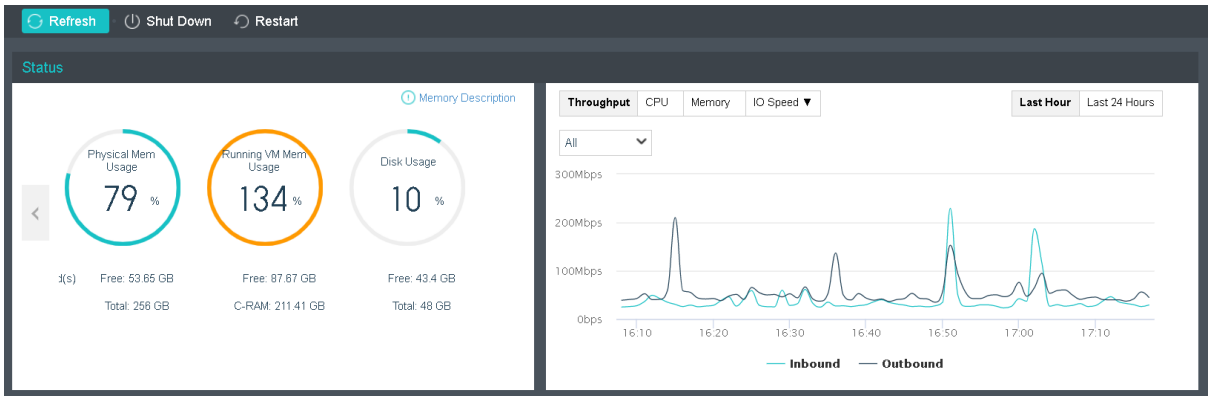
2.5.3 Viewing Node Details

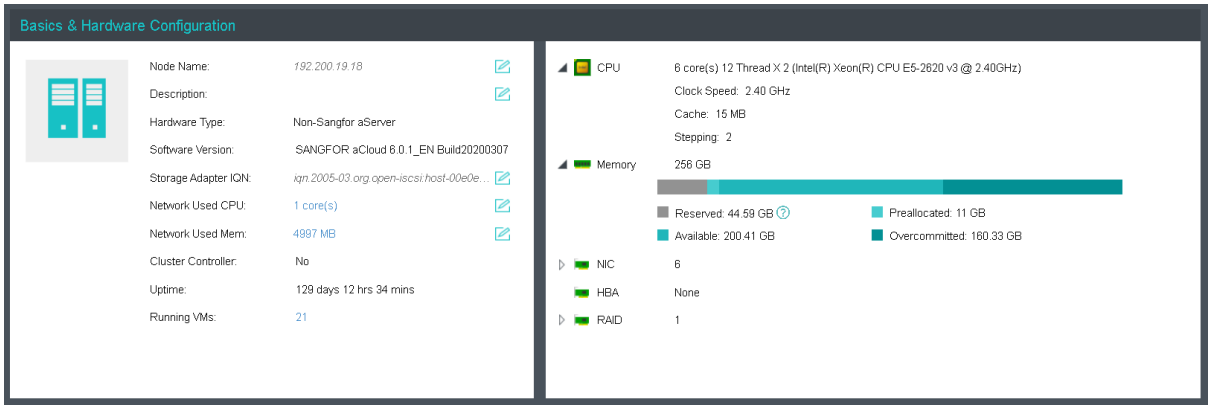
There are the following parts: **Summary, Accessible Storage, Virtual Machine, Virtual Network Devices** as shown below:



2.5.3.1 Node Summary

On the **Summary** page, you may view node status, basics and hardware configurations.





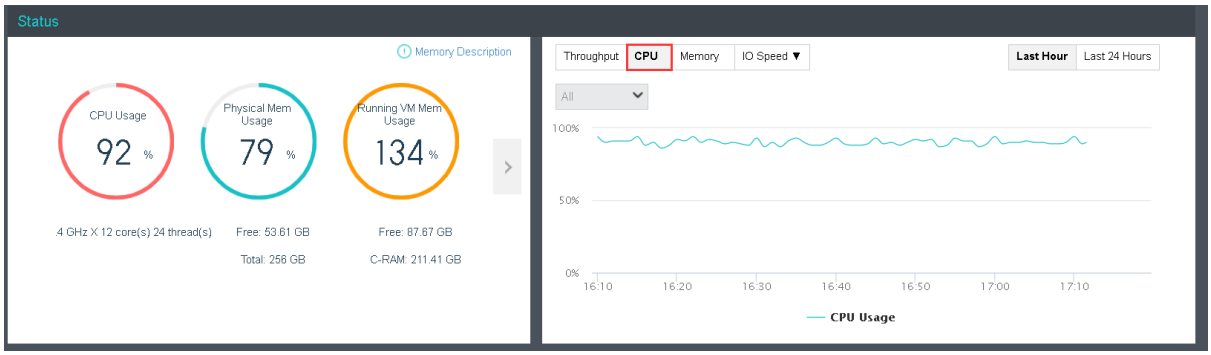
To power off node, click **Shut Down**.

To reset node, click **Restart**.

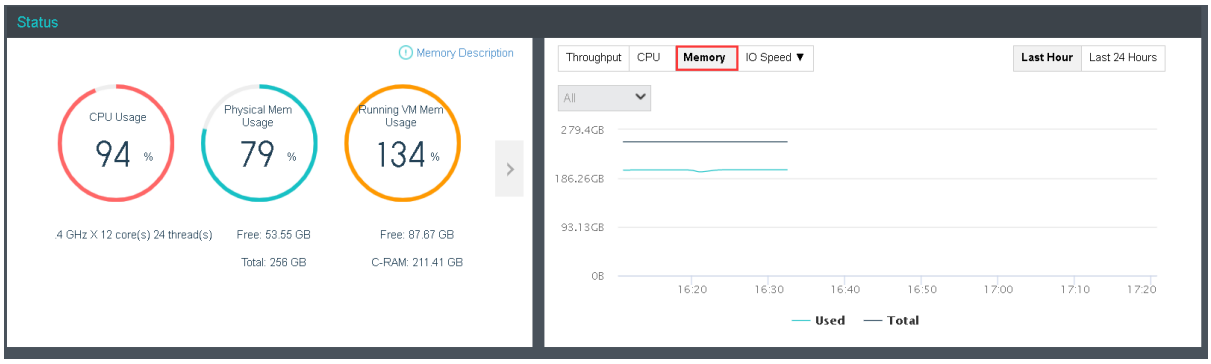
Status: This section displays CPU usage, memory usage, disk usage, throughput, CPU usage trend, memory usage trend, IO speed, etc.

CPU Usage: Displays CPU usage of node. On the right side, you can view CPU usage in

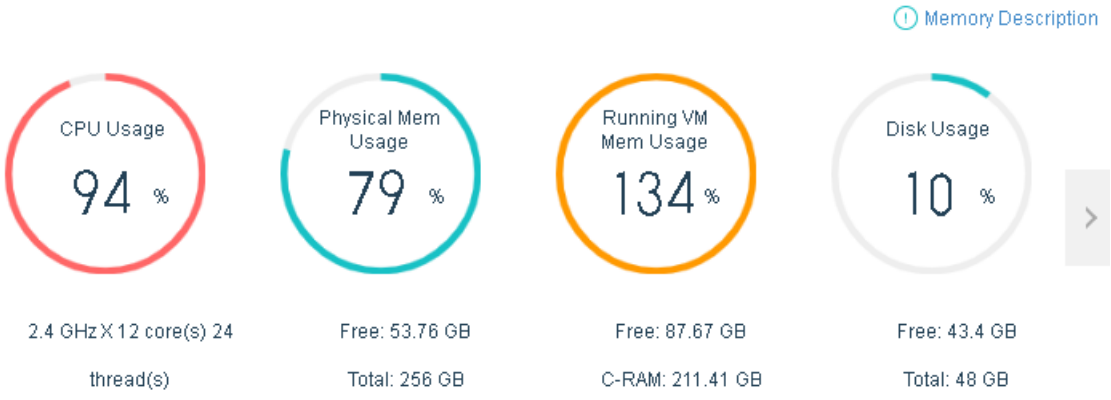
the last hour or 24 hours.



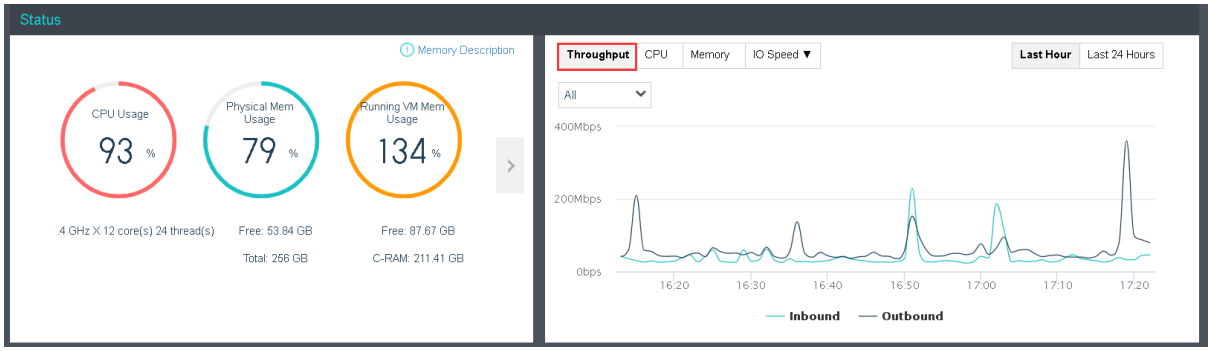
Memory Usage: Displays the total and free memory size respectively, as well as memory usage. On the right side, you can view memory usage in the last hour or 24 hours.



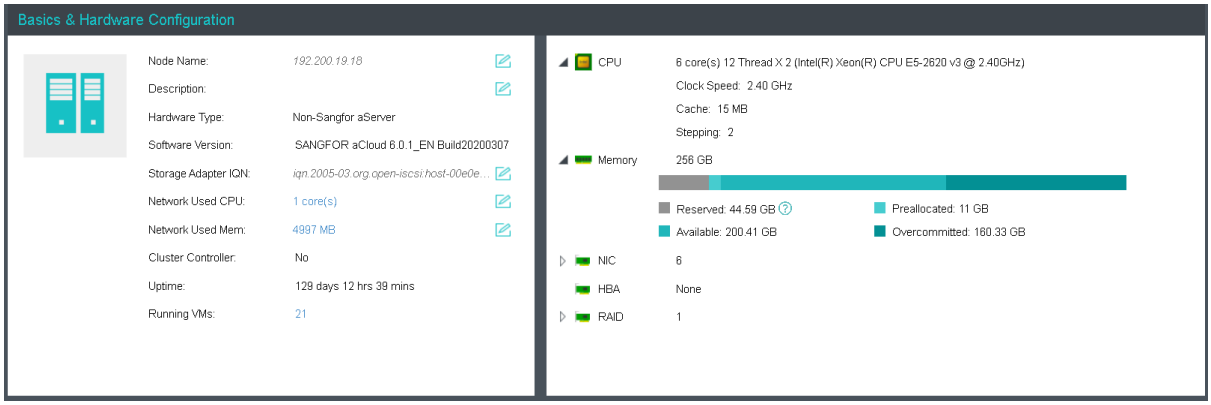
Disk Usage: Displays the total and free disk size respectively, as well as disk usage.



Throughput: Displays the trending of node throughput.

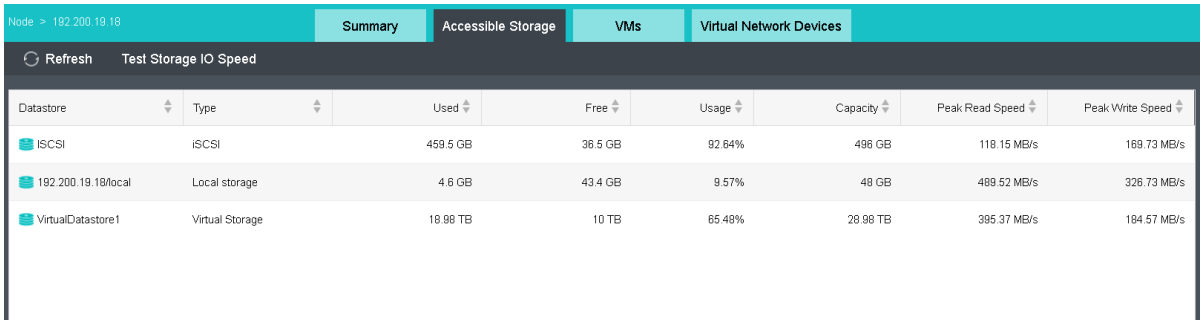


Basics & Hardware Configuration: This section displays basic information and hardware configuration of node. Basic information includes **Node Name, Description, Software Version, Storage Adapter IQN, Network Used CPU, Network Used Mem, Cluster Controller, Uptime, Running VMs**. Hardware configuration is listed on the right side. (**Node Name, Description, Storage Adapter IQN, Network Used CPU** and **Network Used Mem** are editable).

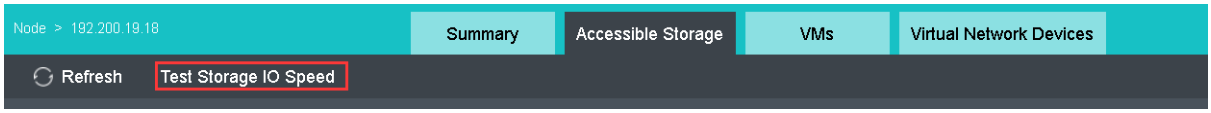


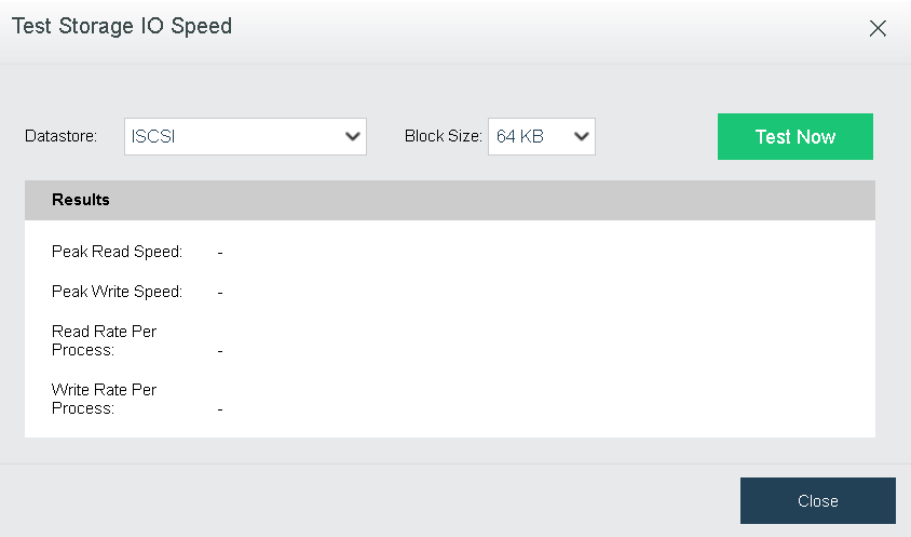
2.5.3.2 Viewing Accessible Storage

On the **Accessible Storage** page, you may view the information of datastores that the node has access to. If a datastore is online, you may see its detailed information, such as **Used, Free, Total Capacity**, ect. If that datastore is offline, **Used, Free** and **Total Capacity** will be zero.



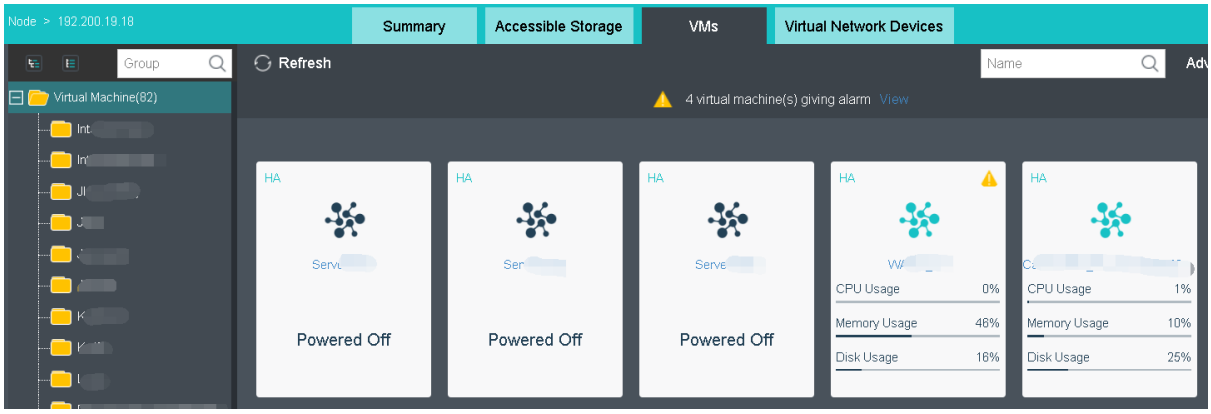
Test Storage IO Speed: It is used to test the peak write and read IO speed.



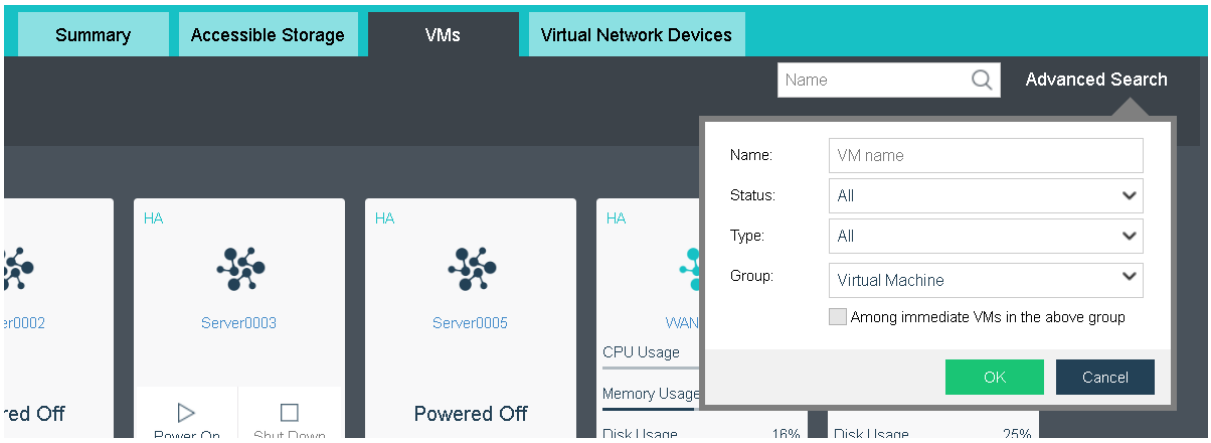


2.5.3.3 Viewing VMs

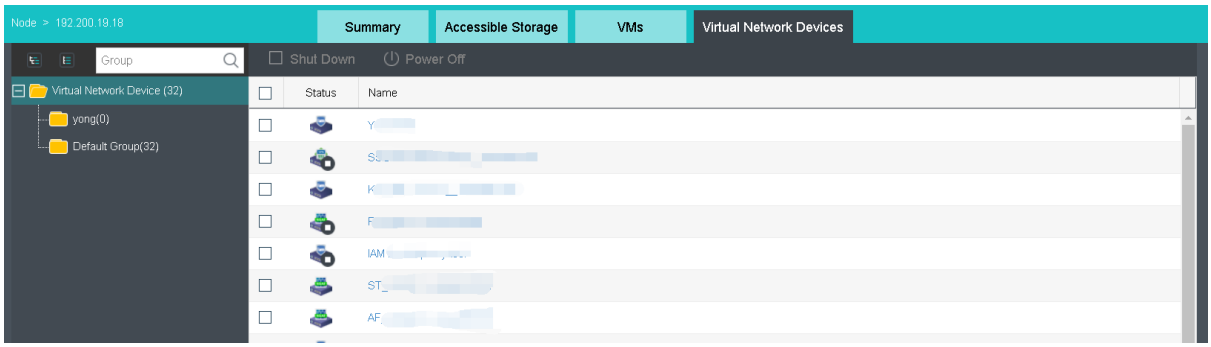
On the **VMs** page, you may view the virtual machines running on the node. Those virtual machines are displayed by group(Virtual machines not running on that node will not be displayed).



Fuzzy match is supported. You may search for virtual machine by VM name or click **Advanced Search** to search for virtual machine by VM status, type and group.



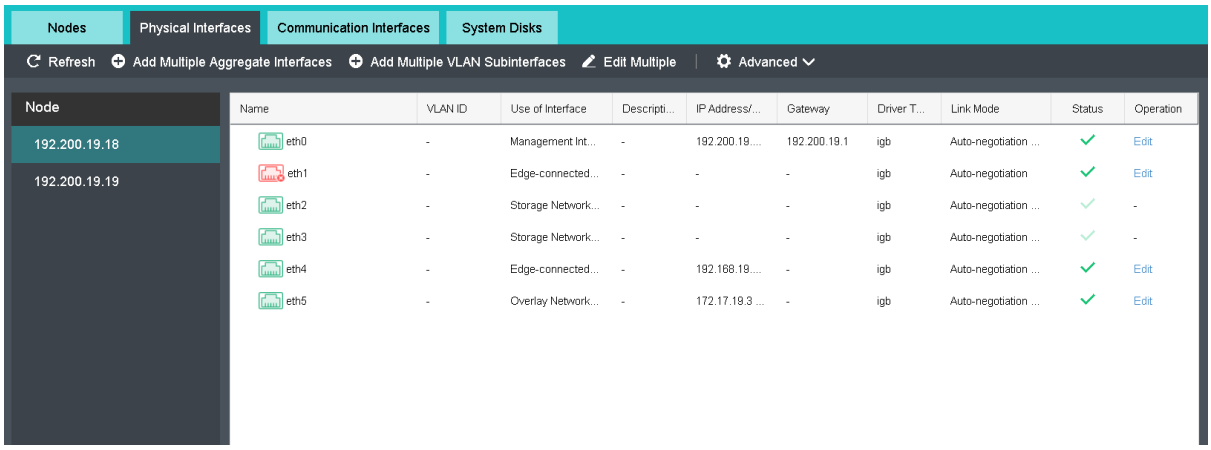
On the Virtual Network Devices page, You may view the network device which running on the nodes. Those network devices are displayed by group(Network devices not running on that node will not be displayed).



2.5.4 Physical Interface

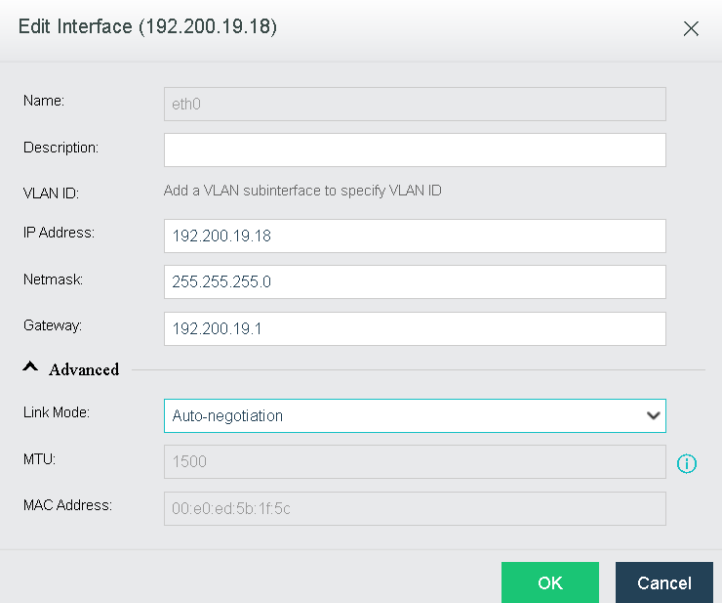
You may view the following information of physical interfaces on the **Physical Interface** tab: **Network, VLAN ID, Use of interface, IP address, Gateway, Driver, Link Mode, Status,**

and Operation.



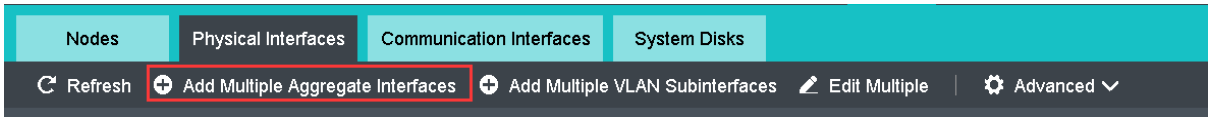
To edit interface, click **Edit** in **Operation** column to enter the **Edit Interface** page.

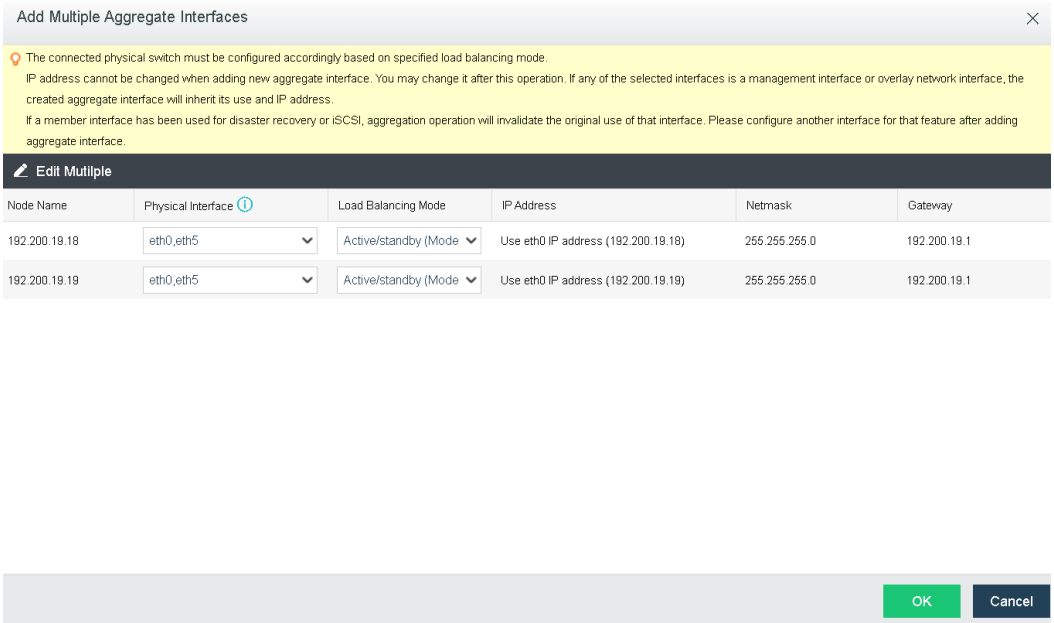
On the following page, you can modify interface settings exclusive of **Name** and **MAC address**.



2.5.4.1 Adding Aggregate Interface

Aggregate interface helps to improve performance of data communication, and supports data redundancy based on IP address and MAC address. When one of the interfaces is not available, data will be transmitted via other interfaces so that service continuity is ensured.



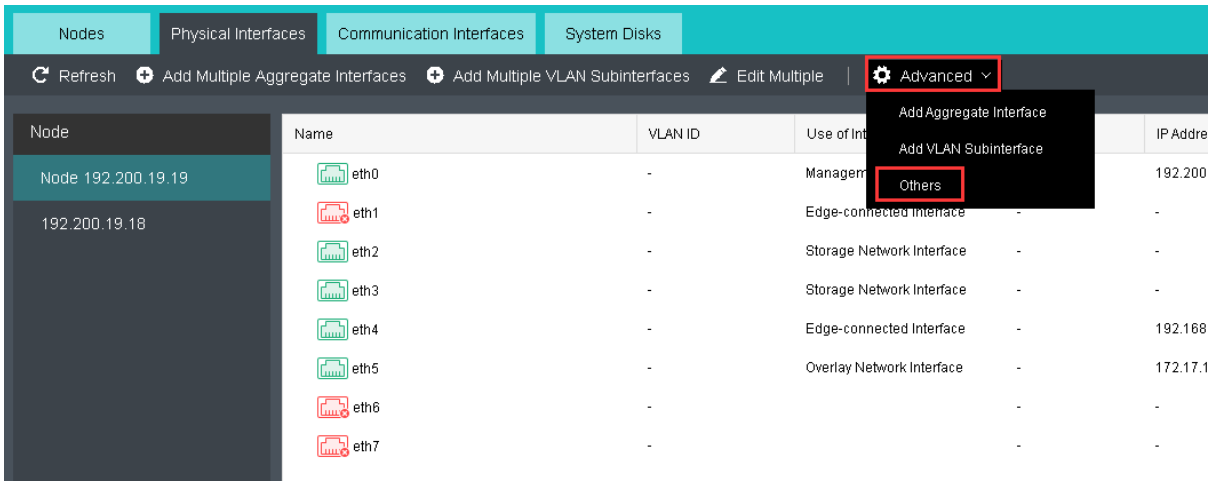


Aggregate interface must be configured on connected physical switch accordingly, otherwise network may be disconnected.

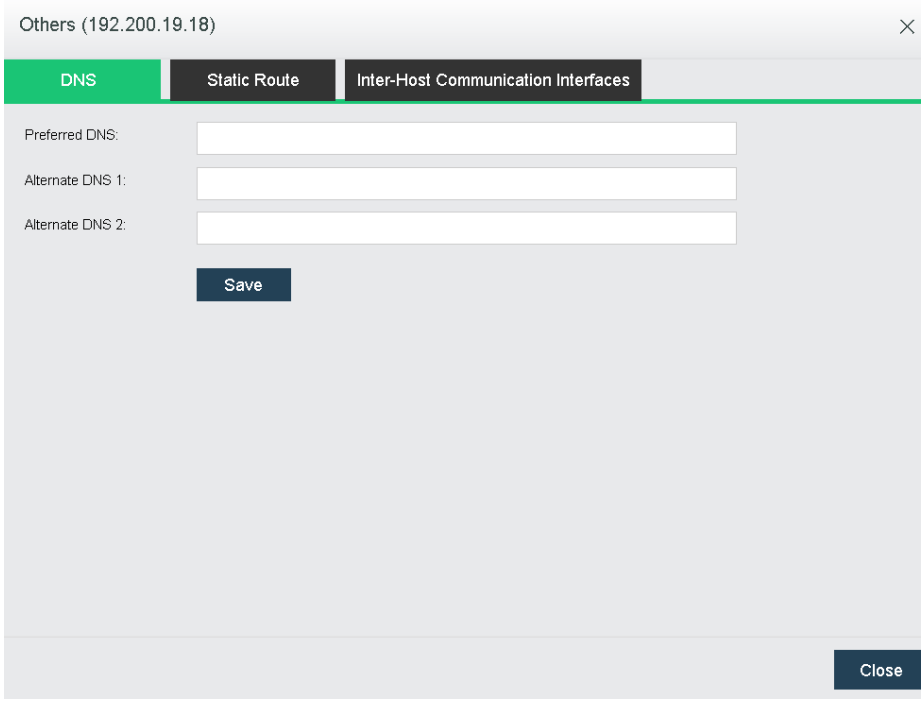
Previous connections on member interfaces must be set up again via aggregate interface, since they are dropped because assigned IP addresses are removed.

2.5.4.2 Configuring Advanced Settings

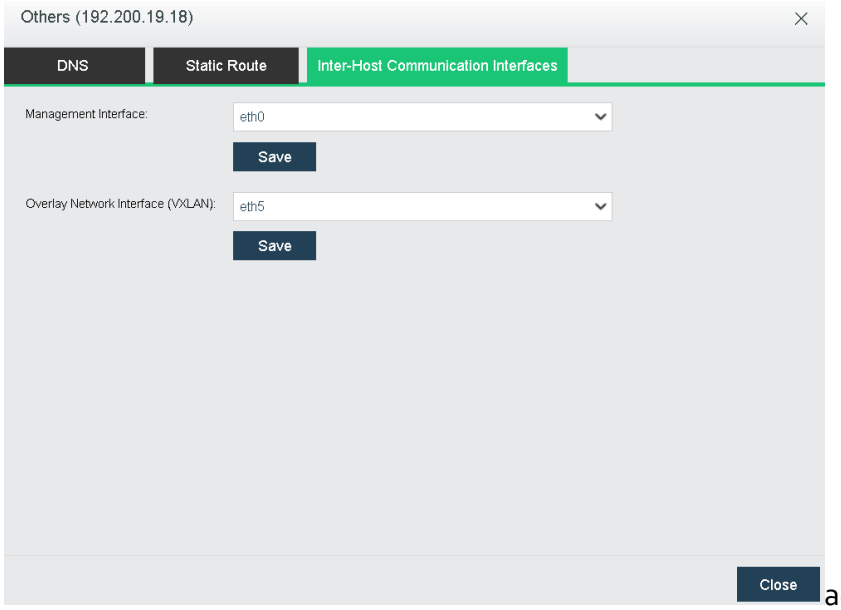
On the **Physical interface** page, you may configure **DNS Server, Static Route,Inter-Host Communication Interfaces** by clicking **Advanced > Other,** as shown on the following page.



DNS Server: It is required when node needs to connect to the Internet to resolve domain name. For instance, DNS server should be configured when the node accesses NFS server through its domain name, synchronizes time, or sends alert email. Up to 3 DNS servers can be configured.



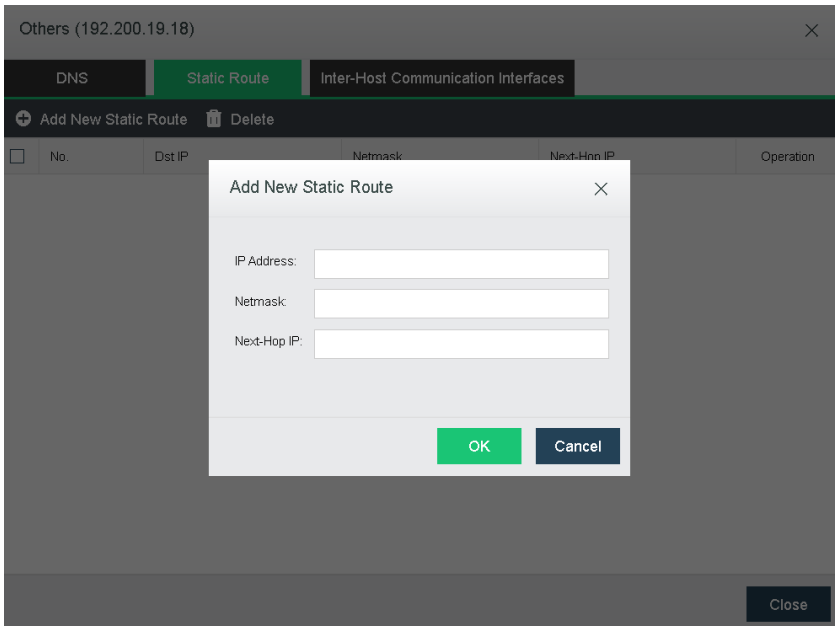
Inter-Host Communication Interface: It includes management interface which is used to manage nodes, and overlay network interface(VXLAN). Overlay network interface is a physical interface used for communication among virtual machines. If there are more than one physical interfaces on host, you need to specify one interface for host communication. IP



addresses of communication interfaces should be on a same network segment.

2.5.4.3 Adding Static Route

To add a static route for node, click **Static Routes** to enter the following page and specify the following fields: **Destination IP**, **Netmask** and **Next-Hop IP**.



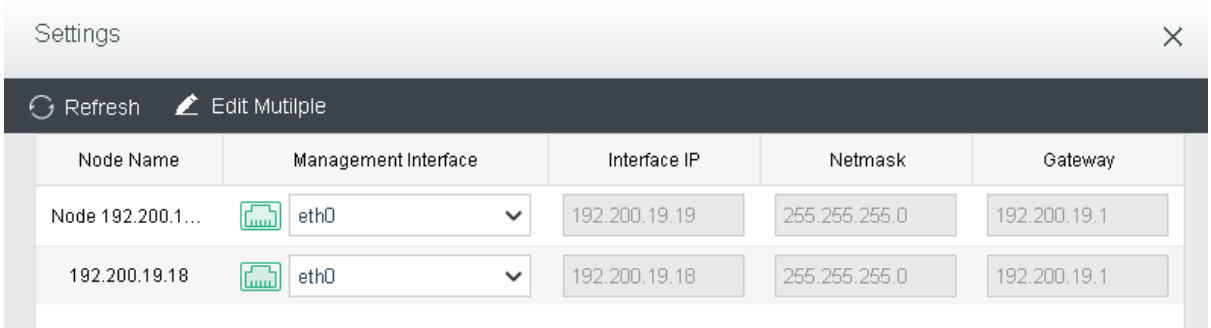
2.5.5 Communication Interface

Under communication interface, you can view or change the configuration for each type of interfaces. Starting from version 6.0.0, flow control function has been added to control the traffic flow for the reused interfaces.

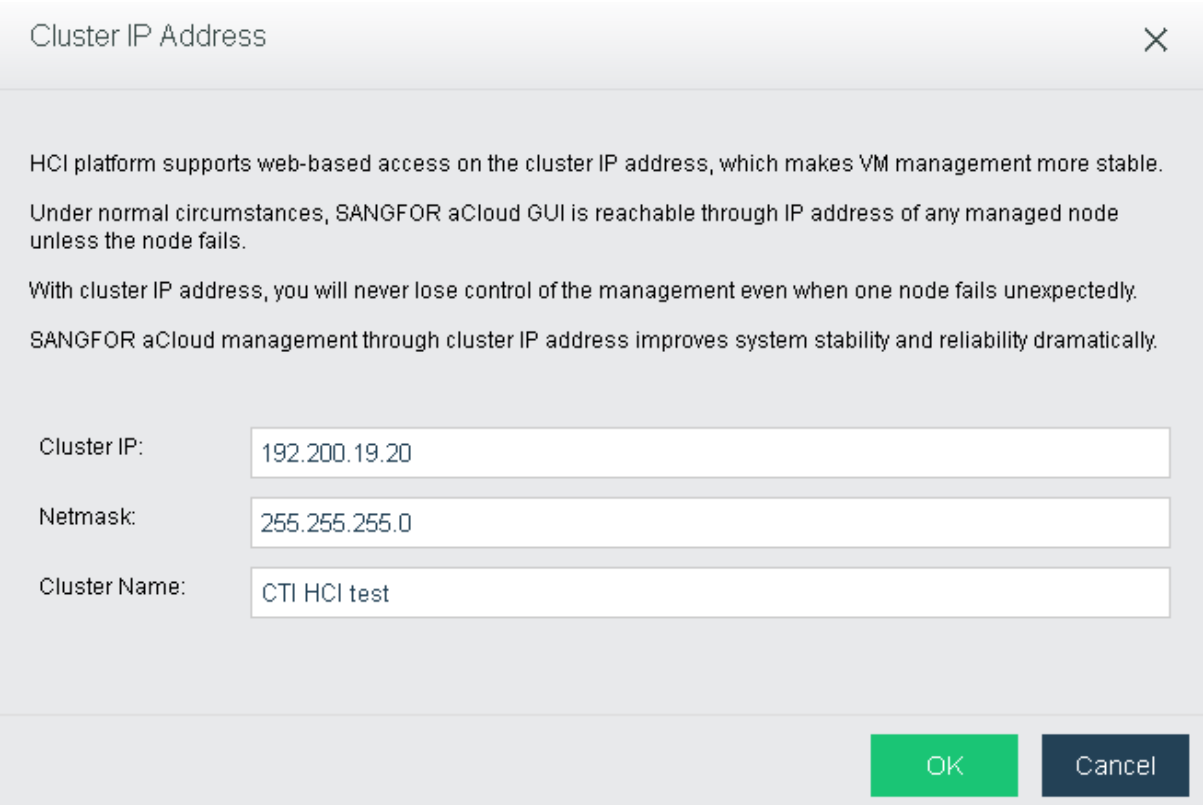
2.5.5.1 Management Interface

Management interface in HCI will be used for several function such as managing the HCI, migrations, connecting external storage, template update, backup and more.

Settings: Allow to select specified physical interface as management interface with the IP address, netmask and gateway configuration.

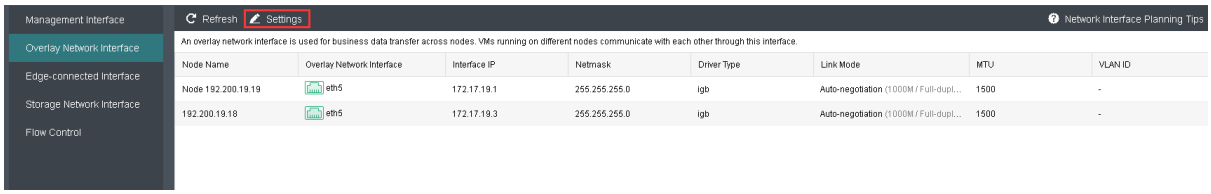


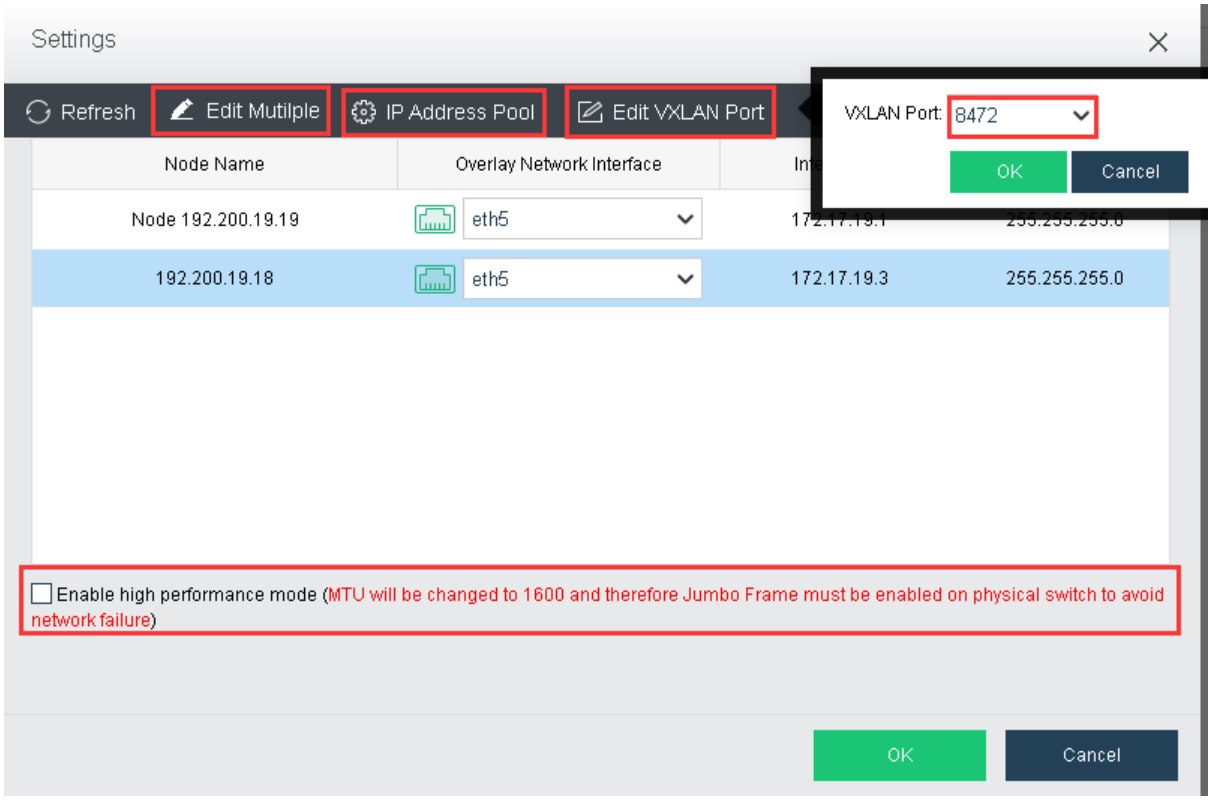
Cluster IP Address: Allow to change cluster settings which included cluster ip, netmask and Cluster name.



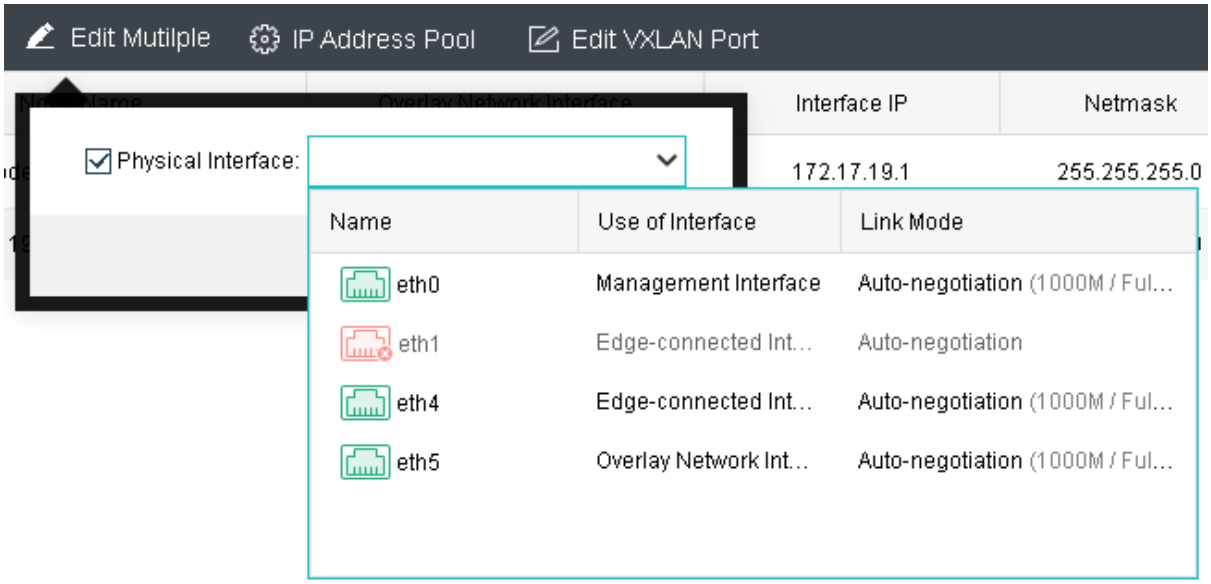
2.5.5.2 Overlay Network Interface

Overlay network interface will be used for inter-nodes communication for the virtual devices and virtual machines.

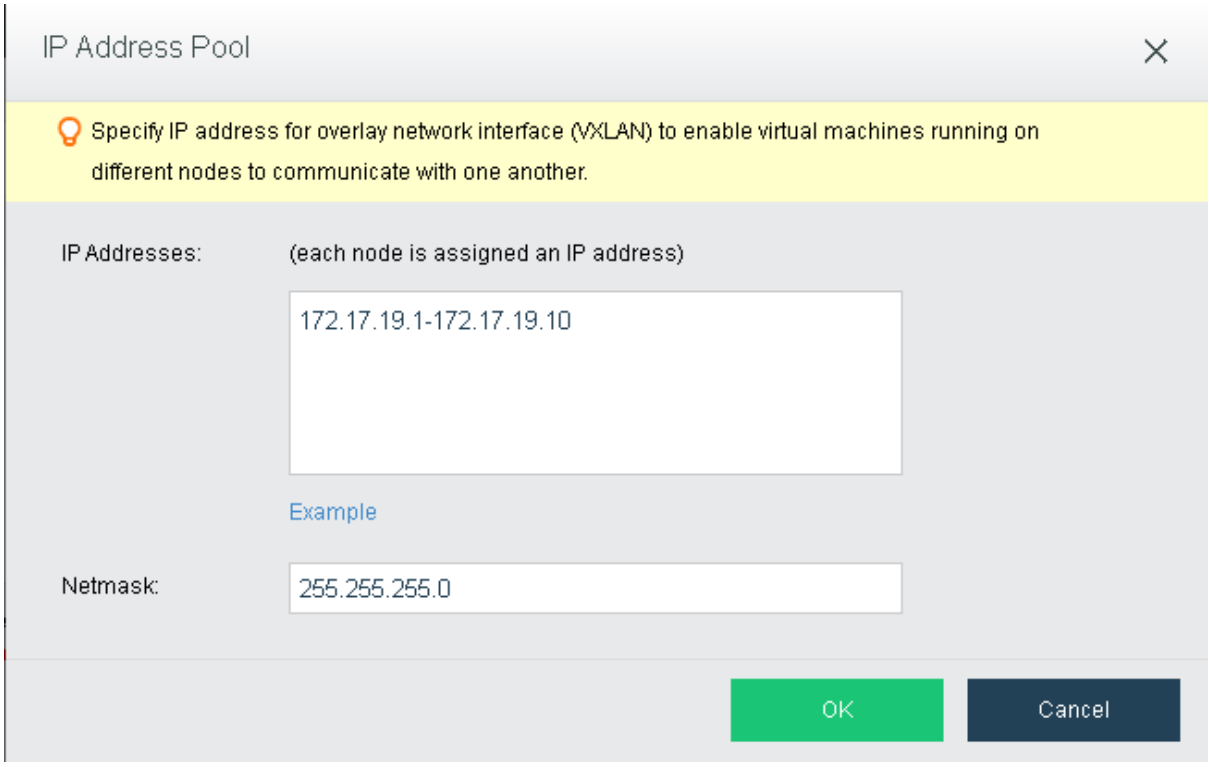




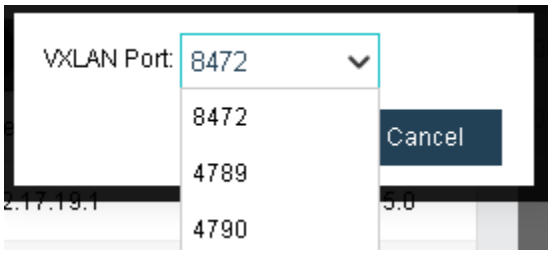
Edit Multiple: Allow to edit the physical interfaces for all nodes.



IP Address Pool: Configure the IP Pool for the overlay network.



Edit VXLAN Port: Change the VXLAN port. By default it will be 8472.

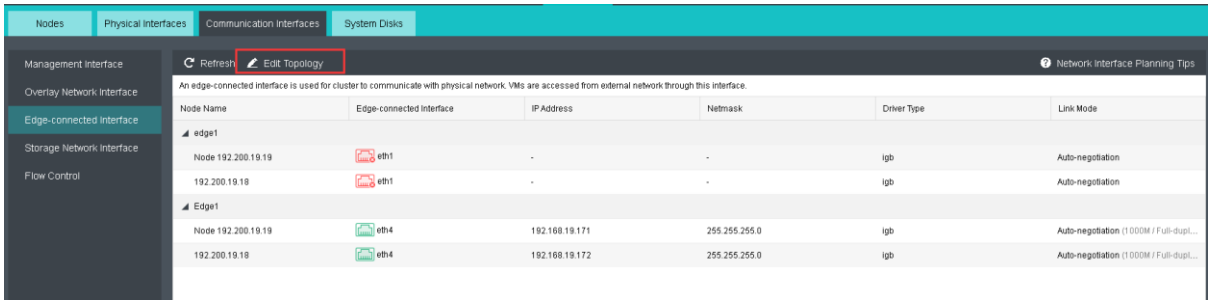


Overlay Network interface: Change the physical interface for overlay network on corresponding nodes.

Enable high performance mode: MTU will be changed to 1600 to improve performance for overlay network. Connected switch are required to enabled Jumbo Frame if this option has been enabled.

2.5.5.3 Edge-connected interface

Edge-connected interface is the interface which forward the traffic from virtual machines and virtual devices to the connected physical switch.

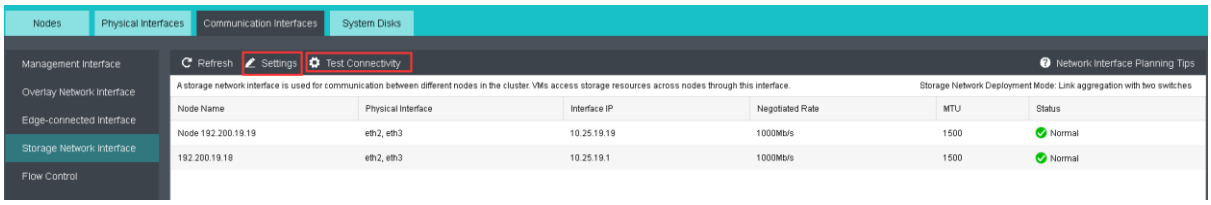


Edit Topology : It will redirect to the **Network** tab where you can edit the edge configuration.

2.5.5.4 Storage Network Interface

Storage network interface will be used to connect the SAN between 2 nodes. It will be used to sync the data and the storage resource across nodes will be access through this interface.

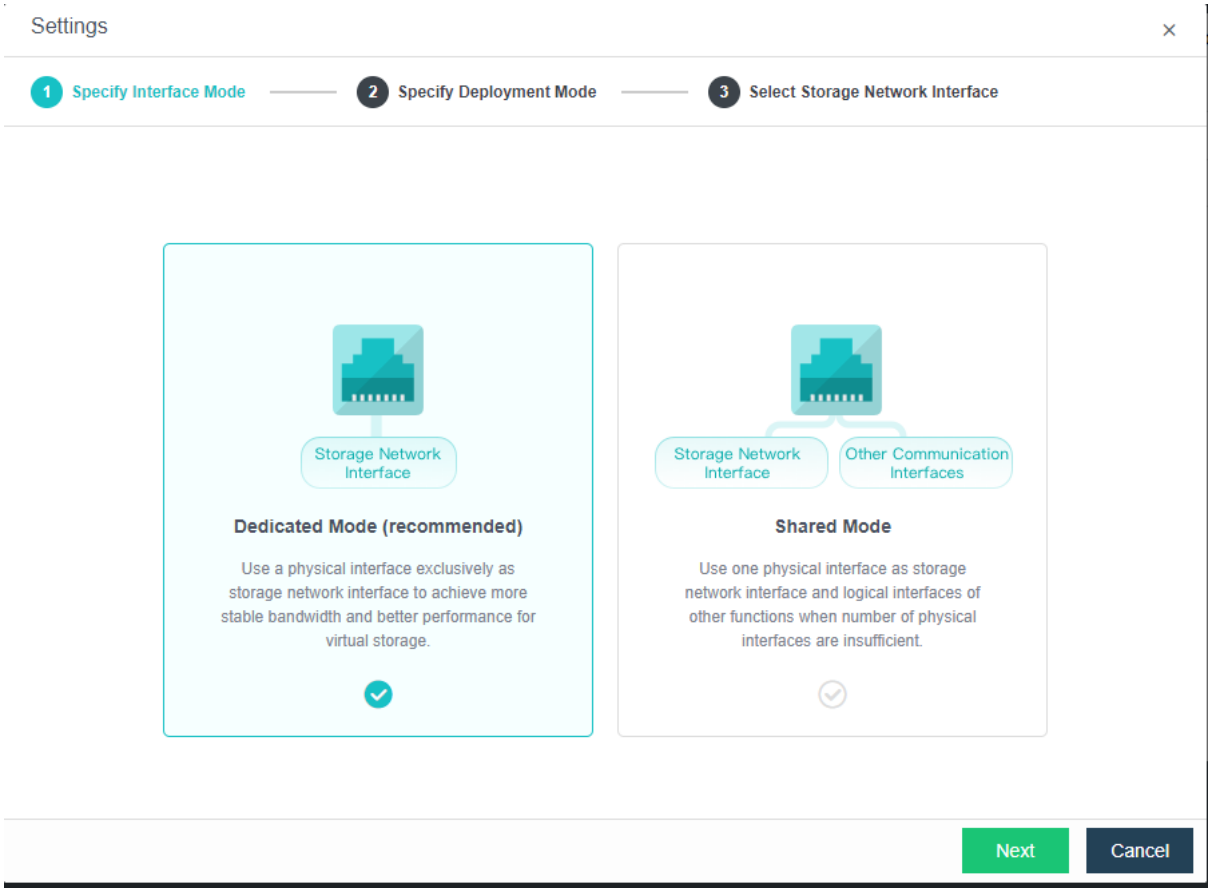
1. Navigate to **Nodes** > **Communication Interfaces** > **Storage Network Interface,** and select **Settings**.



2. Specify Interface Mode:
   a. Dedicated Mode : Use a separate physical NIC as storage network interface for better performance and stable bandwidth.
   b. Shared Mode : Use one physical interface as storage network interface and logical interfaces of other functions when number of physical interfaces are insufficient.

      Precautions:

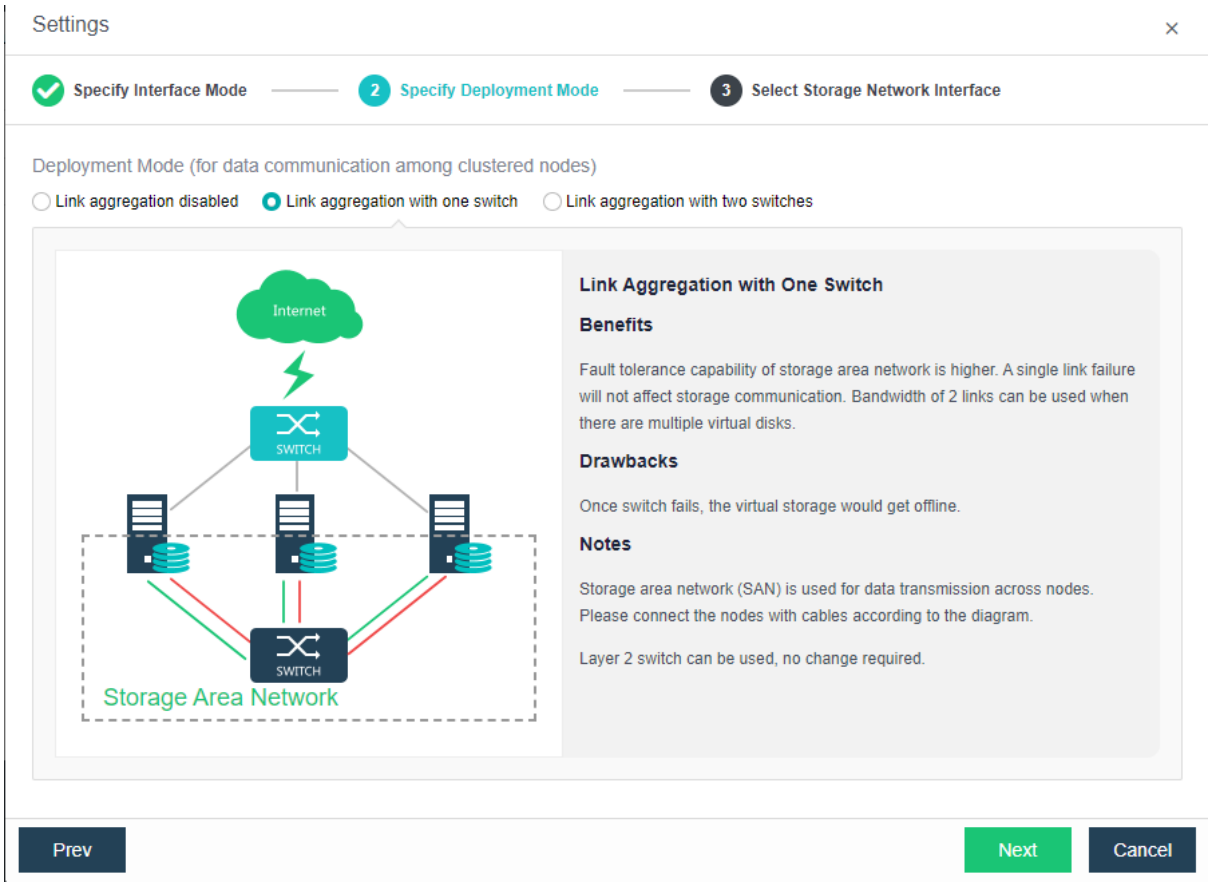
      1. It is required to use aggregate interface for Shared Mode and the member interface must be 10G.
      2. Currently only 2 types of NIC support Shared Mode storage network interface which are Mellanox CX4 and Intel X710.
      3. Changing interface mode required to power off all VM before the operation.



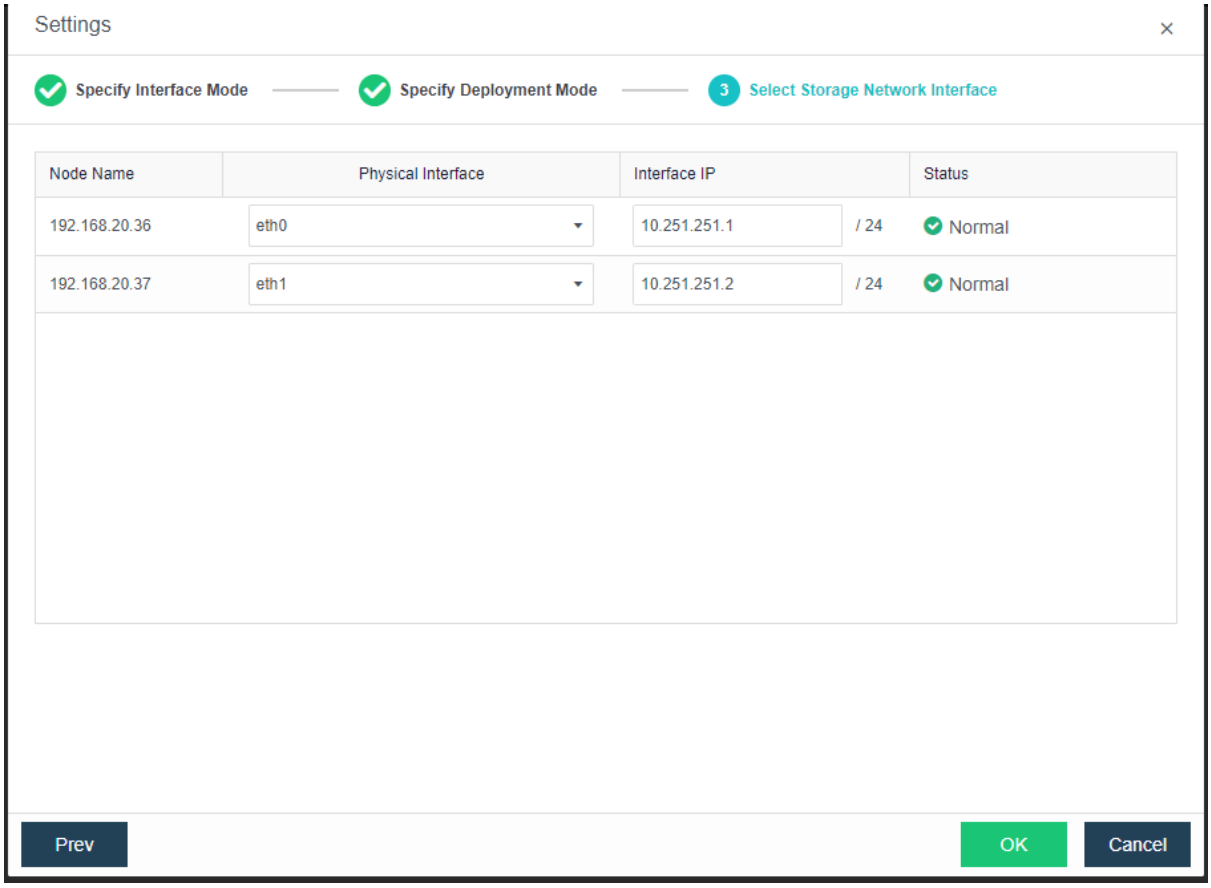
4. Specify Deployment Mode for the storage network interface.
   a. Link aggregation disabled
      - Select this option when only 1 physical NIC available for Storage Network Interface.
      - If there are only two nodes, simply use a cable to connect one another, without using any switch.
      - Drawbacks: Storage on the node will be inaccessible if one link fails.
   b. Link aggregation with one switch
      - Select this option when both physical NIC connected to one switch.
      - Select this option when connecting to a stack switch.
   c. Link aggregation with two switches
      - Select this option when the physical NICs connected to different switch.
      - If there are only two nodes, simply use a cable to connect one another, without using any switch.

Notes: Changing deployment mode for storage network interface required all

VM/NFV to be powered.

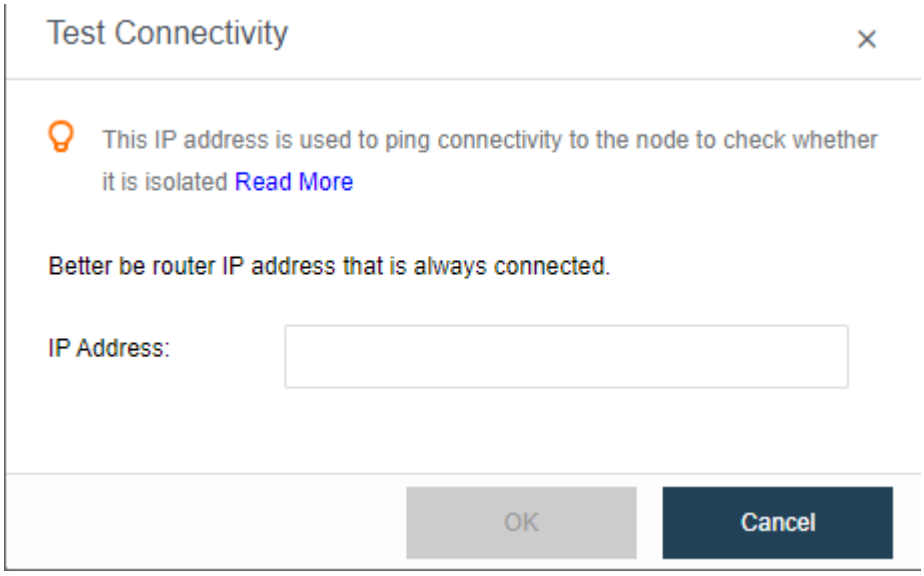


5. Lastly, specify the interface used for storage network and configure the corresponding IP address for communication.



Each node communicates with another one using two physical interfaces which are connected to a same layer 2 switch. Storage network interfaces will be aggregated automatically without the need to configure link aggregation on switch. After the deployment mode is selected, you need to deploy the network according to the digram illustrating deployment architecture of storage area network, and then select storage network interface for each node and configure IP address for that interface.

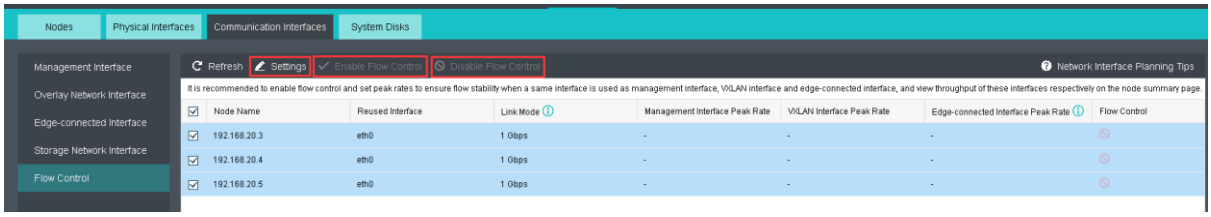
Test Connectivity: This allow to test whether the storage network has been isolated from other network.



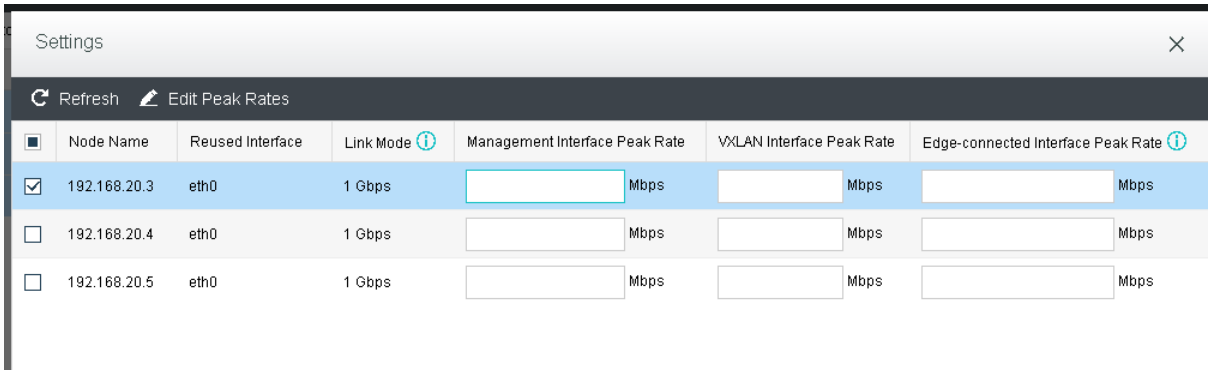
2.5.5.5 Flow Control

Flow control is the function which restrict the peak traffic for each types of interface to ensure the performance for each interface for the network multiplexing port .

Network QoS can be applied to the traffics through the flow control.



Settings: Configure the Peak Rate for each interface accordingly.



Enable Flow Control: Allow to enable the flow control for the selected nodes after peak rate has been configured.

Disable Flow Control: Allow to disable the flow control for the selected nodes after peak rate has been configured.

2.5.6 System disk

Starting from aCloud6.o.o., system disk can be replace individually without replacing the whole node, including the storage disk.

The business integrity and availability can be ensure by replacing the system disk through the following steps:

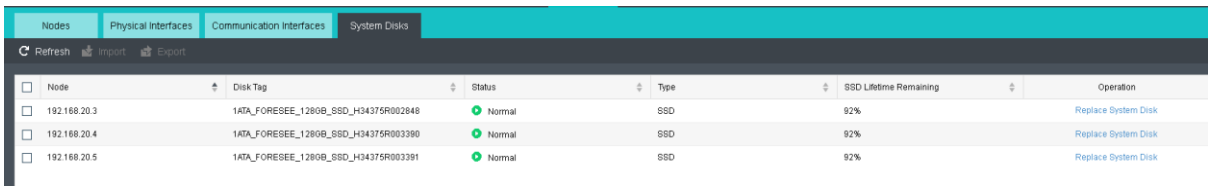
a. Migrate VMs

b. Enter Host Maintenance Mode

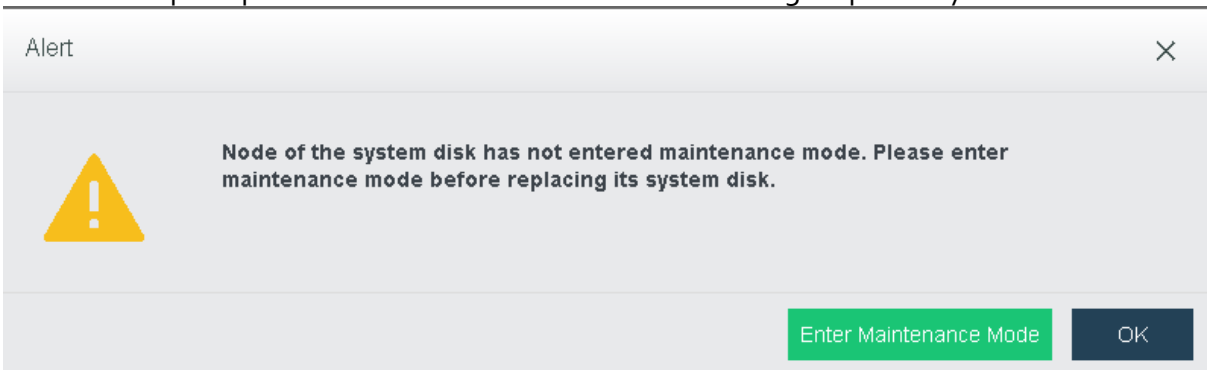
c. System config backup

d. Rebooting and proceed with OS disk replacement

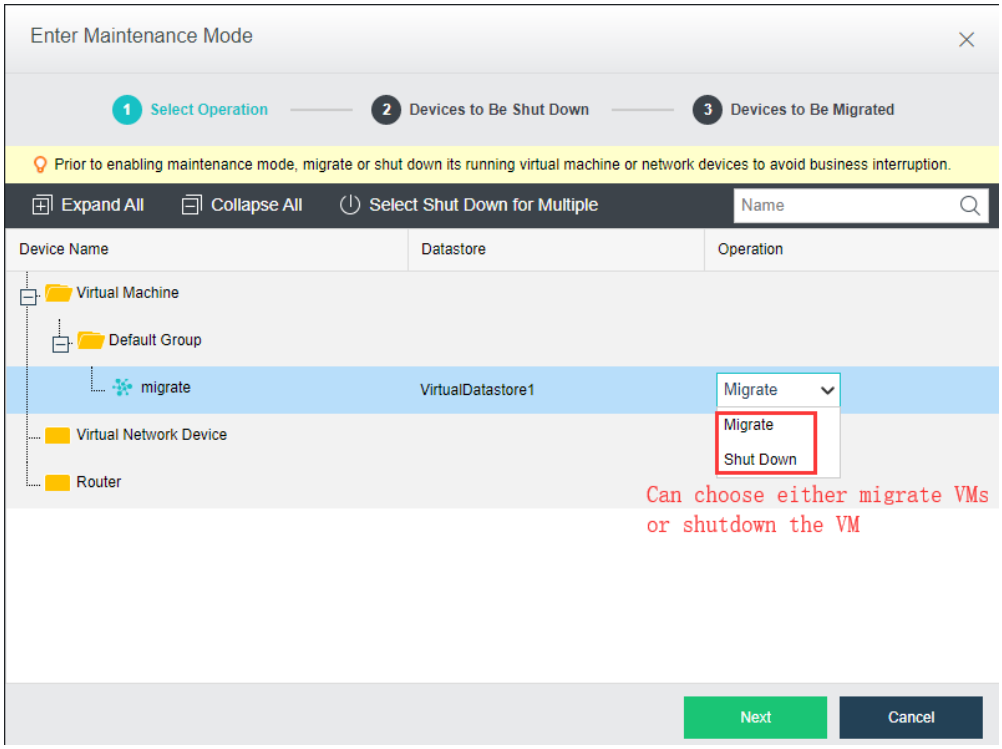
e. ISO guided OS re-installation

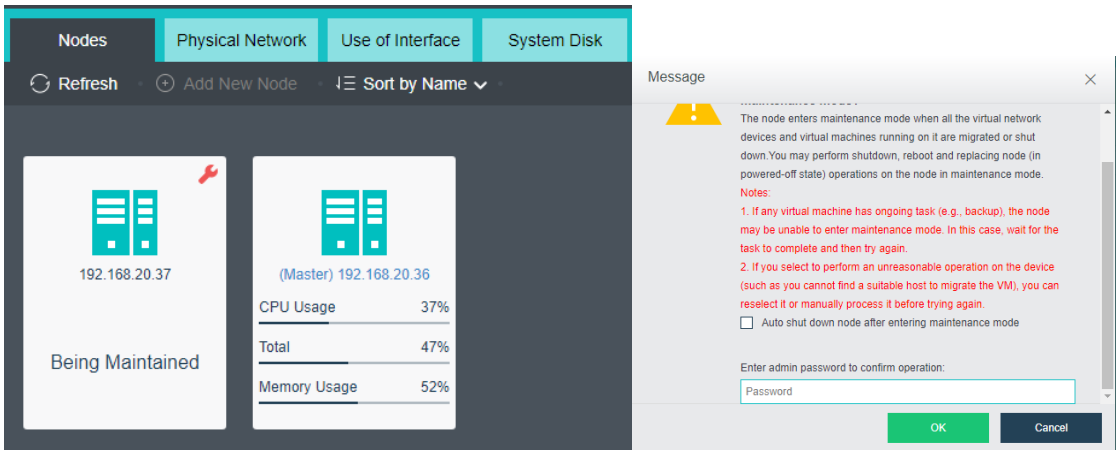


1. You will be prompted to enter maintenance after clicking Repalce System Disk.

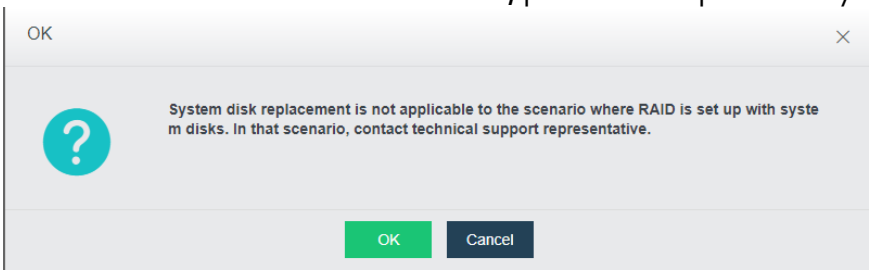


2. Before enter the maintenance mode, it provides the options to migrate VM to another host or shutdown the VM.



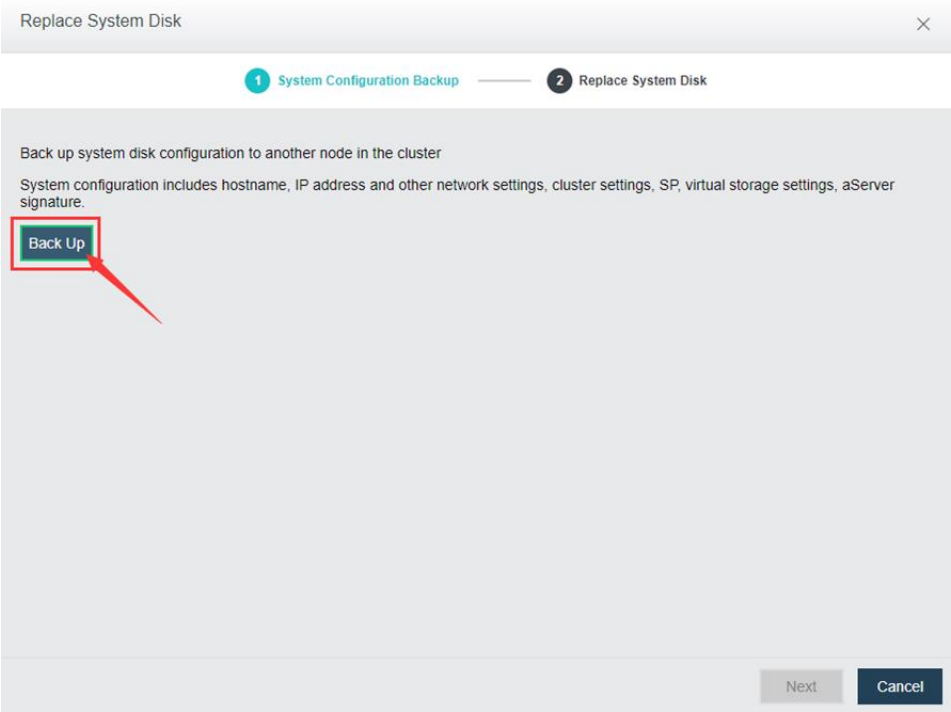


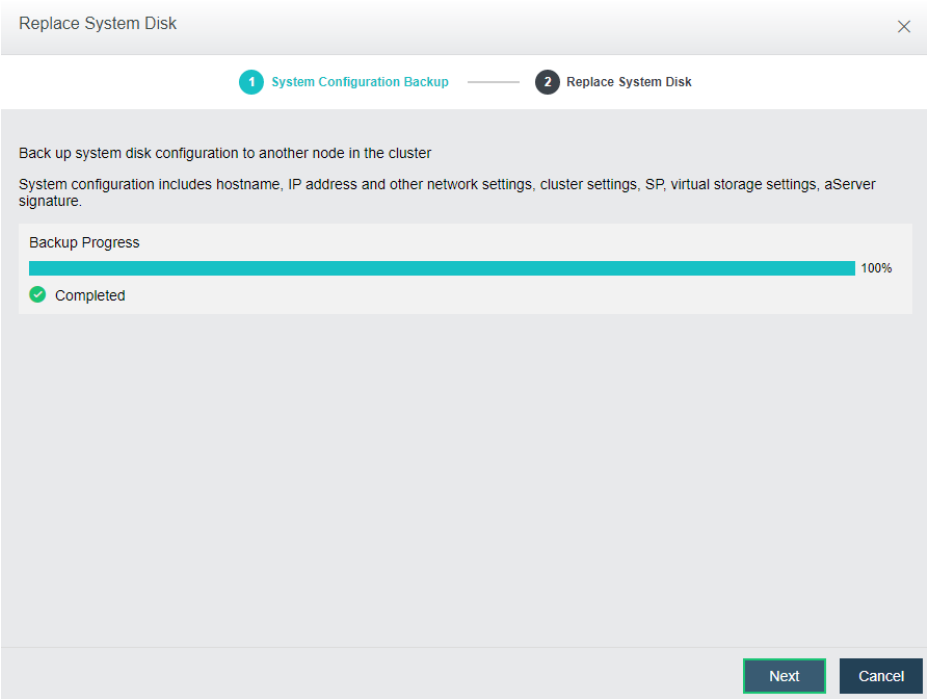
3. After host entered maintenance mode, proceed to replace the system disk.



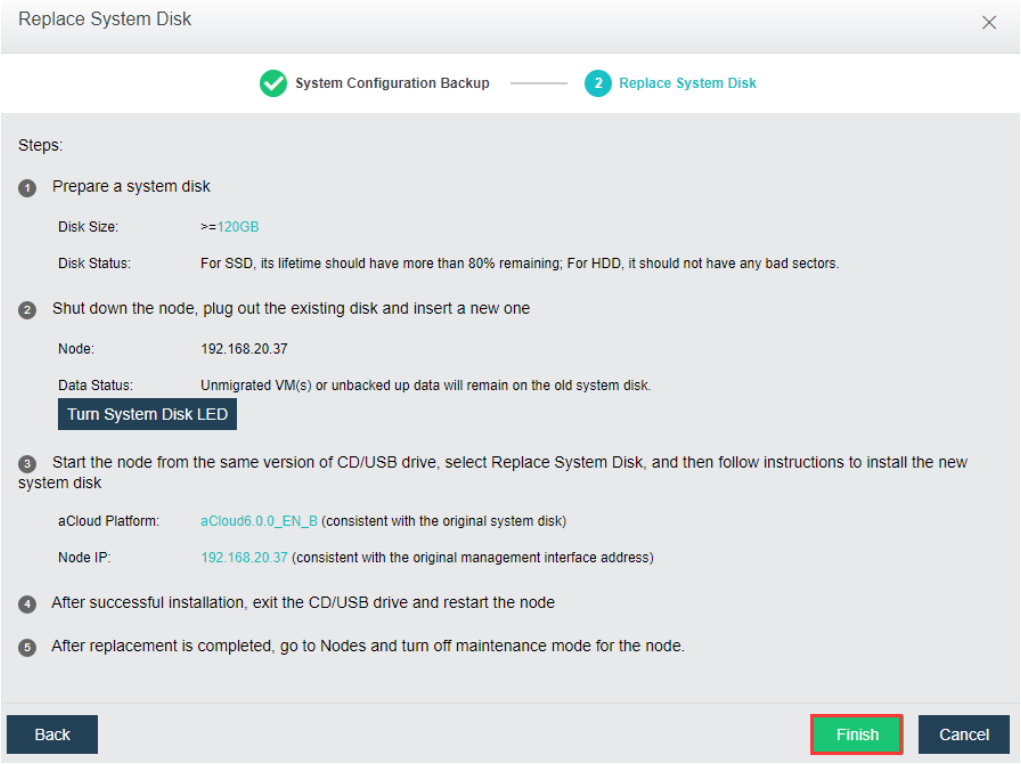
Note: If there have RAID configuration done on the OS disk, kindly contact technical support to assist you on your issue.

4. Click on the backup to save a copy of config into available host.

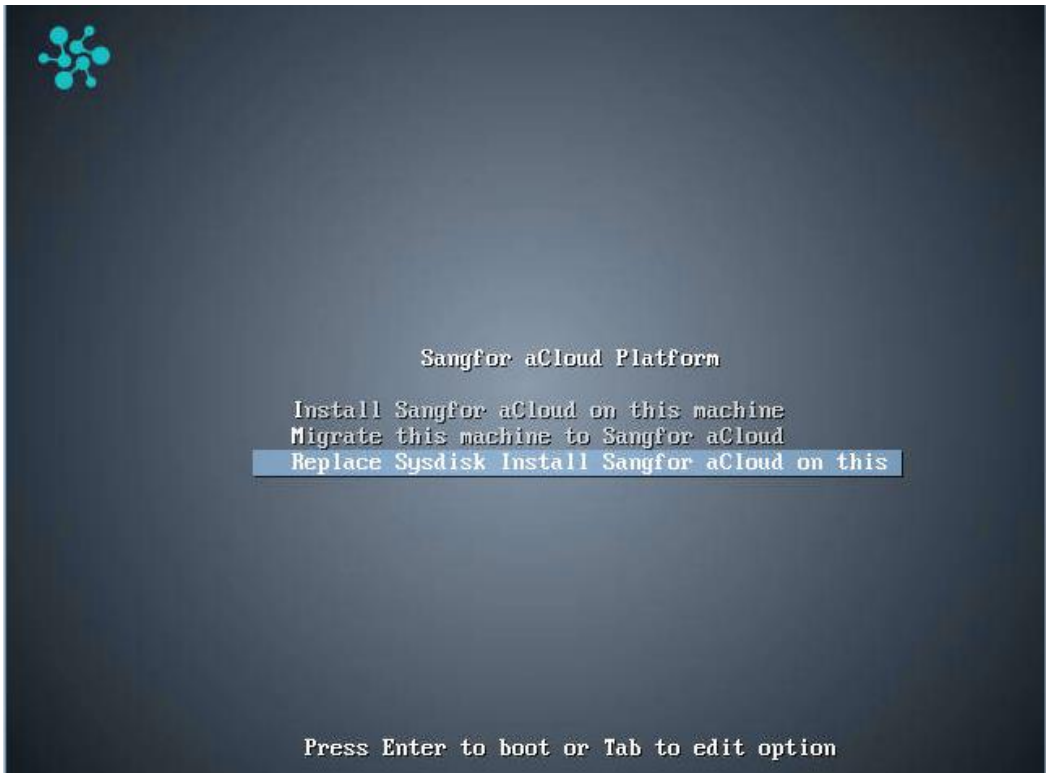




5. Click "finish" to complete the system disk replacement wizard.



6. Make a bootable USB with ISO file HCI 6.0.0 EN or above, and restart the nodes. Select boot from USB.
7. Select Third option "Replace Sysdisk Install Sangfor HCI on this"

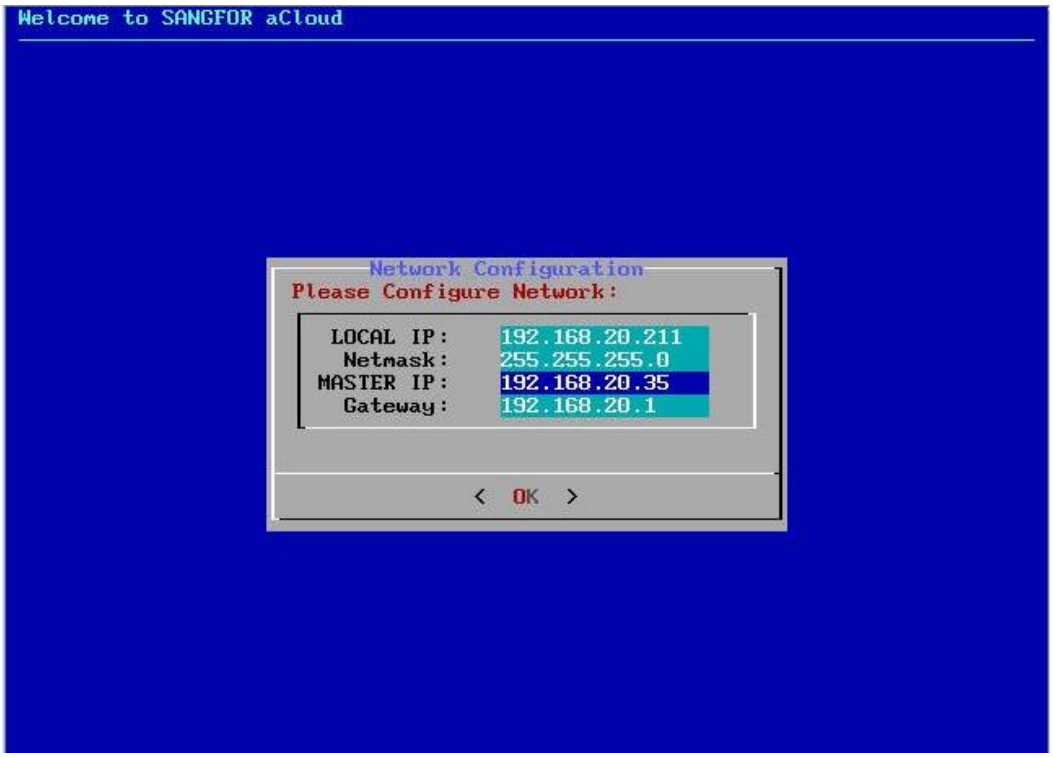


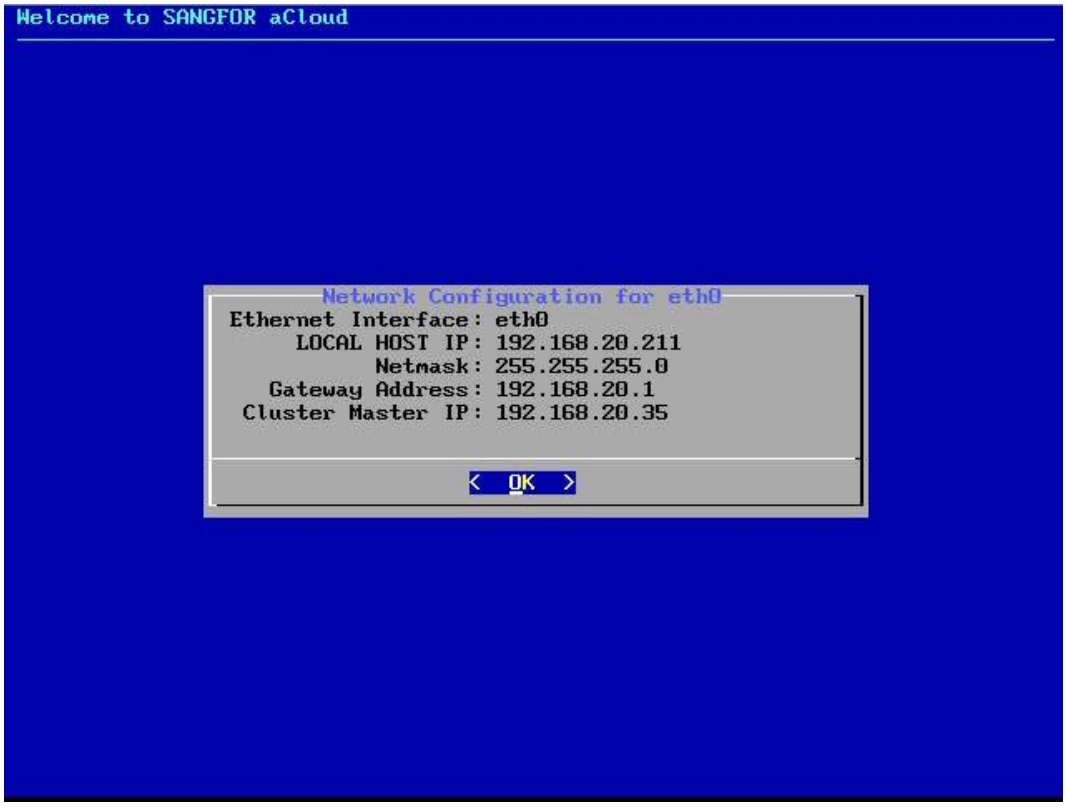
8. Configure network configuration for the booting ISO.
   Local IP: Replacement node IP

   Netmask: Network subnet mask

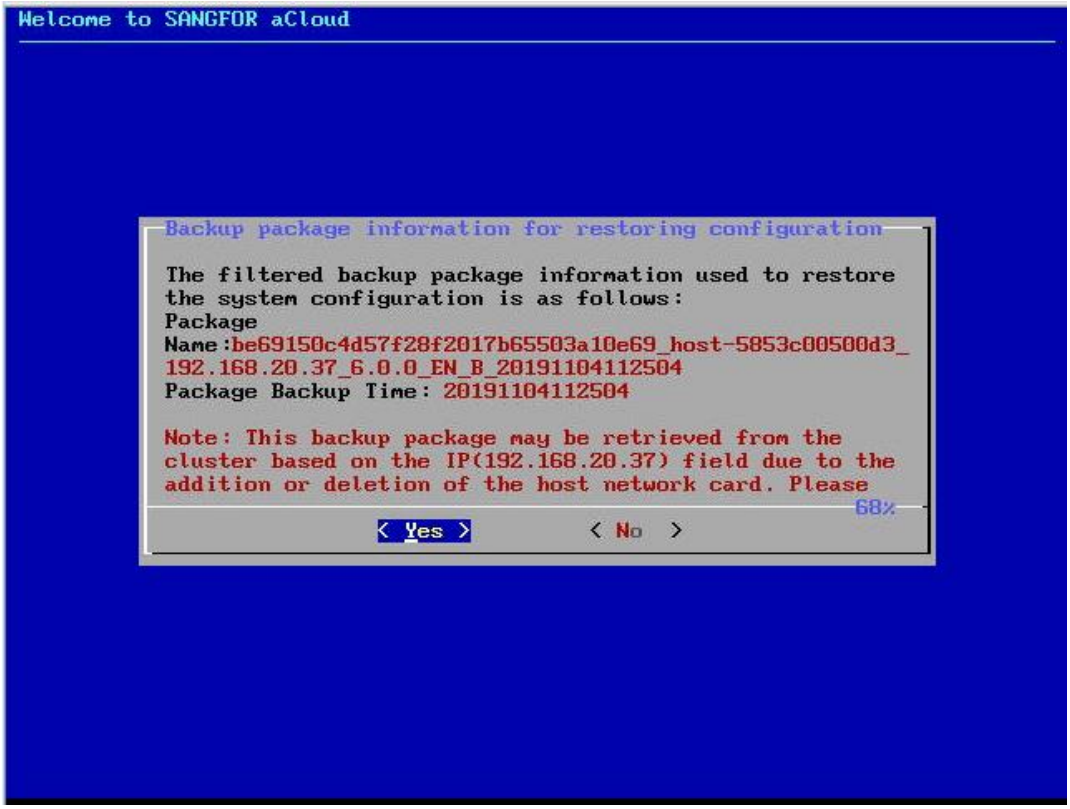
   Master IP: Cluster IP address

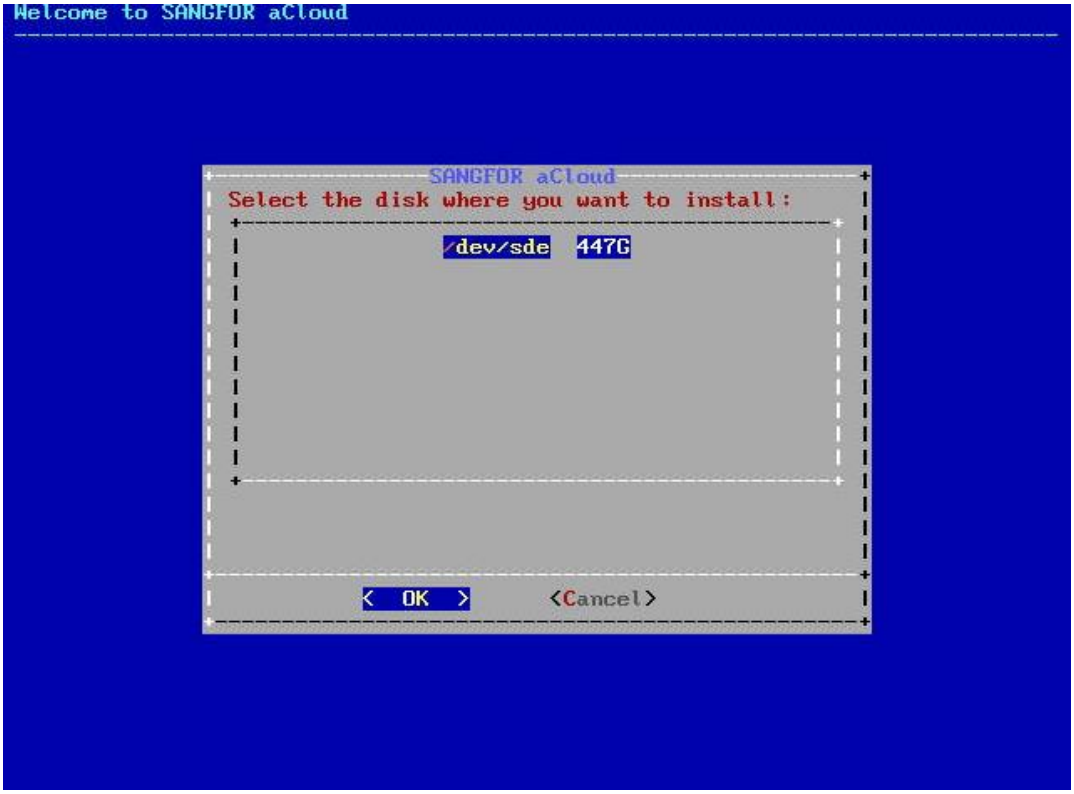
   Gateway: Default gateway for the IP





9. Select Yes to restoring backup configuration from the system.

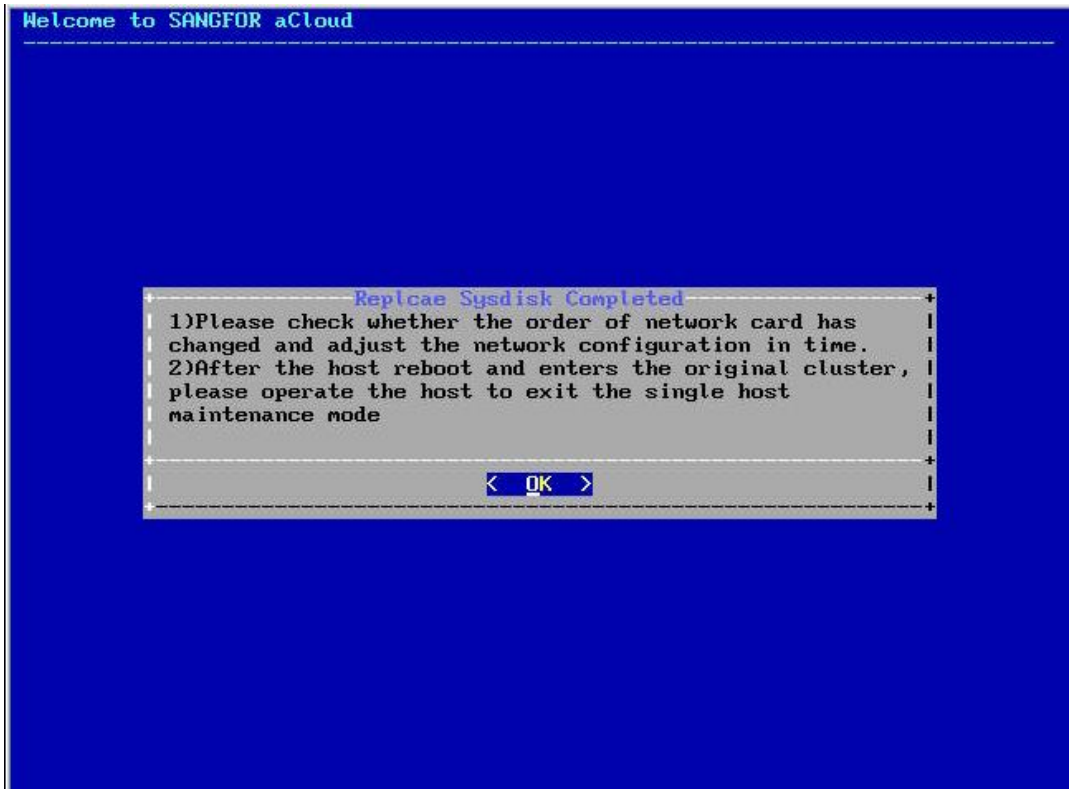




After click ok, it has to wait some time for HCI firmware installation on this new OS disk.

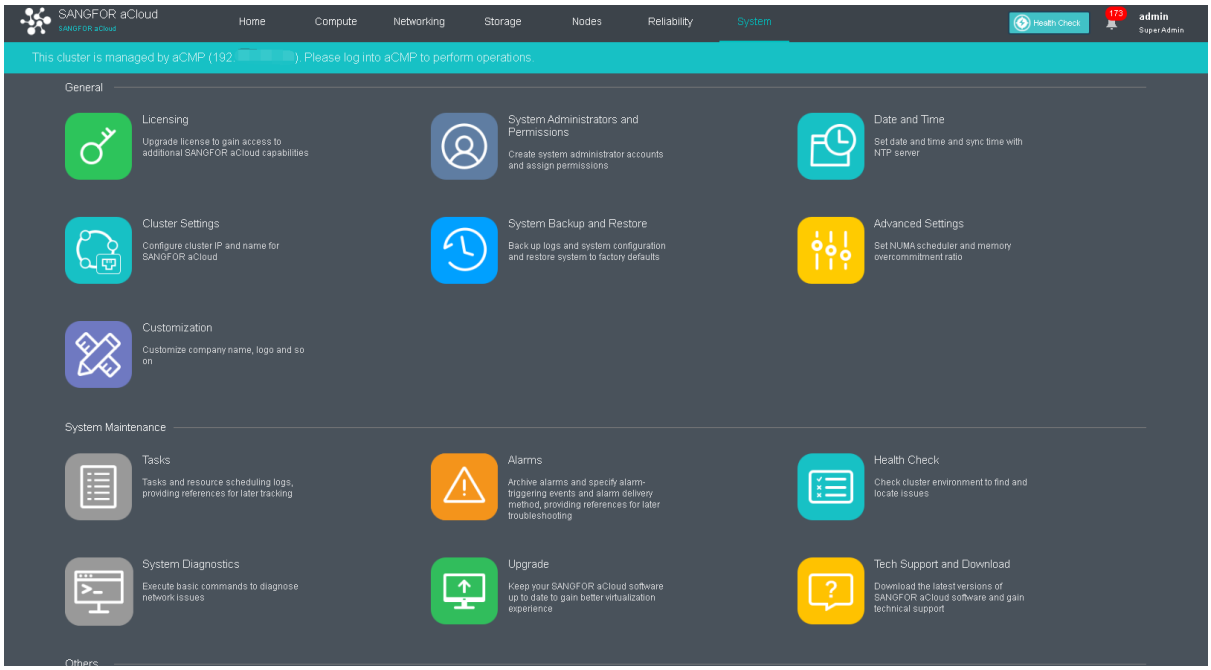
.

10. After all, it has to quit the maintenance mode to verify the new OS disk is working fine.



2.6 System

System includes **General**, **System Maintenance** and **Others**. **General** includes **Licensing, Date and Time, System Administrators and Permissions, Alarm Options, Cluster Settings, System Backup and Restore,** and **VM Backup and Recovery**. **System Maintenance** includes **Tech Support & Download, Logs and Alarms, Upgrade, Health Check** and **Customization**. **Others** includes **Recycle Bin** and **HA & Resource Scheduling**.



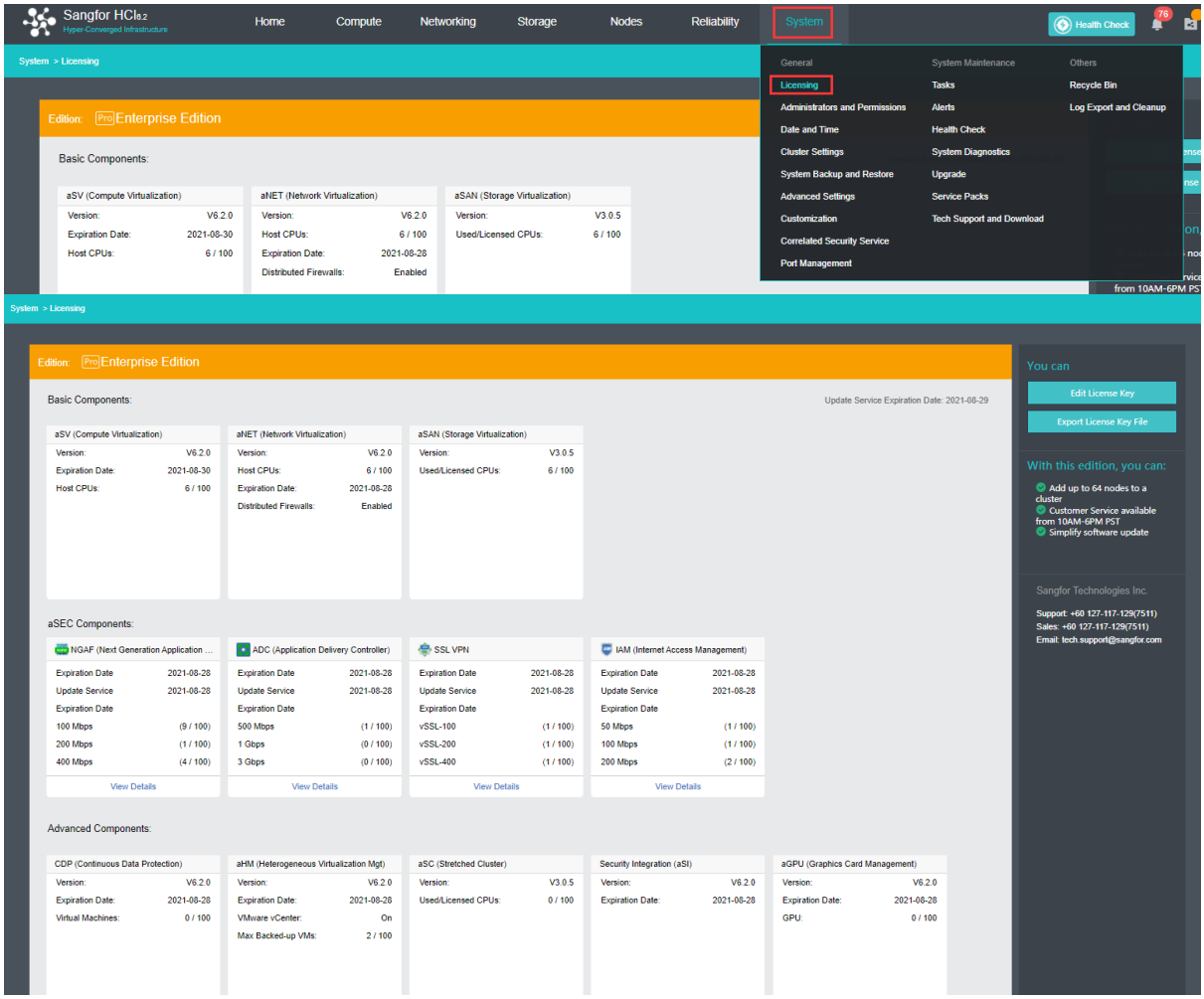
2.6.1 Licensing

It includes **Basic Components, aSEC(Security)** and **Advanced License**. **Basic Components** includes aSV(Compute Virtualization), aNET(Network Virtualization), aSAN(Storage Virtualization), SCP(Sangfor Cloud Platform). aSEC(Security) includes vNGAF, vADC, vIAM, vSSL VPN, vWOC, etc. Advanced License includes CDP(Continuous), aHM(Heterogeneous Virtualization Mgmt), Security Integration (aSI), . aSC (Stretched Cluster) and aGPU (Graphics Card Management).

There are two editions, Trial Edition, and Enterprise Edition.

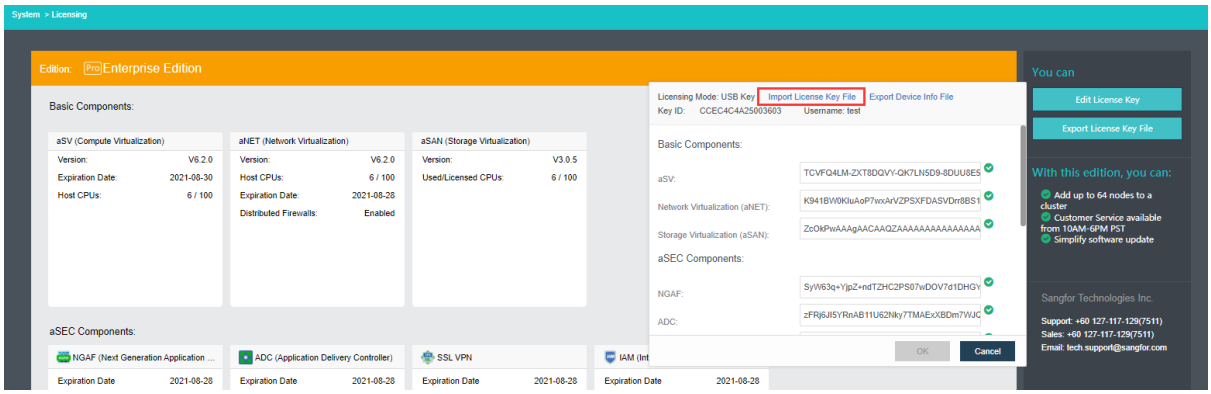
As for **Upgrade To Enterprise Edition**, a USB key is required to be plugged into one clustered node.

The **Enterprise Edition** is shown as follows:

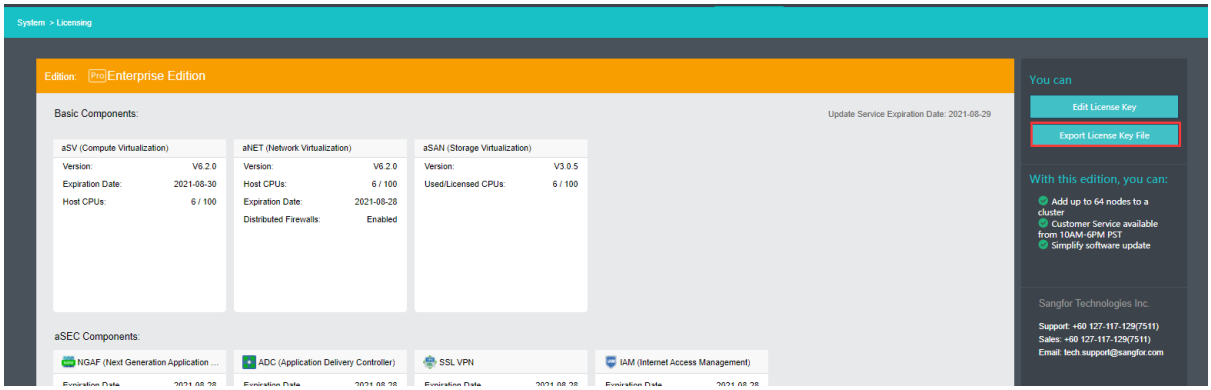


Edit License Key: To edit license key, click **Edit License Key**.

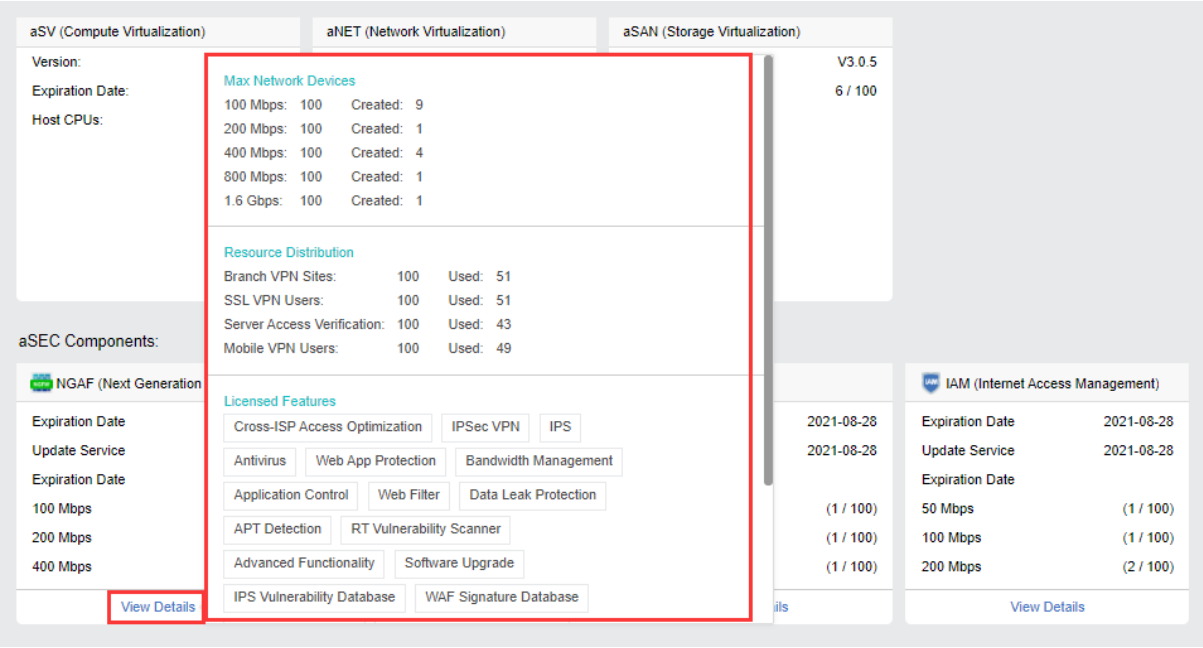
Import License Key File: To import a license key file, click **Import License Key File.**



Export License Key File: To export license key file, click **Export License Key File,** as shown below:

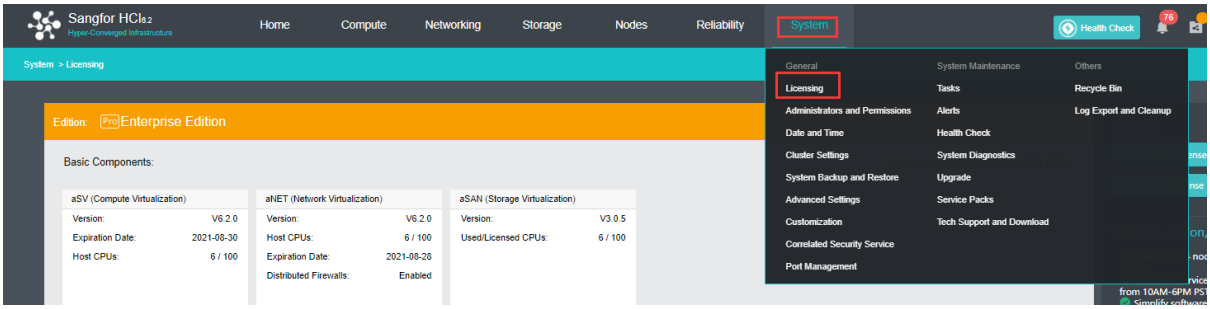


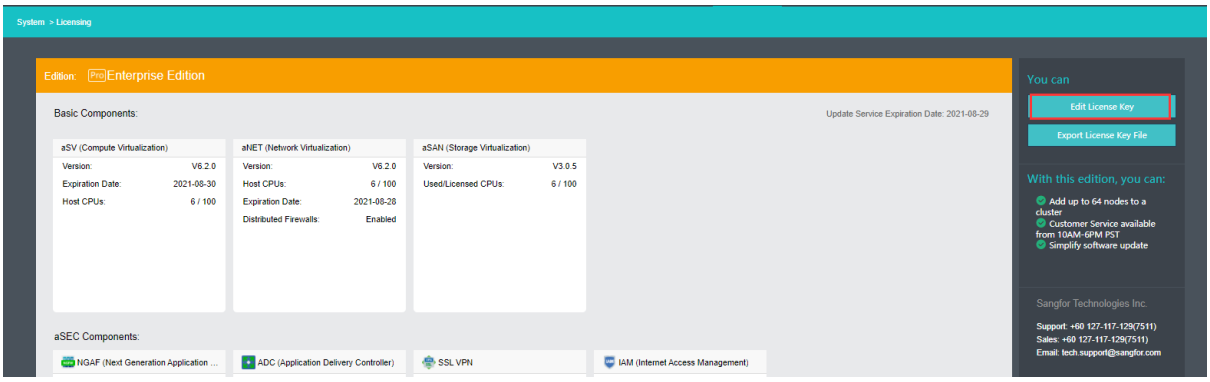
Details: It displays detailed configurations, such as **Max Network Devices, Resource Distribution, Licensed Features,** etc.

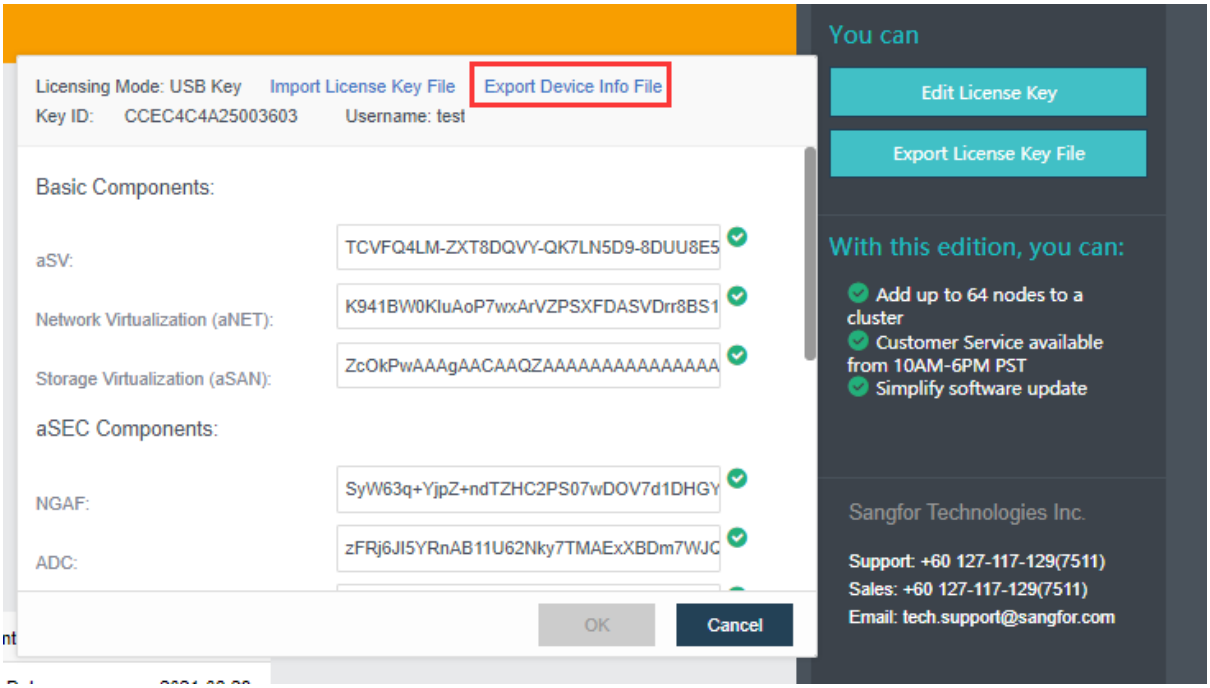


Virtual key function has been added to HCI since version 6.1.0. It allows HCI to be authorized without the physical USB key which might be damaged during the delivery progress.

1. The very first step for the virtual key licensing is to export the device information used to generate the license file. Under **System** > **Licensing,** select **Edit License Key** and select **Export Device Info File**.



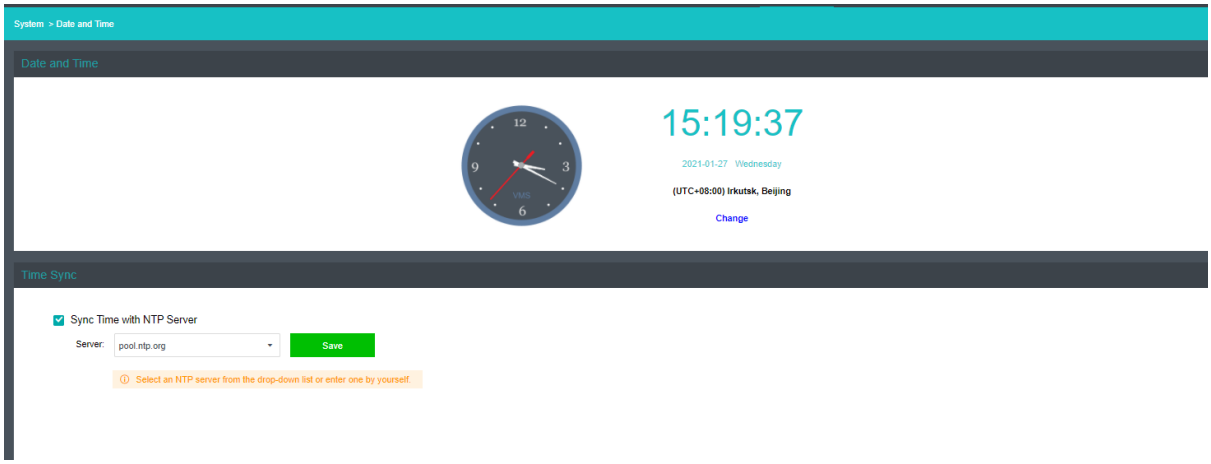




2. After that, provide this file to the corresponding Sangfor personnel for them to apply for the license file.
3. Once the application has been approved or processed, the license file will be generated.
4. Import the license file for the licensing.

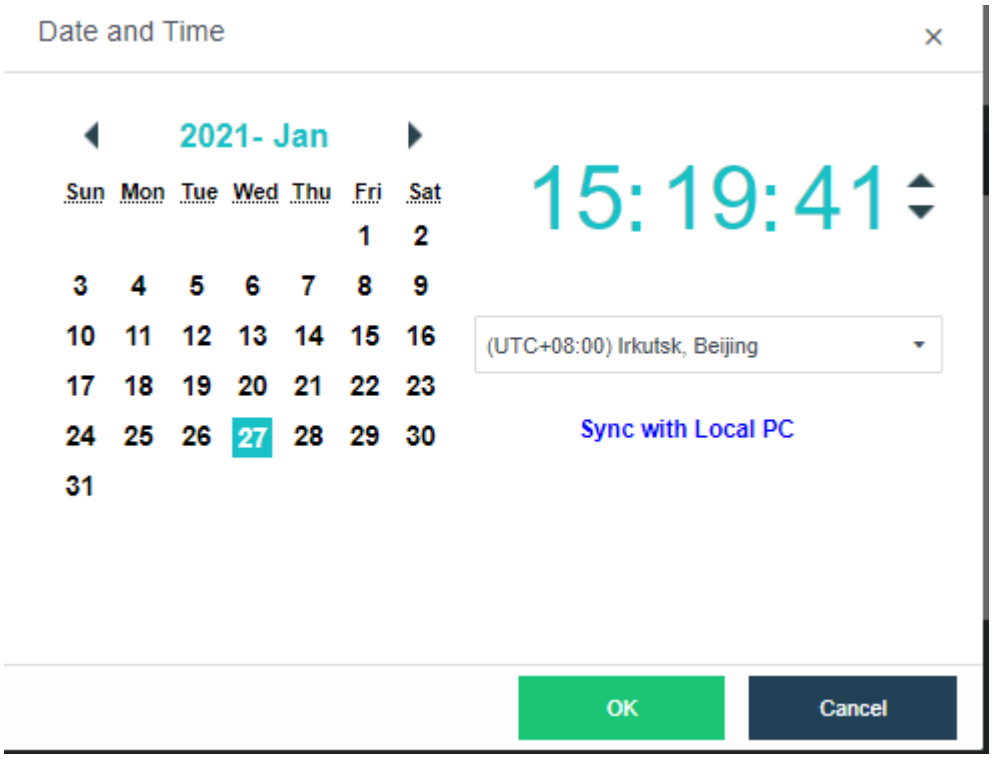
2.6.2 Date and Time

You can change date and time on Sangfor HCI platform and sync its time with NTP server.



2.6.2.1 Changing Date and Time

It displays date and time on SANGFOR HCI platform. To configure date and time, click **Change**.

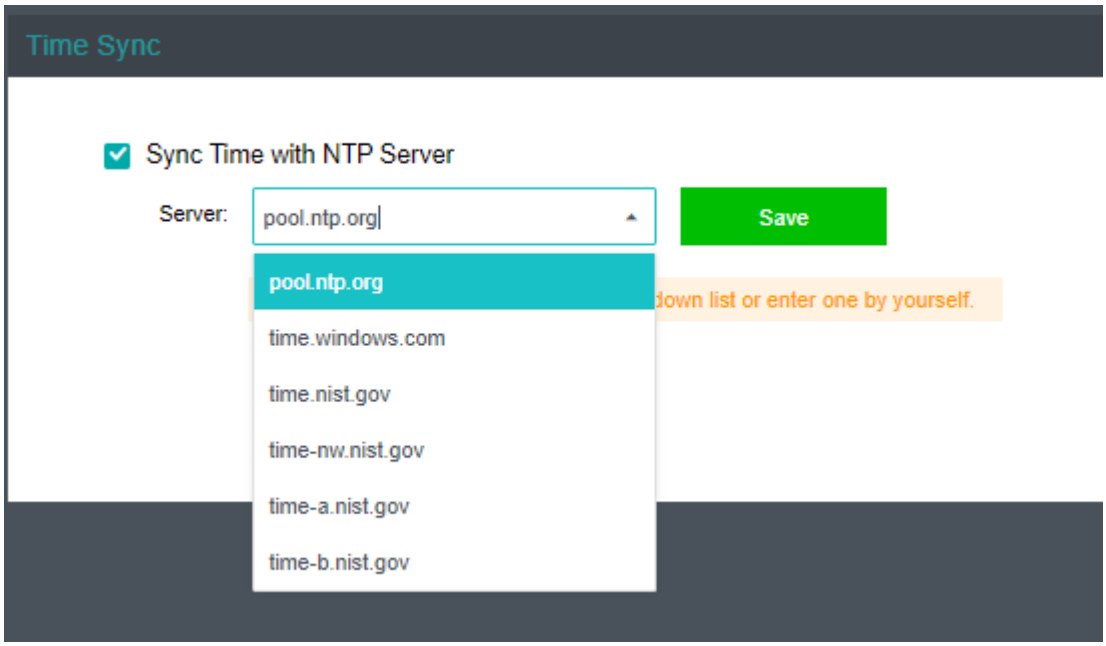


To sync time with local PC, click **Sync with Local PC**. Click **OK** to save the changes.

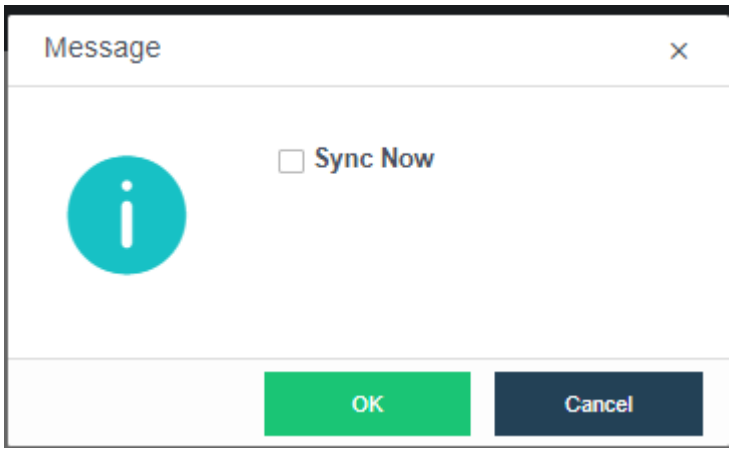
After saving changes to date and time, you need to log in again.

2.6.2.2 Time Synchronization

To sync time with NTP server, select one NTP server from the drop-down list, as shown below:

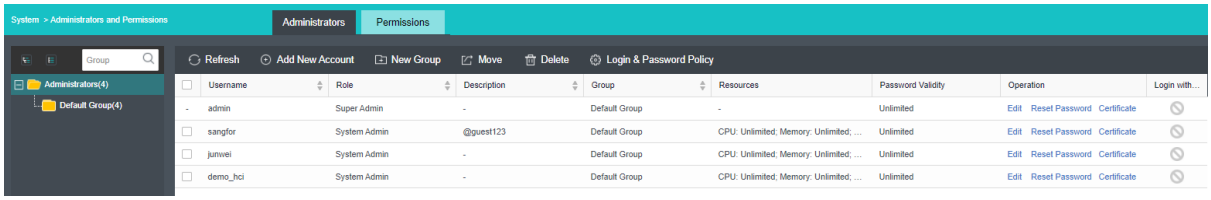


Click **Save** and a dialog box pops up asking whether to sync now, click **OK** to confirm. Synchronizing time with NTP server requires that the DNS server should be configured correctly and network connection is also required.



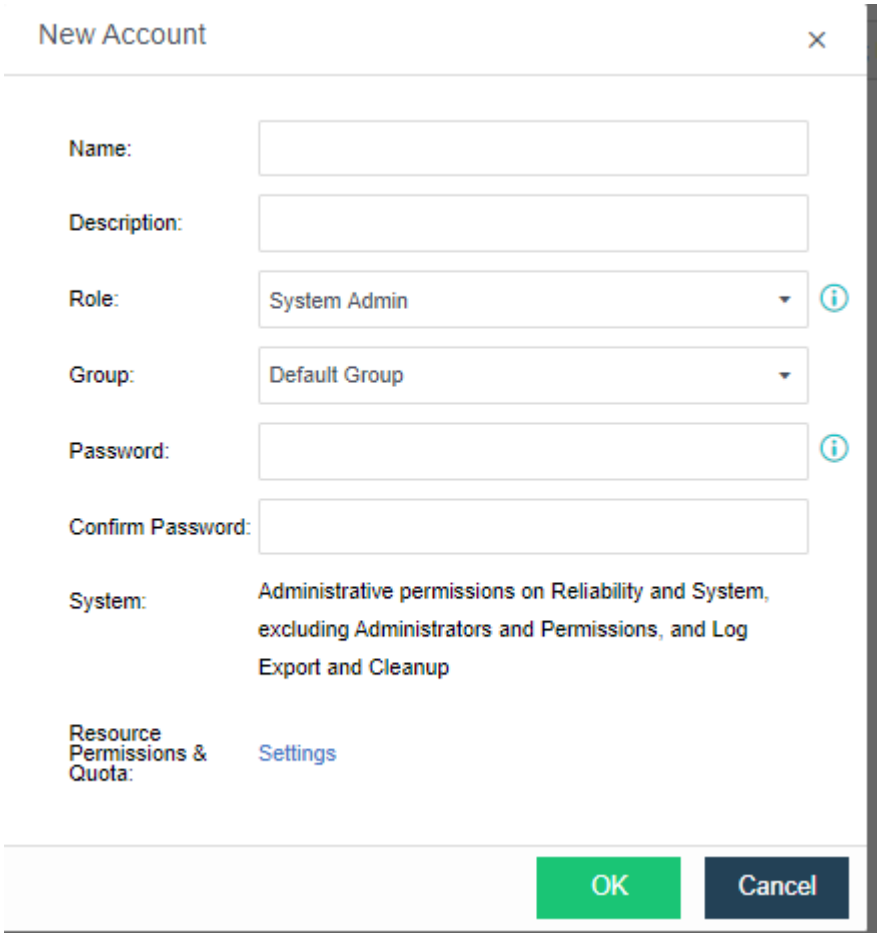
2.6.3 System Administrators and Permissions

You can add multiple admin accounts and assign different privileges to those accounts.



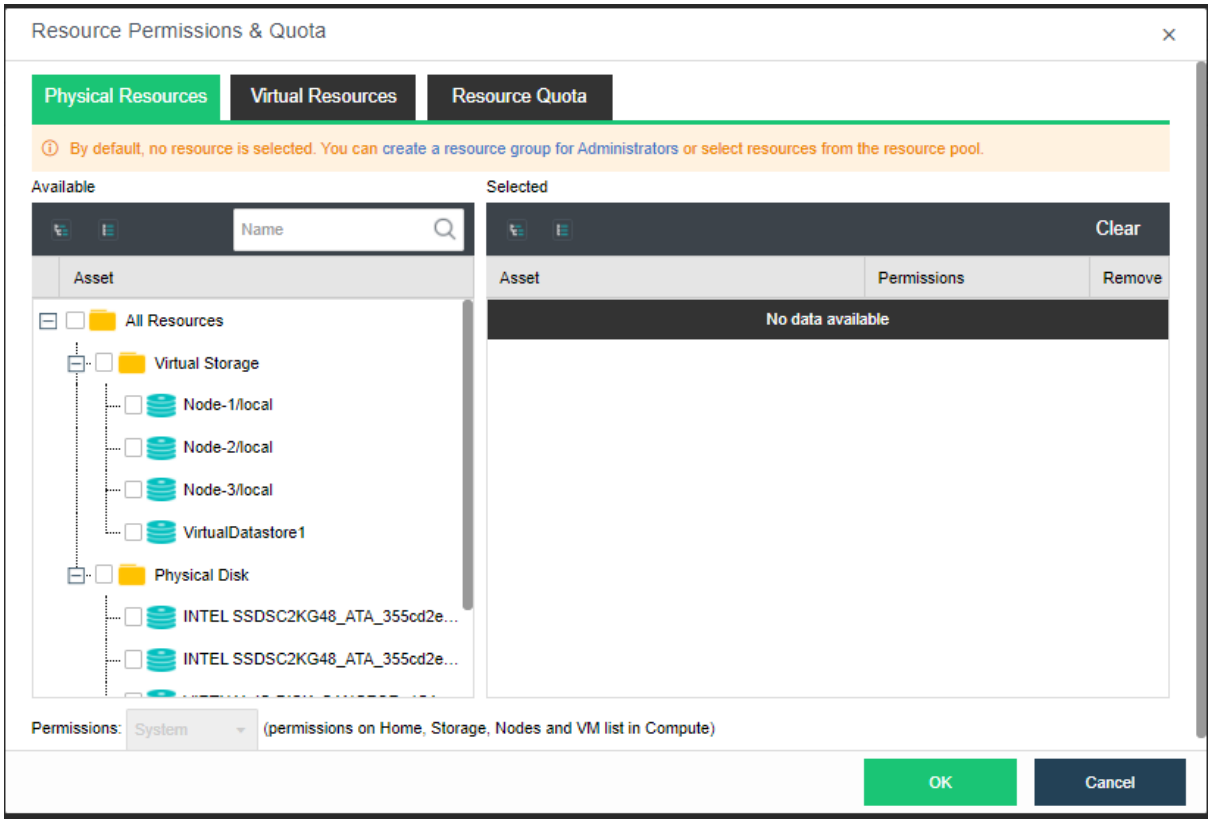
2.6.3.1 Adding Administrator Account

To create an admin account to log into Sangfor HCI, click **System Administrators and Permissions** to enter the following page. To add an admin account, click **Add** to enter the **Add Account** page, as shown below:

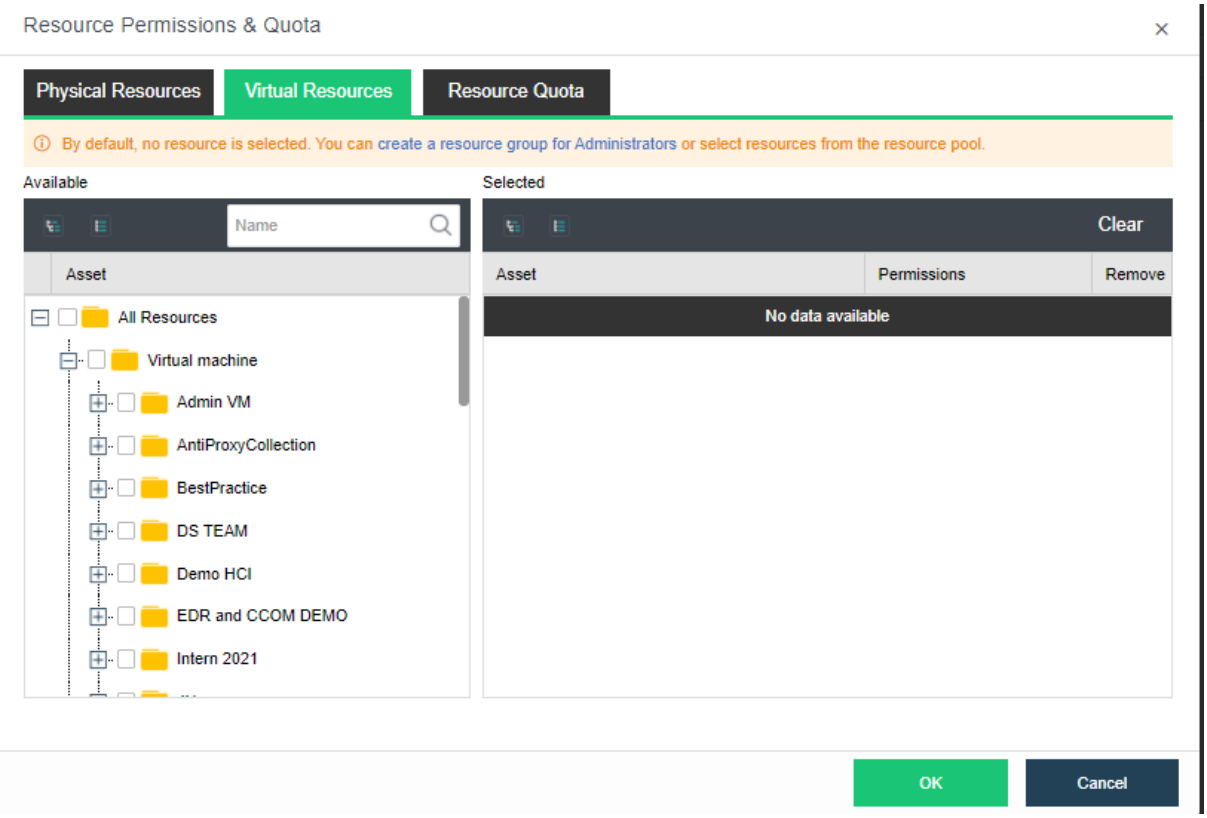


Specify **Name**, **Description**, **Password** and **Retype Password** fields and a group. To avoid typing a wrong password**, Retype Password** field is required. To configure permissions, click **Settings**.

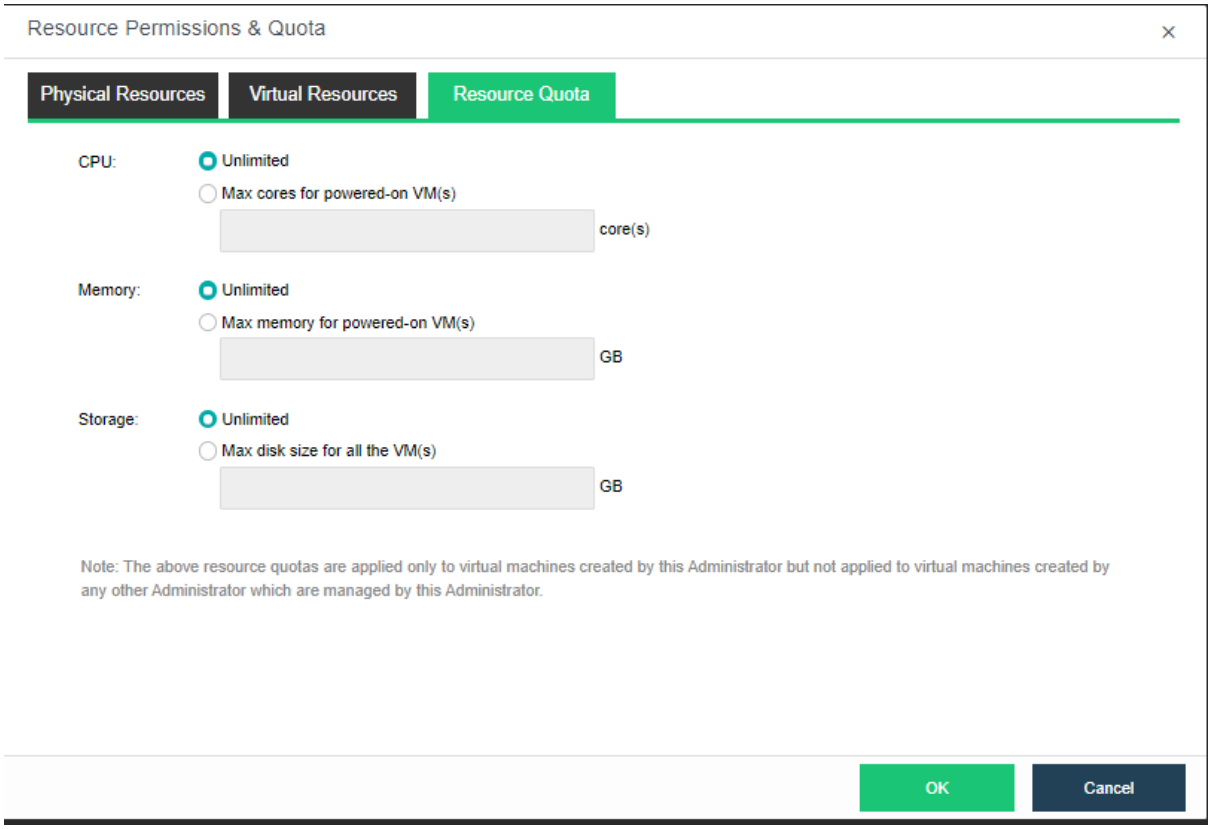
On the **Permissions** page, there are three tabs, **Permissions, Resources** and **System**. As for **Permissions**, it includes permissions on such resources as virtual machines, virtual network, virtual storage and physical disks.



As for **Resources**, it includes CPU, memory and storage. The resources are allocated to the administrator to create virtual machines only, not taken up by virtual machines that are created by other administrators but are managed by this administrator.



As for **System**, it includes **Physical resources, System configuration and maintenance** and **Service maintenance.**



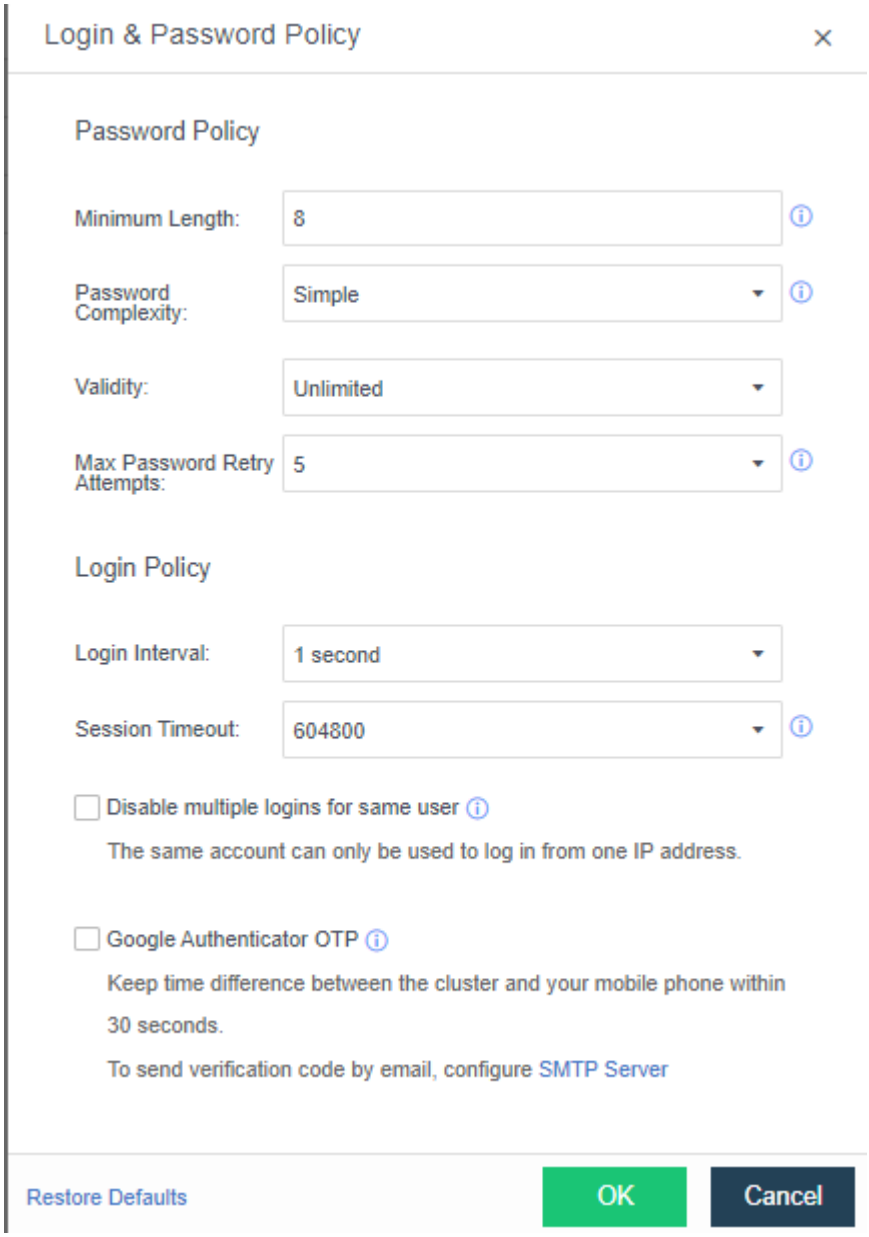
As for **Physical resources**, it includes configuration of **Home**, **Storage** and **Nodes** and view all the virtual machines.

As for **System setting and maintenance**, it includes configuration of some **System General and Maintenance** settings, including Licensing, Data and Time, Alarm Options, Cluster, System Backup and Restore, Tech Support and Download, etc.

As for **Others**, it includes configuration of some System General and Maintenance settings, including VM Backup and Recovery, Recycle Bin, HA and Resource Scheduling.

2.6.3.2 Login & Password Policy

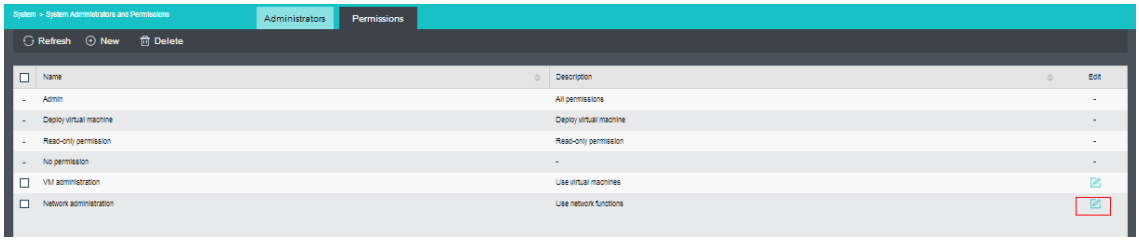
Login and password policy can be configured for all System Administrators account. This helps to improve the security by limiting the password minimum length, retry attempts, validity and timeout session.

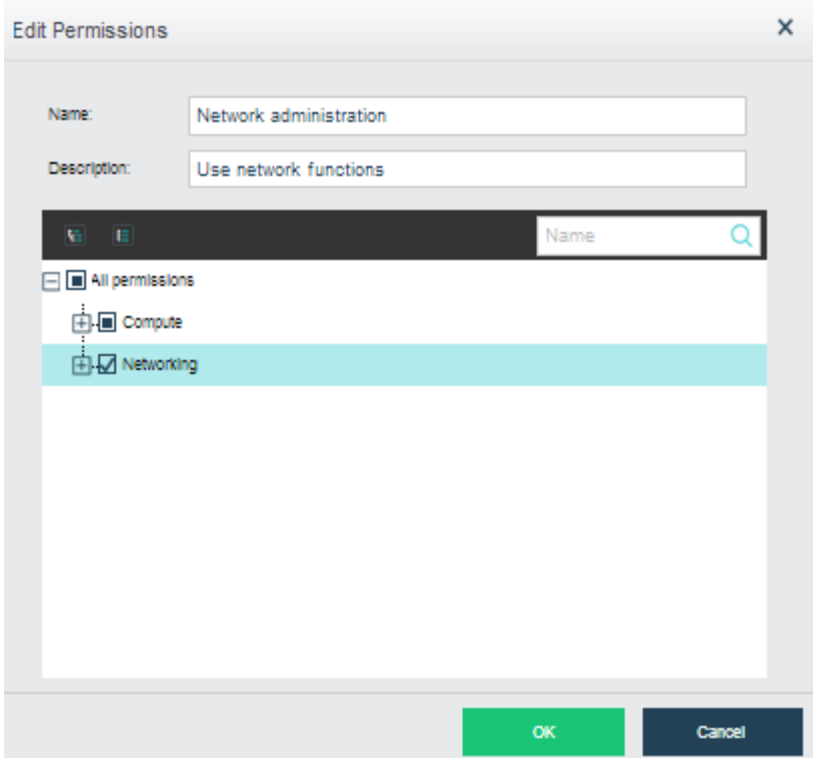


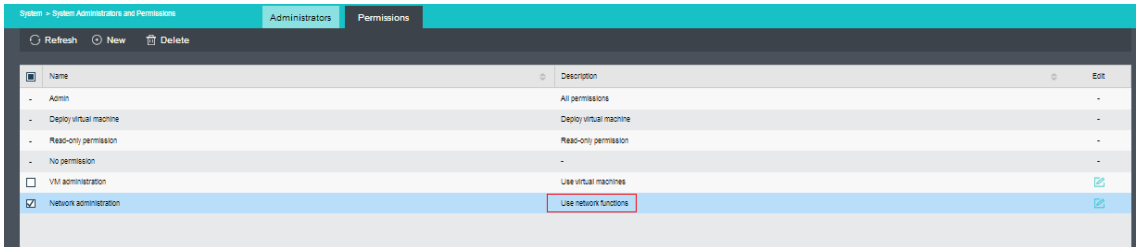
2.6.3.3 Assigning Permissions

On the **Permissions** tab, accounts can be assigned with different permissions, as shown below:

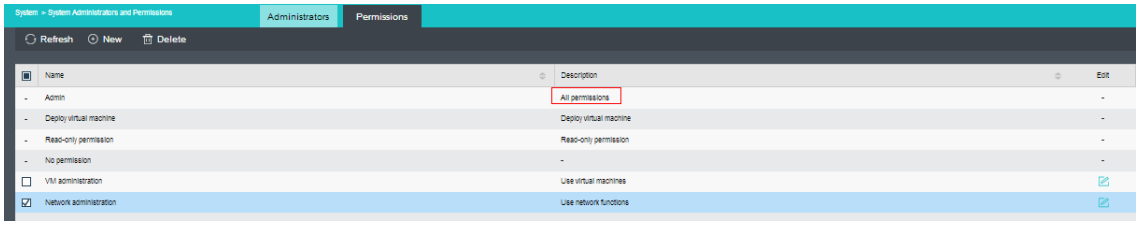
After adding accounts and having assigned permissions to those accounts, you can edit permissions on the **Compute** and **Networking** page, as shown below.







Permission of editing virtual network is similar to that of editing VM

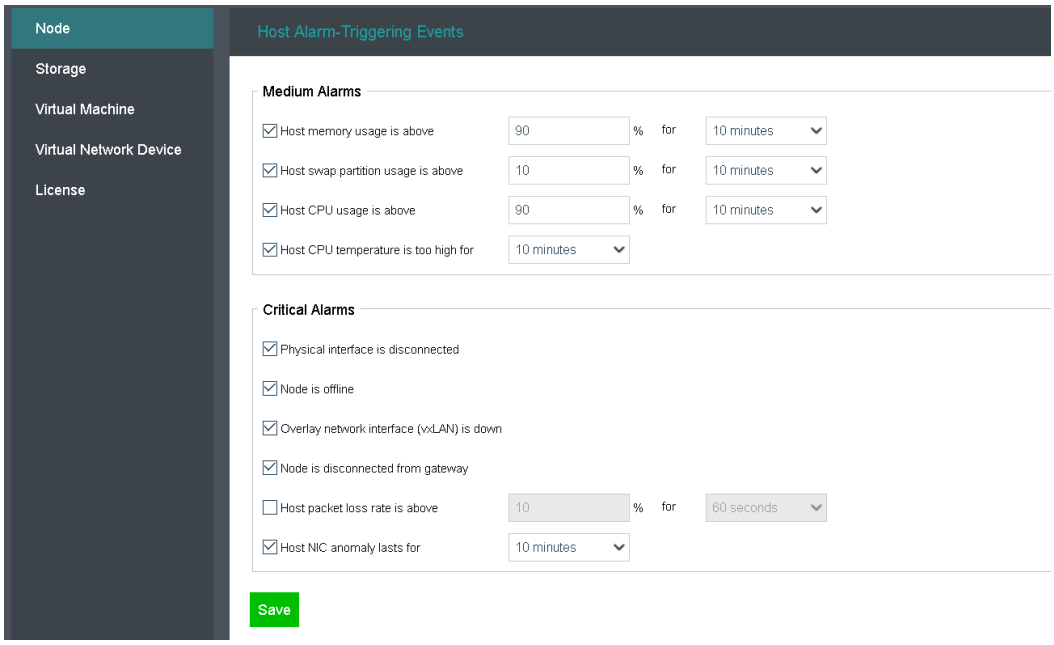


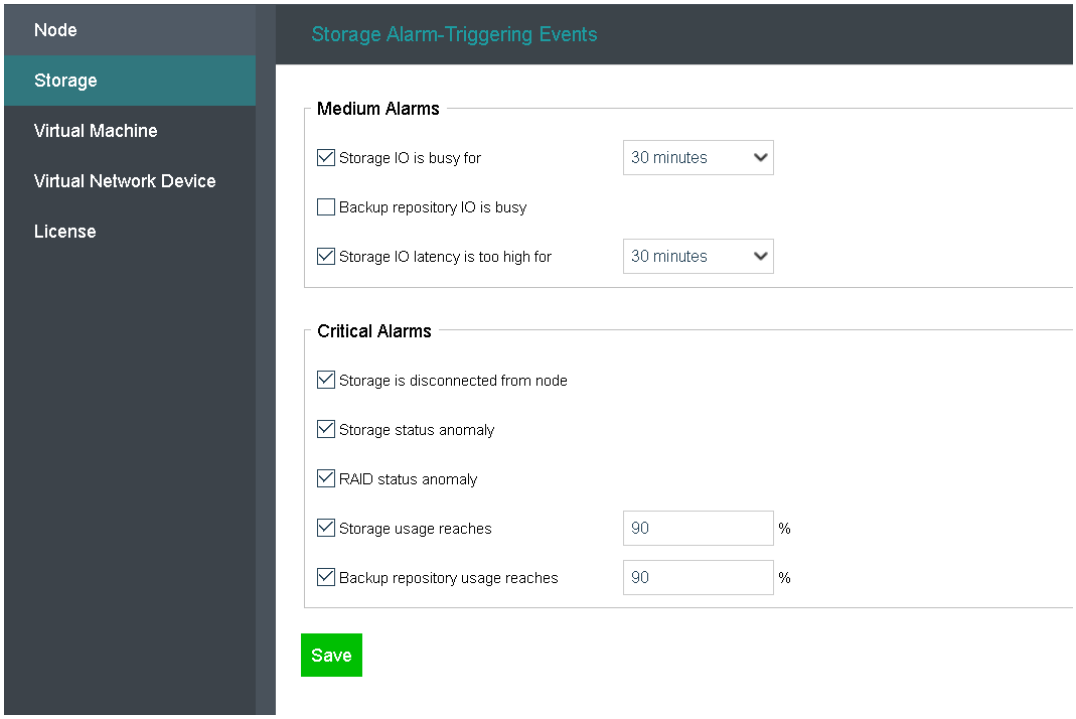
2.6.4 Alarm

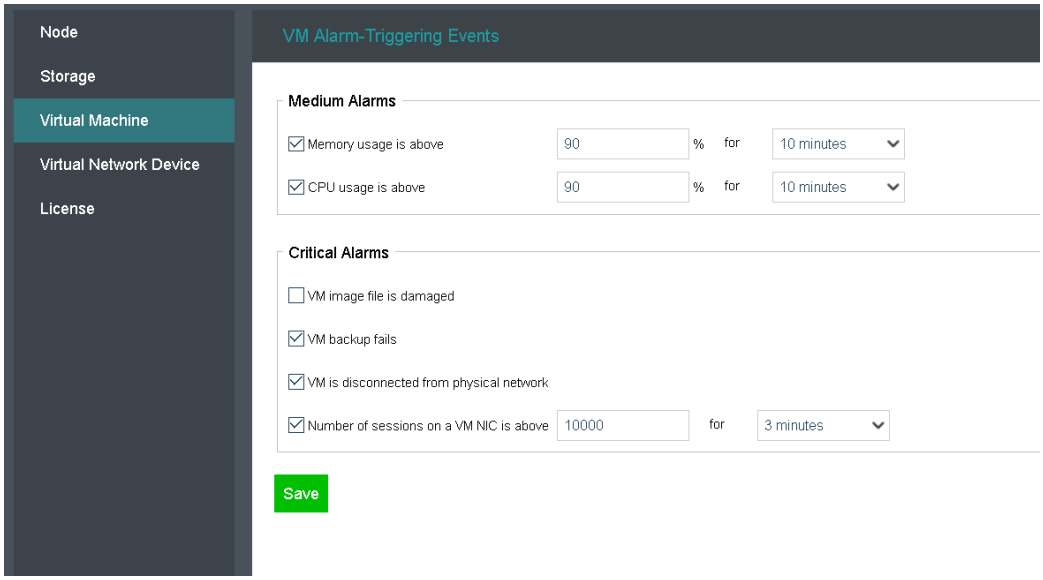
The **Alarm** page includes **Alarm, Alarm Option** and **Alarm Notification.**

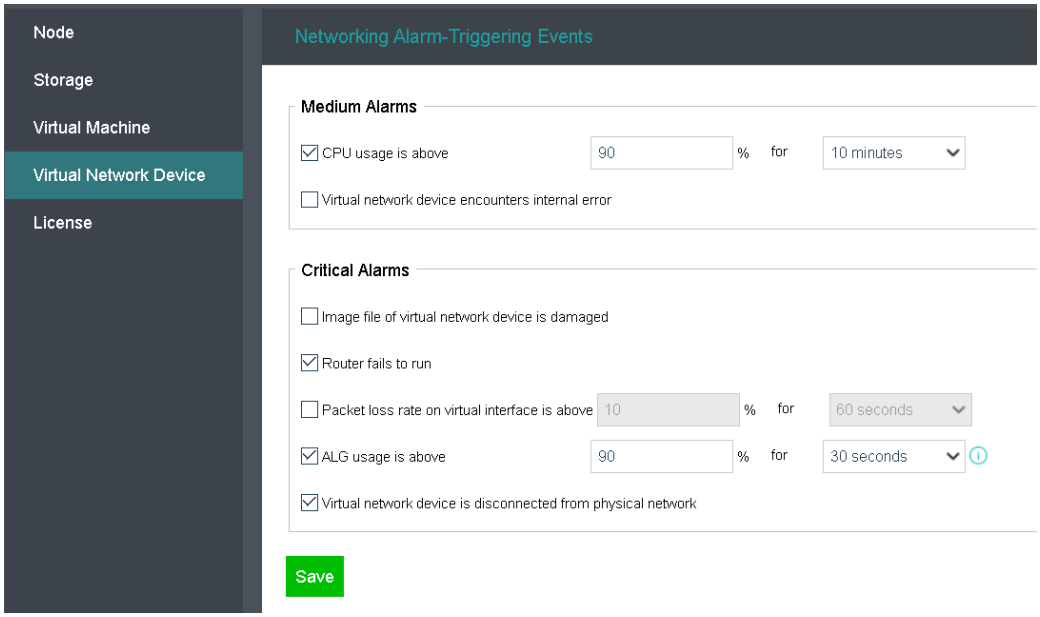
2.6.4.1 Alarm Option

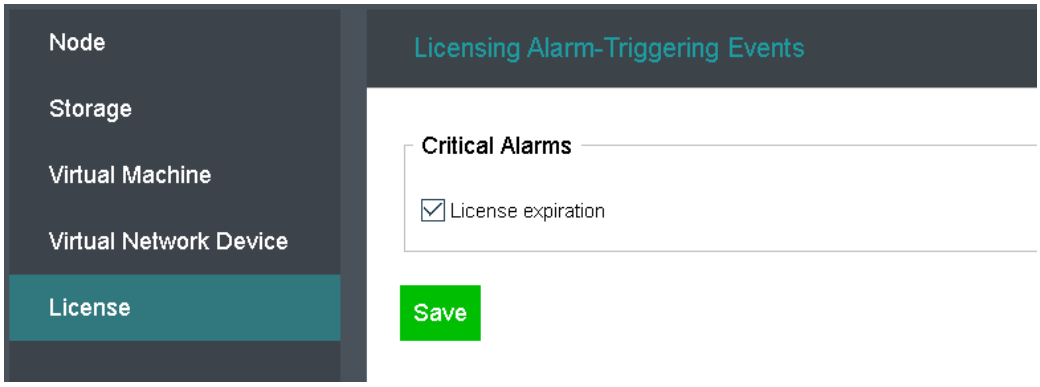
Thresholds for alarm events can be configured, including duration and severity. When thresholds are reached, alarms will be triggered and also alarm logs will be generated. as shown below:




Node
Storage
Virtual Machine
Virtual Network Device
License
Storage Alarm-Triggering Events
Medium Alarms
Storage IO is busy for
30 minutes
Backup repository IO is busy
Storage IO latency is too high for
30 minutes
Critical Alarms
Storage is disconnected from node
Storage status anomaly
RAID status anomaly
Storage usage reaches
90
%
Backup repository usage reaches
90
%
Save


Node
Storage
Virtual Machine
Virtual Network Device
License
VM Alarm-Triggering Events
Medium Alarms
Memory usage is above
90
%
for
10 minutes
CPU usage is above
90
%
for
10 minutes
Critical Alarms
VM image file is damaged
VM backup fails
VM is disconnected from physical network
Number of sessions on a VM NIC is above
10000
for
3 minutes
Save

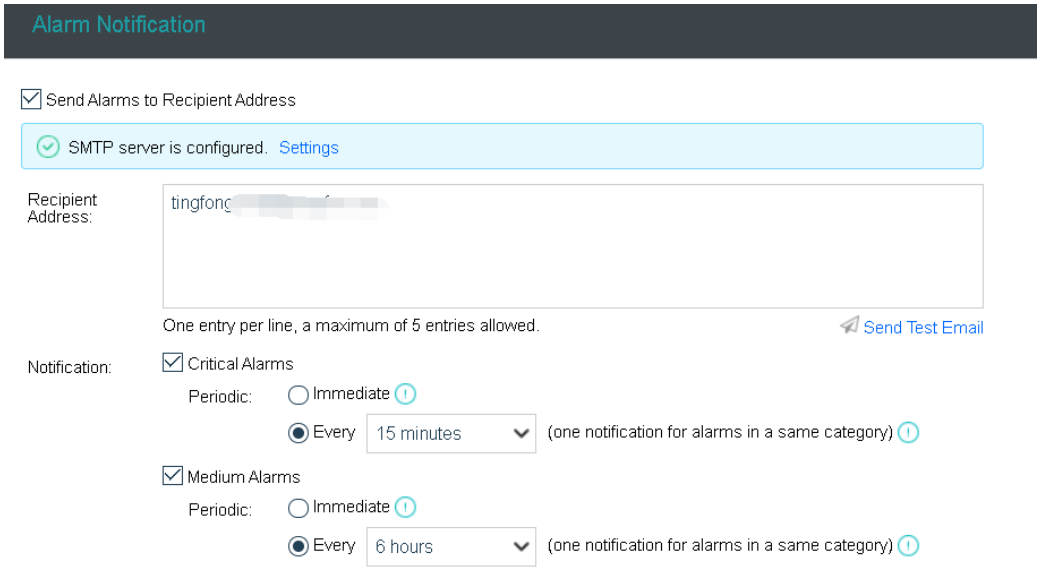


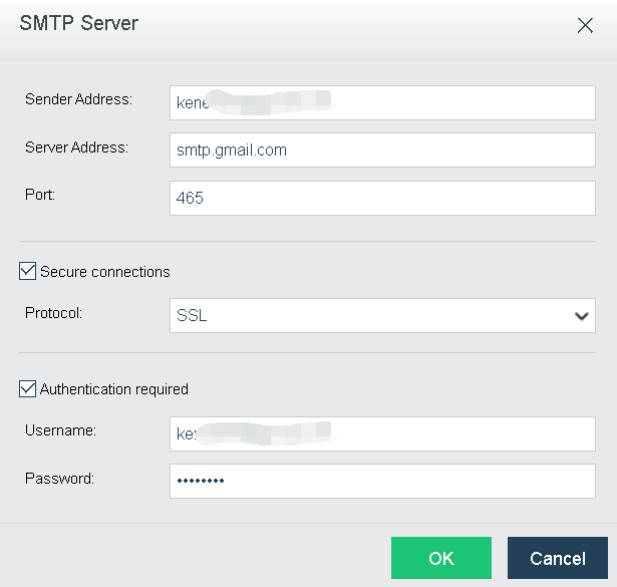


The all **Triggering Event** specify threshold for **Node, Storage, Virtual Machine, Virtual Network** and **License**.

2.6.4.2 Configuring Alarm Notification

To send alarm email, you need check the option **Send alerts to specified email addresses** and then specify **Recipient Email Addresses**, and the recipient email addresses, and configure the SMTP server by clicking on **Settings,** as shown below:





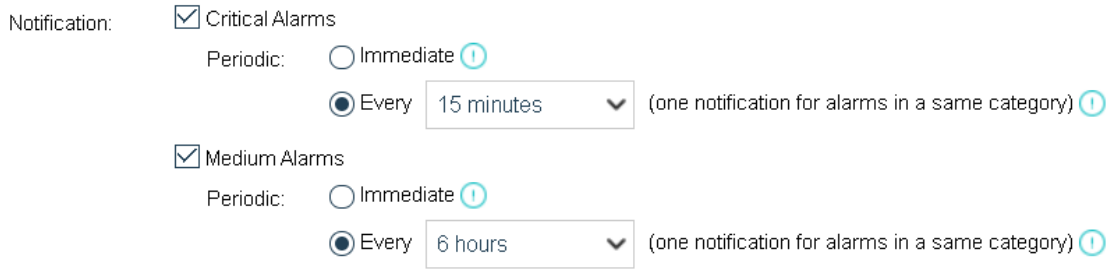
Sender Address: Specifies sender email address.

SMTP Server: Specifies IP address and domain name of SMTP server.

Port: Specifies port of SMTP server. Default port number is 25.

If the SMTP server requires authentication, select **Authentication required,** and enter username and password.

If **For alarm-triggering events of critical alarms and medium alarm occurring within N minutes, send one alert email only (one for each node)** is selected, only one alert email will be sent for alarm-triggering events of the same category within the specified period.

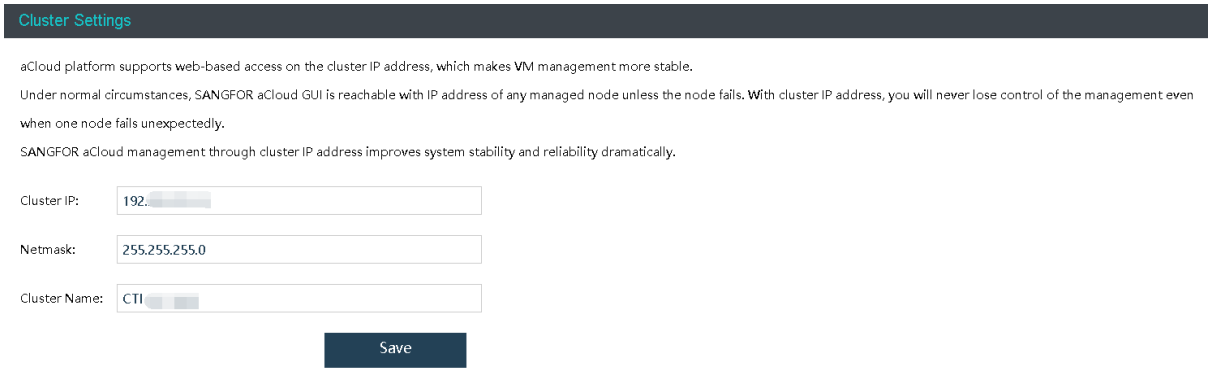


2.6.5 Configuring Cluster

You can configure cluster, management interface and overlay network interface.

2.6.5.1Cluster Settings

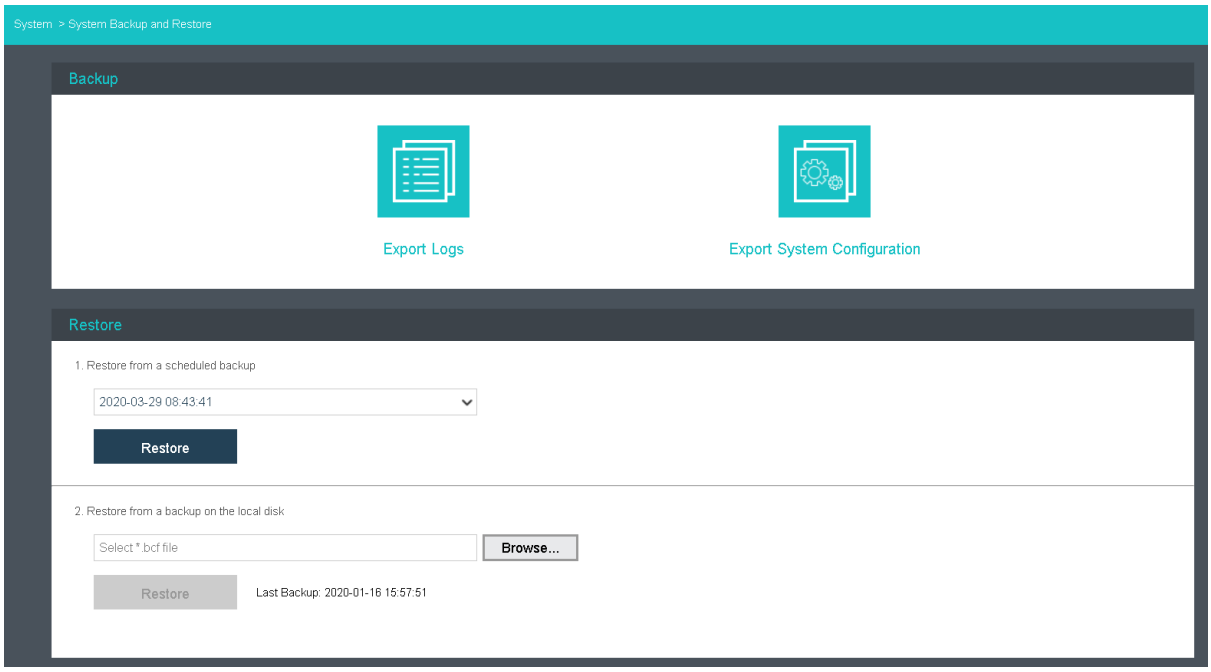
It supports web-based access, on the cluster IP address, which makes VM management more stable. Under normal circumstances, Sangfor HCI GUI is reachable with IP address of any managed node unless the node fails. With cluster IP address, you will never lose control of the management even when one node fails unexpectedly. Sangfor HCI management through cluster IP address improves system stability and reliability dramatically.



Sangfor HCI can communicate with aCMP on the cluster IP address. To use relevant features of aCMP, the following should be configured, **Cluster IP**, **Netmask** and **Cluster Name**, and click **Save** to save the changes.

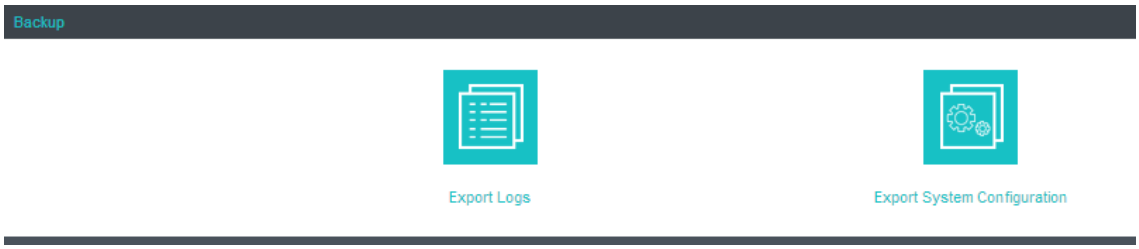
2.6.6 System Backup and Restore

It includes backing up and restoring configurations of system and virtual network devices, and also restoring to factory defaults.



2.6.6.1 System Backup

It includes **Export Logs** and **Export System Configuration,** as shown below:

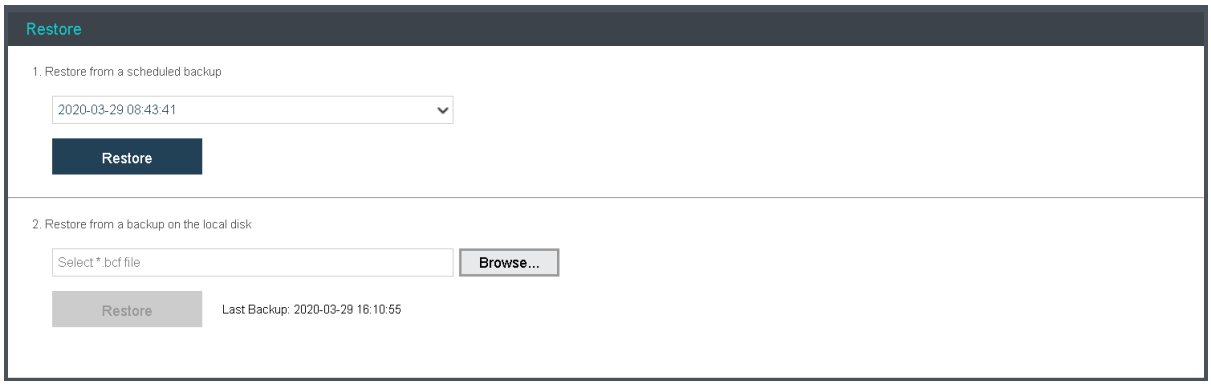


Export Logs: Click to back up logs of specified period and specified nodes onto local disk.

Export System Configuration: Click to back up system configurations.

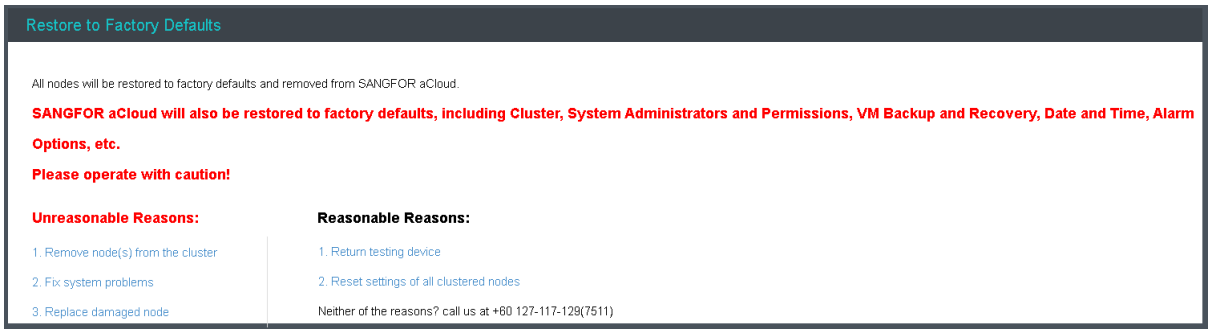
2.6.6.2 System Restore

There are two options, including restoring system settings from a scheduled backup or restoring system settings from backup on the local disk.



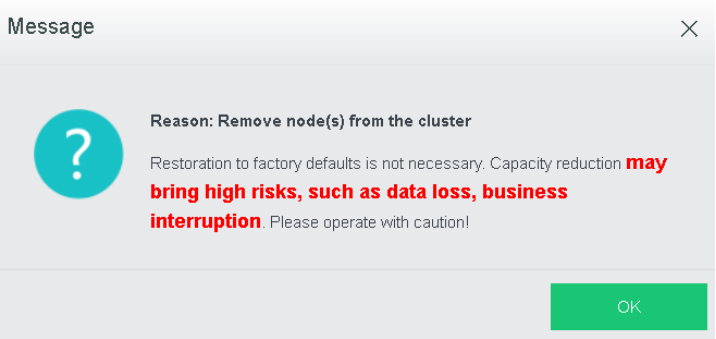
2.6.6.3 Restoring System to Factory Defaults

You may click **Restore to Factory Defaults** to restore Sangfor HCI to its factory defaults. All nodes will be restored to factory defaults and removed from Sangfor HCI. You need to add them again. Sangfor HCI will also be restored to factory defaults, including Cluster Settings, System Administrators and Permissions, VM Backup and Recovery, User Experience Improvement Program, Date and Time, and Alarm Options.

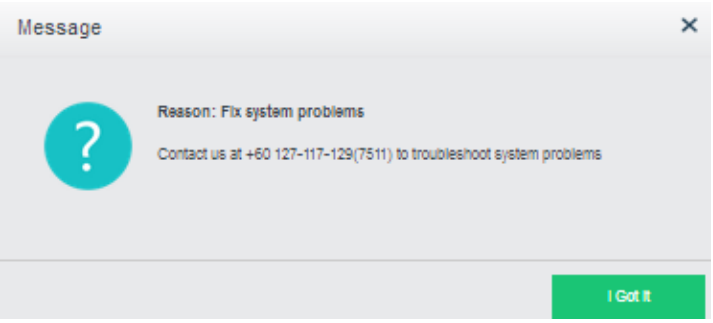


The following are unreasonable reasons for restoration operation:

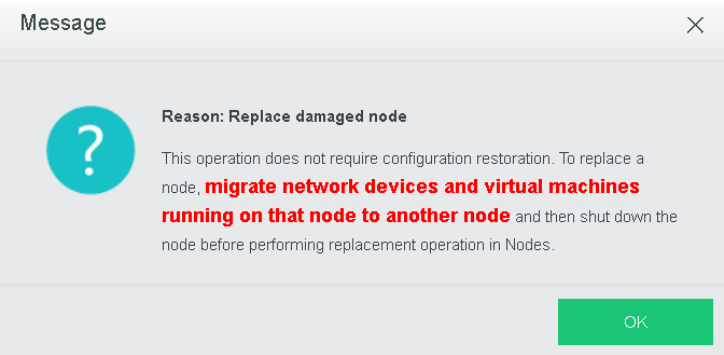
1. Remove node(s) from the cluster



2. Fix system problems



3. Replace damage node

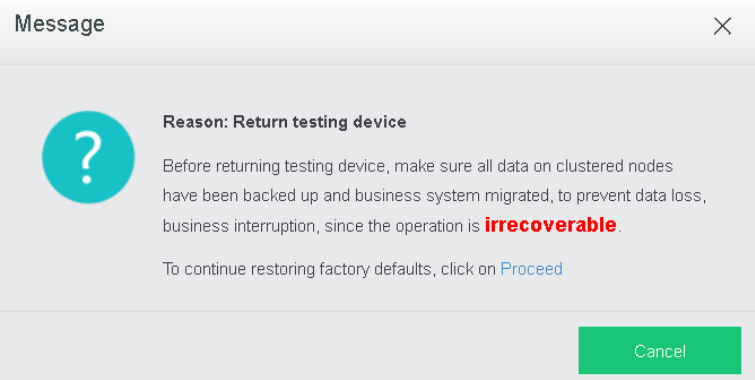


The following are reasonable reasons for restoration operation:

1. Return testing device

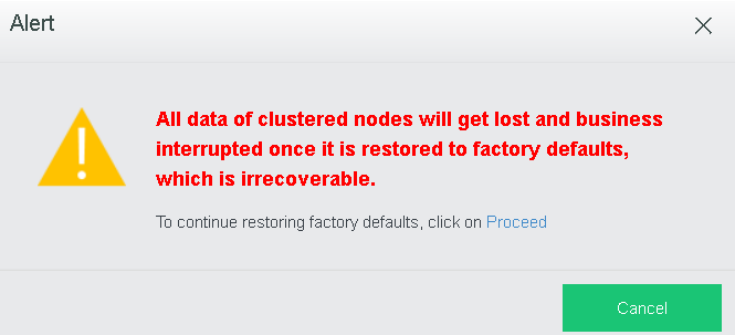
   Before returning testing device, make sure all data on clustered nodes have been backed up and business system has been migrated, to prevent data loss, business interruption, since the operation is not irrevocable. Please operate with caution.

2. Click **Proceed** to restore settings to factory defaults.

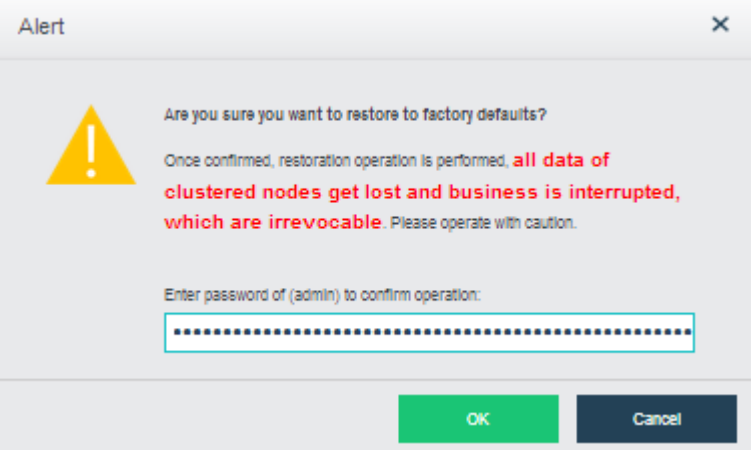


All data of clustered nodes will get lost and business interrupted after this operation which,is irrevocable. Please operate with caution.

3. Click **Proceed** to continue restoring factory defaults.



Click **OK** to start restoring factory defaults. All data of clustered nodes will get lost and business interrupted after this restoration operation, which is irrevocable. Enter password of the current username to confirm operation:

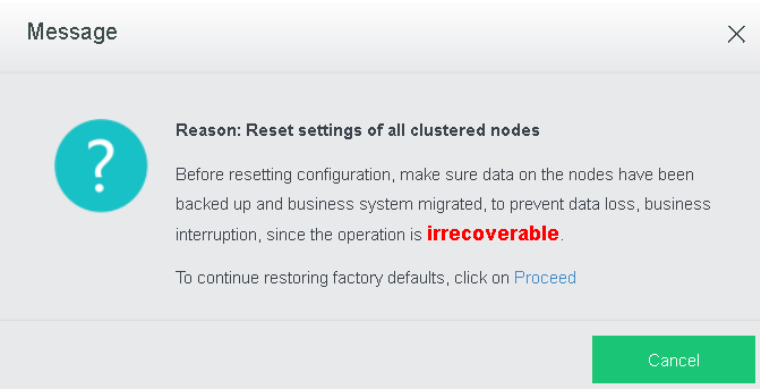


4. Reset cluster settings

Before resetting cluster settings, make sure all data on clustered nodes have been backed

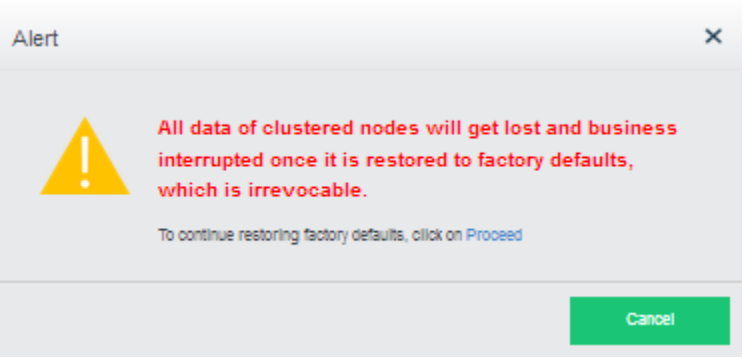
up and business system has been migrated. All data of clustered nodes will get lost and business interrupted after this restoration operation, which is irrevocable.

5. Click **Proceed** to continue restoring factory defaults.

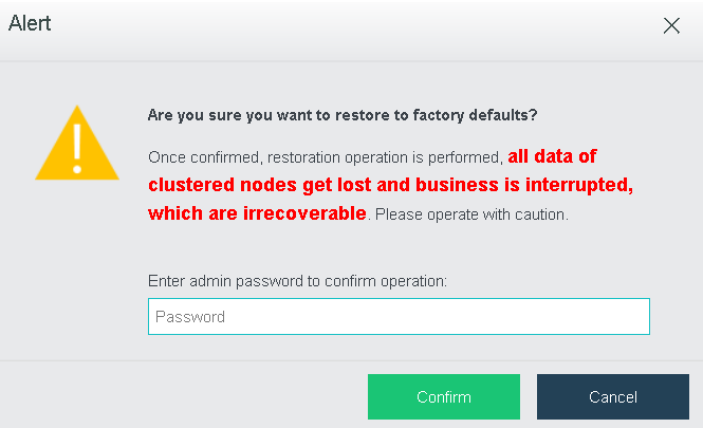


All data of clustered nodes will get lost and business interrupted after this restoration operation, which is irrevocable.

6. To continue restoration operation, click **Proceed** again.



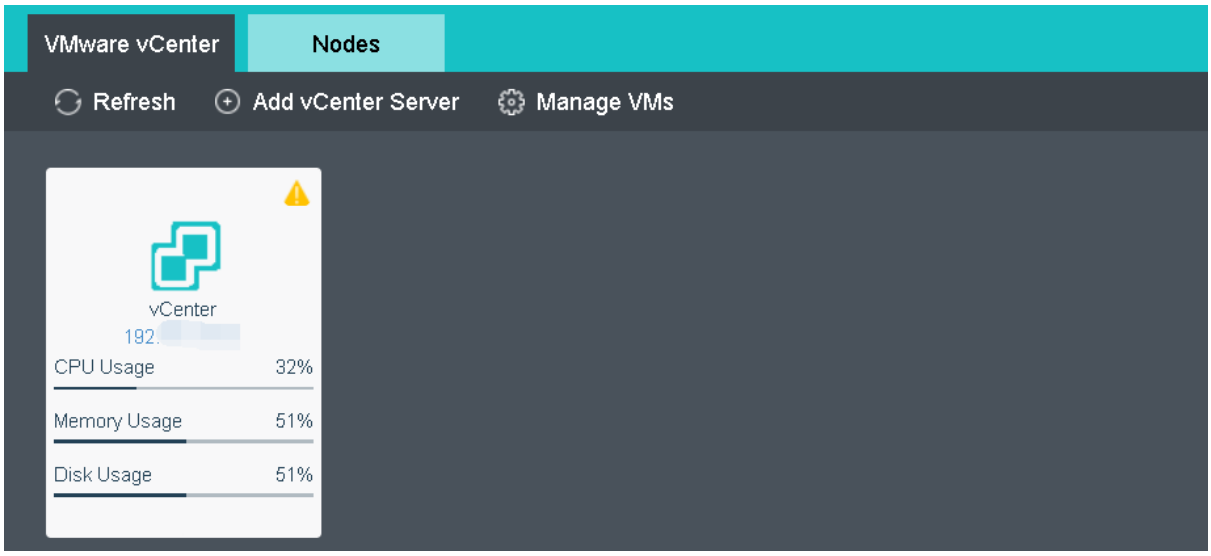
7. Click **OK** to start restoring factory defaults. All data of clustered nodes will get lost and business interrupted after this restoration operation, which is irrevocable. Enter password of the current username to confirm operation:



If you have other reasons, contact us at +60 127-117-129(7511)

2.6.7 VMware vCenter

In **Nodes> VMware vCenter**, there are two tabs, **VMware vCenter** and **Nodes.** vCenter servers can be added, monitored and deleted.

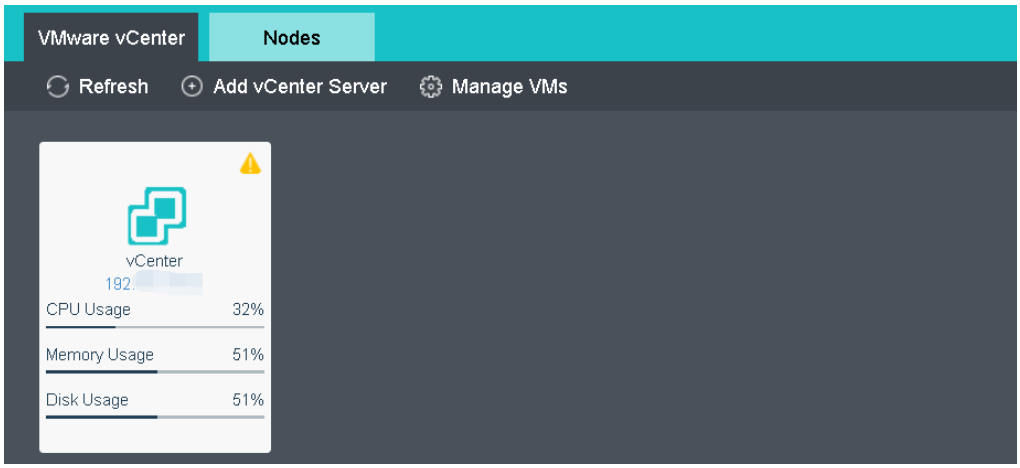


Currently only vCenter server 5.0, 5.1, 5.5, 6.0,6.5 and 6.7can be added.

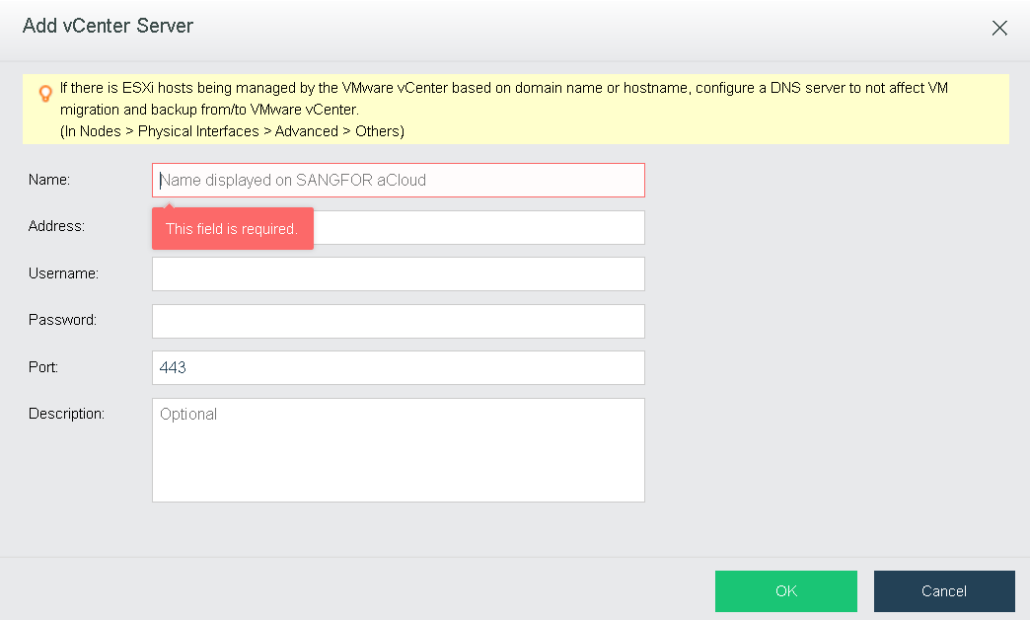
To add a vCenter server, click **Add vCenter Server** to enter the following page and specify **Name, Address, Username, Password, Port and Description**, and then click **OK** to start adding vCenter server and check whether the vCenter server has been added successfully.

2.6.7.1 Adding VMware vCenter

On the **VMware vCenter** tab, it displays the vCenter servers that have been added.

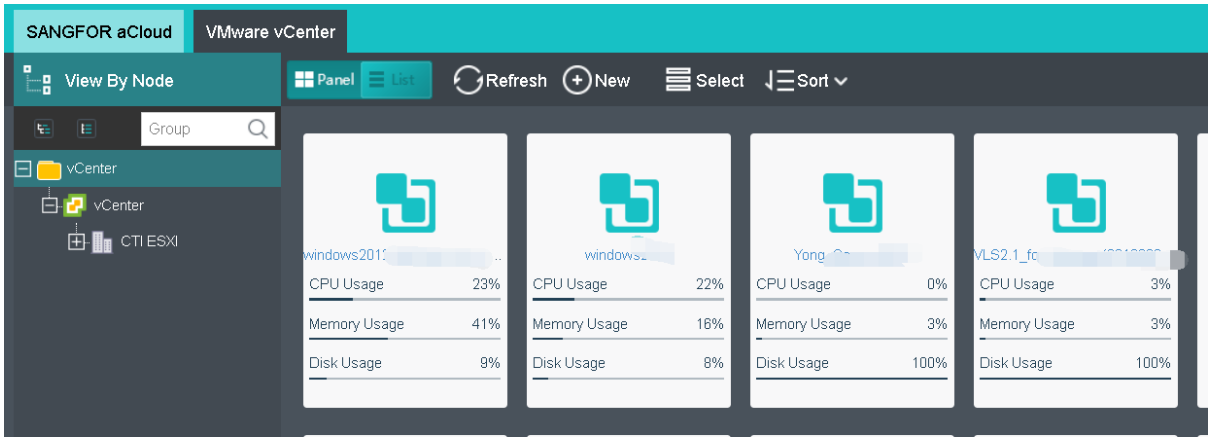


To add a vCenter server, click **Add vCenter Server** to enter the following page and specify **Name, Address, Username, Password, Port and Description**, and then click **OK** to start adding vCenter server and check whether the vCenter server has been added successfully.

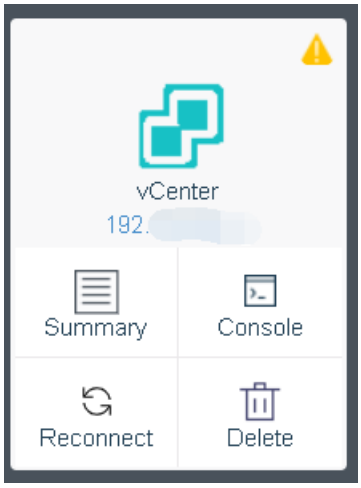


To view VMs running on VMware vCenter server, click **Manage VMs**. For details about those virtual machines, refer to the

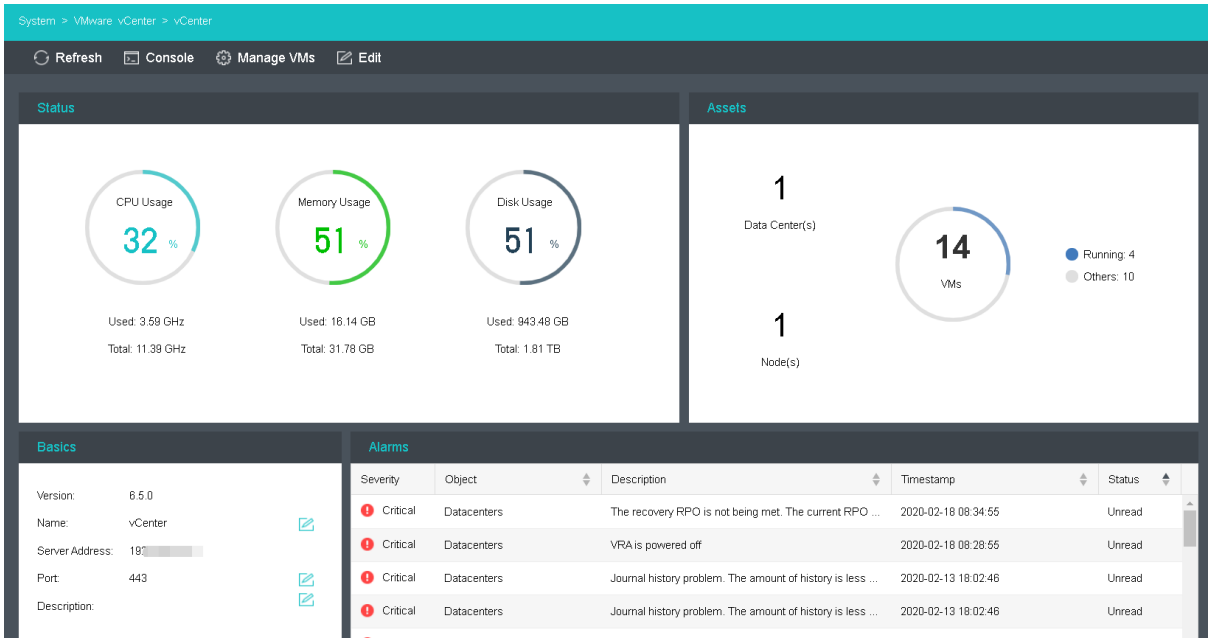
2.2.2 **Managing Virtual Machines in** VMware vCenter section



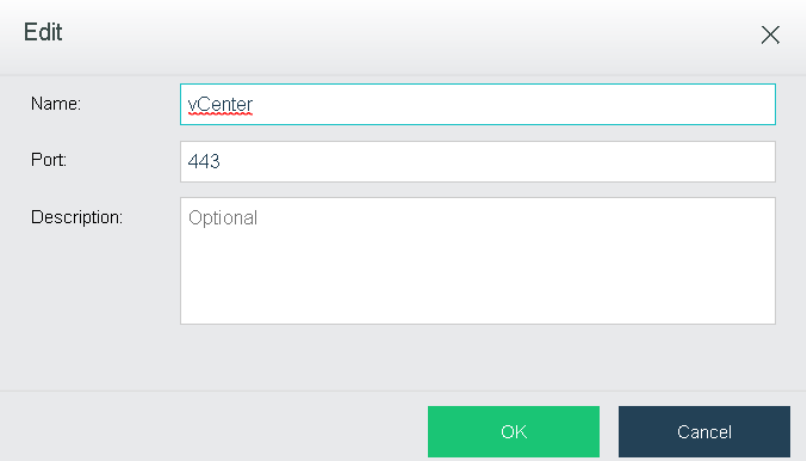
On the **VMware vCenter** tab, you can view detailed information of vCenter servers, enter Web administrator console of VMware vCenter server, reconnect Sangfor HCI platform to vCenter server or delete vCenter server, as shown below:



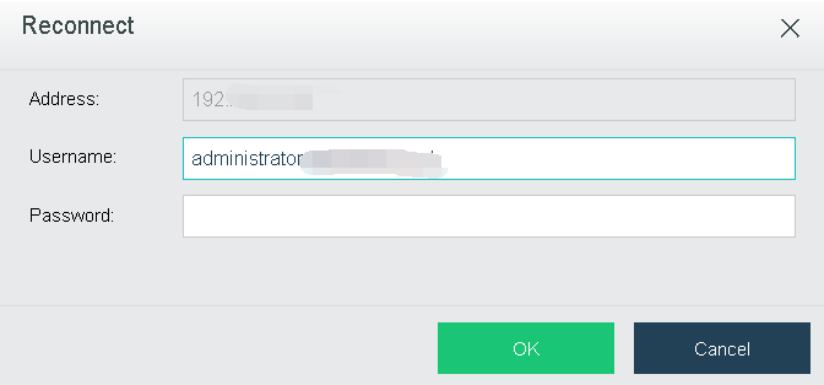
Click on the IP address of a vCenter server or click Summary to enter the **Summary** page, you will see the following information of that vCenter server: status, basics, alarms, etc, as shown below:



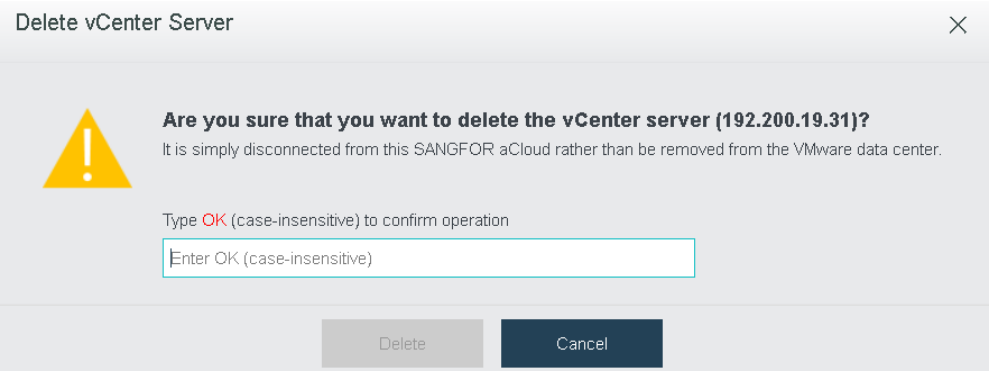
To edit vCenter server's name, port or description, click **Edit**, as shown below:



To reconnect Sangfor HCI to vCenter server, click **Reconnect**, and enter password to start reconnection.



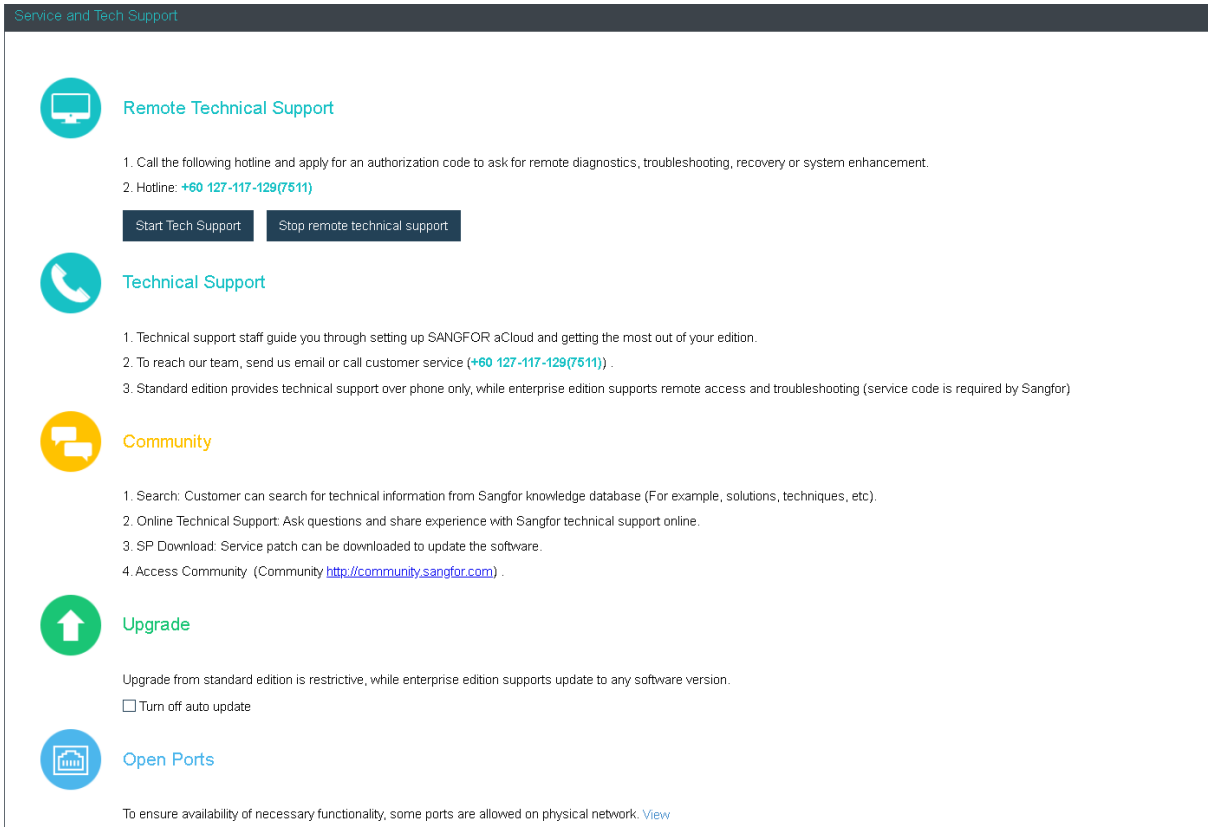
To delete a vCenter server, click **Delete** to remove it from Sangfor HCI platform and disconnect Sangfor HCI from that vCenter server but it will not be removed from the VMware vCenter. Type **OK** to confirm operation.



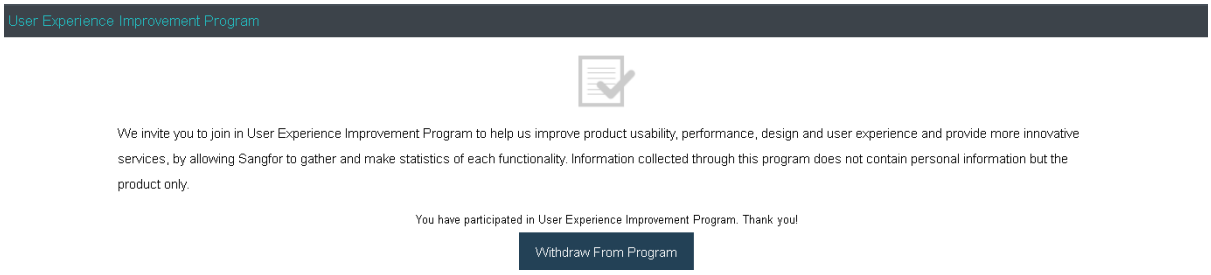
2.6.8 Tech Support & Download

2.6.8.1 Services

Sangfor provides the following services, **Technical Support**, **Community**, **Upgrade**, etc, which are available to both Standard Edition and Enterprise Edition.

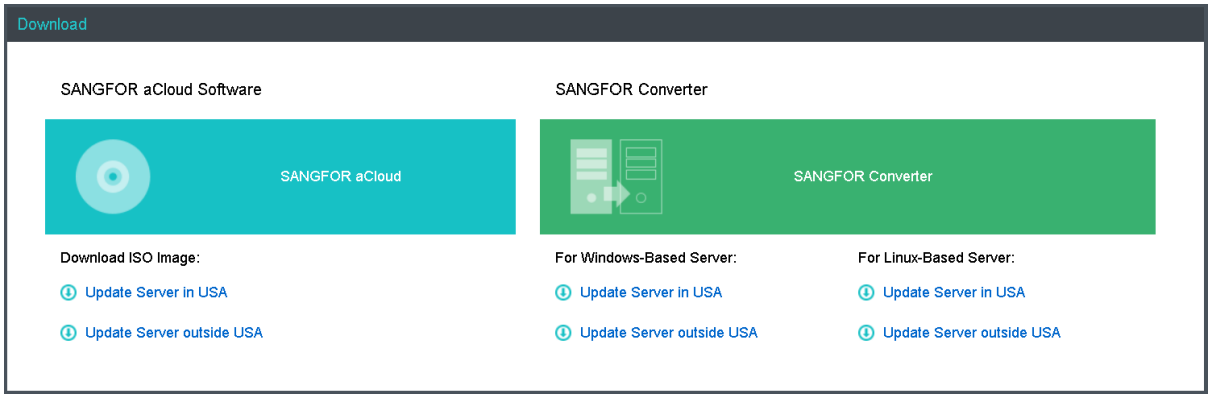


To help us improve product usability and user experience, you can take participate in **User Experience Improvement Program**.



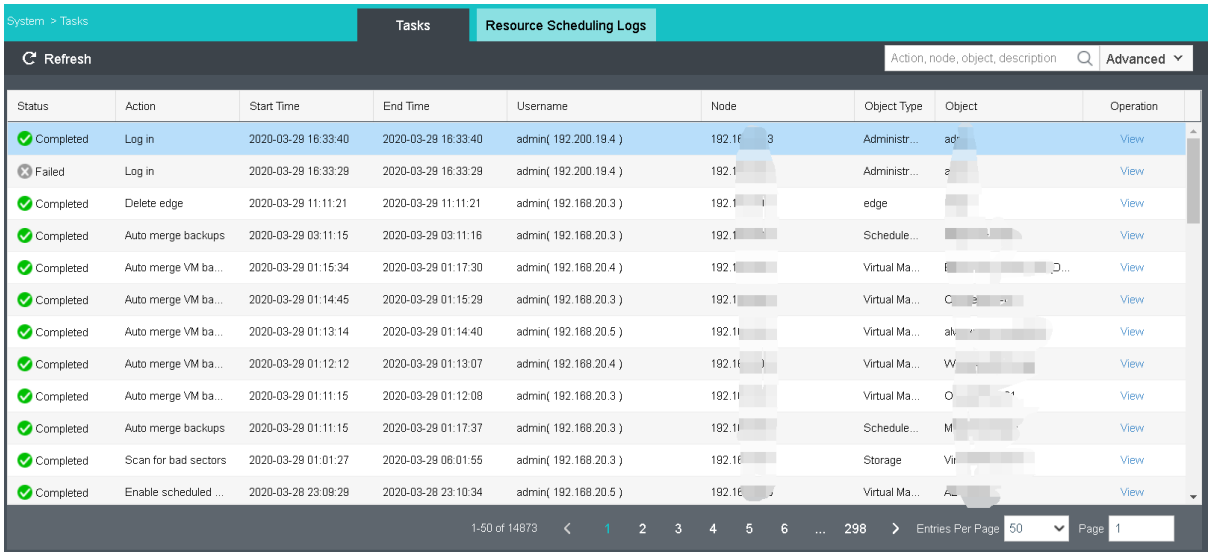
2.6.8.2 Software Download

On the **Download** page, you can download Sangfor HCI software and Sangfor Converter.



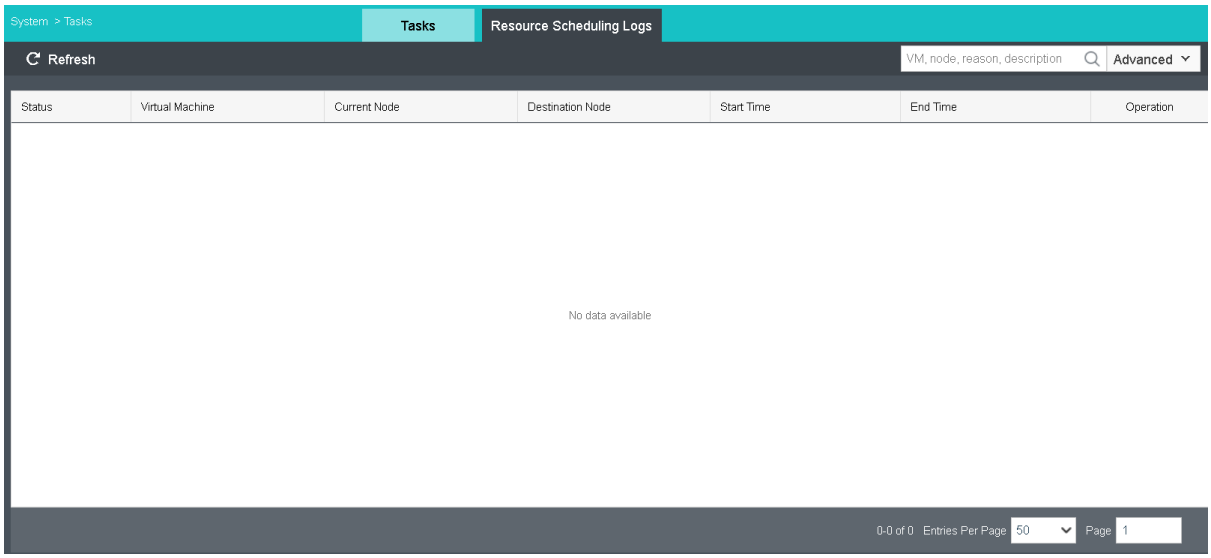
2.6.9 Task

It includes **Tasks** and **Resource Scheduling Logs**.



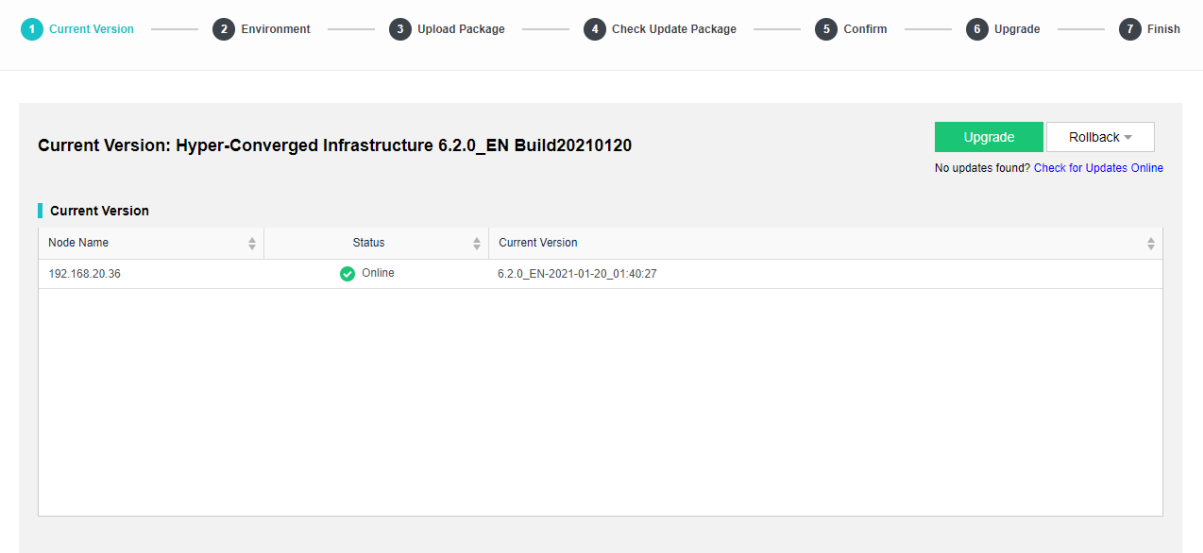
Tasks: It records all kinds of operations, such as creating new VM, etc. Each log contains the following information: **Status, Action, Start Time, End Time, Username, Node, Object Type, Object** and **Operation**. To view log details, click **View** in **Operation** column.

Status:	Completed
Action:	Log in
Start Time:	2020-03-29 16:33:40
End Time:	2020-03-29 16:33:40
Username:	admin(192.200.19.4)
Node:	192.168.20.3
Object Type:	Administrators
Object:	admin
Description:	

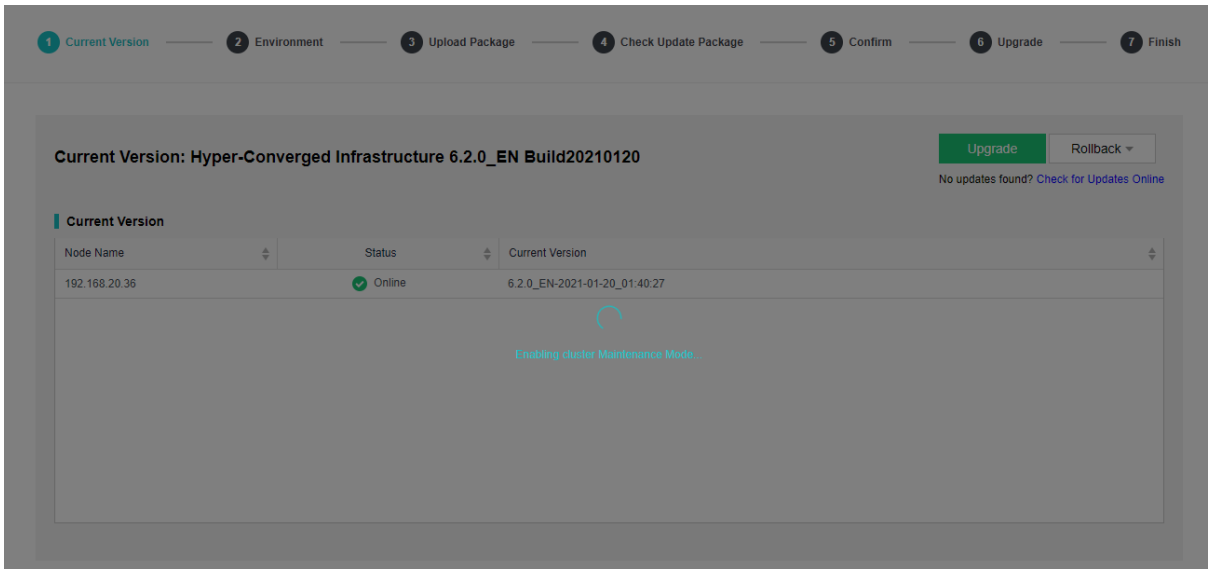


2.6.10 System Upgrade

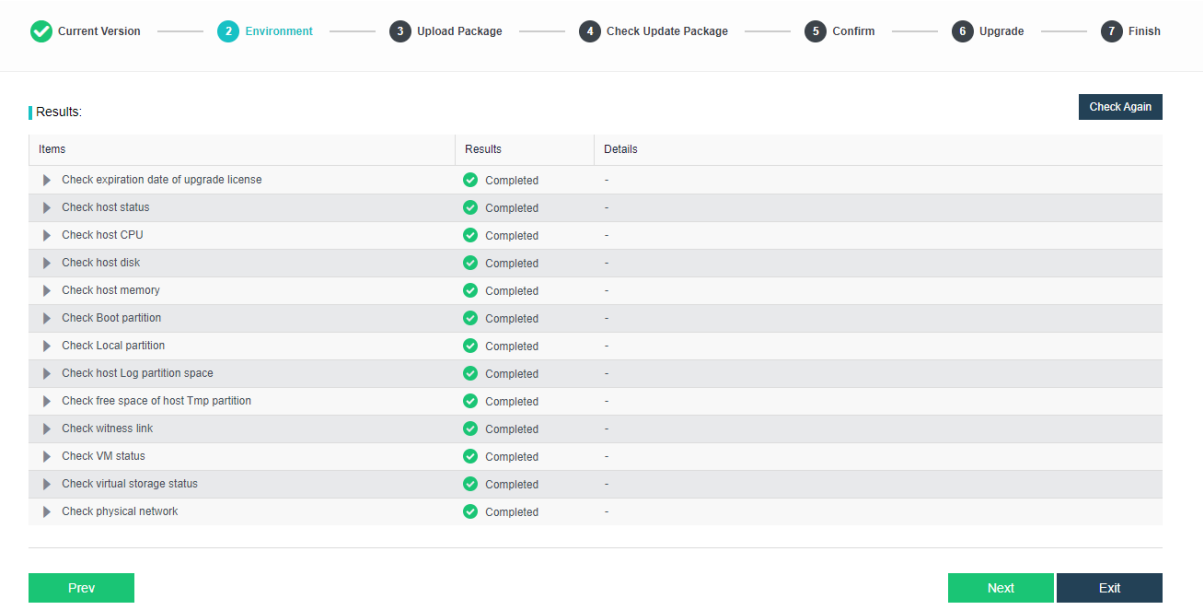
In **System > Upgrade,** you can see the upgrade page as below:



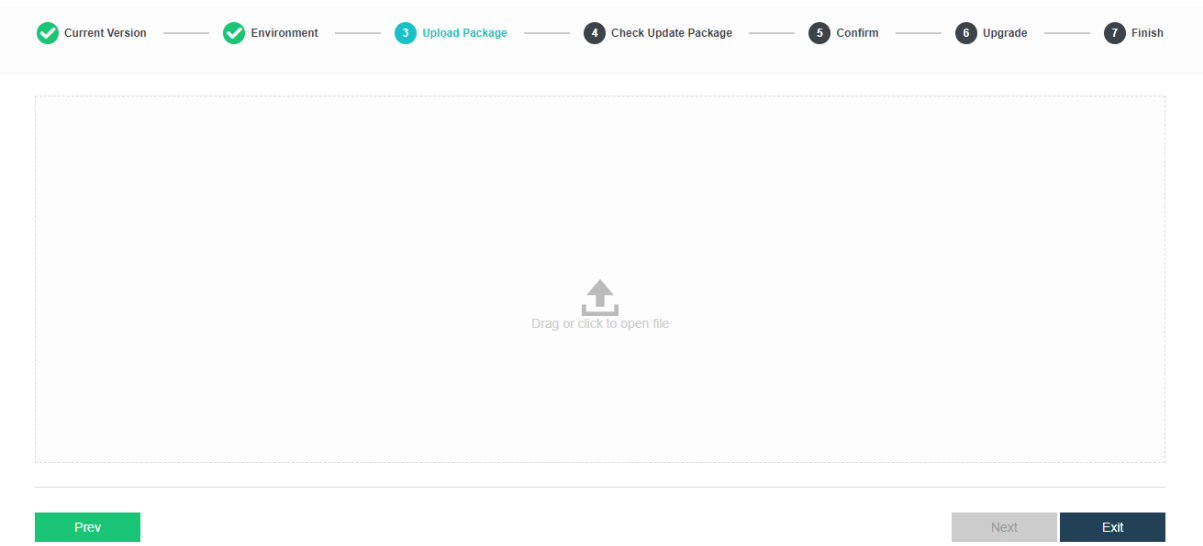
Click Upgrade and the device will enable the maintenance mode automatically as below:



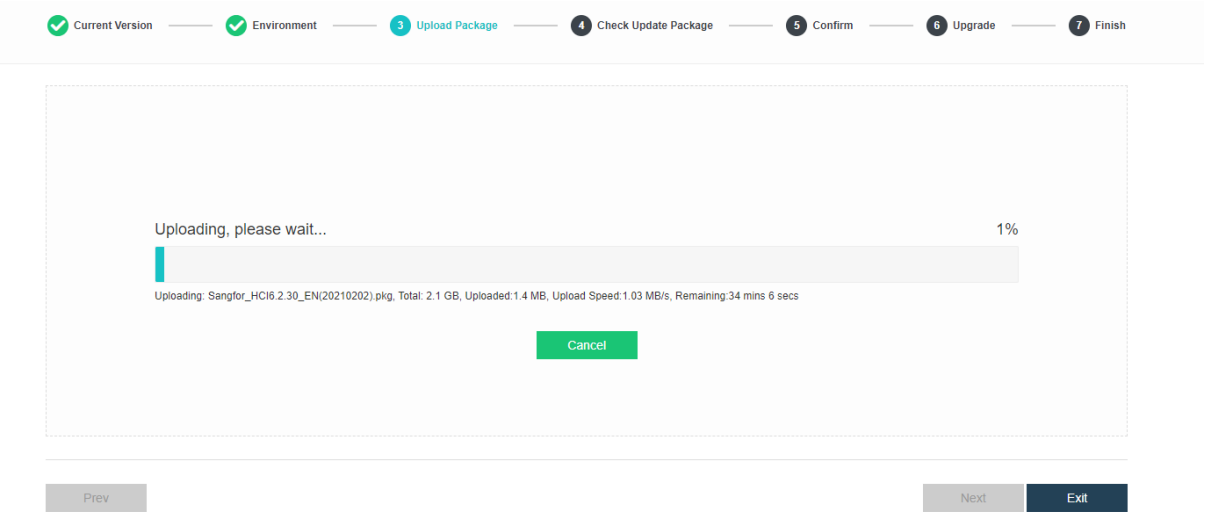
Then, the device will perform checking on the hardware status. If the devive pass all the check, it will display message as below:



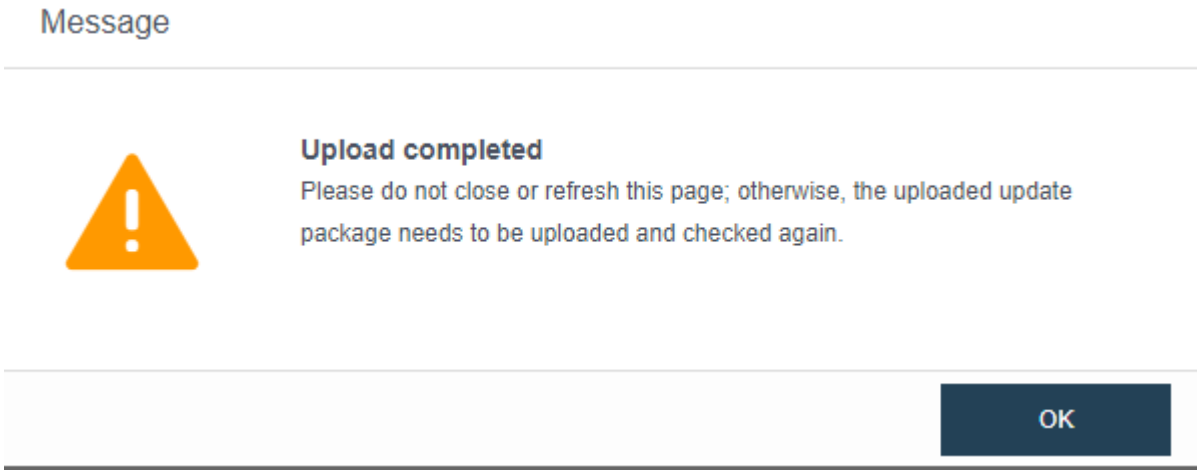
Click 'Next' and enter into the Upload Package page as below:



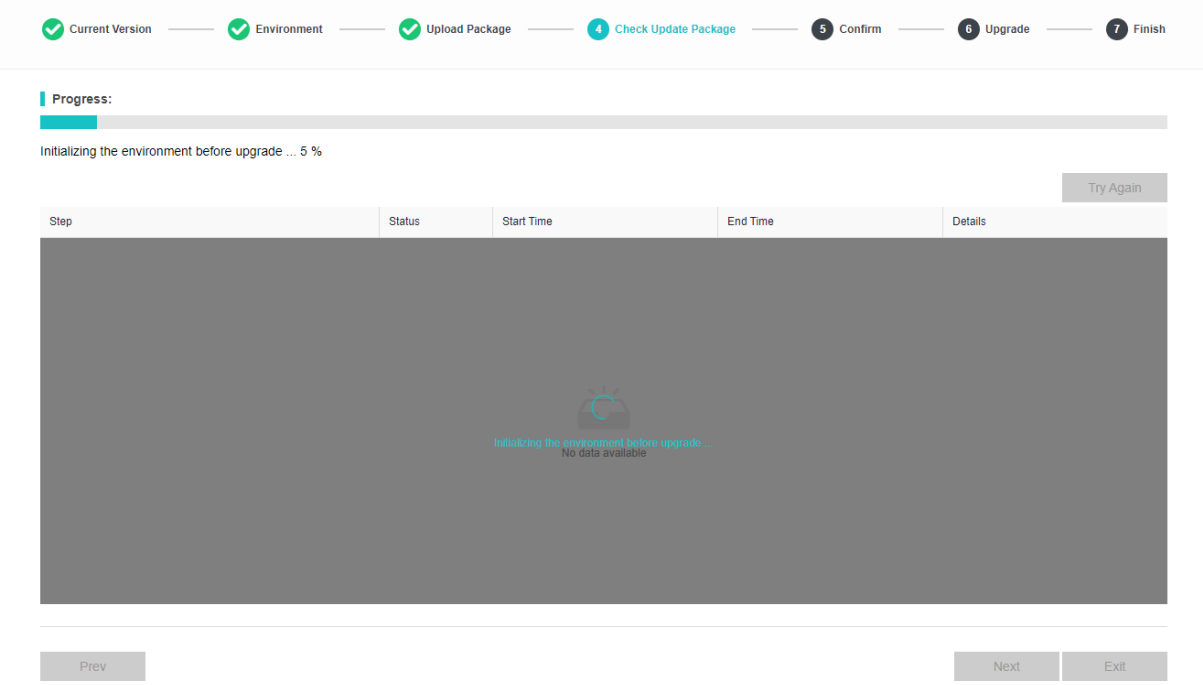
In this step, we can either click on the 'Drag or click open file' to upload the upgrade package, or directly drag and drop the file into the provided space:



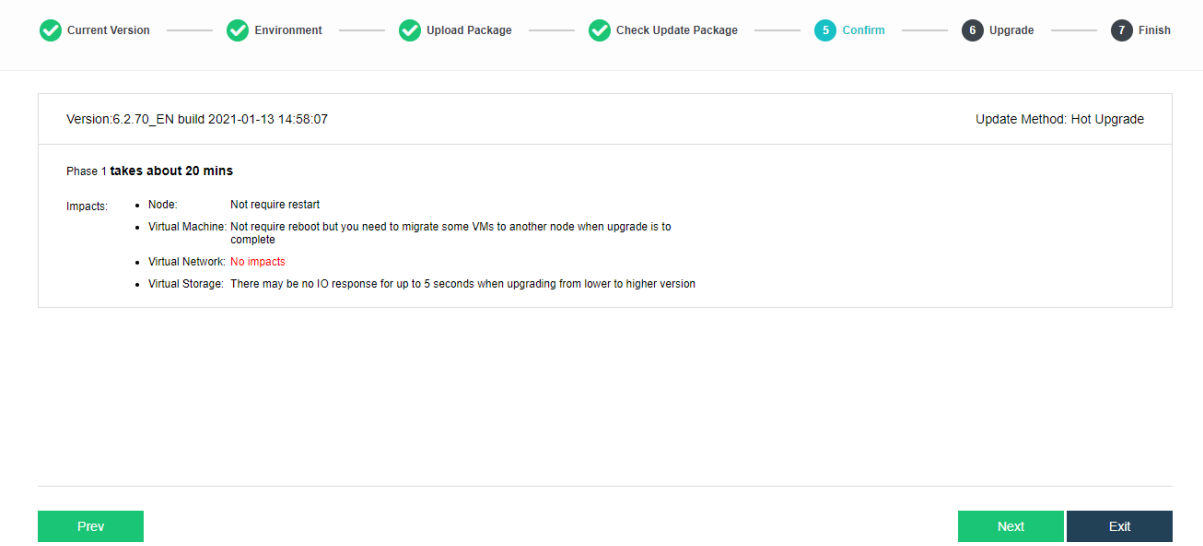
After upload completed, click OK and proceed to next step.



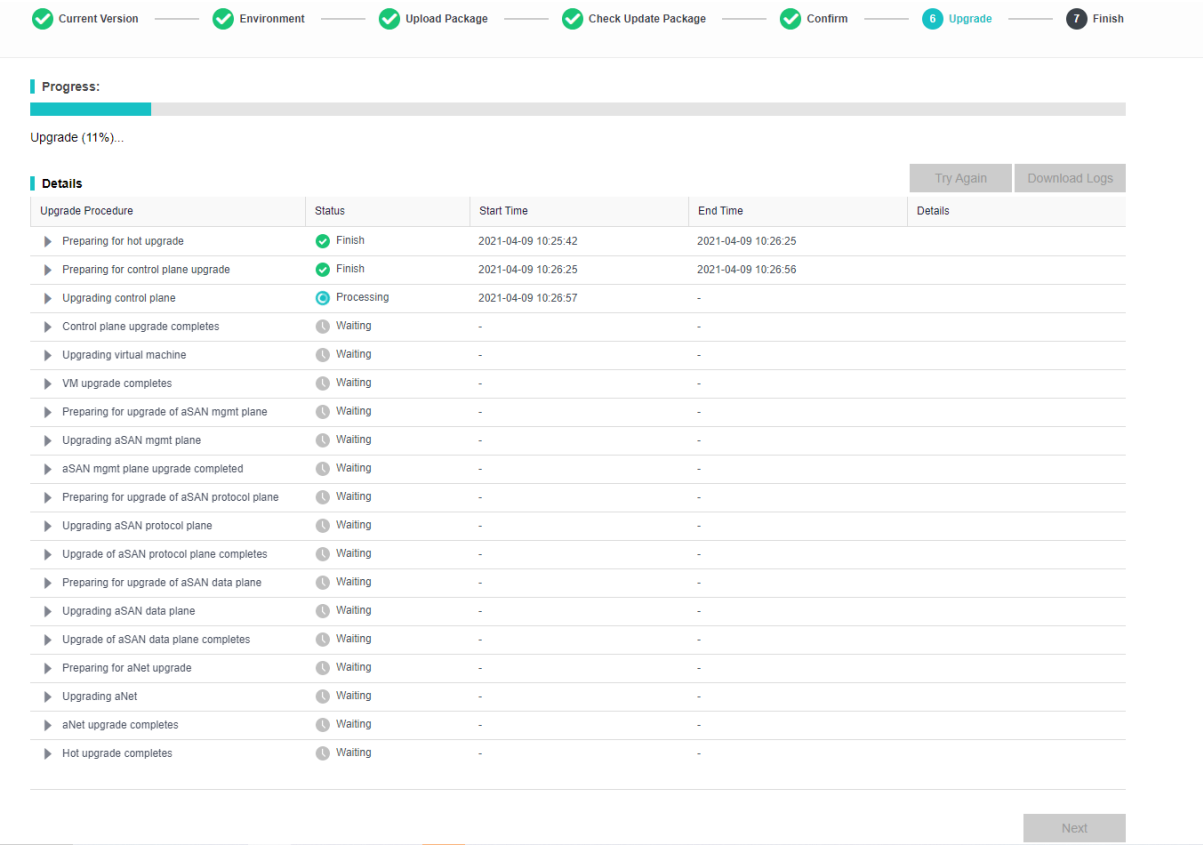
Click **Next** and then HCI will do initializing checking on the package.



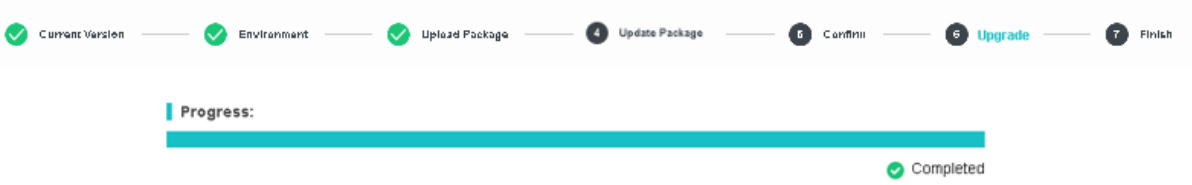
After the package done checking, the upgrade impact will be show.



It will begin the upgrade and the page will display as below:

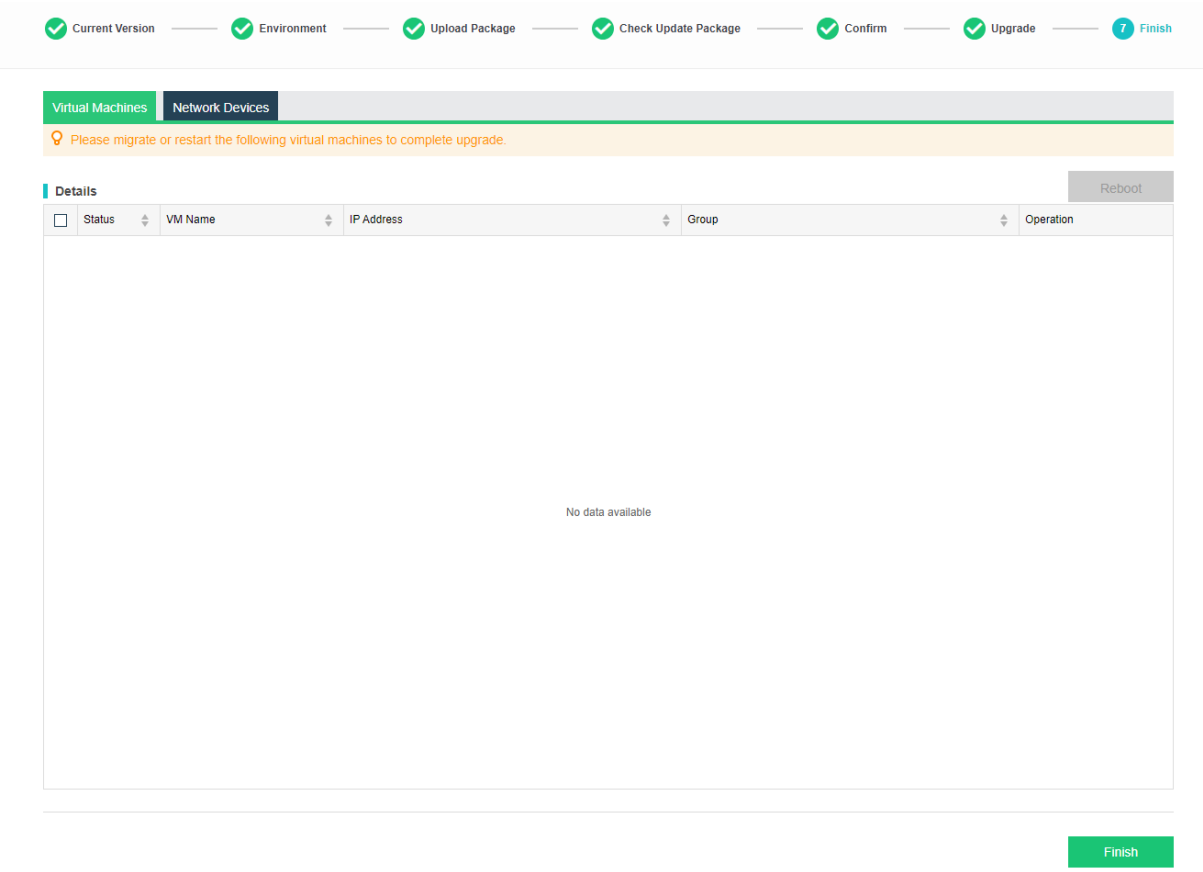


It will take some times for the device to finish upgrade:



After upgrade completed, click Next.

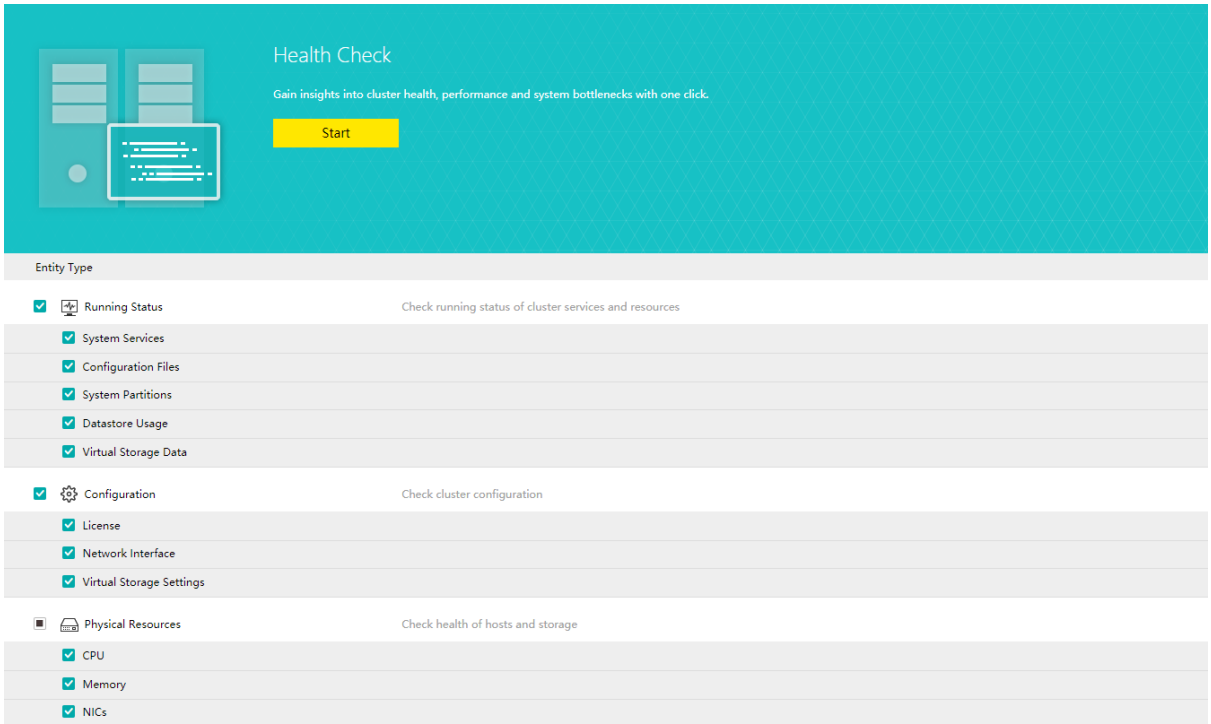
Click Finish to quit from maintenance mode and upgrade.



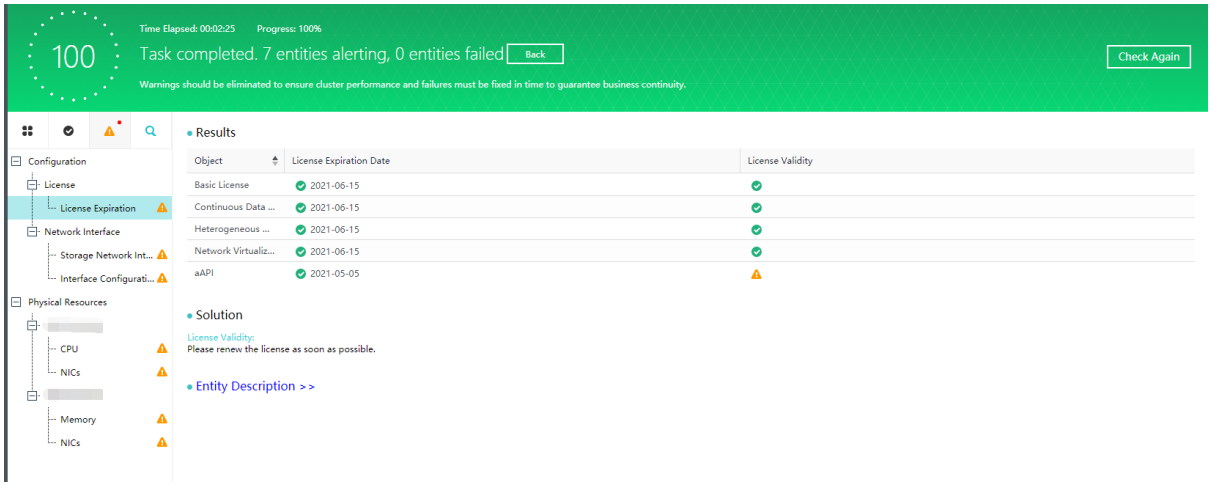
2.6.11 Cluster Health Check

It enables you to gain insight into cluster health and operating status, and help you locate specific problems (related with hardware, platform or business), and offers solutions, so as to ensure that Sangfor HCI platform operates properly and to achieve easy maintenance.

Types of entities to be detected are **Running Status, Configuration** and **Physical Resources**.



After health check completes, you will see the score and results.



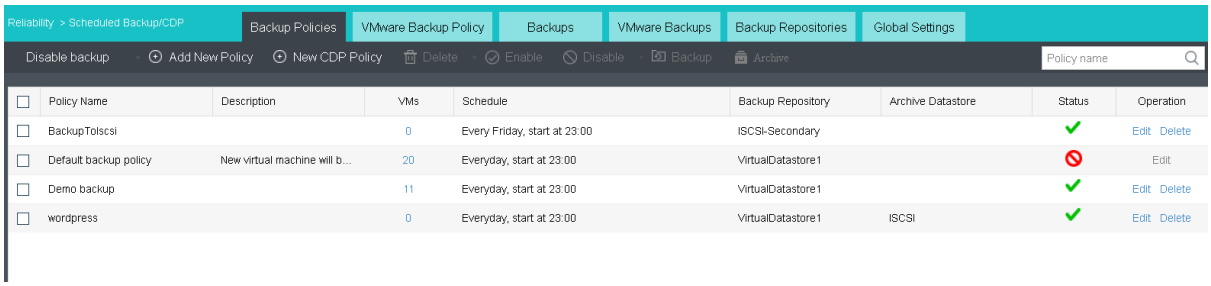
If there is something wrong with storage, the specific issue will be detected, and the corresponding solution will also be offered.

2.6.12 VM Backup and Recovery

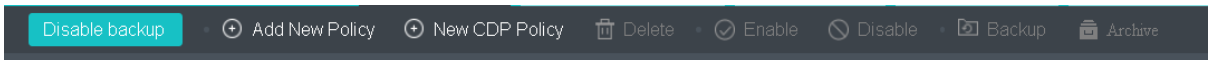
In this Internet era, data has become the first productivity and data security has gained more and more attention. Data loss or data damage, no matter due to human behaviors or natural disaster, will bring about immeasurable loss to enterprises. Therefore, restoring data from data replicas in the case of data loss becomes more important. On Sangfor HCI platform, the first backup is a full copy of data and the successive backups are incremental backups in which successive copies of the data contain only that portion that has changed since the preceding backup copy was made, which backs up less amount of data, occupies less space, and speeds up backup process as well. When a full recovery is needed, the restoration process needs the last full backup plus all the incremental backups until the point of restoration. Incremental backups are desirable as they reduce storage space usage, and are quicker to perform.

2.6.12.1 Sangfor Backup Policy

With scheduled backup policy, virtual machines can be automatically backed up during specified period of time.



On the toolbar, there are **Enable/Disable backup**, **New Backup Policy**, **New CDP Policy**, **Delete**, **Enable**, **Disable** and **Backup**, as shown below:



Enable/Disable backup: To enable or disable backup, click **Enable backup** to enable backup or **Disable backup** to disable backup.

New Backup Policy: To add a new backup policy, click **New Backup Policy**. For details, refer to **2.6.12.1.1 Adding New Backup** Policy section.

To add a new CDP policy, click **New CDP Policy**. For details, refer to **2.6.12.1.2 Adding New CDP** Policy section.

To delete backup policy, select the policy you want to delete and click **Delete**.

Enable: To enable a backup policy, click **Enable**, or click on the icon.

To disable a backup policy, click **Disable**, or click on the icon .

To manually execute a backup policy, select a policy and click **Backup**.

To archive the backup to another backup repository, select the policy and click on **Archive**.

To search for a backup policy, enter the policy name in the search box Policy name .

On the **Backup Policy** tab, it displays policy name, description, the number of virtual machines to be backed up, backup repository, backup period, status and operation, as shown below:

Policy Name	Description	VMs	Schedule	Backup Repository	Archive Datastore	Status	Operation
BackupToIscsi		0	Every Friday, start at 23:00	ISCSI-Secondary			Edit Delete
Default backup policy	New virtual machine will b...	20	Everyday, start at 23:00	VirtualDatastore1			Edit

Policy Name: Displays name of Sangfor backup policy.

Description: Displays descriptive information of Sangfor backup policy.

VM(s): Displays the number of virtual machines to be backed up. To view the virtual machines, click on the number under **VM(s)**.

Backup Repository: Displays backup repository.

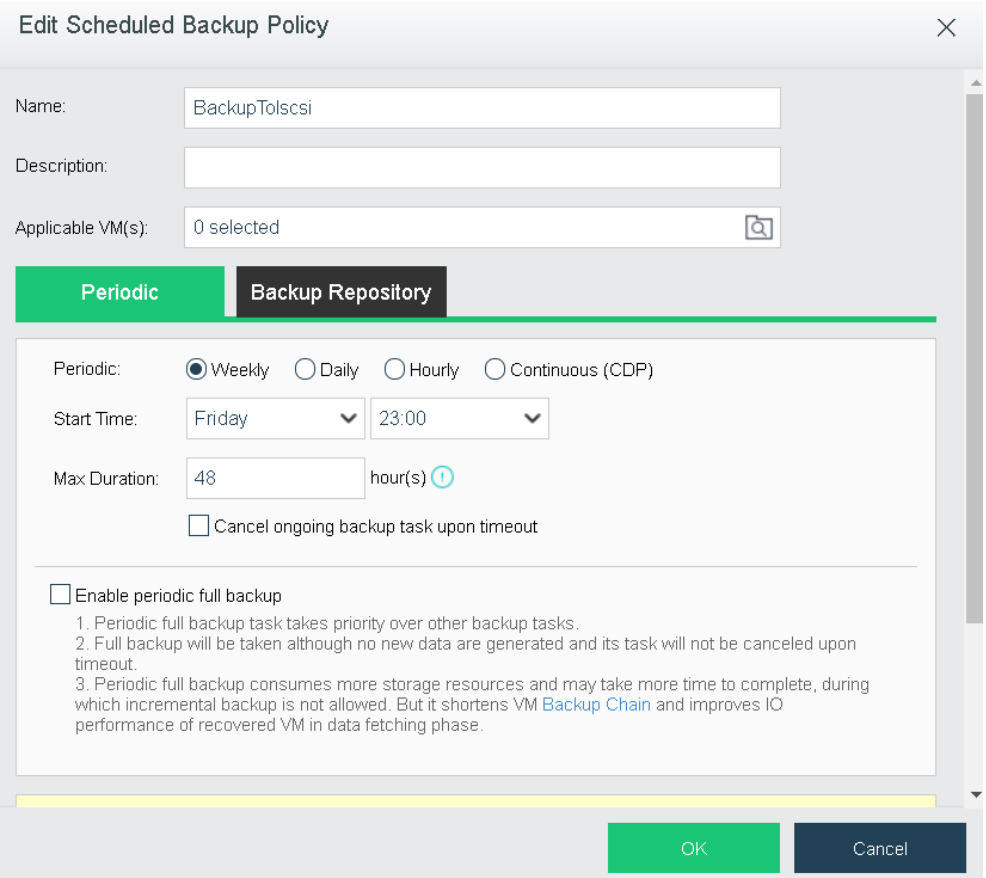
Schedule: Displays backup period.

Archive Datastore: Display the datastore to store the archive backup.

Status: Displays status of the backup policy, enabled or disabled. To enable a backup policy, click on the icon. To disable backup policy, click on the icon.

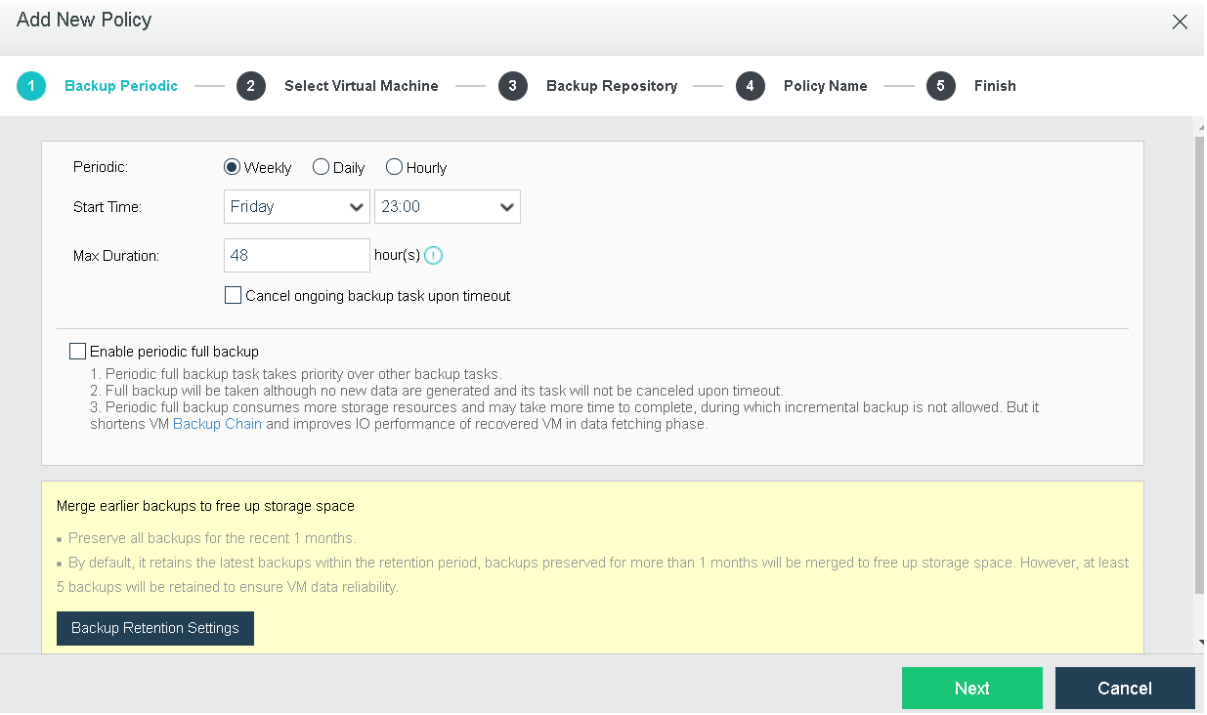
Operation: To edit or delete a backup policy, click **Edit** or **Delete** under **Operation**. The default scheduled backup policy cannot be deleted.

To edit a backup policy, click **Edit** and enter the following page:



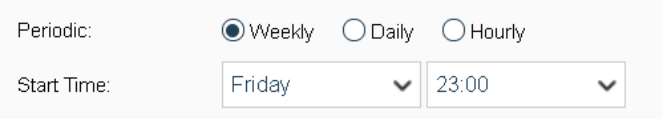
2.6.12.1.1 Adding New Backup Policy

To add a new backup policy, click **New Backup Policy**, and then follow the wizard to specify backup periodic, select virtual machine, specify backup repository and policy name, as shown below:

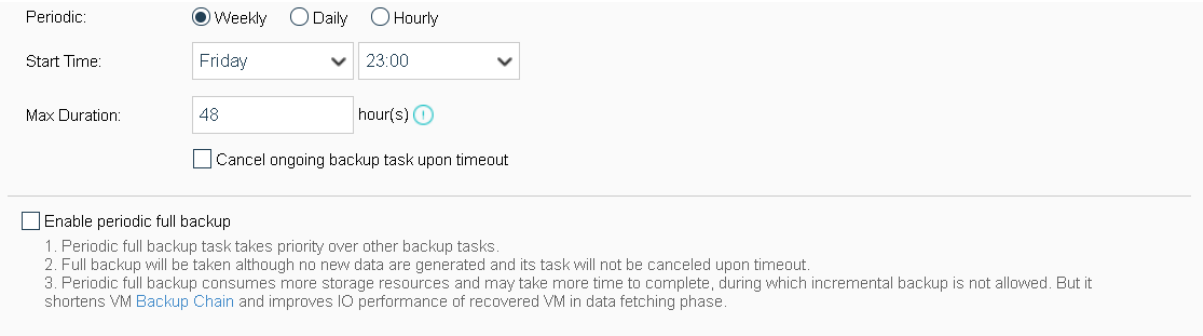


1. Specify **Backup Periodic.**

   Backup periodic can be on weekly basis, daily basis and hourly basis. A**utomatic backup cleanup** can be selected to have backups deleted automatically.



Weekly: Select **Weekly** and configure as follows:

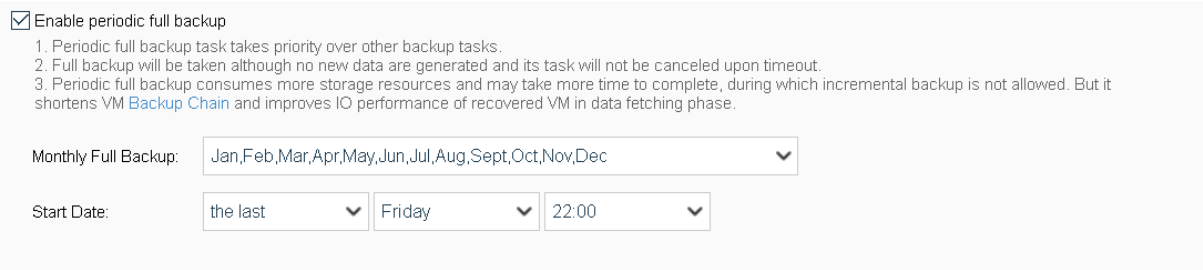


On weekly basis: Options are from **Sunday** to **Saturday**.

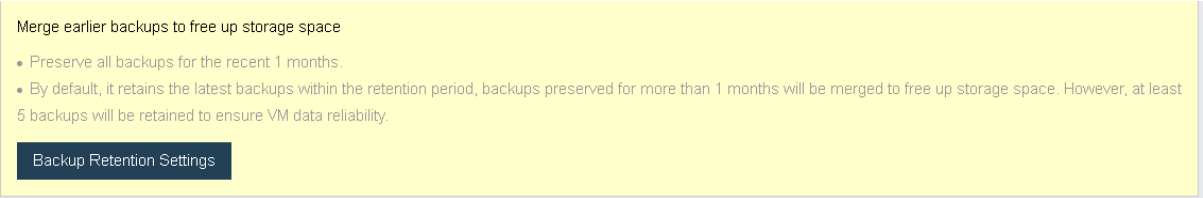
Start Time: It specifies time to start backup. Since backup may bring impacts to system service, select a period that service is not busy.

Max Duration: It specifies the longest period that the backup operation can last. New backups only occur within this time range and will not stop once starts. However, the backup tasks having not started yet will resume when the time range arrives again. You may select **Cancel ongoing backup task upon timeout** based on your own needs.

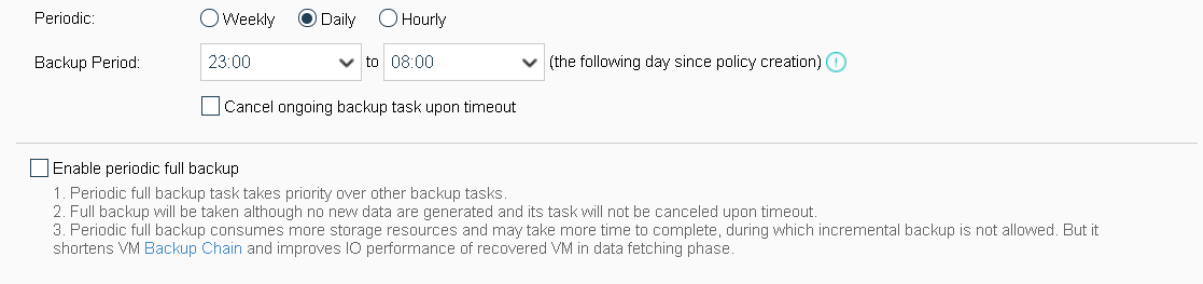
Enable periodic full backup: Full backup will be created periodically on the specific time and date instead of only incremental backup created.



Backup Retention Setting: It specifies the longest period that backups will be kept. The longest period is three months.

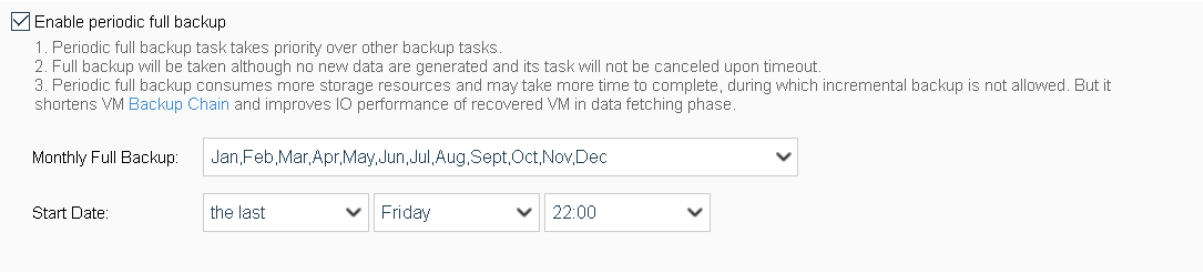


Daily: To have data backed up on daily basis, choose Daily for Periodic, as shown below:

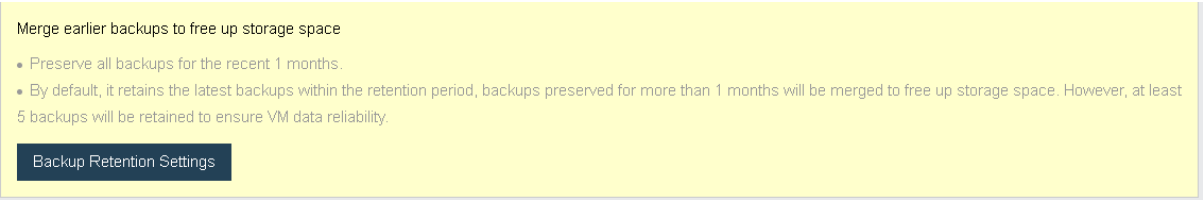


Backup Period: It specifies the longest period that the backup operation can last. New backups only occur within this time range and will not stop once starts. However, the backup tasks having not started yet will resume when the time range arrives again. You may select **Cancel ongoing backup task upon timeout** based on your own needs.

Enable periodic full backup: Full backup will be created periodically on the specific time and date instead of only incremental backup created.

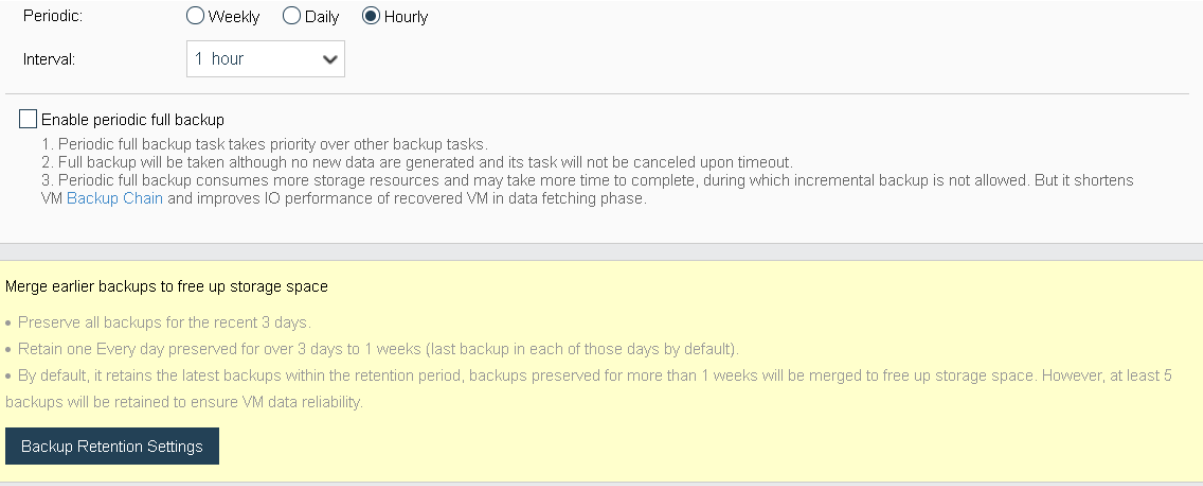


Backup Retention Setting: It specifies the longest period that backups will be kept. The longest period is three months.



You may enable Automatic backup cleanup to automatically preserve all the backups for the previous 3 days, one backup (the last one) for the earlier week and one backup for each of the even earlier weeks (the one created on Sunday only).

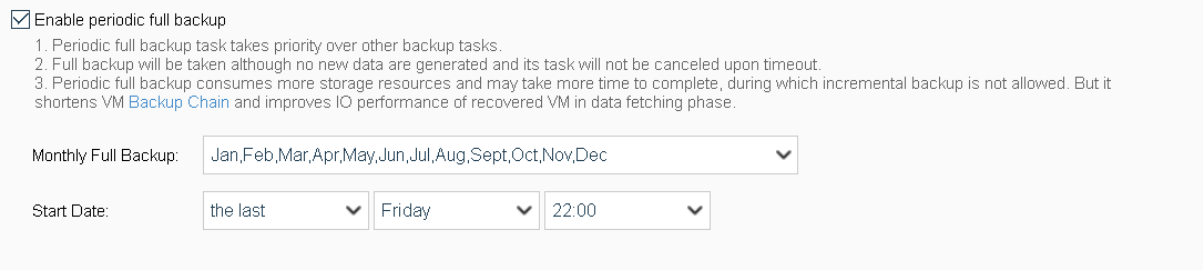
Hourly: To have data backed up on hourly basis, select **Hourly** as **Periodic,** as shown below:



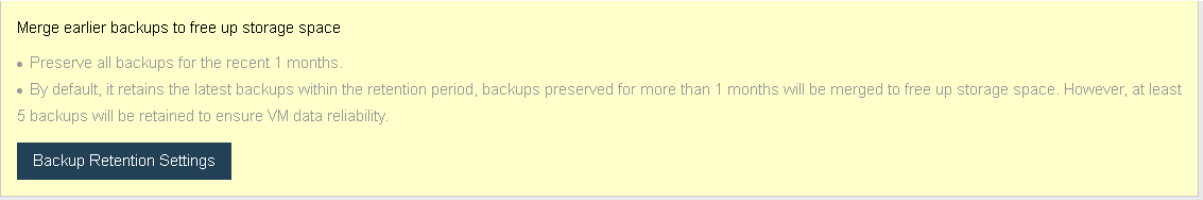
Interval: The minimum interval is 1 hour.

Enable periodic full backup: Full backup will be created periodically on the specific time and

date instead of only incremental backup created.



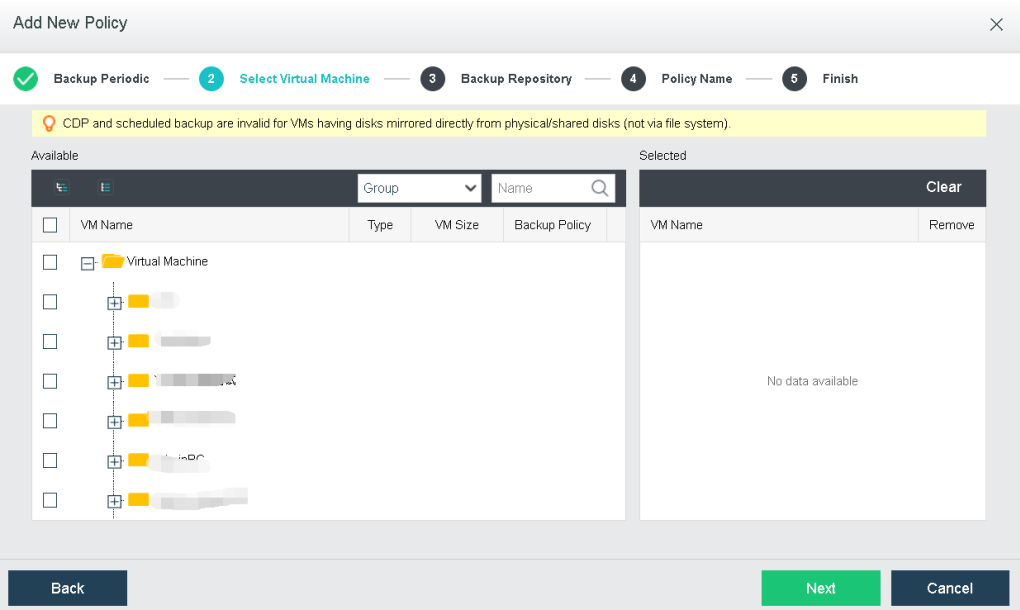
Backup Retention Setting: It specifies the longest period that backups will be kept. The longest period is three months.



You may enable **Automatic backup cleanup** to automatically preserve all the backups for the previous 3 days, one backup (the last one) for the earlier week and one backup for each of the even earlier weeks (the one created on Sunday only).

2. Select virtual machine(s).

   Select the virtual machine(s) you want to back up. You may view the virtual machines by **Group**, **Node**, **Datastore** or select **All** to view all the virtual machines, or you may enter the name of the virtual machine in the search box to search for a specific virtual machine. Select virtual machines under **Available** and then the selected virtual machines will be added to the **Selected** list on the right, as shown below:



Clear: To clear the selected virtual machines, click '**Clear**'.

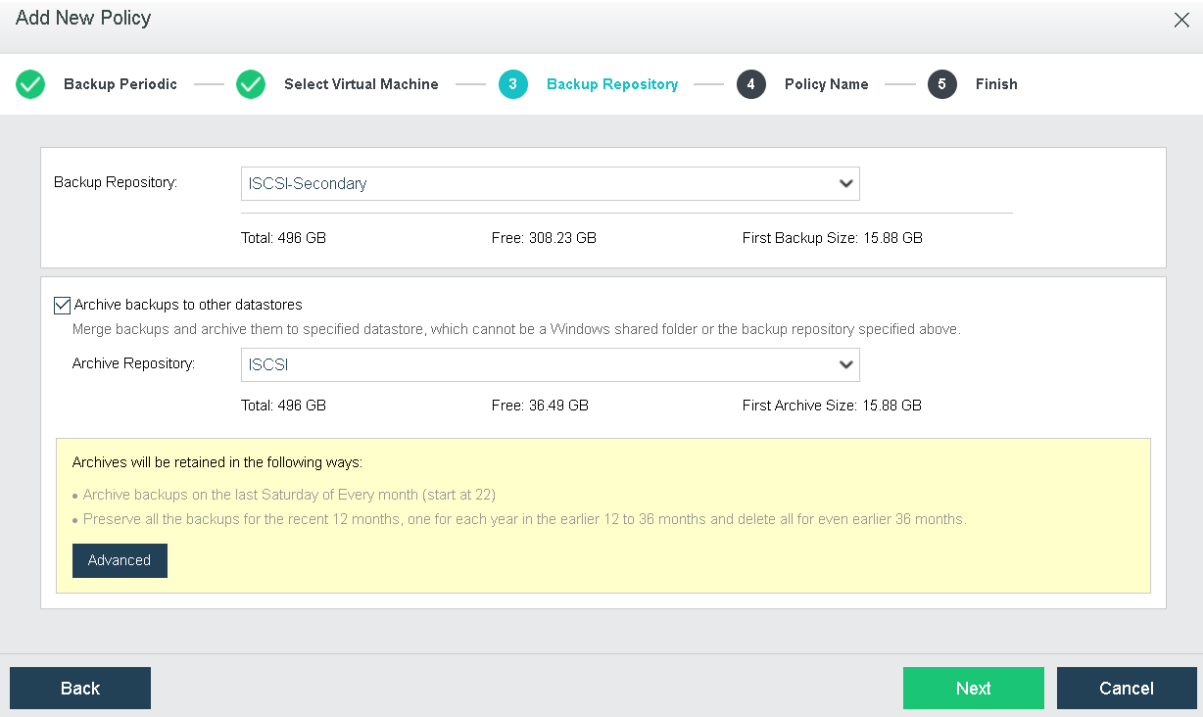
To remove a virtual machine from the selected list, click

CDP or data protection is not applicable to virtual machines having disks mapped directly from physical or shared disks, rather than via file system.

One virtual machine cannot be associated with more than one backup policy. If the virtual machine is associated with a new policy, it will be removed from the previous policy.

---

3. Specify backup repository to store virtual machine backups, as shown below:

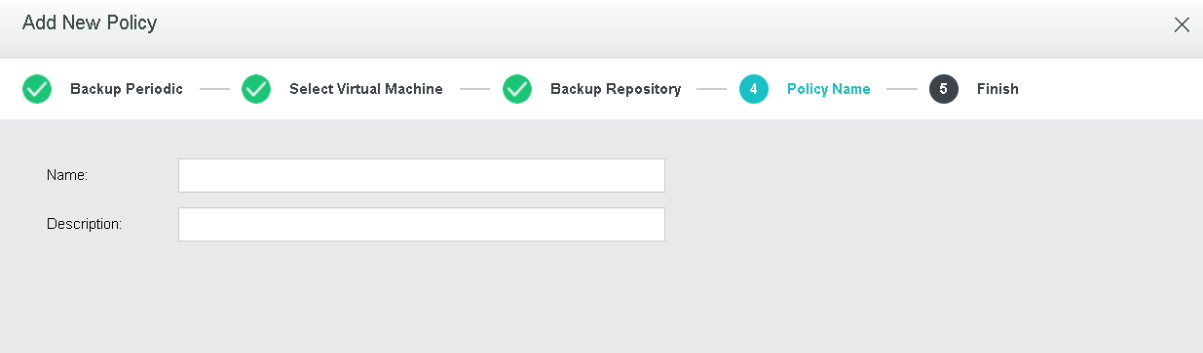


Backup Repository: It specifies backup repository, you may select an existing datastore or choose to add a new Windows shared folder. Once the backup repository is specified, total capacity, available backup repository size and first backup size of the selected data store will be displayed.

Archive backup to other datastore: Specifies a repository to store the archive backup.

Note that next backup will have all data backed up if backup repository is changed, please operate with caution.

4. Specify a name for the new backup policy.

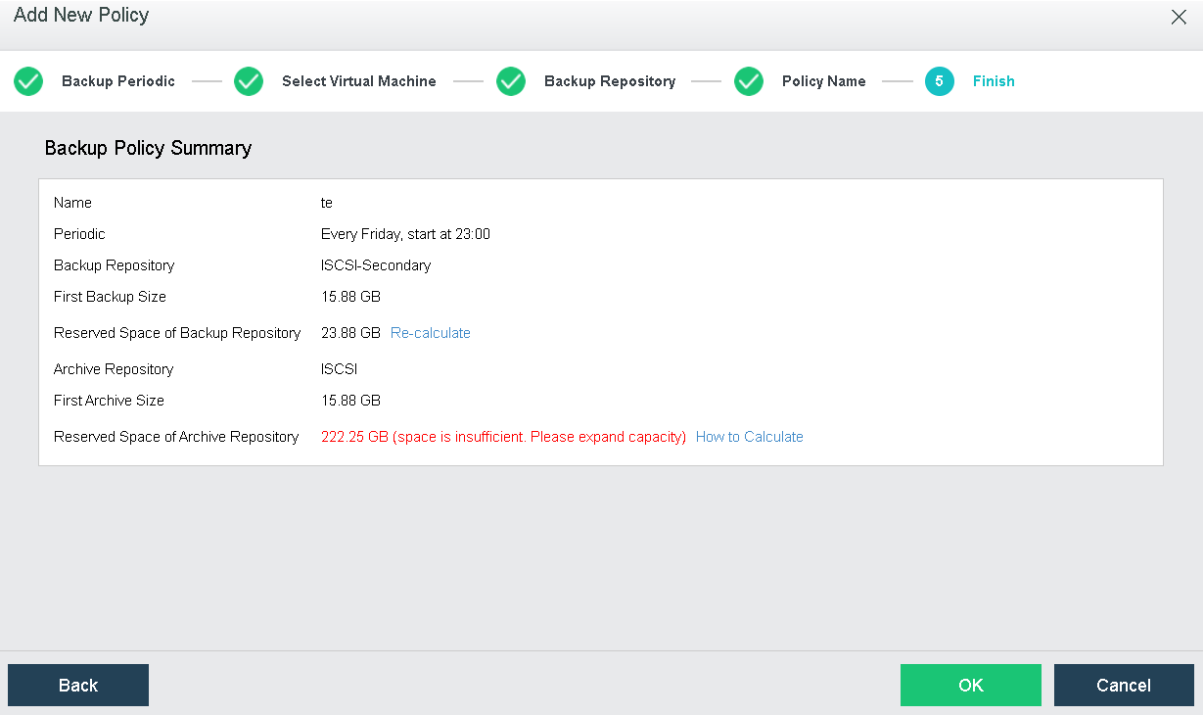


Name: Specifies name of the backup policy

Description: Specifies description of the new backup policy.

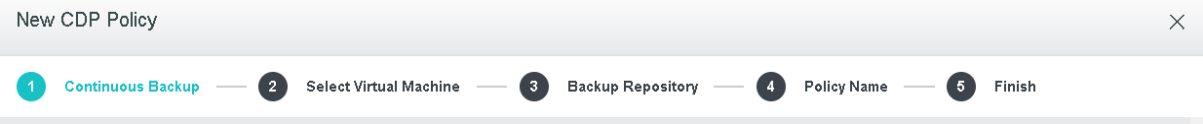
5. Confirm the configurations and then click **OK** to save the settings.

   It displays basic settings of the backup policy, such as **Name, Retention Period, Backup Repository and First Backup Size,** as shown below:



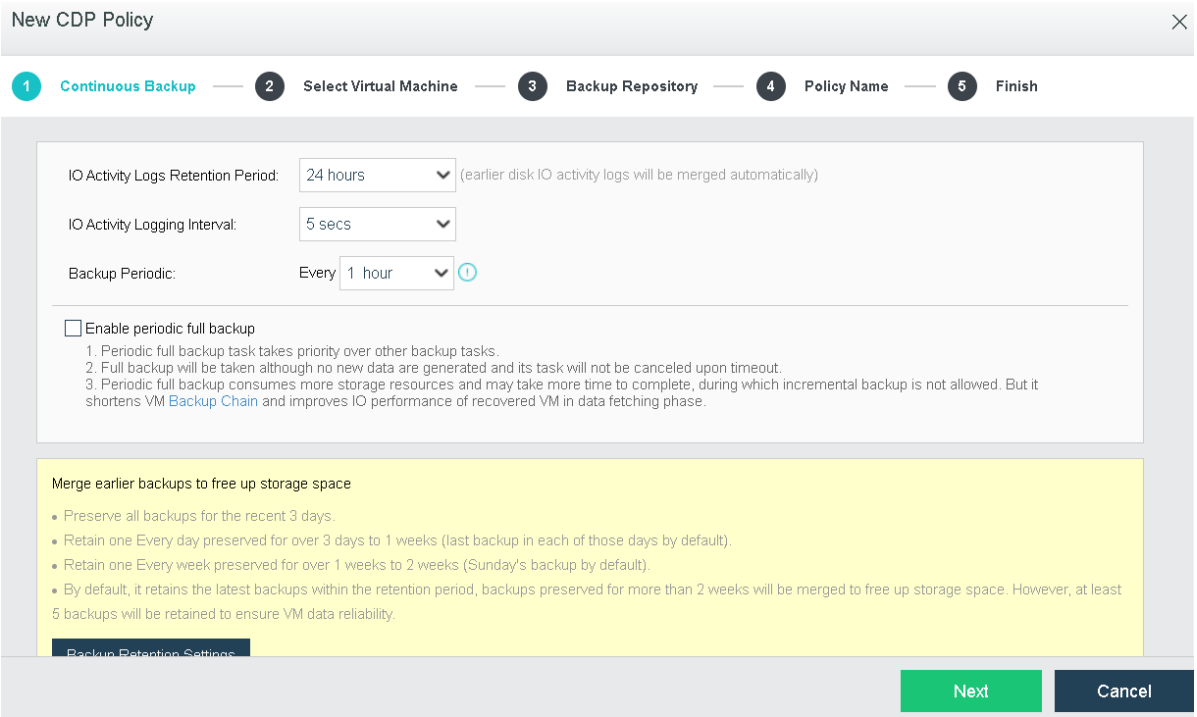
2.6.12.1.2 Adding New CDP Policy

To add a new CDP policy, click **New CDP Policy to enter the following page and then follow the wizard to** specify continuous backup period, select virtual machine(s) and backup repository, and specify policy name, as shown below:



1. Configure **Continuous Backup**.

   It involves the configurations of the following fields: **IO Activity Logs Retention Period, Backup Periodic, Backup Retention Period.** And **Automatic backup cleanup** is optional.



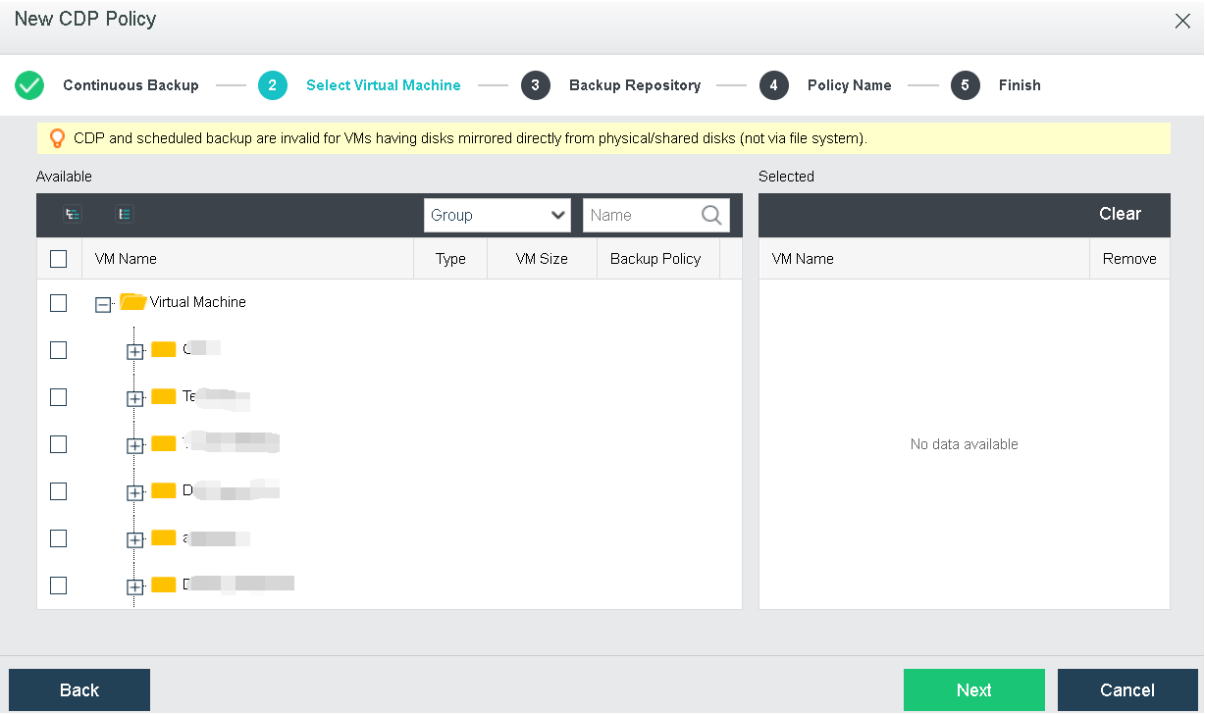
IO Activity Logs Retention Period: Specifies how long IO activity logs will be preserved. The longest period is 3 days. Earlier disk IO activity logs will be deleted automatically once the specified period is reached.

Backup Periodic: Specifies how often backup task is executed. The minimum backup periodic is one hour.

Retention Period: It specifies how long backups will be kept. The longest period is three months.

You may enable Automatic backup cleanup to automatically preserve all the backups for the previous 3 days, one backup (the last one) for the earlier week and one backup for each of the even earlier weeks (the one created on Sunday only).

2. Select the virtual machine(s) you want to back up. You may view the virtual machines by **Group, Node, Datastore** or select **All** to view all the virtual machines, or you may enter the name of the virtual machine in the search box to search for a specific virtual machine. Select virtual machines under **Available** and then the selected virtual machines will be added to **Selected** on the right, as shown below:



Clear: To clear the selected virtual machines, click **Clear**.

To remove a virtual machine from Selected list, click

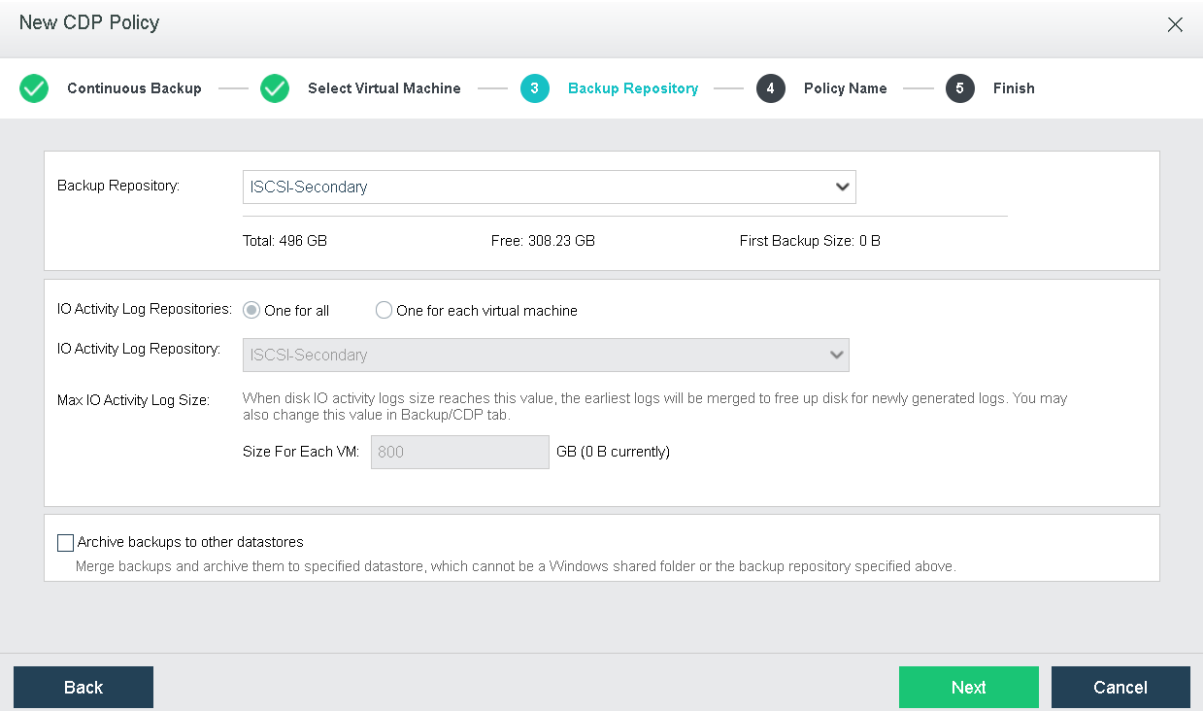
CDP or scheduled backup is not applicable to virtual machines having disks mapped directly from physical or shared disks, rather than via file system.

One virtual machine cannot be associated with more than one backup policy. If the virtual machine is associated with a new policy, it will be removed from the previous policy.

Template and virtual machines deployed from template do not support CDP.

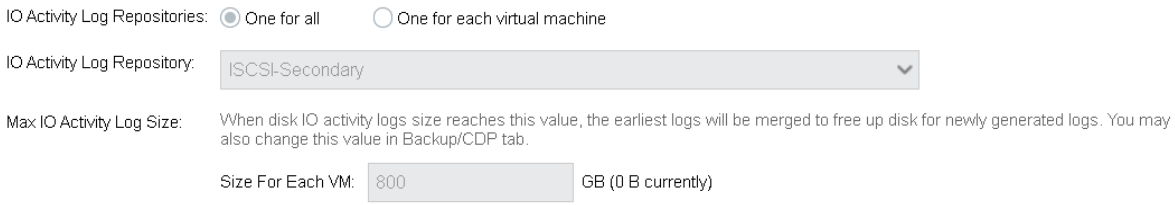
---

3. Specify backup repository to store backups and configure IO activity log related options, as shown below:



Backup Repository: It specifies backup repository, you may select an existing datastore or choose to add a new Windows shared folder. Once backup repository is specified, total capacity, available backup repository size and first backup size of the selected datastore will be displayed.

IO Activity Log Repositories: There are two options: **One for all, One for each virtual machine,** which enables you to specify a same IO activity log repository for all the virtual machines at a time or specify different IO activity log repository for each virtual machine, as shown below:



IO Activity Log Repository: The repository should be a datastore that node(s) where the selected virtual machine(s) reside has access to. The default IO activity log repository is same with backup repository.

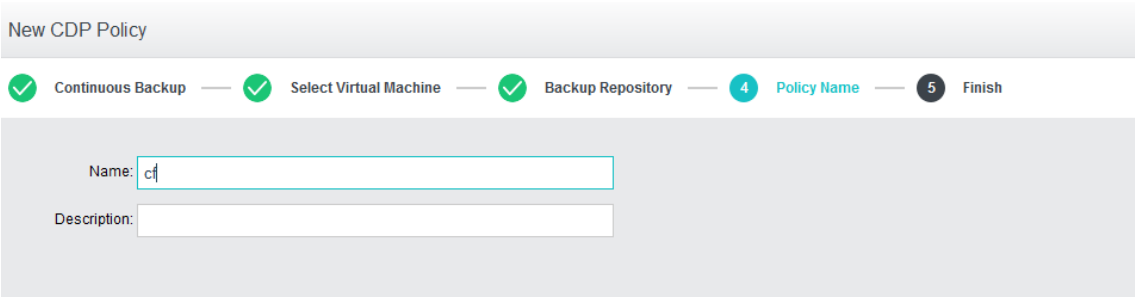
Max Log Size: When disk IO activity logs size reaches this value, the earliest logs will be deleted to free up disk for newly generated logs. You may also change this value in

Backup/CDP tab. Max log size should be between 100GB and 10240GB, and should not be greater than the free space of the specified IO activity log repository.

If IO read and write speed is lower than 50MB/s, CDP service may stop due to low storage performance. Therefore, datastore with better performance is recommended.

4. Configure a distinguish name for the new CDP policy.

   On this tab, you may fill in basic information for the new CDP policy such as policy name and description.

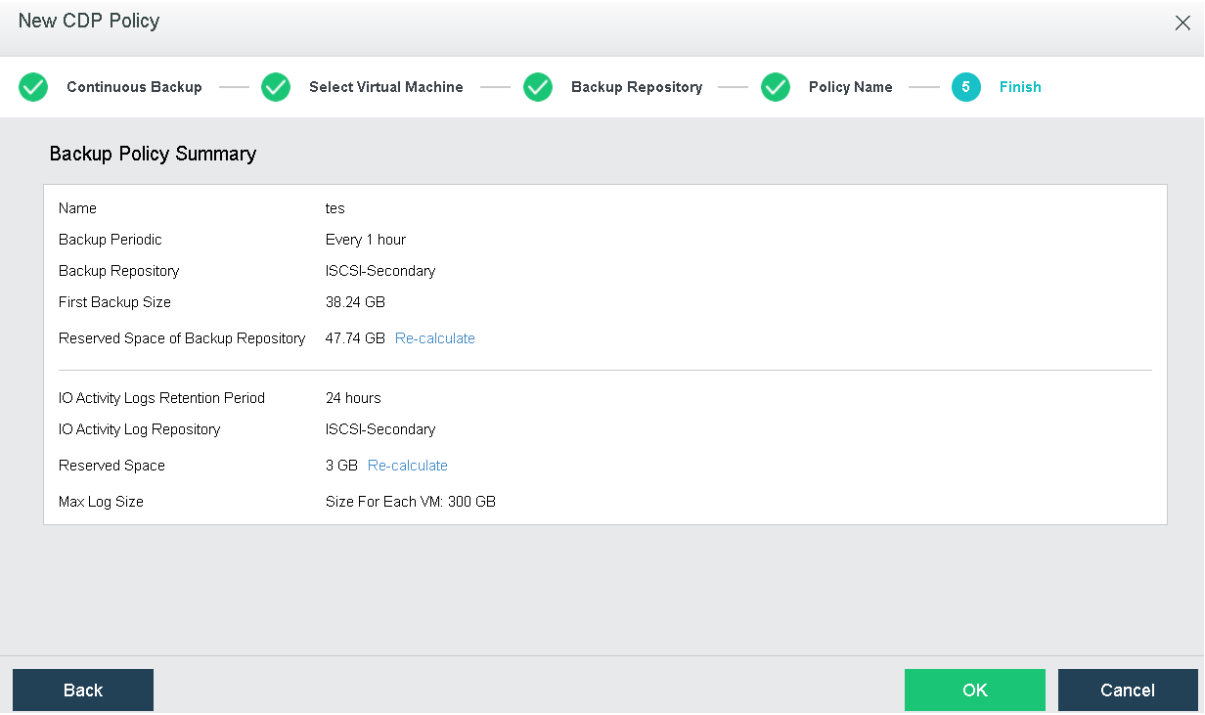


   Name: Specifies name of the new backup policy.

   Description: Specifies description of the new backup policy.

5. Confirm the configurations and then click **OK** to save the settings.

   It displays the basic settings of the new CDP policy, such as **Name, Backup Retention Period, Backup Repository and First Backup Size, IO Activity Logs Retention Period, IO Activity Log Repository and Max Log Space,** as shown below:

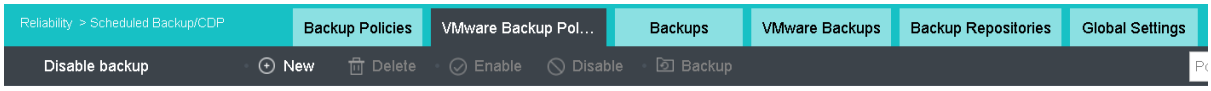


CDP can be started only for the virtual machine which is powered on and associated with a CDP policy. Template and virtual machines deployed from template do not support CDP.

2.6.12.2 VMware Backup Policy

Virtual machines in VMware vCenter can be backed up to Sangfor HCI platform without installing any third-party software or plugin and purchasing backup storage. Virtual machine can be recovered on HCI platfrom or recovered to VMware vCenter

On the toolbar, there are **Enable/Disable backup, New, Delete, Enable, Disable** and **Backup,** as shown below:



Enable: To enable or disable backup, click **Enable backup** to enable backup or **Disable backup** to disable backup.

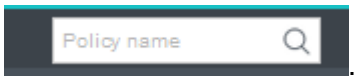
To add a new VMware backup policy, you may click **New**.

To delete the selected backup policy, you may click **Delete**.

To enable the backup policy, you may click **Enable** or click on the icon.

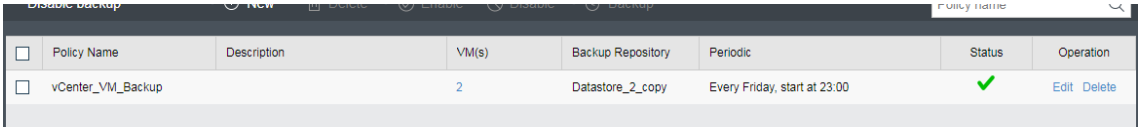
To disable the backup policy, you may click **Disable** or click the icon.

To execute the selected backup policy, you may click **Backup**.

To search for a VMware backup policy, enter the policy name in the search box 

.

On the **VMware Backup Policy** tab, it displays policy name, description, the number of virtual machines, backup repository, backup periodic, status and operation, as shown below:



Policy Name	Description	VM(s)	Backup Repository	Periodic	Status	Operation
vCenter_VM_Backup		2	Datastore_2_copy	Every Friday, start at 23:00	✔	Edit Delete

Policy Name: Displays name of the new VMware backup policy.

Description: Displays descriptive information of the new VMware backup policy.

VM(s): It displays the number of virtual machines to be backed up. To view virtual machines, click on the number under **VM(s)**

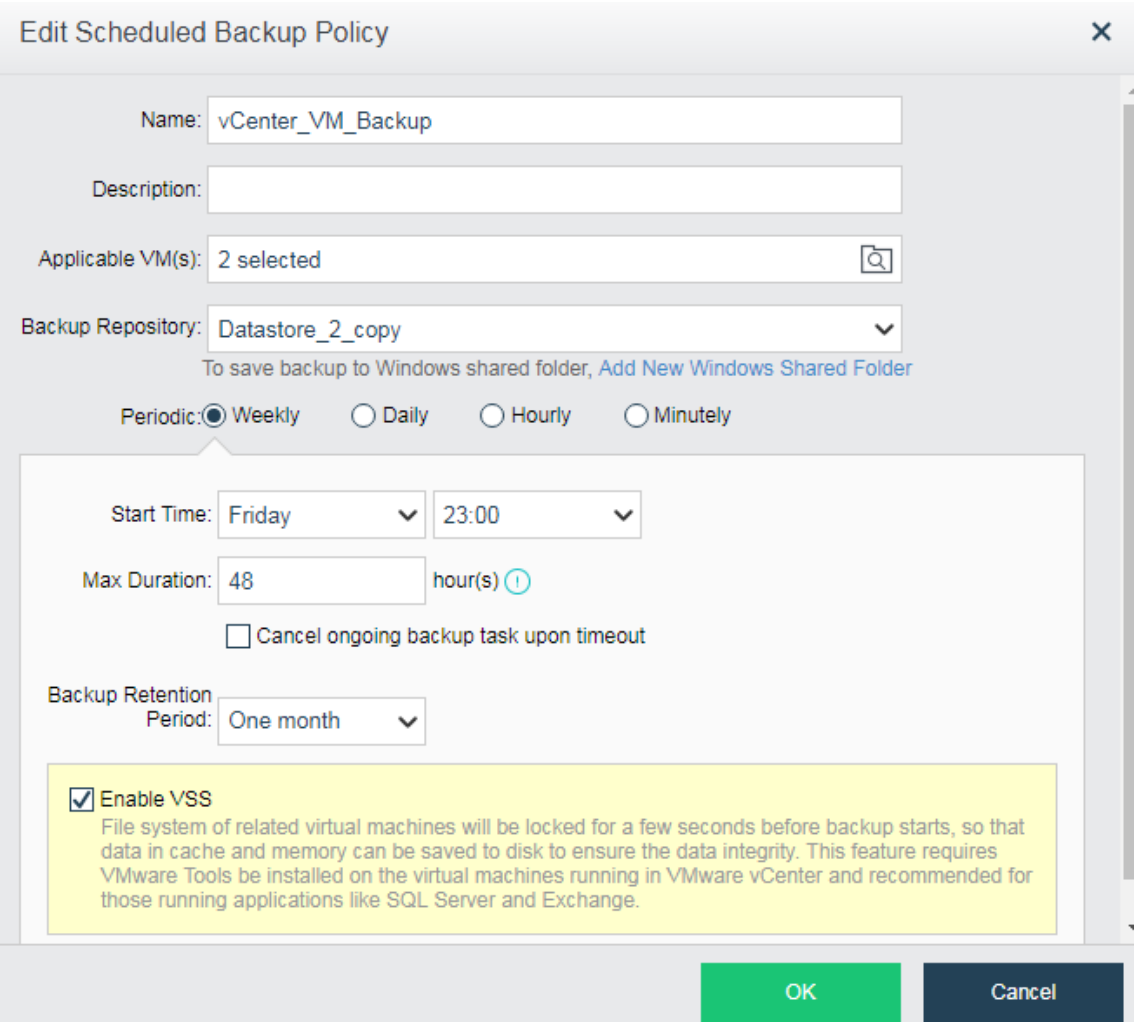
Backup Repository: It displays backup repository.

Periodic: It displays backup periodic.

Status: It displays status of the backup policy, enabled or disabled. To enable backup policy, click on the icon. To disable backup policy, click on the icon.

Operation: To edit or delete a backup policy, click **Edit** or **Delete** under **Operation**. The default scheduled backup policy cannot be deleted.

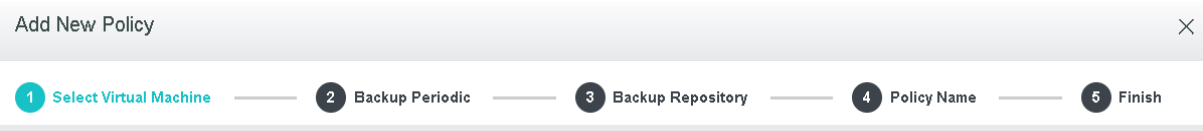
To edit a backup policy, click **Edit** and enter the following page:



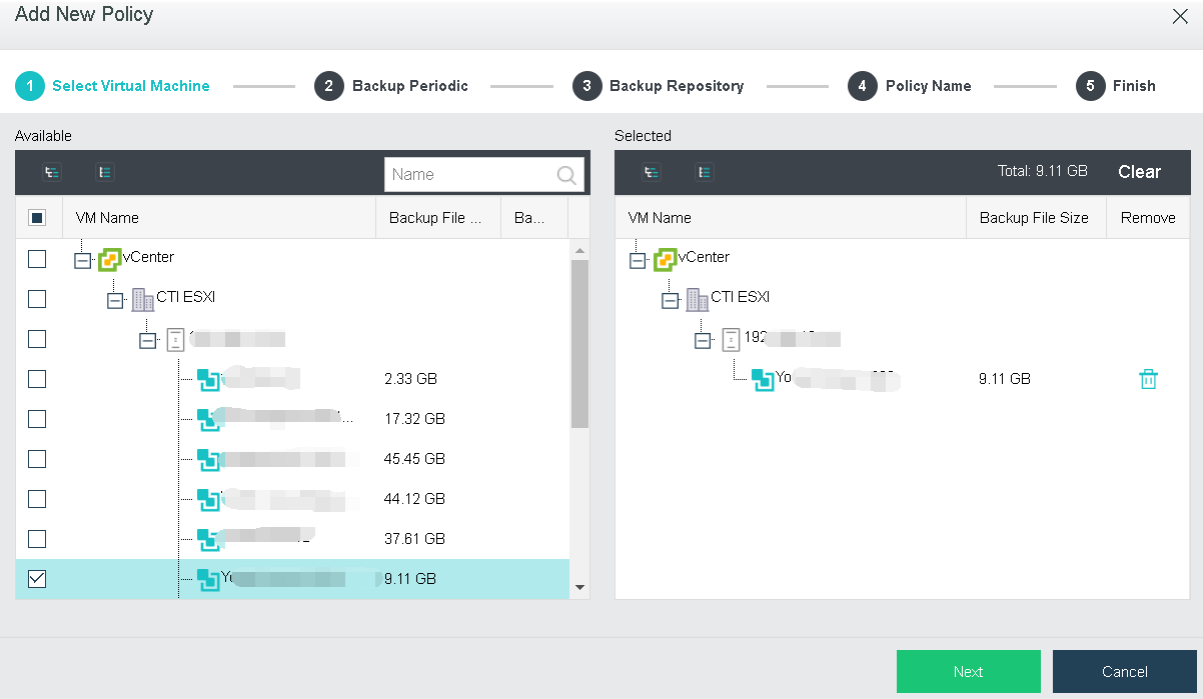
Adding VMware Backup Policy

To add a new VMware backup policy, do as follows:

1. Go to **System > VM Backup and Recovery > VMware Backup Policy,** click **New** to enter the following page.



2. Select the virtual machine(s) you want to back up. You may enter the name of the virtual machine in the search box to search for a specific virtual machine. Select virtual machines under **Available** and then the selected virtual machines will be added to **Selected** on the right, as shown below:

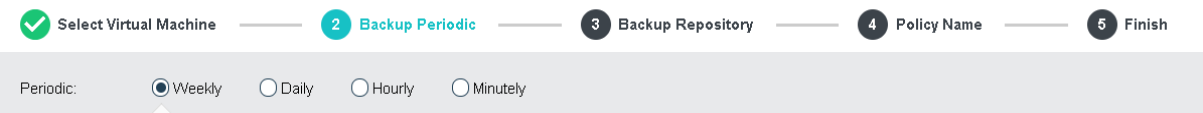


Clear: To clear the selected virtual machines, click **Clear**.

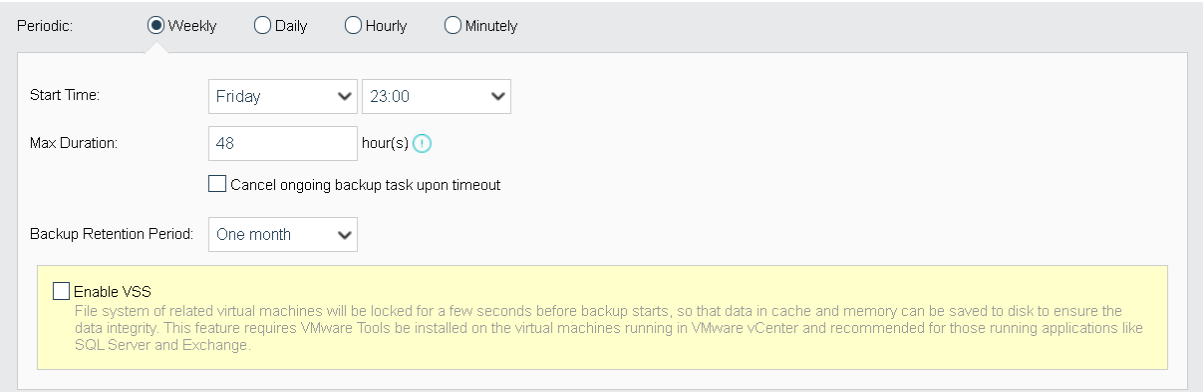
To remove a virtual machine from the Selected, click 🗑

3. Specify **Backup Periodic**.

Backup periodic can be on weekly basis, daily basis, hourly basis and minutely basis. There are another two options: **Cancel ongoing backup task upon timeout, Enable VSS.** You may enable those options based on your own needs.



Weekly: Select **Weekly** and configure the fields on the following page:



On weekly basis: Options are from **Sunday** to **Saturday**.

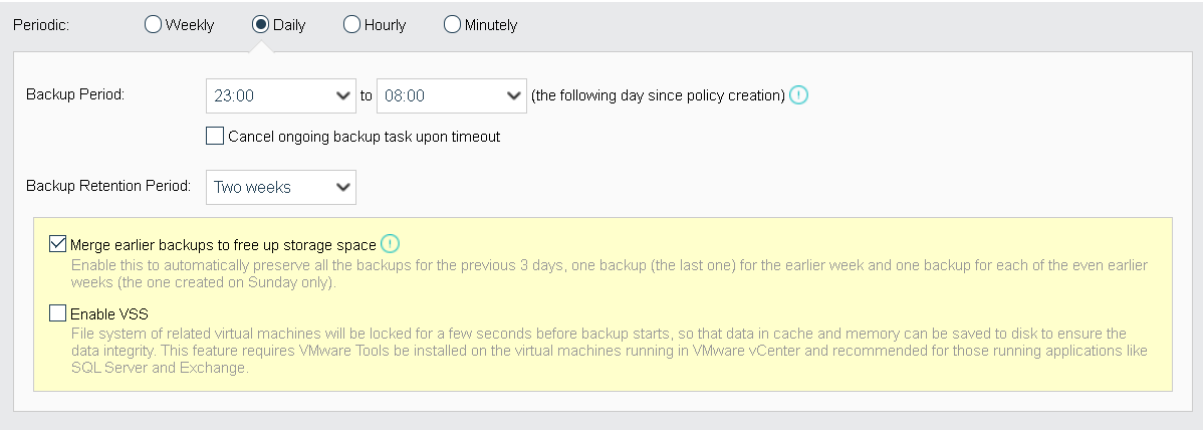
Start Time: It specifies time to start backup. Since backup may bring impacts to system service, select a period that service is not busy.

Max Duration: It specifies the longest period that the backup operation can last. New backups only occur within this time range and will not stop once starts. However, the backup tasks having not started yet will resume when the time range arrives again. You may select **Cancel ongoing backup task upon timeout** based on your own needs.

Backup Retention Period: It specifies the longest period that backups will be kept. The longest period is three months.

You may select the option **Enable VSS** based on your own needs. Once that option is selected, file system of related virtual machines will be locked for a few seconds before backup starts, so that data in cache and memory can be saved to disk to ensure the data integrity. This feature requires VMware Tools to be installed on the virtual machines running in VMware vCenter and is recommended for those running applications like SQL Server and Exchange.

Daily: To have VM(s) backed up on daily basis, select Daily for Periodic and configure the related fields, as shown below:



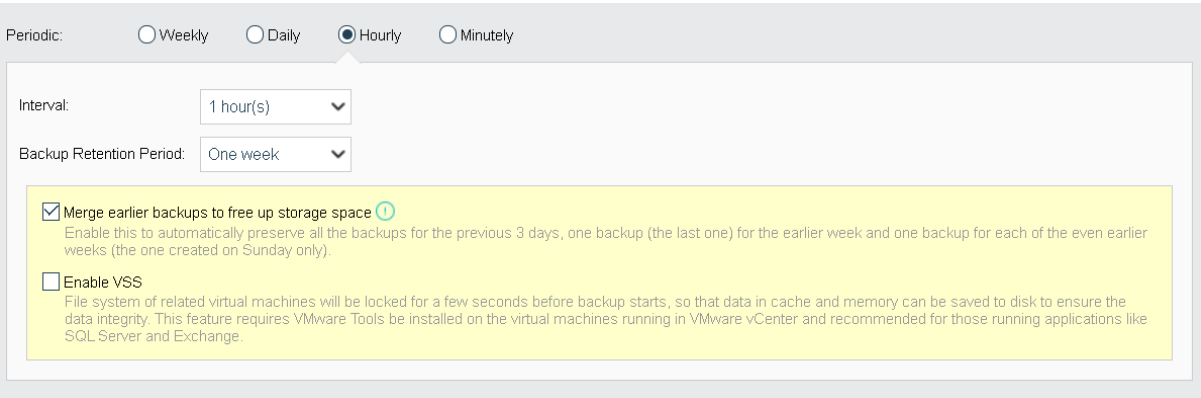
Backup Period: It specifies the longest period that the backup operation can last. New backups only occur within this time range and will not stop once starts. However, the backup tasks having not started yet will resume when the time range arrives again. You may select **Cancel ongoing backup task upon timeout** based on your own needs.

Backup Retention Period: It specifies the longest period that backups will be kept. The longest period is three months.

You may select **Merge earlier backups to free up storage space** preserve all the backups for the previous 3 days, one backup (the last one) for the earlier week and one backup for each of the even earlier weeks (the one created on Sunday only).

You may select the option **Enable VSS** based on your own needs. Once that option is selected, file system of related virtual machines will be locked for a few seconds before backup starts, so that data in cache and memory can be saved to disk to ensure the data integrity. This feature requires VMware Tools to be installed on the virtual machines running in VMware vCenter and is recommended for those running applications like SQL Server and Exchange.

Hourly: To have VM(s) backed up on hourly basis, select Hourly for Periodic and configure the related fields, as shown below:



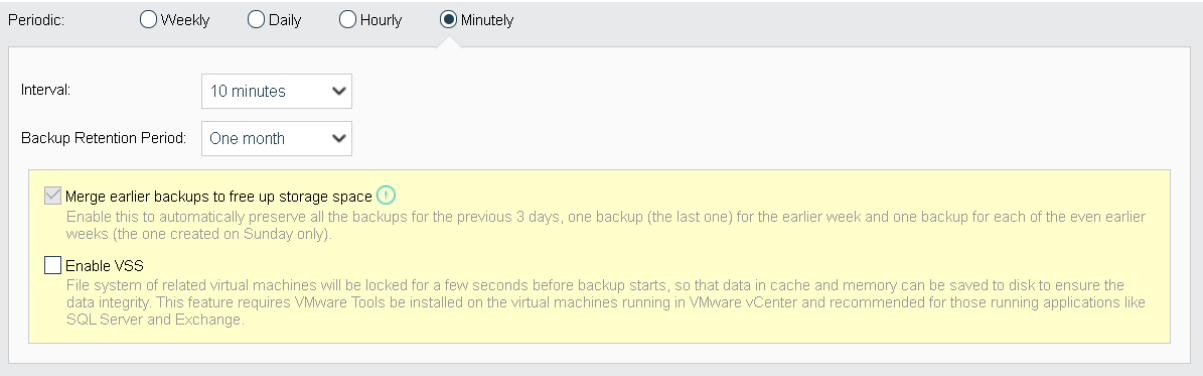
Interval: Specifies the interval of backup occurs. The minimum interval is 1 hour.

Backup Retention Period: It specifies the longest period that backups will be kept. The longest period is three months.

You may select **Merge earlier backups to free up storage space** to automatically preserve all the backups for the previous 3 days, one backup (the last one) for the earlier week and one backup for each of the even earlier weeks (the one created on Sunday only).

You may select the option **Enable VSS** based on your own needs. Once that is selected, file system of related virtual machines will be locked for a few seconds before backup starts, so that data in cache and memory can be saved to disk to ensure the data integrity. This feature requires VMware Tools to be installed on the virtual machines running in VMware vCenter and is recommended for those running applications like SQL Server and Exchange.

Minutely: To have VM(s) backed up on minutely basis, select Minutely for Periodic and confiudre the related fields, as shown below:



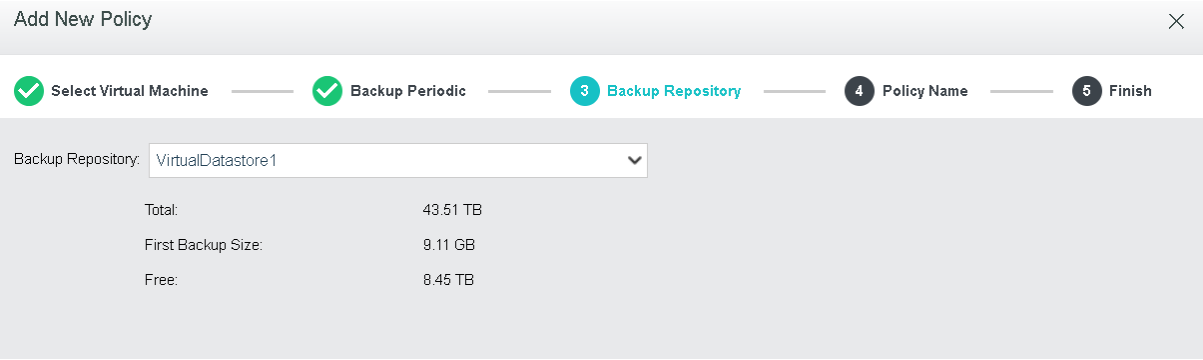
Interval: Specifies the interval of backup occurs. The minimum interval is 10 minutes.

Backup Retention Period: It specifies the longest period that backups will be kept. The longest period is three months.

You may select **Merge earlier backups to free up storage space** to automatically preserve all the backups for the previous 3 days, one backup (the last one) for the earlier week and one backup for each of the even earlier weeks (the one created on Sunday only).

You may select the option **Enable VSS** based on your own needs. Once that option is selected, file system of related virtual machines will be locked for a few seconds before backup starts, so that data in cache and memory can be saved to disk to ensure the data integrity. This feature requires VMware Tools to be installed on the virtual machines running in VMware vCenter and is recommended for those running applications like SQL Server and Exchange.

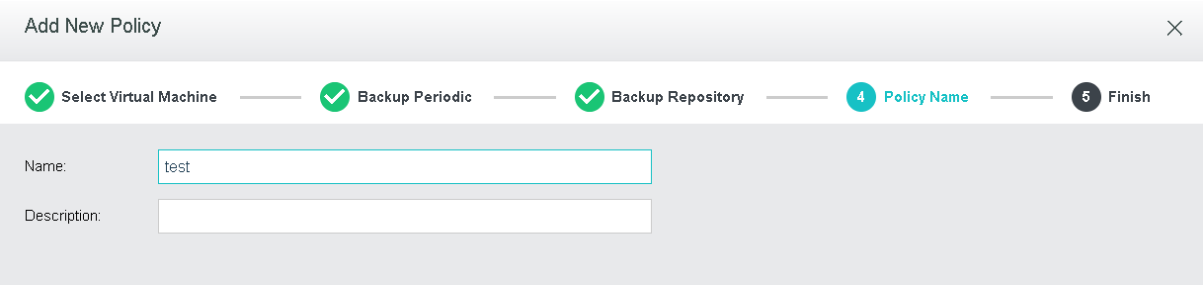
4. Specify backup repository to store VM backups, as shown below:



Backup Repository: It specifies backup repository, you may select an existing datastore. Once the backup repository is specified, total capacity, available backup repository size and first backup size of the selected datastore will be displayed.

Note that next backup will have all data backed up if backup repository is changed, please operate with caution.

5. Specify name and description for the new policy on the following page:

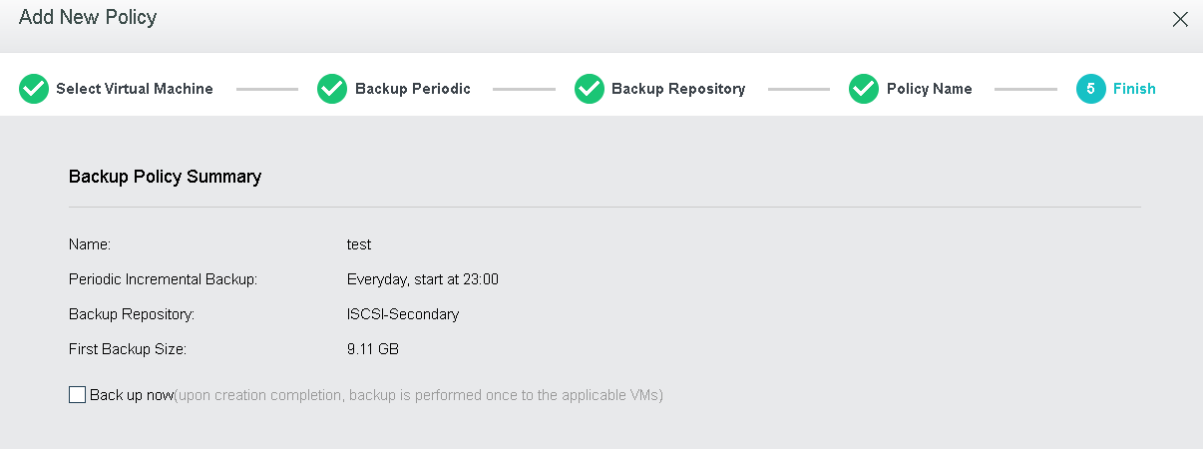


Name: Specifies name of the new backup policy.

Description: Specifies description of the new backup policy.

6. Confirm configurations and click **OK** to save the settings.

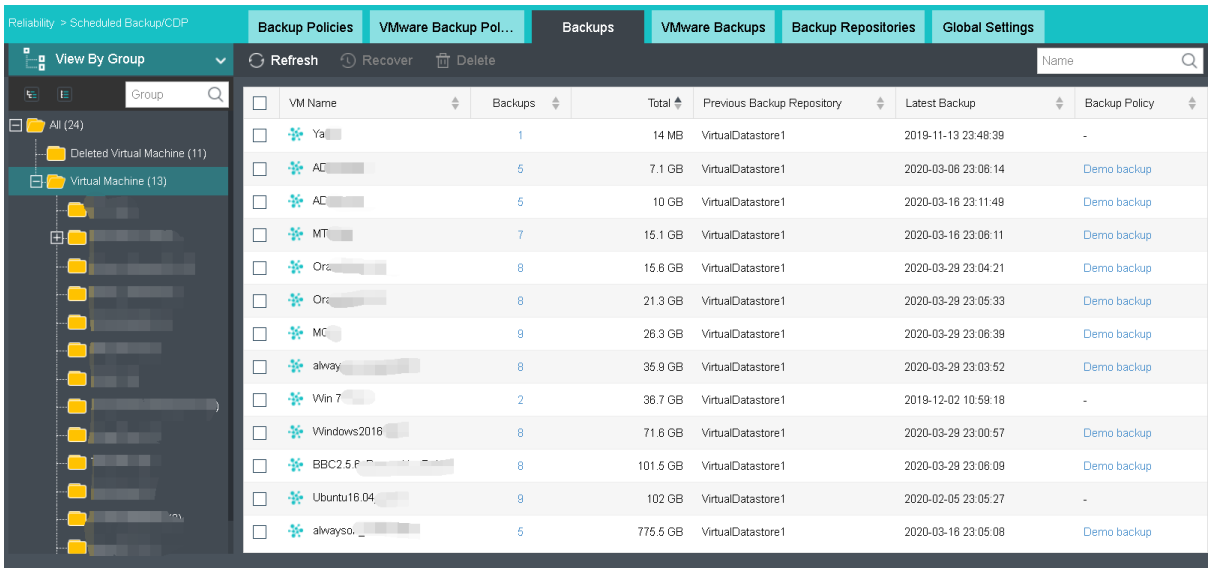
It displays the basic settings of the backup policy, such as **Name, Periodic Incremental Backup, Backup Repository and First Backup Size.** To have VM(s) backed up upon completion of backup policy creation, you may select **Back up now option**, as shown below:



2.6.12.3 Backups

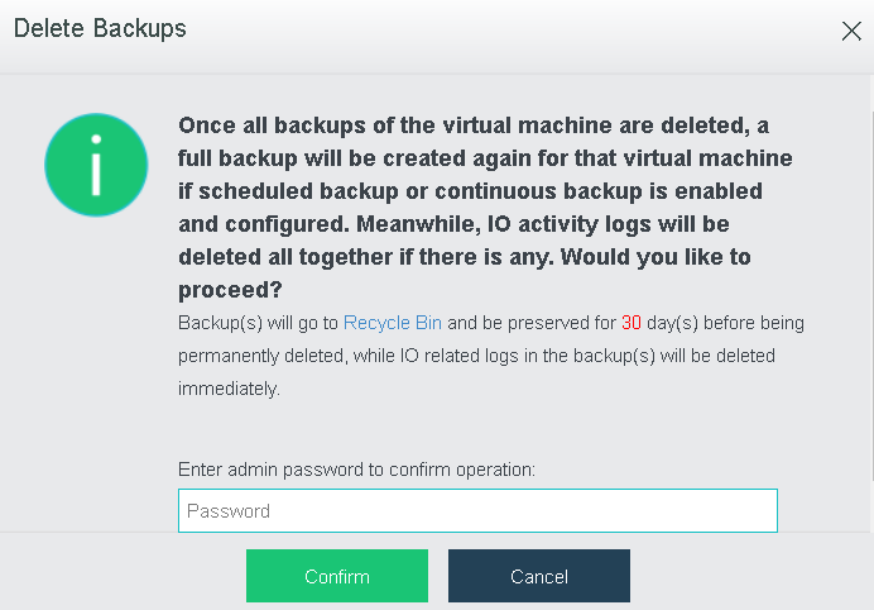
On the **Backups** tab, VM backups can be displayed by VM group, node, datastore and backup repository. Such information as VM name, number of backups, total size, previous backup

repository, last backup and backup policy will be displayed.



Recover: Select backed up virtual machines and restore them to their previous status and configuration. You may also go to Backup/CDP tab to perform recovery operation. For details, refer to Recovering Virtual Machine in Backup/CDP section.

Delete: To delete backups of virtual machine, select the virtual machine and click **Delete**. If scheduled backup or continuous backup policy is configured and enabled, a full backup will be created again for the virtual machine. IO activity logs will also be deleted if there is any. Backups will go to Recycle Bin and be preserved for 30 days, but IO activity logs will be deleted immediately and cannot be recovered any more. This operation requires you to enter password of the username to confirm.



VM Name: It displays the name of the virtual machine that has been backed up.

Backups: It displays the number of backups. You may click on the number to view detailed information of backups of the virtual machine. For details, refer to the **2.2.1.16 Configuring Backup**/CDP section.

Total Size: It displays total size of the backup files of the virtual machine.

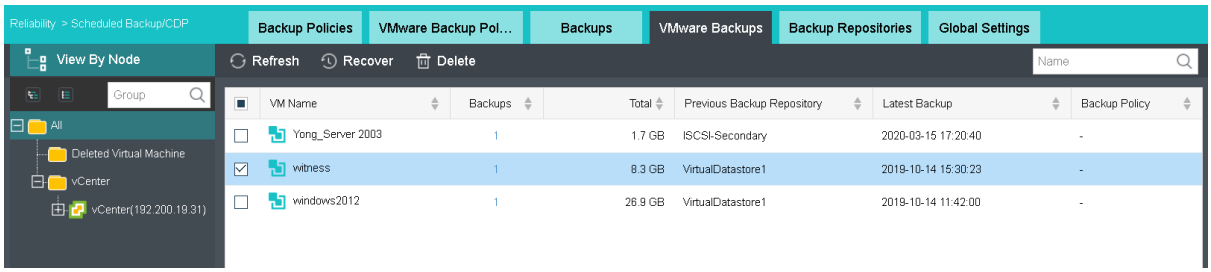
Previous Backup Repository: It displays the previous backup repository.

Lastest Backup: It displays time that the last backup happens.

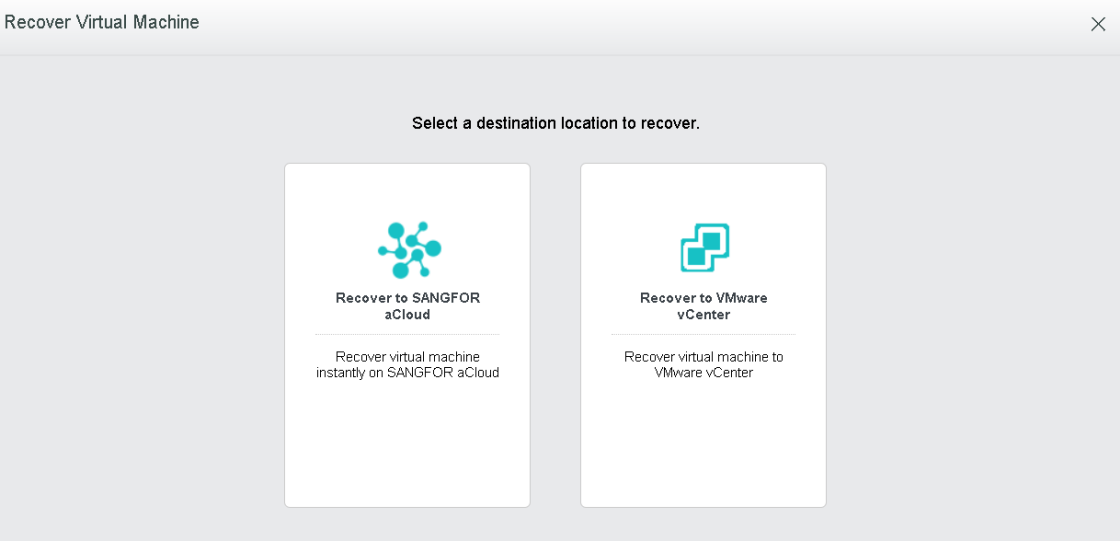
Backup Policy: It displays the backup policy with which the virtual machine is associated. You may click on the backup policy to edit it.

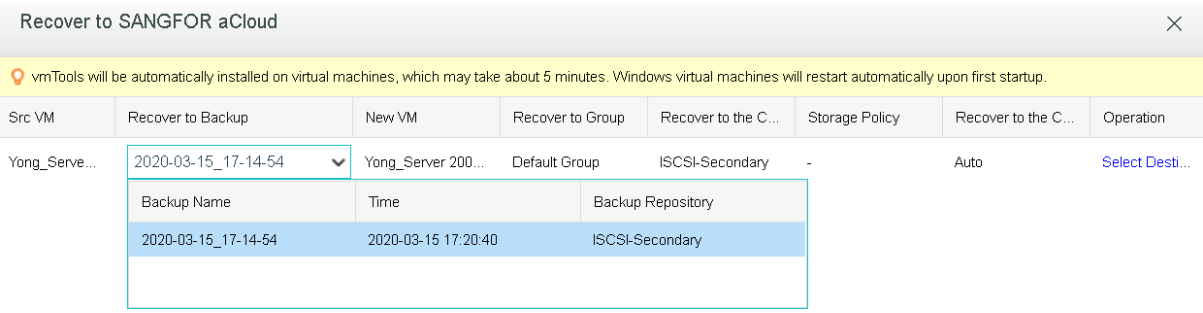
2.6.12.4 VMware Backups

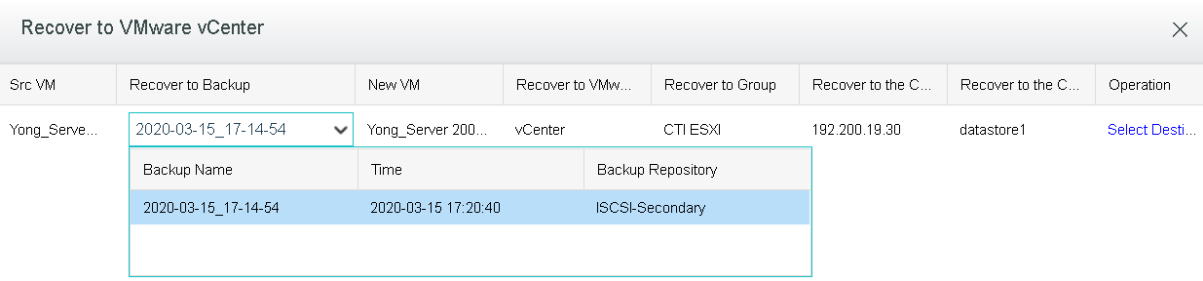
On the **VMware Backups** tab, VM backups can be displayed by node. Such information as VM name, number of backups, total size, previous backup repository, last backup and backup policy will be displayed.



Recover: Select backed up virtual machines and recover them to their previous status and configuration. Virtual machine can be recovered on Sangfor HCI platform or recovered to VMware vCenter, as shown below:

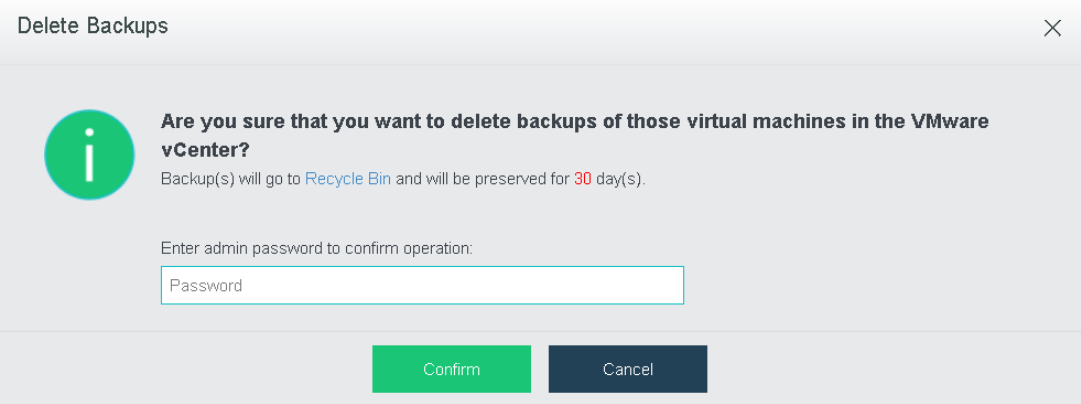






You may also recover virtual machine on **Backup** tab in VM summary. For details, refer to the **2.2.2.9** VM Recovery section.

Delete: To delete backups of the virtual machine, select the virtual machine and click **Delete**. The backups will go to the **Recycle bin** and will be preserved for 30 days. This operation requires you to enter password of the username to confirm.



VM Name: It displays the name of virtual machine that has been backed up.

Backups: It displays the number of backups. You may click on the number to view detailed information of backups of the virtual machine. For details, refer to the **2.2.2.8 VM** Backup section.

Total Size: It displays total size of the backup files of virtual machine.

Previous Backup Repository: It displays the previous backup repository.

Last Backup: It displays time when the last backup happens.

Backup Policy: It displays the backup policy that virtual machine is associated with. You may click on the backup policy to edit it.

2.6.12.5 Backup Repositories

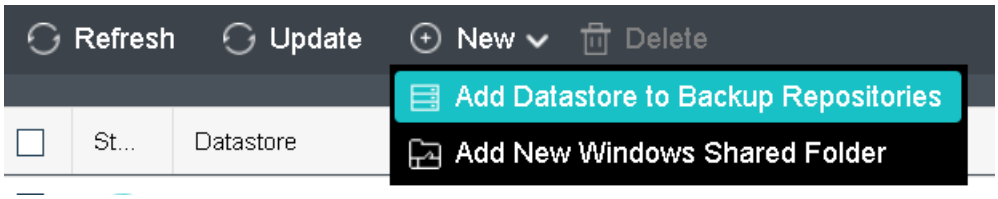
It displays available repositories for backups of virtual machines.

On the toolbar, there are **Refresh, Update, New, Delete** and **Advanced,** as shown below:

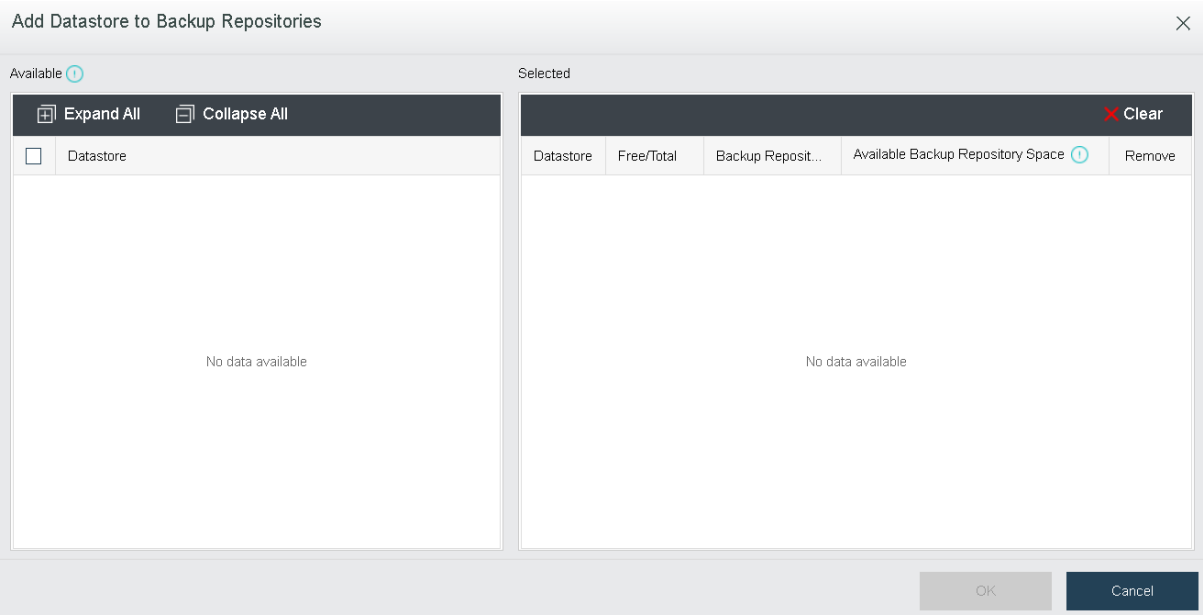
To refresh the page, you may click **Refresh**.

To update backups, you may click **Update**.

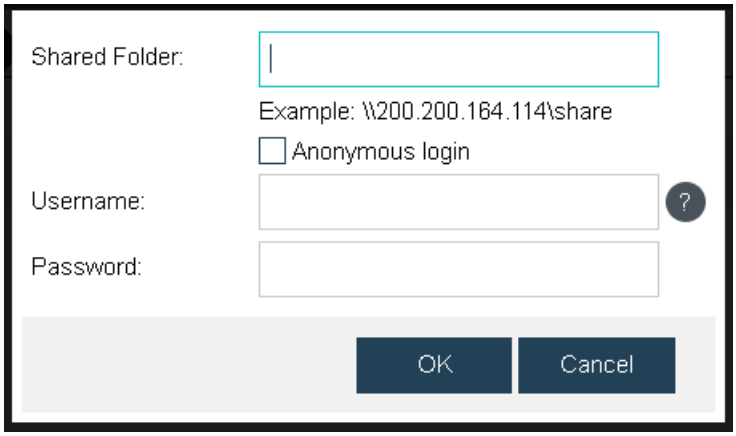
To add backup repository, you may click **New**. You may choose **Add Datastore to Backup Repositories** or **Add New Windows Shared Folder**.



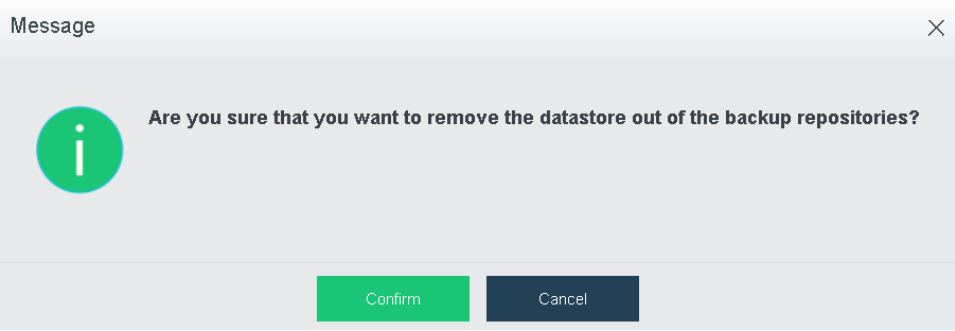
Add Datastore to Backup Repositories: Click it to enter the following page which displays available datastore and selected datastore list. The **Selected** list displays the free and total size of selected datastore, etc.



Add New Windows Shared Folder: To add a new Windows shared folder for storing backups, click **Add New Windows Shared Folder**.

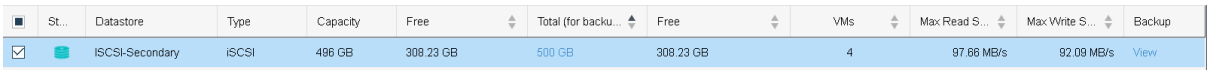


Delete: To move the datastore out of the backup repository, select the datastore(s) and click **Delete**.

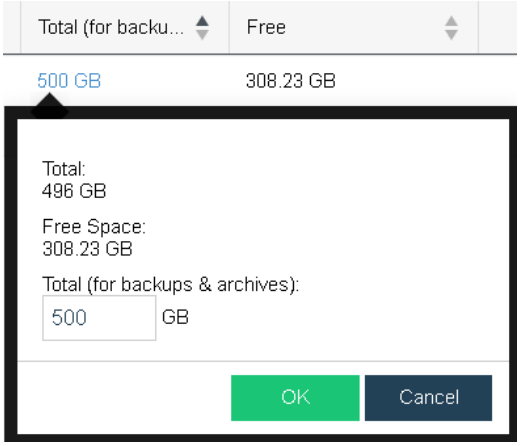


Virtual machines running on Sangfor HCI platform and VWware vCenter can be backed up to the same backup repository.

On the **Backup Repositories** tab, it displays status of backup repository, name of the datastore, type, total capacity, free space, total and free backup repository space, the number of virtual machines that have been backed up, max read speed, max write speed, and backup file, as shown below:

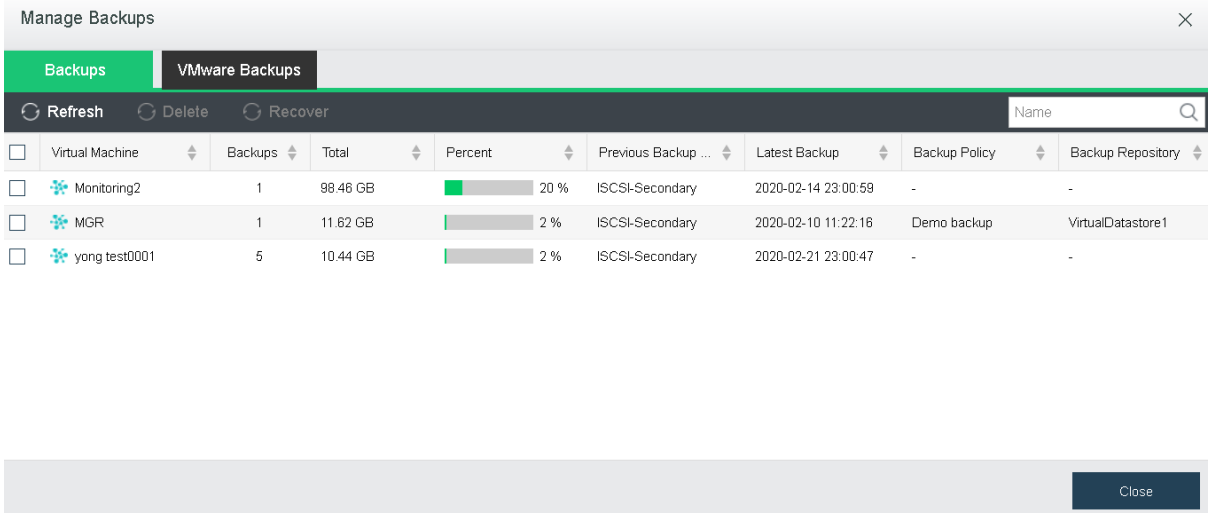


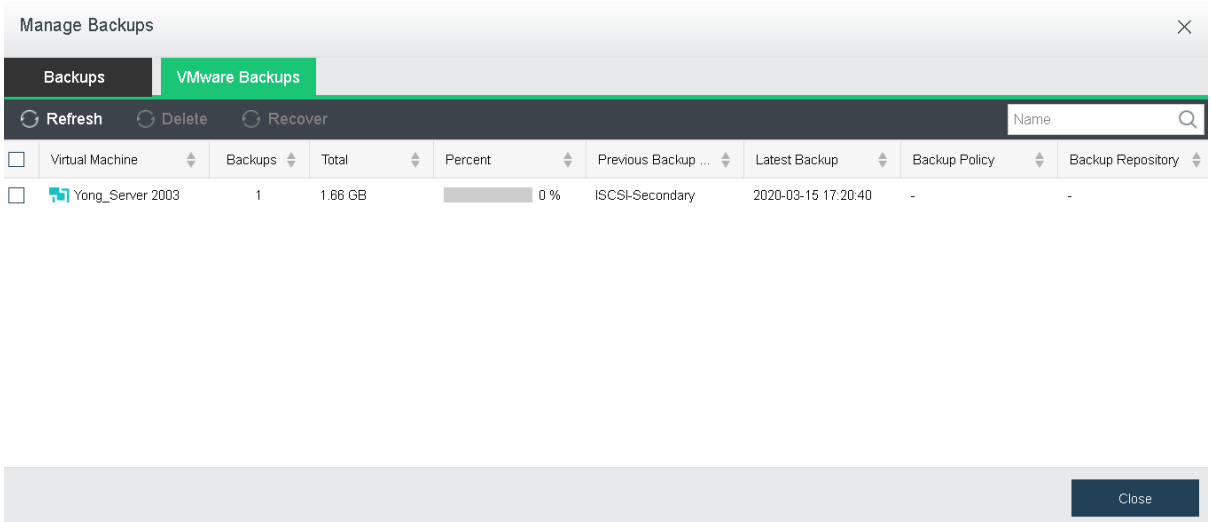
Total(For backup & archive): It displays size of backup repository. You may click on the number to edit it, as shown below:



Backup: To view and manage the backups, click **View under the** Backup **column**, as shown

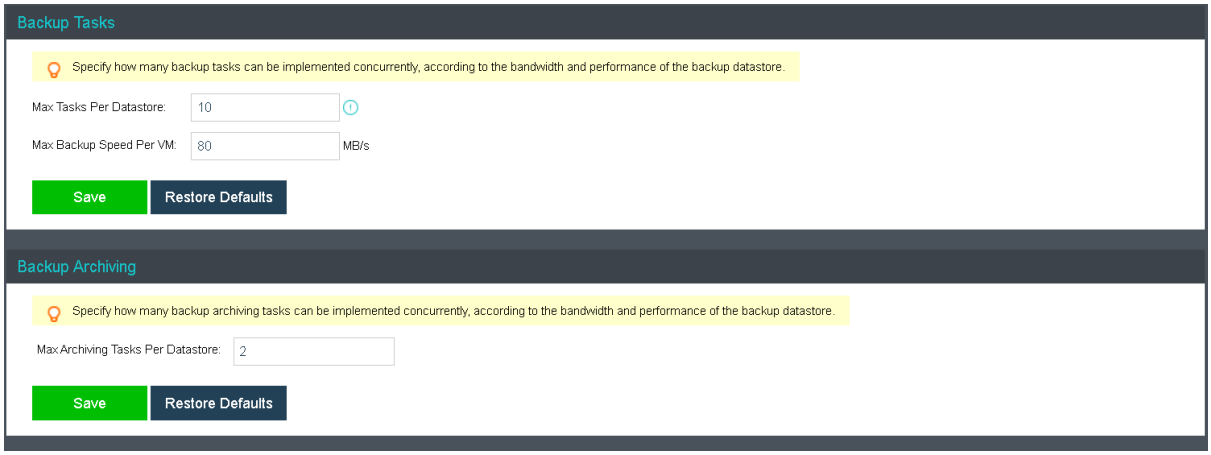
below:

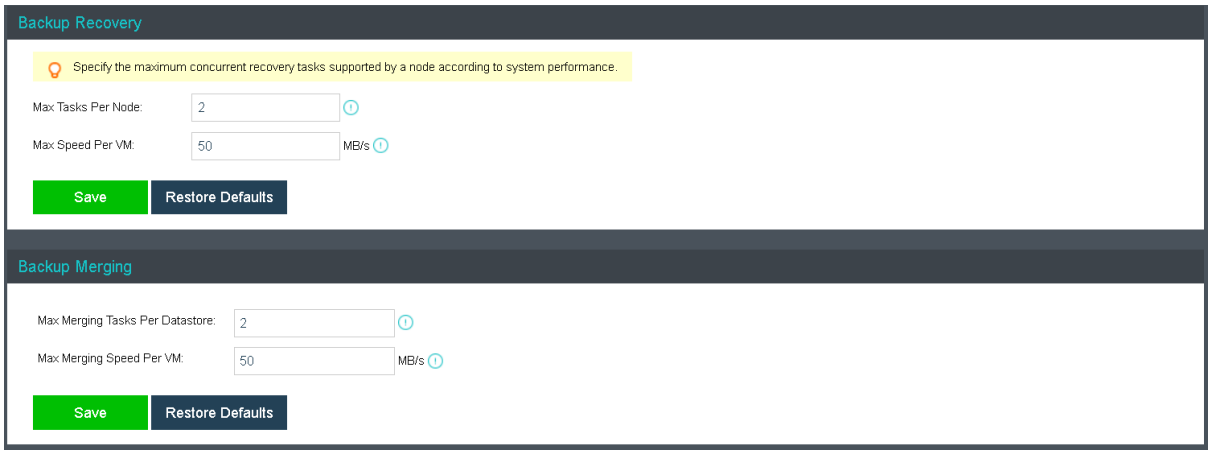




2.6.12.6 Global Settings

On the **Global Settings** tab, you can specify maximum concurrent backup tasks per storage and max concurrent recovery tasks per node and max recovery speed per VM, as shown below:





Backup Tasks: Specify how many backup tasks can be implemented concurrently, according to the bandwidth and performance of the backup datastore.

Backup Archiving: Specify how many backup archiving tasks can be implemented concurrently, according to the bandwidth and performance of the backup datastore.

Backup Recovery: Specify the maximum concurrent recovery tasks supported by a node according to system performance.

Backup Merging: Specify how many merging task can be implemented concurrently, according to system performance.

2.6.13 Recycle Bin

2.6.14 Data Erasure

Function Description

The HCI Data Erasure function enables users to choose to completely erase existing data during resource recovery. The user can choose to completely erase the existing data during resource recovery by customizing the number of overwrites according to the regulatory requirements or business needs.

Precaution

1. When using the data erasure function, it will occupy CPU and IO resources, and the erase process takes some time, so it is recommended to do it when the business is idle.

2. Data will not be recovered after erasing.

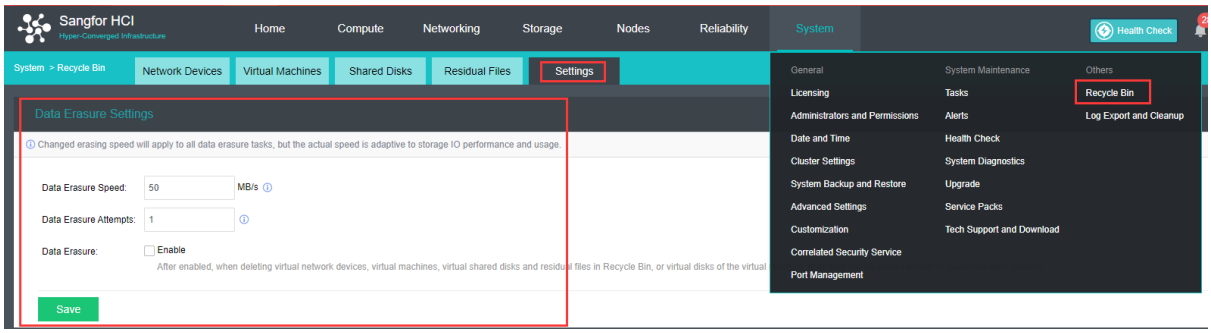
3.The actual rate will be dynamically adjusted according to the storage IO performance and busy level.

Prerequisites

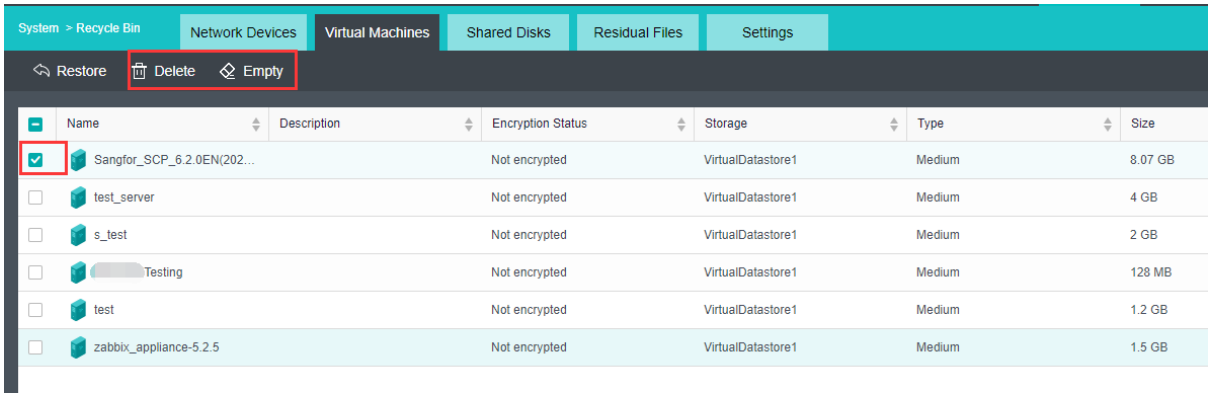
The virtual machine has been deleted and placed to the recycle bin.

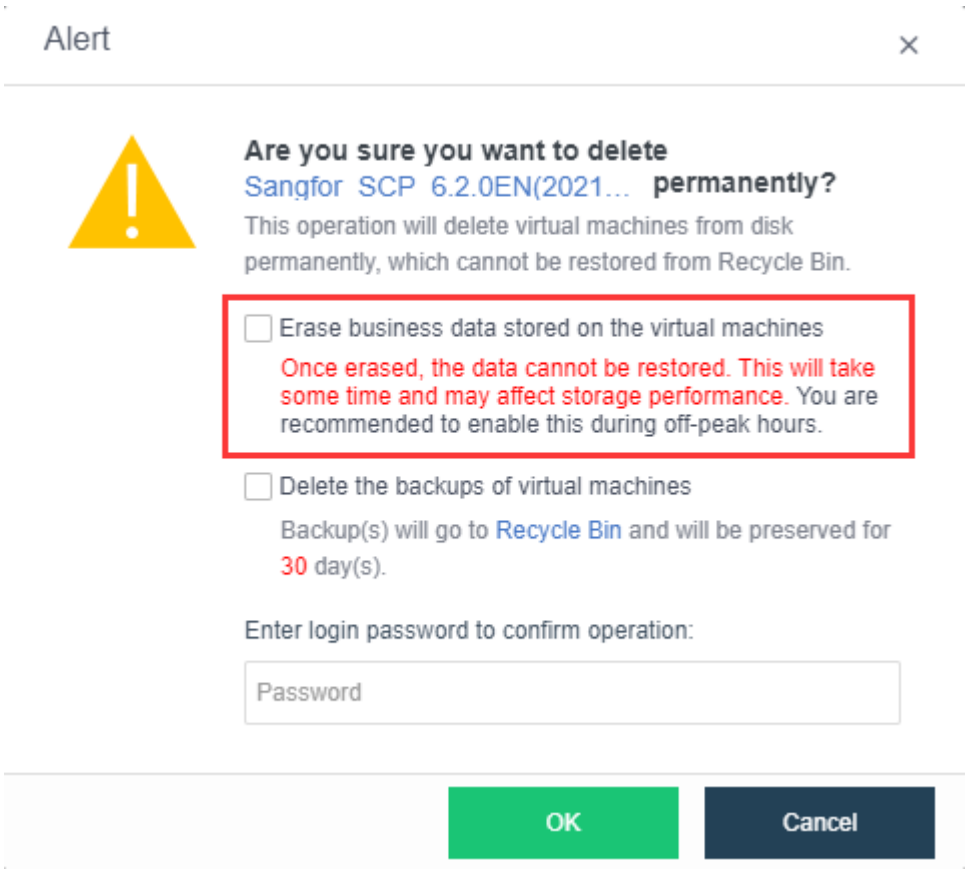
Operation steps

1. Navigate to **System** > **Recycle Bin** and click the **Settings** tab to configure the data erasure speed and attempt.
2. When **Data Erasure** is checked by default, the data will be erased when deleting virtual network devices, virtual machines, virtual shared disks, residual files in the Recycle Bin, as well as when deleting virtual disks of virtual machines to ensure data security.



3. Click the **Virtual Machines** tab. Select the virtual machine, click **Delete** or **Empty** to prompt for the "Erase business data of the virtual machine at the same time" option. Check this option and enter the HCI administrator password to completely wipe the business data of the virtual machine.

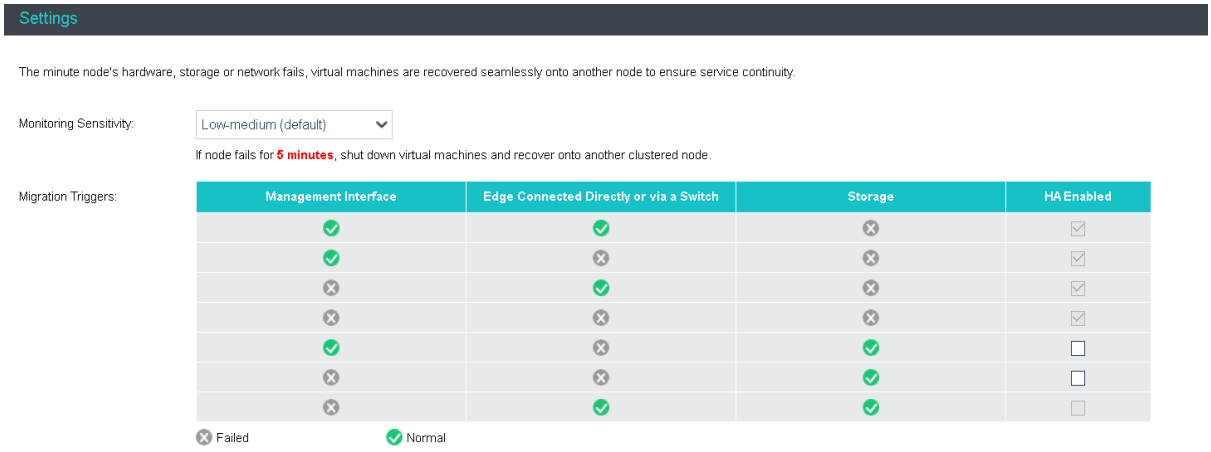




2.6.15 High Availability & Resource Scheduling

2.6.15.1 High Availability

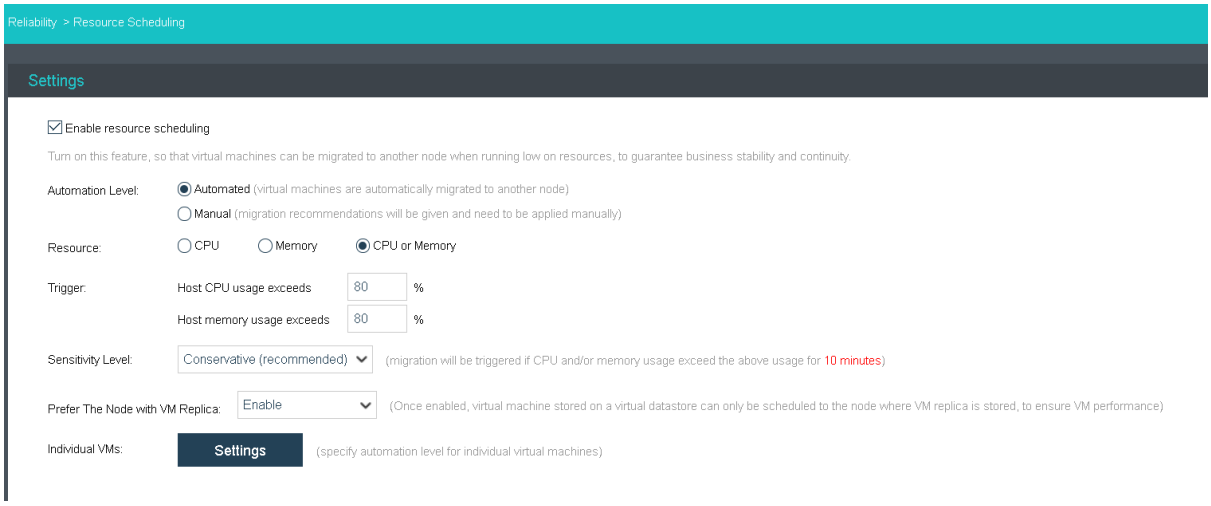
Migration upon node failure is applicable to shared storage only. HA will be triggered when node's hardware, storage or network fails for a period of time, and virtual machines(including virtual network devices) will be recovered seamlessly onto another node to ensure service continuity.



Due to the fact that CPU and memory data of virtual machines are not synchronized among different nodes, data may be lost when virtual machines are migrated onto another node.

2.6.15.2 Resource Scheduling

Resource scheduling refers to migrating virtual machines to another node when running low on resources, so as to guarantee business stability and continuity. Resource scheduling will be triggered if CPU and/or memory usage of node exceed(s) the threshold that has been specified, and virtual machines will be migrated according to the automation level. Virtual machines will be migrated to nodes whose CPU and/or memory usage is low, so as to lowering resource usage of nodes to be within the threshold.



You may specify threshold for CPU or memory(50%-90%), or for both. Migration recommendations will be given when threshold is reached.

You may specify sensitivity level, conservative(recommended) or aggressive. If conservative is selected, migration will be triggered if CPU and/or memory usage exceed the above usage for 10 minutes. If aggressive is selected, migration will be triggered if CPU and/or memory usage exceed the above usage for 3 minutes.

You may also specify automation level(manual and automated). If manual is selected, migration recommendations will be given when threshold is reached and virtual machines will be automatically migrated to another node.

2.6.15.3 Automated Hot Add

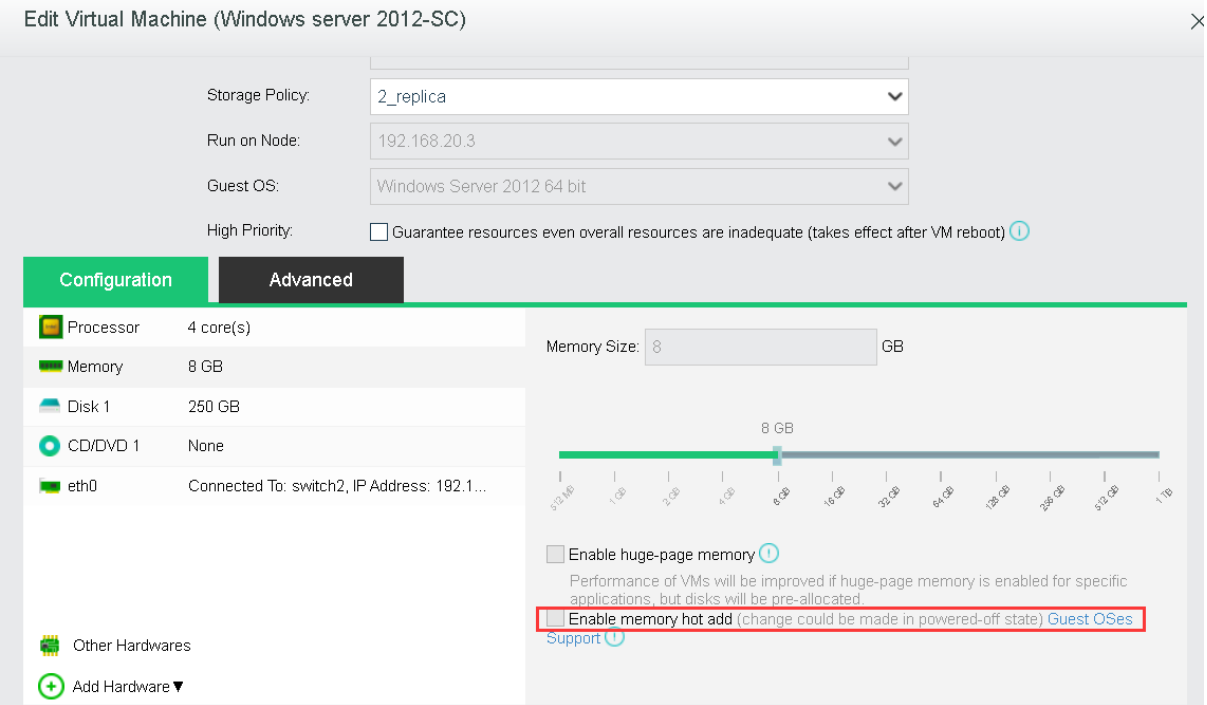
Automated hot add refers to adding CPU, memory, NIC and disks to virtual machines manually or automatically when virtual machines are running.

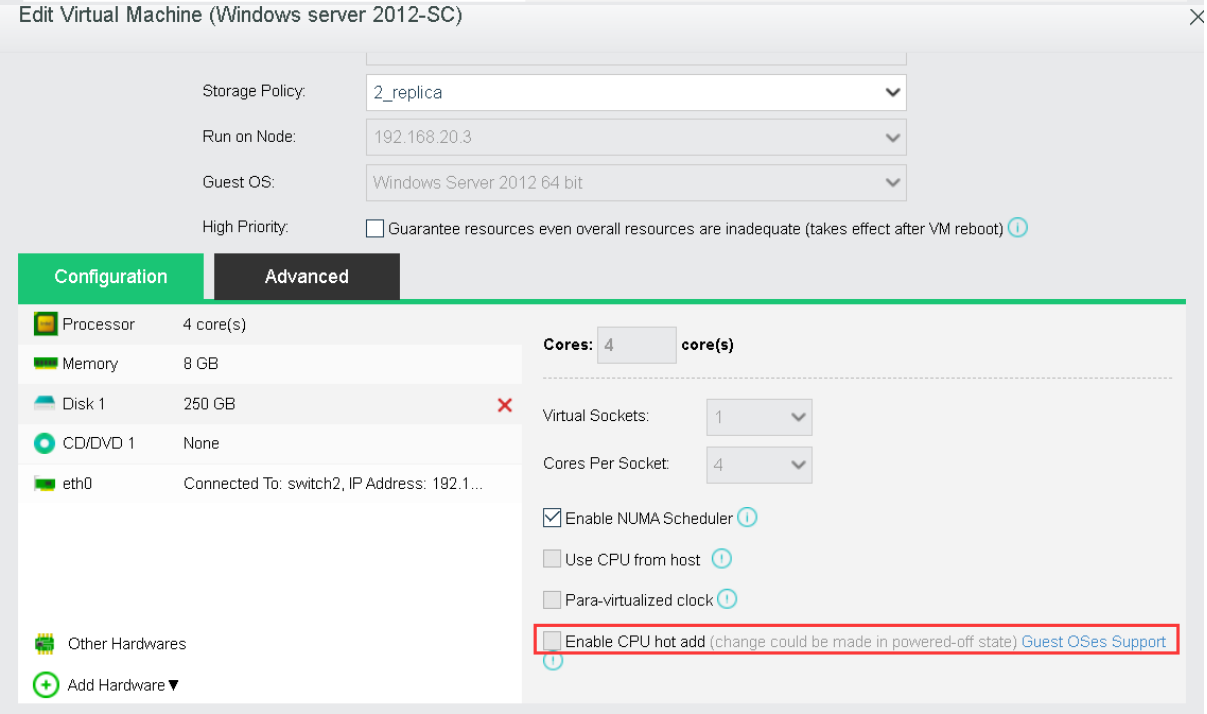
All the VM operating systems support automated disk and NIC hot add. Some VM operating systems do not support automated CPU and memory hot add. Refer to operation system list or contact relevant OS developers.

You may check resource usage regularly and add resources according to actual situations, so as to ensure proper operation of businesses. Configure automated hot add as follows:

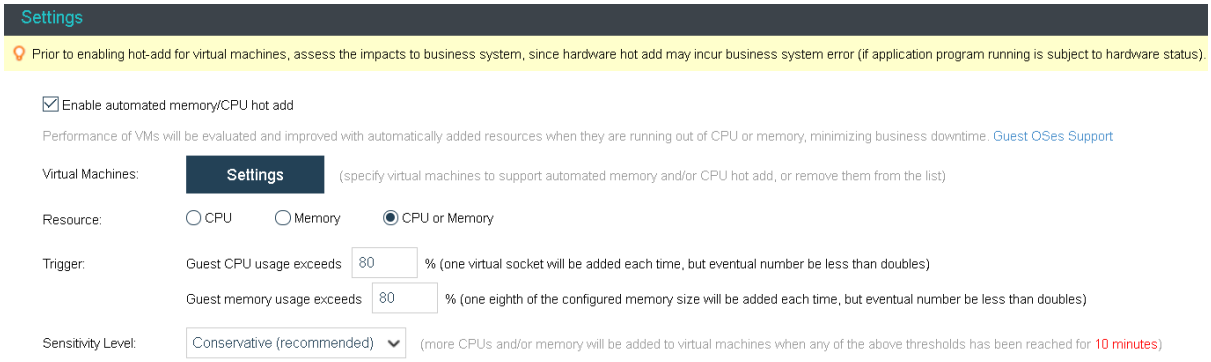
1. Enterprise edition is required.
2. Ensure that there are virtual machines in the cluster which support automated hot add.
3. Install vmTools.

4. Go to edit virtual machines to enable CPU hot add and memory hot add.

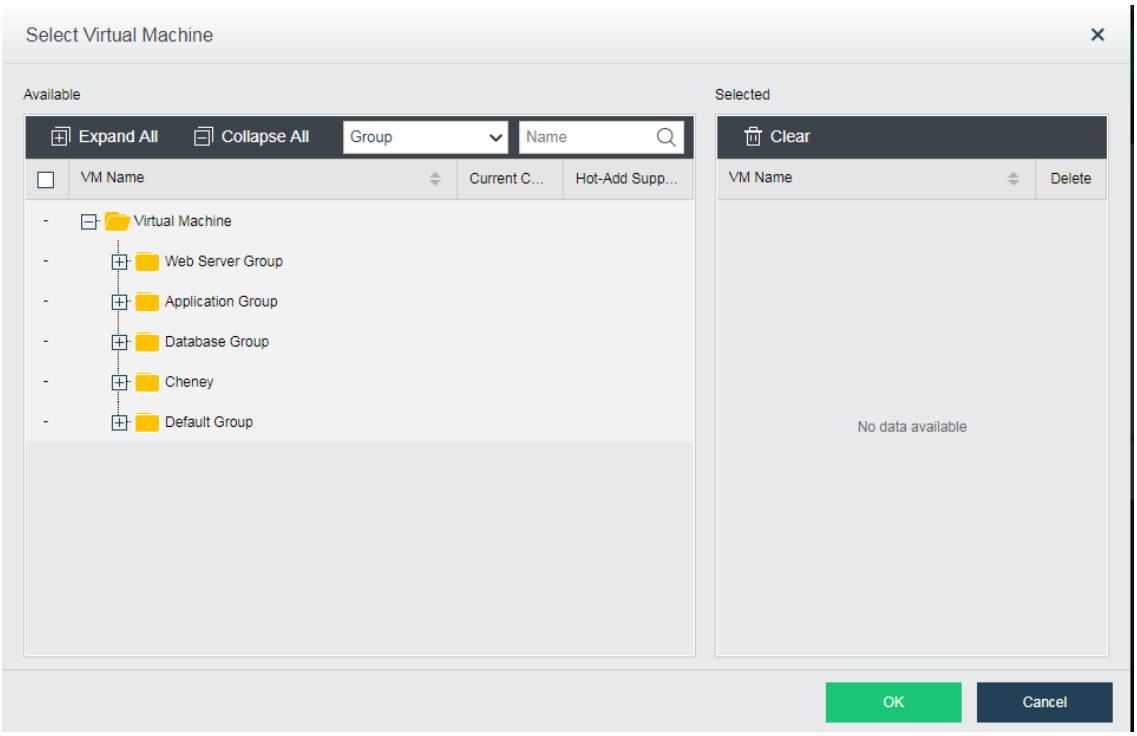




5. Go to **System > HA & Resource Scheduling > Automated Hot Add**, select **Enable automated memory/CPU hot** add, and configure **Resource, Trigger** and **Sensitivity Level** fields.



6. Add virtual machines to the VM list which support automated hot add.



7. Click **OK** to save changes.

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road,Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com

2.6.16 VM Scheduling

Function Description

In the VM scheduling page, you can add a new VM scheduling policy or select a policy to edit or delete. Through the scheduling policy, you can achieve precise control over the running location of VMs to meet the demand of dual-live.

Precaution

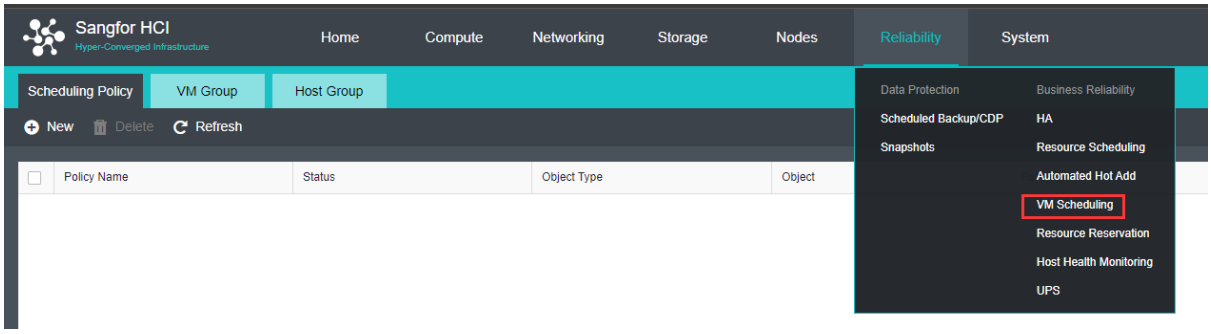
After a VM scheduling is added to a running VM, the VM must be restarted to take effect.

Prerequisites

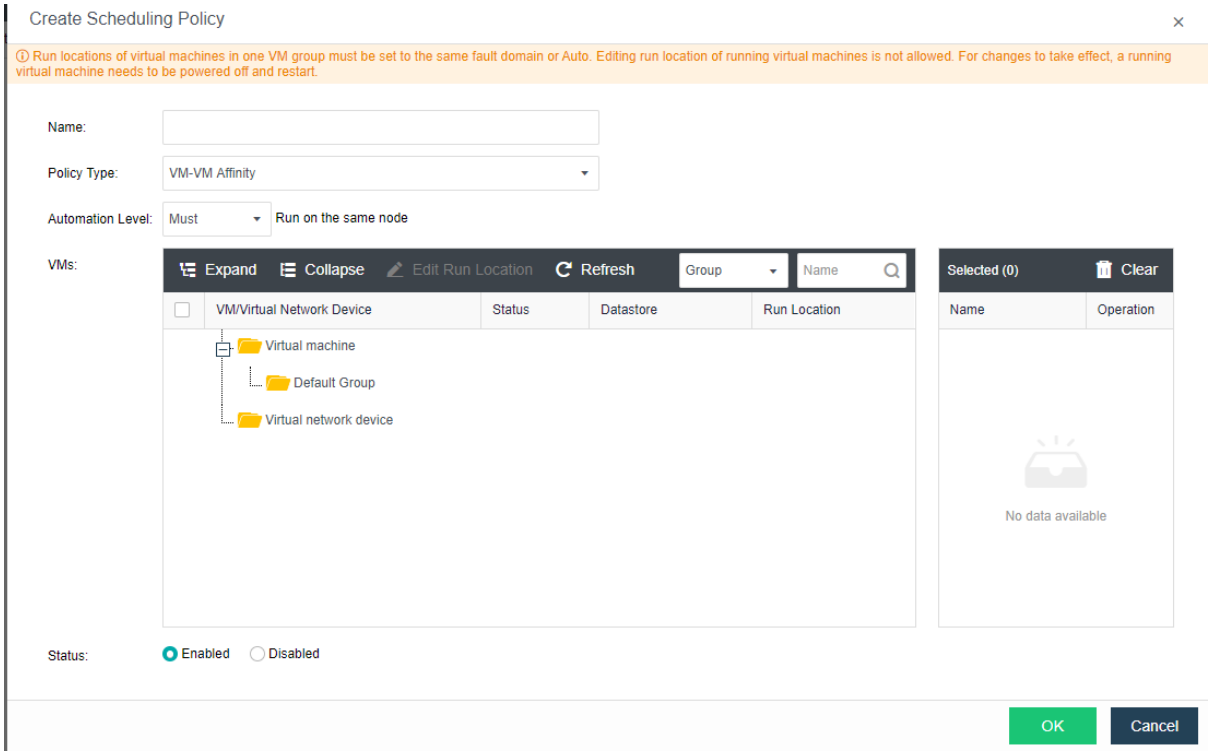
None

Operation steps

1. Navigate to Reliability > VM Scheduling.



2. Add a scheduling policy, and select the policy type.
   a. VM-VM Affinity – Scheduling based on selected VM to be running on same nodes..
   b. VM-VM Anti Affinity – Scheduling based on selected VM to be running on different nodes.
   c. VM Group Anti Affinity – Scheduling based on VM group to be running on different nodes while the VM in same VM group will be running on same node.
   d. VM-Host Affinity – Scheduling based on VM group to be run on nodes in a Host Group.



2.6.16 Advanced Settings

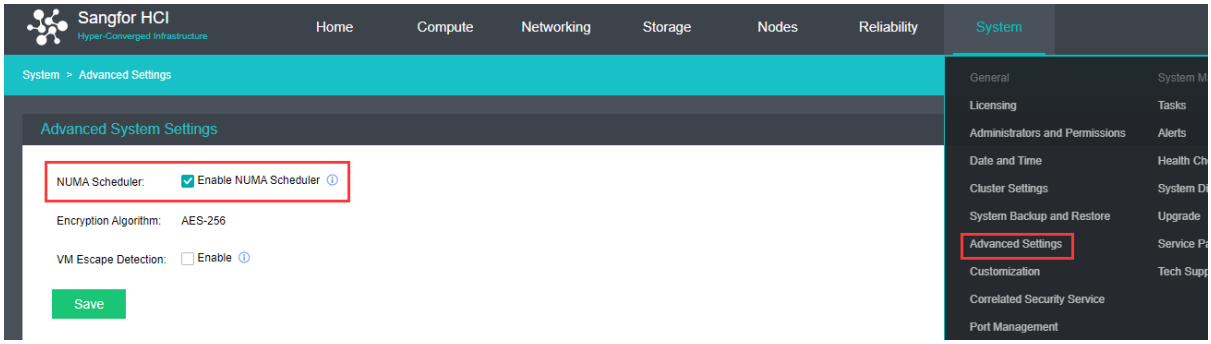
On the **Advanced Settings** tab, you can enable NUMA scheduler which can speed up memory access and improve VM performance. It takes effect after VM restart.

Besides, memory overcommitment ratio can also be configure or adjust under Advanced Settings tab.

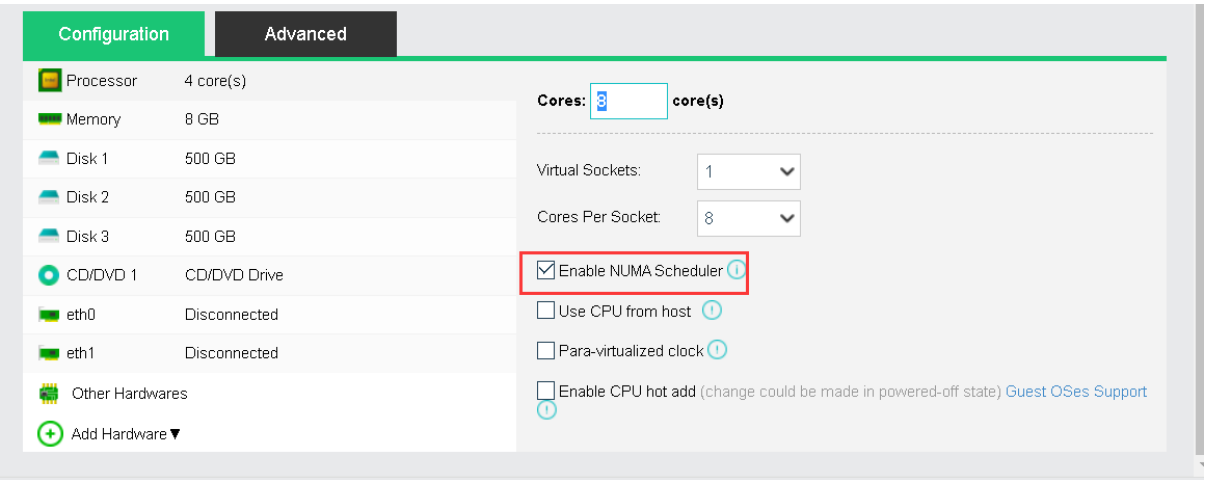
NUMA Scheduler

Once **NUMA scheduler** is enabled, it will be applied to all the virtual machines on the nodes in the cluster and it takes effect after VM reboot.Once disabled, it will be applied to all the virtual machines on the nodes in the cluster immediately. To enable NUMA scheduler for a virtual machine,do as follows:

1. Make sure the current version is Enterprise edition.
2. Make sure that the virtual machine has more than 8 cores and vmTools installed.
3. Go to **System > Advanced Settings,** select **Enable NUMA scheduler**.



4. Go to **Compute** and edit the virtual machine for which you want to enable NUMA scheduler, and then select **Enable NUMA Scheduler** option, as shown below:



5. Click **OK** to save the changes.

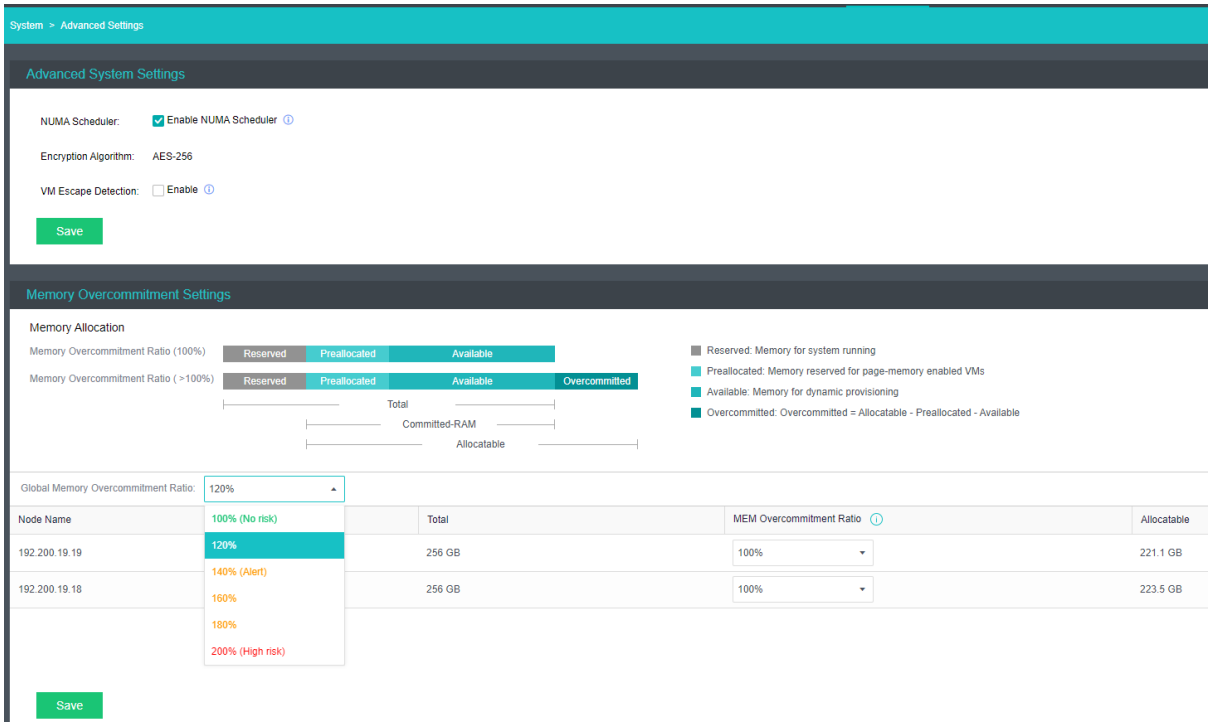
Once **Enable NUMA scheduler** is selected in **System > Advanced Settings**, you may also enable or disable NUMA scheduler on a specific virtual machine. Enabling NUMA scheduler takes effect after VM reboot while disabling NUMA scheduler takes effect immediately.

To project NUMA topology into a virtual machine, make sure that virtual machine has more than 8 cores and vmTools has been installed.

Memory overcommitment

Memory overcommitment is a concept in computing that covers the assignment of more memory to virtual computing devices (or processes) than the physical machine they are hosted, or running on, actually has.

You may configure the memory overcommitment ratio under **System** > **Advanced Settings**.



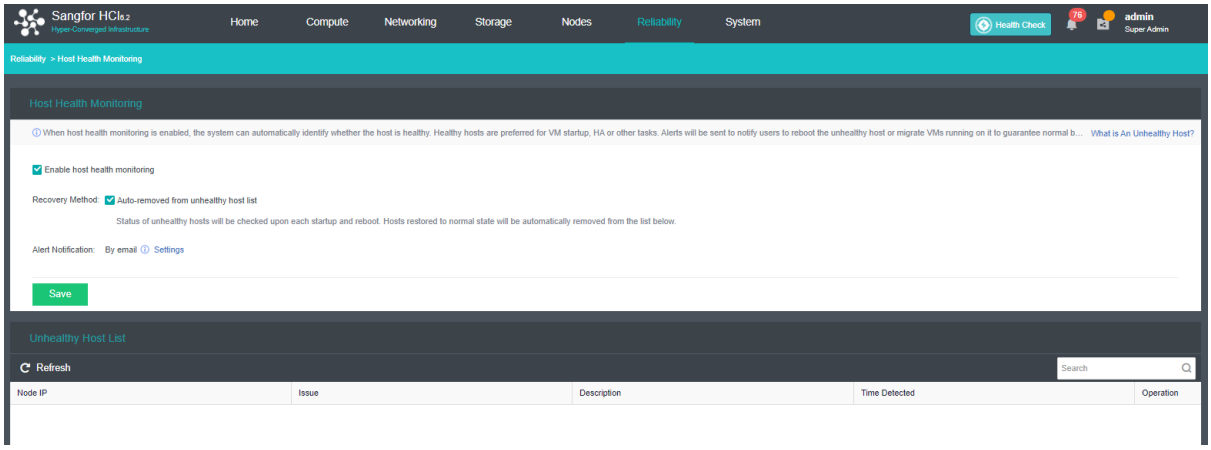
Memory allocation: User can view the explanation of the memory allocation for better understanding.

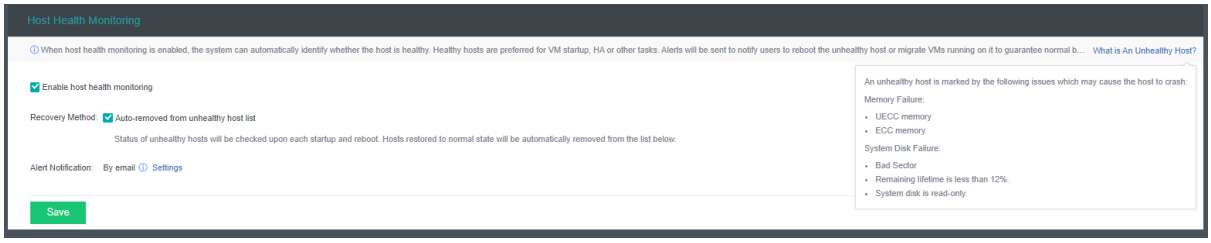
Global Memory Overcommitment Ratio: Configure the memory overcommitment ratio for all nodes inside the cluster.

MEM Overcommitment Ratio: Change the memory overcommitment ratio for different nodes.

2.6.17 Host health monitoring

Host health monitoring monitors whether the system disks and memory of hosts in the cluster are in a healthy state. These features will automatically reduce the priority of unhealthy host in the process of VM startup, HA, and other tasks. Only support to detect the host memory ECC/UECC failure, HDD bad sector, SSD remaining lifetime, and system disk read-only issue.





To enable the host health monitoring, require to enable the option "Enable host health monitoring".

To remove the unhealthy host automatically, select "Auto-removed from unhealthy host list". The status of unhealthy hosts will be checked upon each startup and reboot. Hosts restored to the normal state will be automatically removed from the list below.

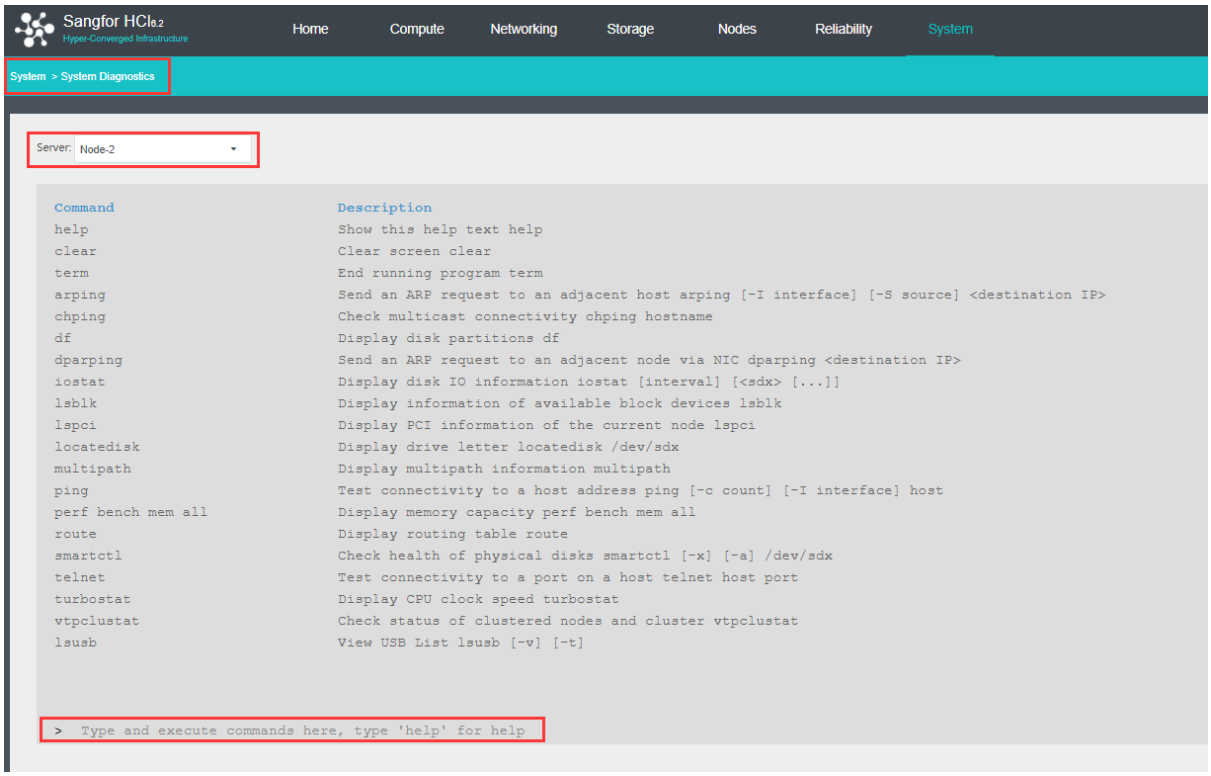
To notify the user, you can configure the alarm notification by email.

HCI automatically detects the unhealthy host and display in the unhealthy host list. The issue and solution will be also displayed in the list.

To remove the unhealthy host manually, you can click on the remove operation remove the host from the list after resolving the issue.

2.6.18 System Diagnostics

Simple troubleshooting and information gathering can be carry out throughout the command available on **System** > **System Diagnostics**.



Server: Select the corresponding node to execute the command.

> : Enter the available command shown above to execute.

2.6.19 PaaS Correlated

Function Description

The KubeManager platform supports docking to virtual storage aSAN or file storage NFS for data persistence storage, so that users can store business data outside the application Pod and protect the application data from being affected when the application Pod fails. To interface KubeManager platform with aSAN storage, you need to use PAAS correlated function in Correlated Security Service.

Precaution

No

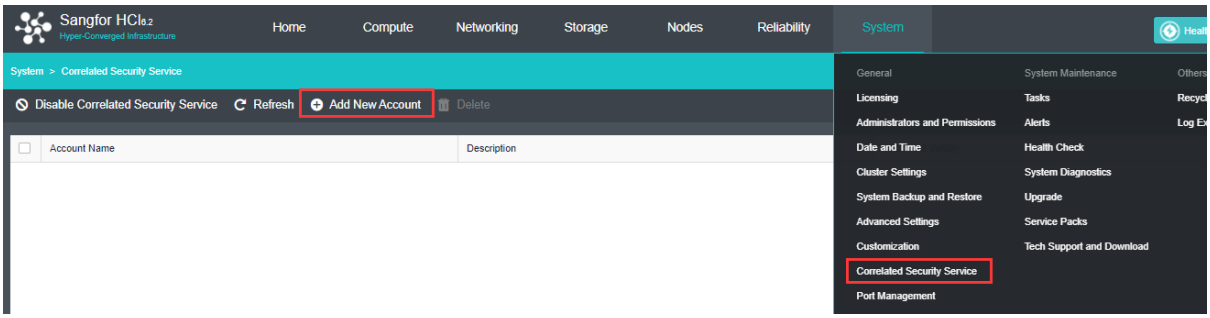
Prerequisites

1. aSI license is required for HCI platform.

2. The KubeManager platform and HCI platform can communicate normally.

Operation steps

1. Login to the HCI web console, navigate to **System** > **Correlated Security Services**, and click **Add New Account**.



2. Customize the account information.

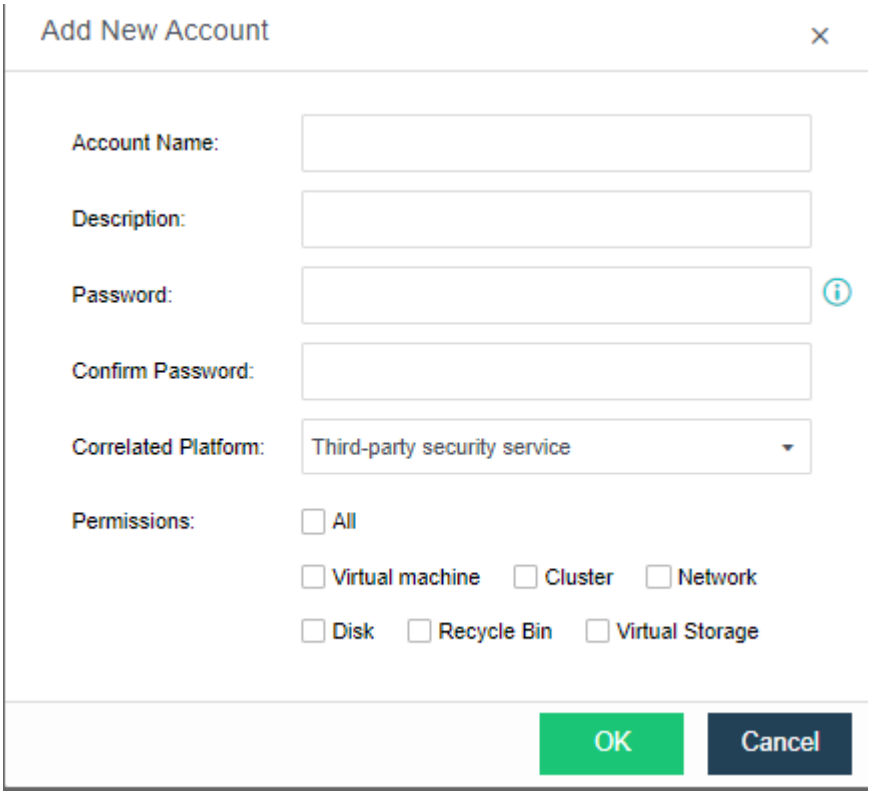
   Account name: Name of the account, for example: simon.

   Description: Account description, for example: simon-paas.

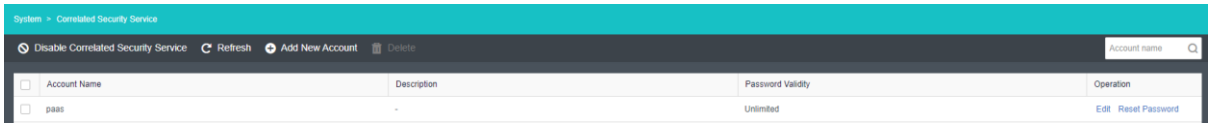
   Password: Password of the account.

   Correlated Platform: PaaS.

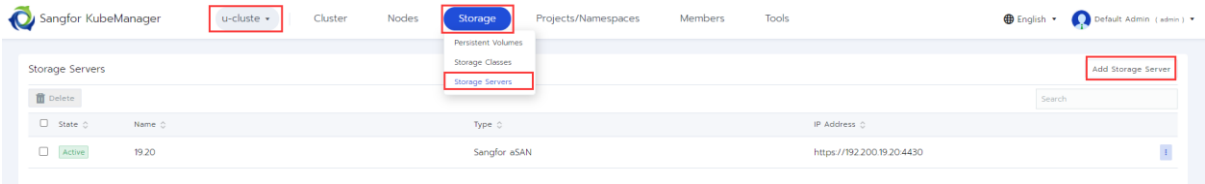
   Permission: Check Virtual Storage (checked by default).



3. Click <OK> and the service account is added.



4. Login to KubeManager platform, switch to the cluster where you want to add storage server,navigate to **Storage** > **Storage Servers**, and click **Add Storage Server**.



5. Enter the name of the storage server, select the corresponding storage type, and configure the basic information of the server.
    a. Name: Customize the server name.
    b. Type: Support Sangfor NFS and Sangfor aSAN storage servers; Sangfor aSAN is recommended, with high reliability and stable performance.
    c. c. NFS server information.

       Server address: the address of the NFS server.

       Storage path: The path where the NFS server is stored.

       Version: The version of the NFS server.
    d. aSAN Server Information.

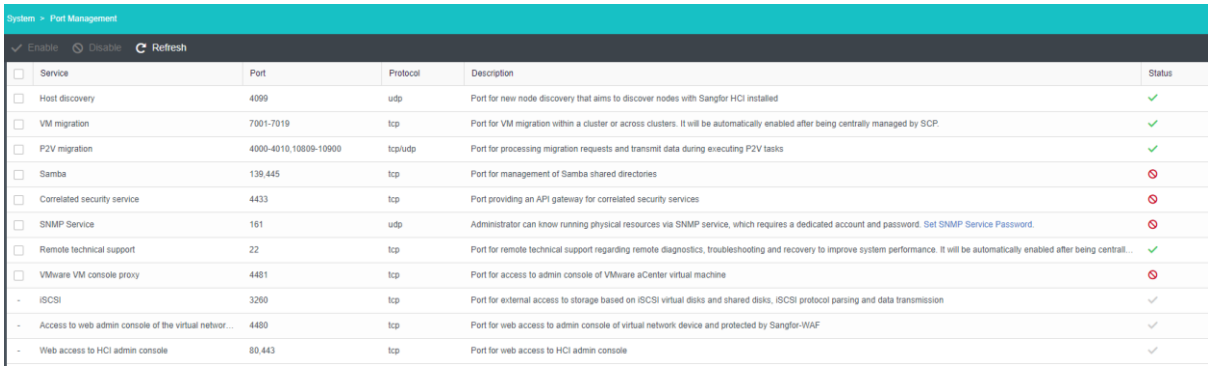
       Gateway address: https:// HCI cluster IP:4433.

       Authenticated Account: The name of the service account added in step 2.

       Authenticated Password: The password of the service account added in step 2.
6. Click **Save** to finish adding the storage server.

2.6.20 Port Management

The listening port on HCI for different purposes can be view and manage on **System** > **Port Management** starting from version 6.1.0.

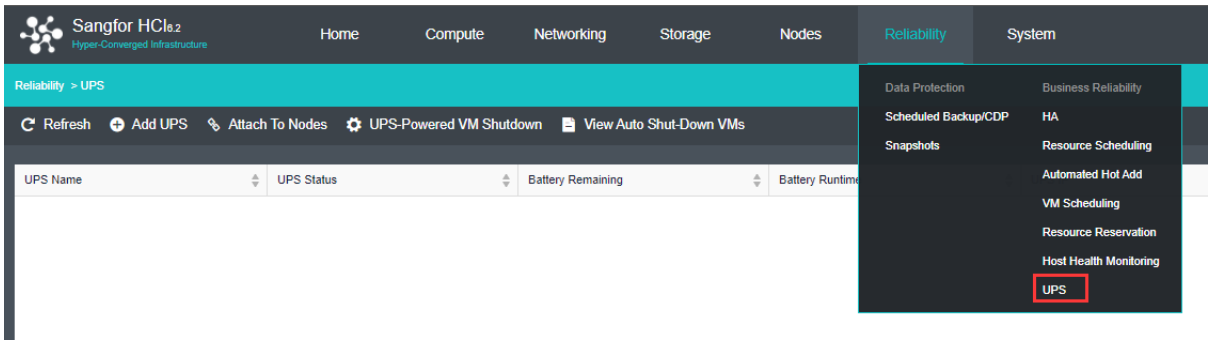


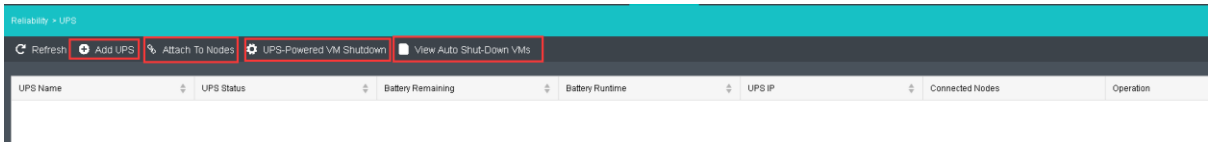
2.6.21 UPS

By integrating UPS to HCI, VM is protected when the power grid is down. It protects the VM from immediately shutting down and allow the VM to shut down properly when a certain condition is met.

HCI integrates with UPS through SNMP (simple network management protocol) protocol. UPS vendor provides the OID (object identifier) library and through SNMP protocol, HCI is able to receive the battery usage of the UPS and take actions when the battery usage is below certain threshold.

Configure the UPS setting under **Reliability** > **UPS**





Add UPS: Add new UPS to the HCI.

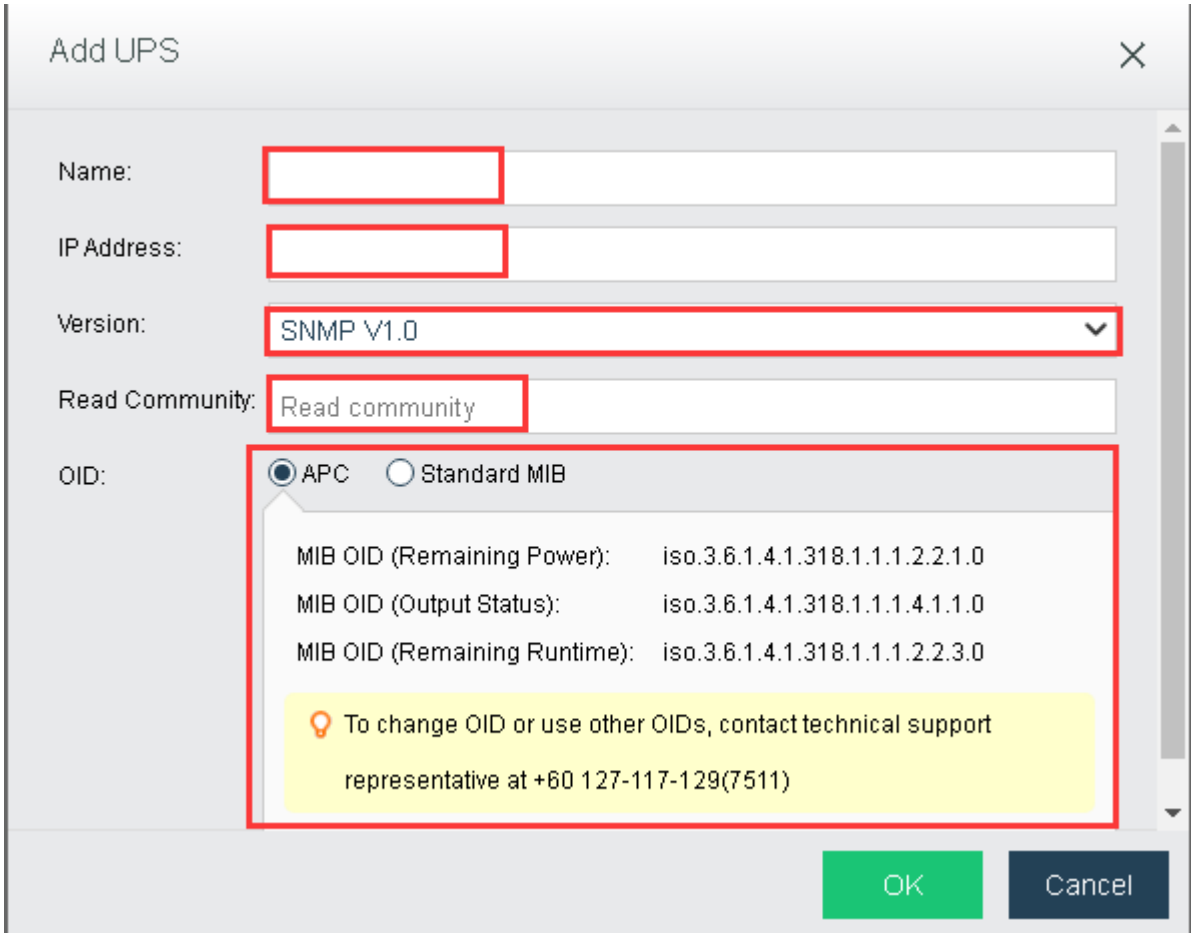
i. Name : Enter the name for the UPS.

ii. IP Address : IP Address of the UPS.

iii. Version : SNMP version with 3 options, version 1,2 and 3.

iv. Read Community : The read community in the SNMP setting.

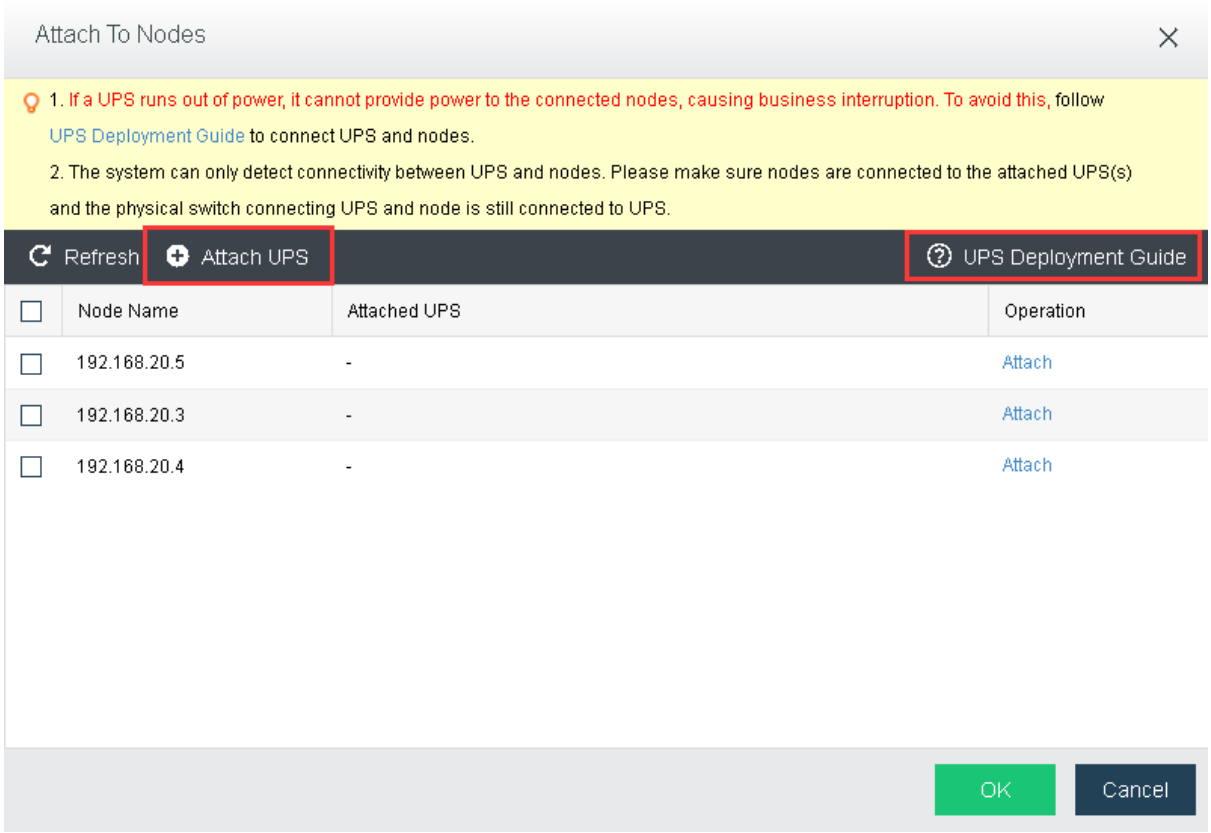
v. OID : Select whether it is APC or Standard MIB. For other OID, please contact Sangfor Support teams for further assistance.

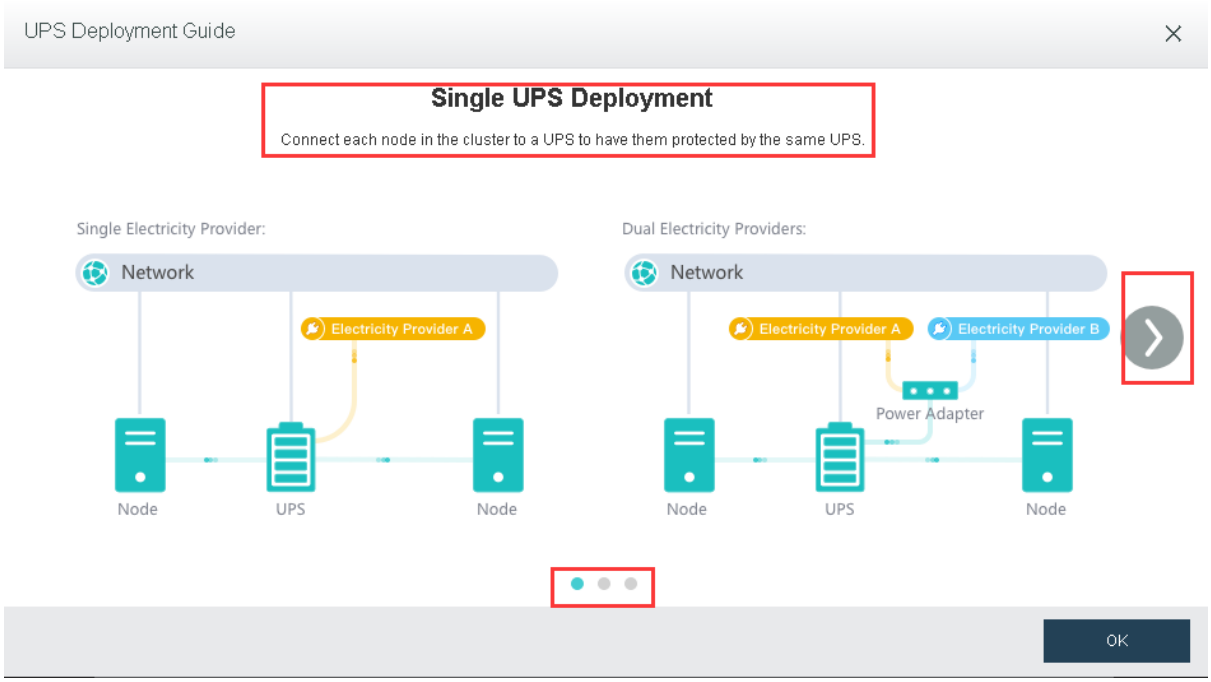


Attach To Nodes: Select the corresponding nodes to attach with the UPS.

i. **Attach UPS**: Select the UPS to be attach to the selected nodes.

ii. **UPS Deployment Guide**: View the UPS deployment guide for different scenario with single UPS, 2 UPS and multiples UPS.



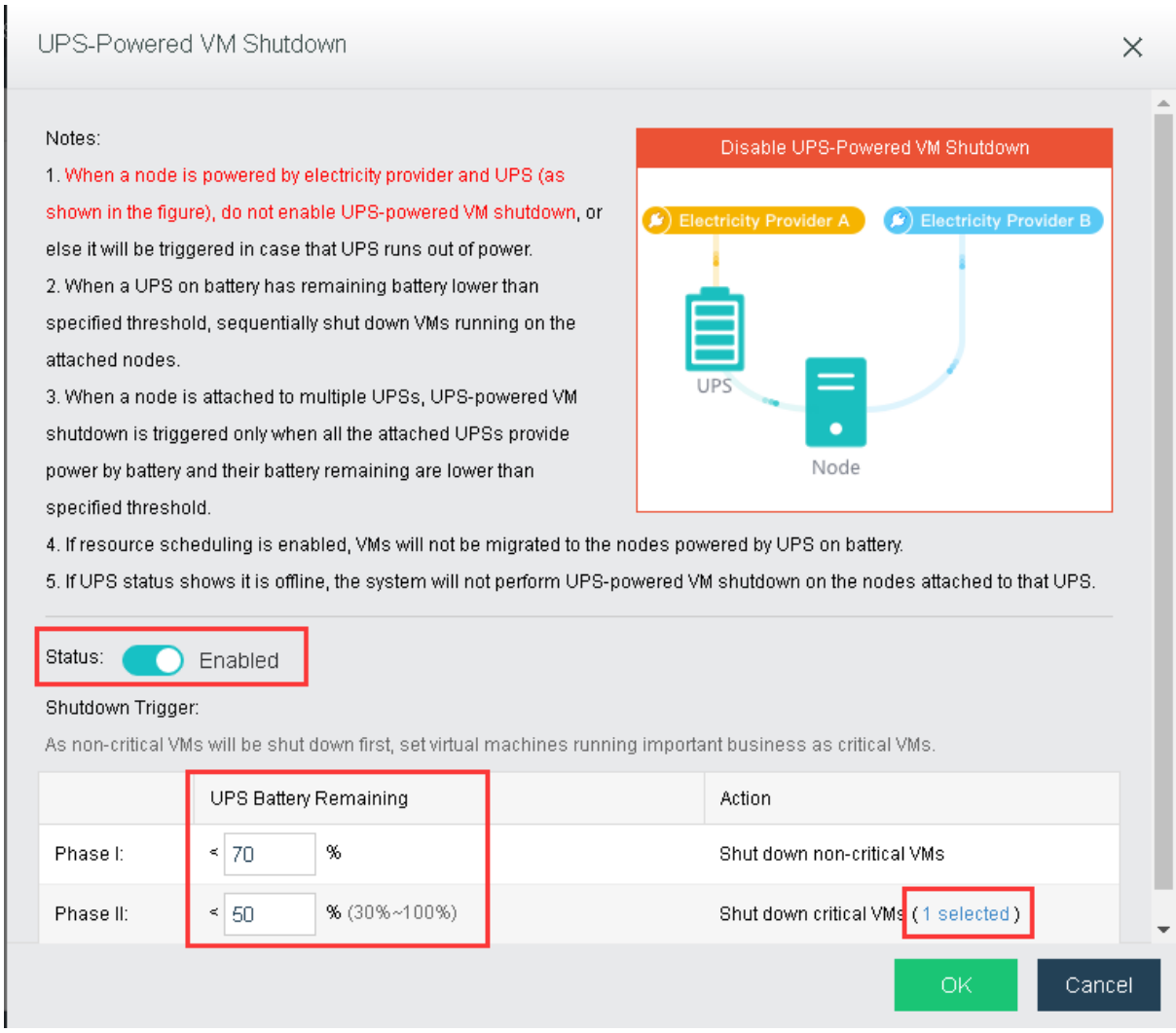


UPS-Powered VM Shutdown : When the node is powered by UPS only, this function allow to shutdown VM follow by phases along with the battery percentage.

i. Status: Do not enable this function when the node is powered by both UPS and eletricity provider.

ii. UPS Battery Remaining: Configure the battery percentage to shutdown the VM accordingly.

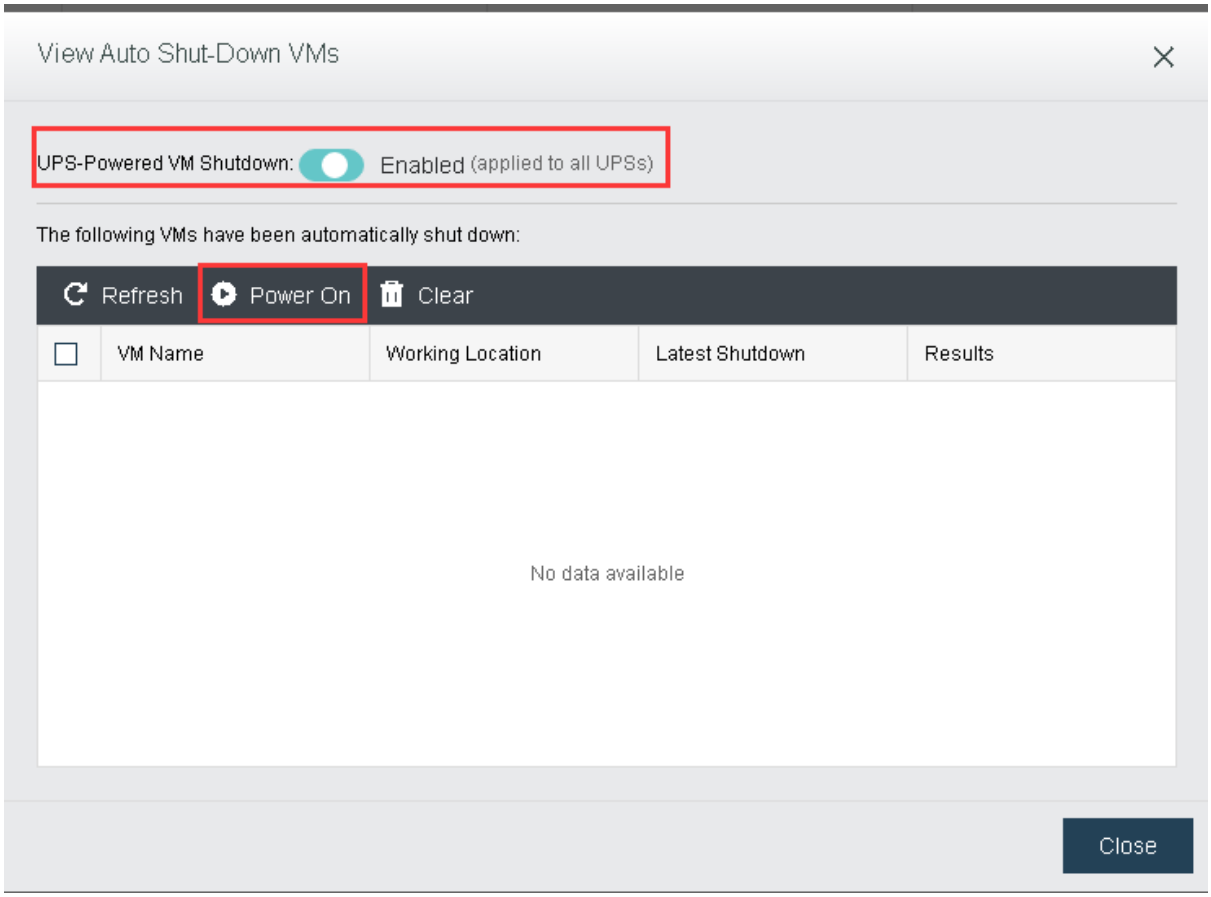
iii. Critical VM: Select the important vm as critical VM for phase II.



View Auto Shut-down VMs: The VM shutdown by the UPS-Powered VM Shutdown module can be view and select to power on.

i. UPS-Powered VM Shutdown: Same configuration with the Status in UPS-Powered VM Shutdown.

ii. Power On: Power on the selected powered off VM.



2.6.22 Online SP package

2.6.21.1 Online SP settings

The online patch service can obtain the latest patch information from the online patch platform regularly to ensure the stability and security of the device.

The management network can connect to the HCI equipment of the Internet, and directly access the Sangfor online patch platform to update the latest patch information. For HCI devices in the internal network of the management network, if the virtual machine can access the Internet, you can use the Sangfor network proxy virtual machine to update the patch; if the virtual machine network cannot connect to the Internet, you can use a third-party network proxy to access the online patch platform; The SP patch server is deployed on the Internet for patch updates.

Precautions

1. After the patch service is configured, the connectivity must be tested to ensure that the platform can connect to the patch server.

2. It is not recommended that the management network can directly access the online patch service platform, because directly exposing HCI to the public network is not conducive to the security of the platform.

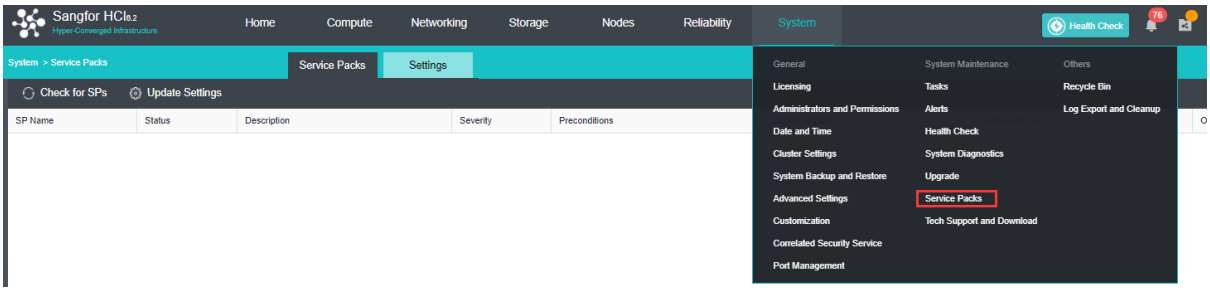
3. Use Sangfora network proxy virtual machine to access the online patch platform mode. After importing the network proxy virtual machine, do not modify the virtual machine name (the default name is: _SangforaOperation_VM_WorkStation_), otherwise the proxy service will become invalid.

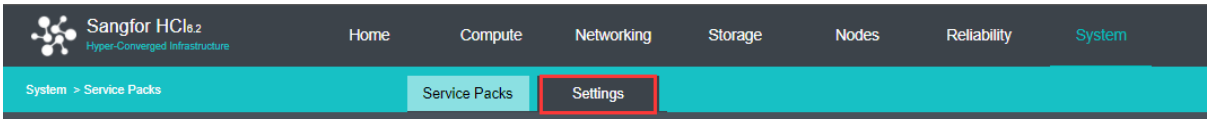
Precondition

The customer network needs to release the address update1.sangfor.net of Sangfor's patch server to ensure that the platform can access the patch server.

Operation Step

1. Enter the System > Service Packs interface, and click the Settings tab.

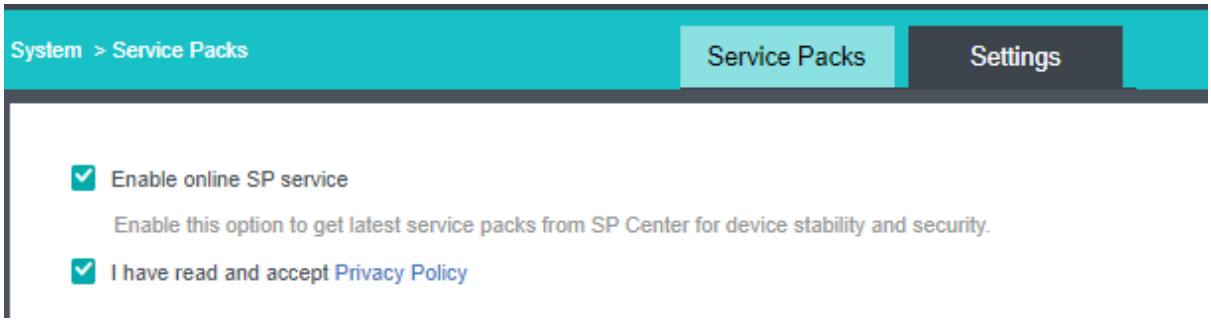




2. Click SP Center Addresses to ensure that the patch server has been allowed on the customer network. The requirements are shown in the table below.

Server IP Address	Description	Requirement
https://cloudbgcop.sangfor.com	Cloud Service IP Address.	Must be allow.
http://update1.sangfor.net	Online Patch Platform IP Address.	Allow at least one of the IP, it is recommended to allow multiple.
http://update2.sangfor.net		
http://update3.sangfor.net		
http://121.46.26.221		

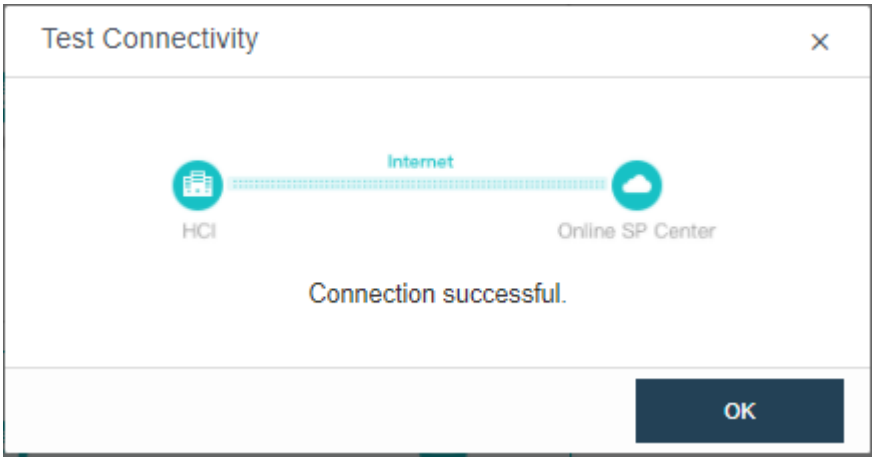
3. Check the "Enable online SP service" option.
4. Check the " I have read and accept Privacy Policy" option.



5. According to the HCI deployment scenario and network conditions, select an appropriate online platform communication method for setting. (After selecting the corresponding scene and configuring, skip other scenes and go to step 6 for configuration).

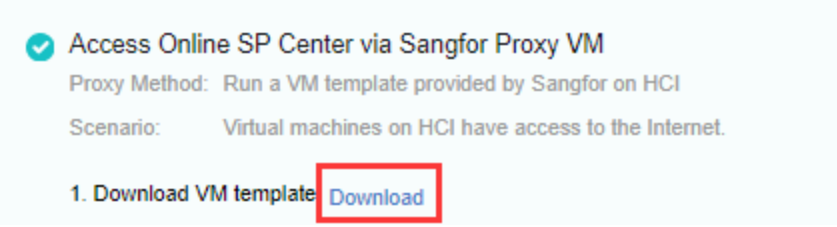
Scenario 1: Directly access the online patch platform.

- Select [Direct Access to Online SP Center] for communication mode settings, test the connectivity and save the settings.

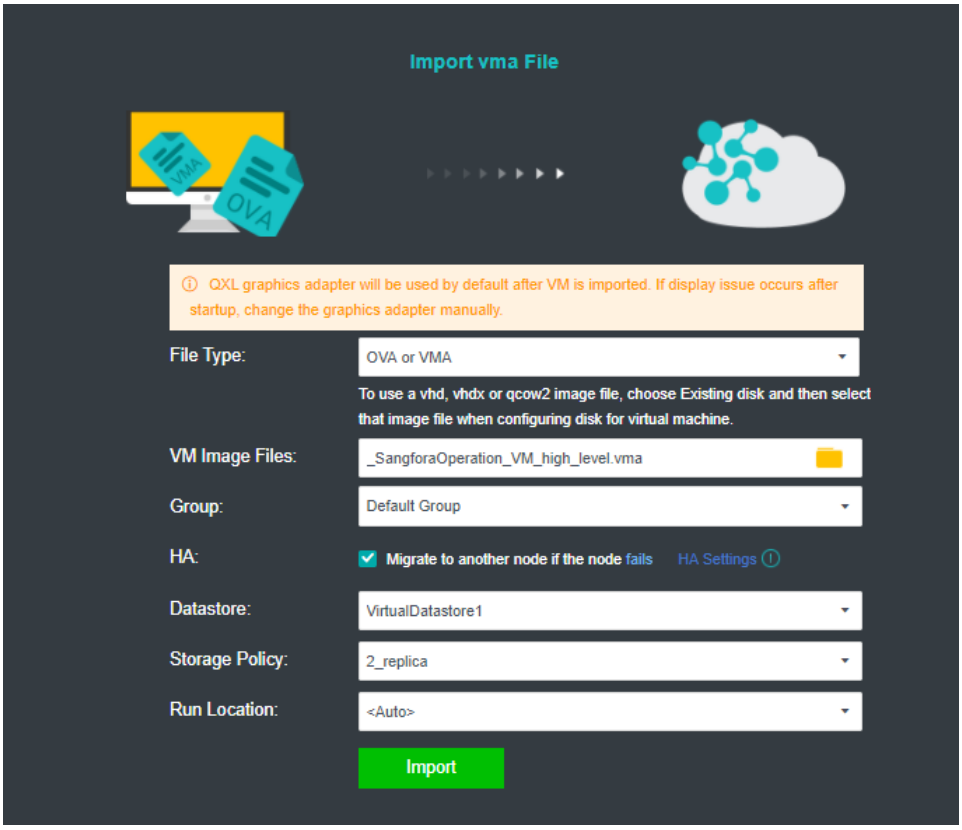


Scenario 2: The HCI platform cannot be connected to the Internet, but virtual machines that can be connected to the Internet can be deployed on the HCI.

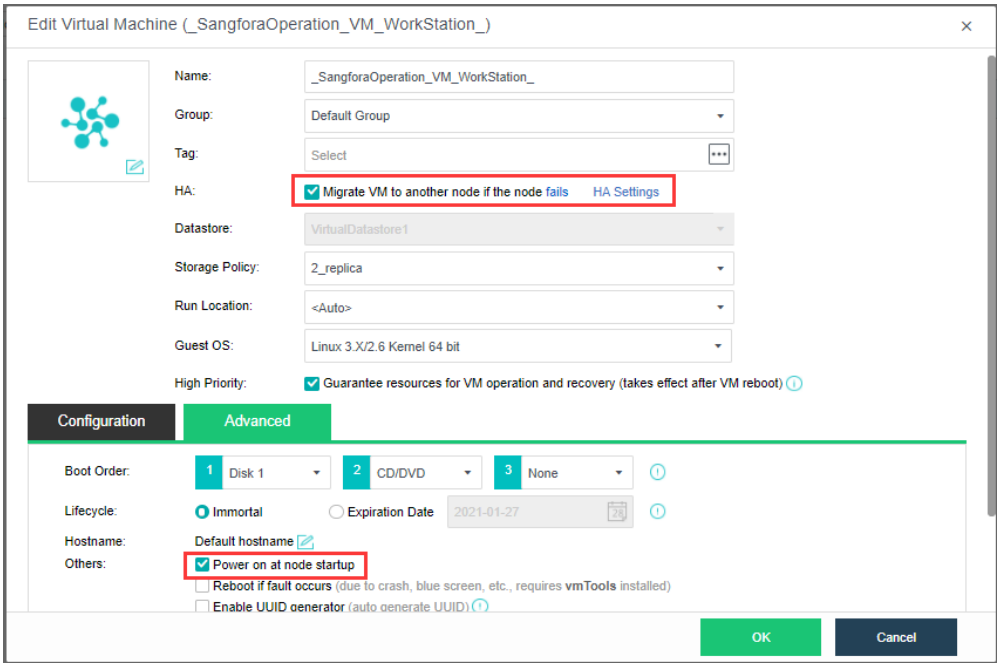
- Download the virtual machine template.



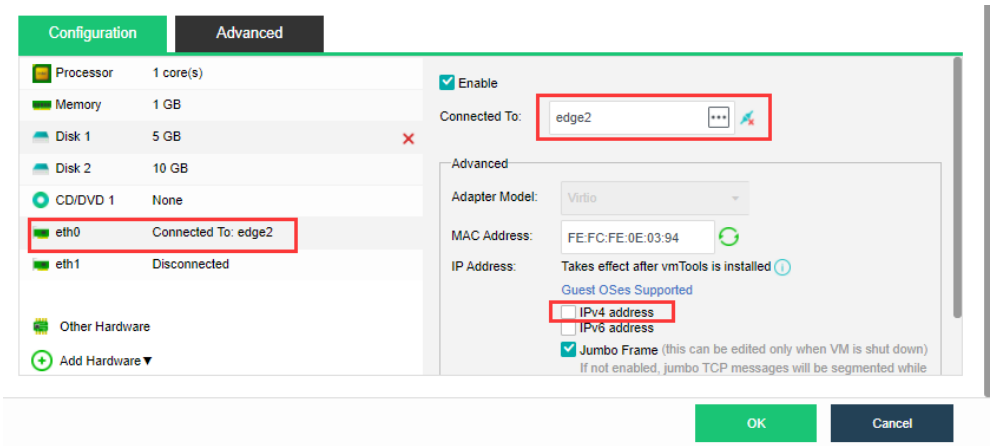
- Import the downloaded VM template into HCI. When importing the template, it is recommended to configure as following:
  a. HA: Enable.
  b. Datastore: Shared datastore for all nodes, for example virtual storage.
  c. Run location: <Auto>.

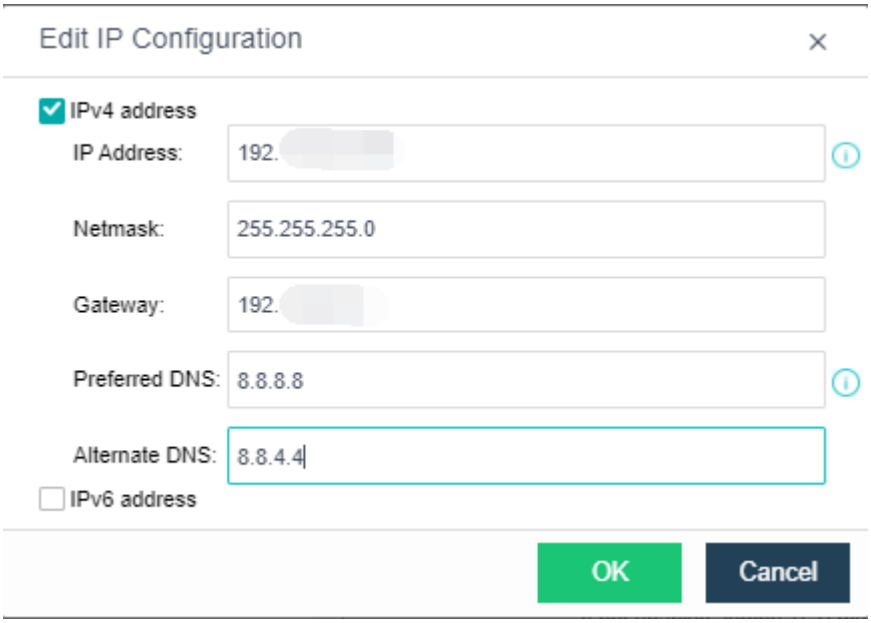


- Edit the virtual machine, view the Advanced configuration, and confirm that HA is enabled as well as the "Power on at node startup".

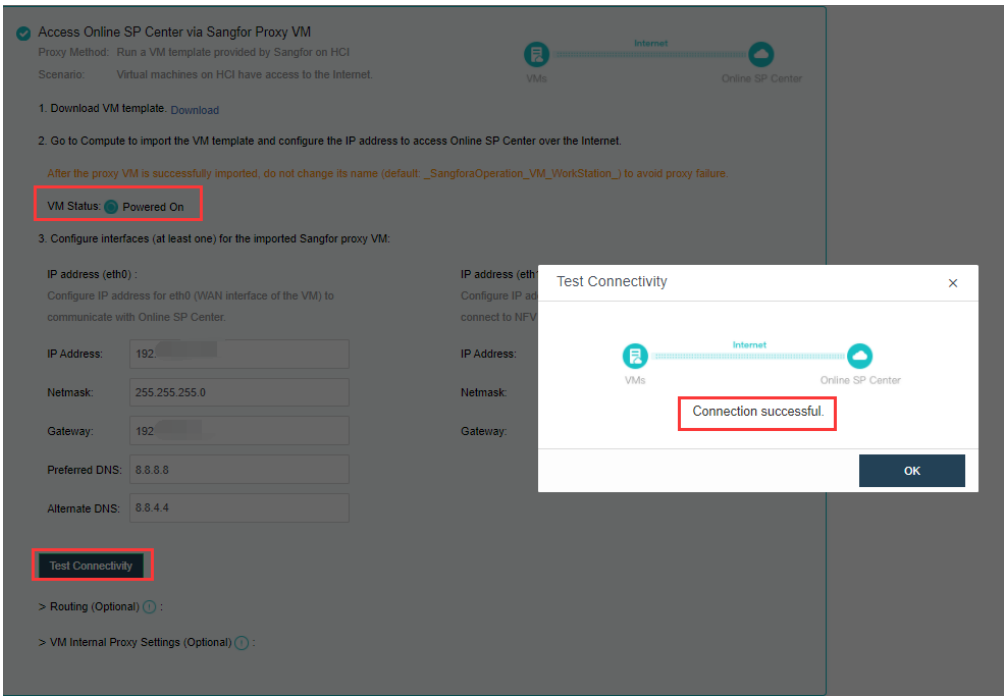


- Configure the virtual machine etho to connect to the physical exit, and ensure that the physical exit can access the external network. Modify the IP settings on the page, configure the planned address to the virtual machine, and start the virtual machine.



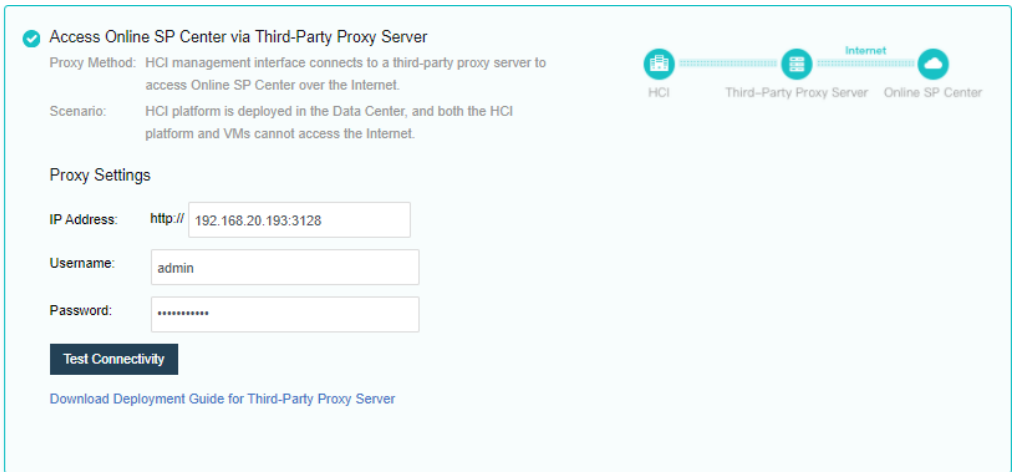


- As shown in the figure below, in the online patch platform communication mode settings, configure etho's IP, subnet mask, gateway (optional), preferred DNS (optional), alternative DNS (optional), test connectivity, and ensure the IP Access to the online patch platform address. (Eth1 is the internal network port of the proxy virtual machine. If there is an NFV device, you need to configure the eth1 network port to connect to the NFV device. The configuration method refers to the configuration of the etho port to connect to the network where the NFV device is located).



Scenario 3: The HCI platform cannot be networked, but it can be networked through a third-party agent.

- The network deployment is shown in the figure above. In this scenario, a third-party proxy server is selected to access the online patch platform.



- Click <Download Deployment Guide for Third-Party Proxy Server>, the downloaded content is a compressed package named "Proxy_Squid_Deployment_Guidance.rar", which contains document descriptions and recommended agent installation packages and configuration files.
- Refer to the downloaded configuration guide, install and configure a third-party agent program on the proxy server, and confirm that the proxy server can access the Sangfor online patch server. Deploy 2 network ports as shown in the figure below, one can access the Internet to connect to the Sangfor patch server, and the other can access the hyper-converged platform of the intranet.

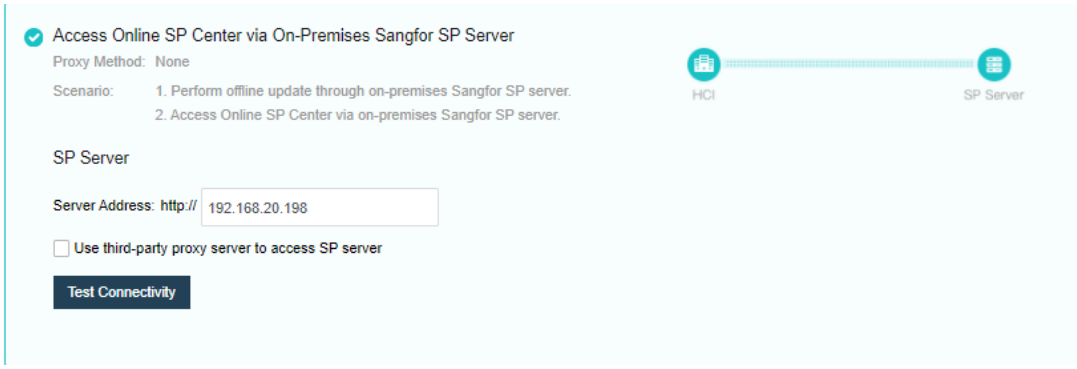
```
[root@localhost ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr FE:FC:FE:2F:1B:B6
          inet addr:192.200.244.33  Bcast:192.200.244.255  Mask:255.255.255.0
          inet6 addr: fe80::fcfc:feff:fe2f:1bb6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1533230 errors:0 dropped:43718 overruns:0 frame:0
          TX packets:58615 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:338489413 (322.8 MiB)  TX bytes:6926447 (6.6 MiB)

eth1      Link encap:Ethernet  HWaddr FE:FC:FE:B5:C0:EF
          inet addr:10.250.0.20  Bcast:10.250.0.255  Mask:255.255.255.0
          inet6 addr: fe80::fcfc:feff:feb5:c0ef/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:95080 errors:0 dropped:0 overruns:0 frame:0
          TX packets:230 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7877420 (7.5 MiB)  TX bytes:69578 (67.9 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

[root@localhost ~]# ping update1.sangfor.net
PING update1.sangfor.net.cdn20.com (113.96.140.206) 56(84) bytes of data.
64 bytes from 113.96.140.206 (113.96.140.206): icmp_seq=1 ttl=54 time=8.04 ms
64 bytes from 113.96.140.206 (113.96.140.206): icmp_seq=2 ttl=54 time=8.44 ms
64 bytes from 113.96.140.206 (113.96.140.206): icmp_seq=3 ttl=54 time=7.52 ms
64 bytes from 113.96.140.206 (113.96.140.206): icmp_seq=4 ttl=54 time=8.19 ms
64 bytes from 113.96.140.206 (113.96.140.206): icmp_seq=5 ttl=54 time=8.55 ms
^C
--- update1.sangfor.net.cdn20.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 7.521/8.150/8.552/0.361 ms
[root@localhost ~]# _
```

- Fill in the proxy address (IP+port, example: 10.250.0.20:3128) set in the second step on the HCI platform. And the proxy authentication user name and password set during the deployment of the proxy server.
- The IP address is the IP of the internal network port of the proxy server.
- The port is the publishing port of the proxy service, and the default is 3128.
- Click <Test Connectivity> to confirm that the network is connected.

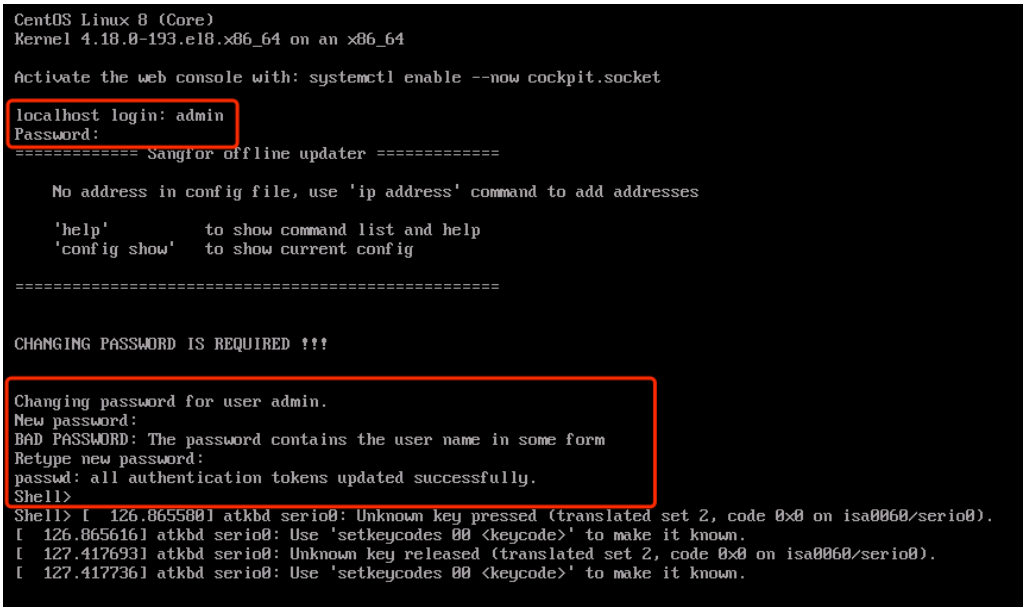
Scenario 4: The HCI platform cannot be connected to the Internet, and the SP patch server has been set up in the local data center.

The customer uses multiple products of Sangfor and cannot connect to the Internet. At this time, only one Sangfor intranet SP patch server is deployed in the data center. Then, when updating the patch offline, the administrator only needs to upload the patch package to the intranet SP. It can be installed on the patch server, and each product obtains the patch package update by itself, without the administrator having to log in to multiple product platforms one by one to upgrade.

Customers who use Sangfor multiple products only need to deploy one Sangfor intranet SP patch server, which can act as a unified agent of the online patch platform for networking, and download and cache patch packages to distribute to many products.



- In this scenario, select the "Use a locally built SP patch server" method.
- Contact Sangfor technical support to obtain the vma template of the offline patch server.
- Import the virtual machine of the offline patch server in [Virtual Machine\New\Import Virtual Machine].
- After importing, click <Go to Virtual Machine>. Click <Edit> virtual machine. Edit the network card and connect to the planned network.
- Open the console and enter the default username and password, admin/Sangforupdater. After successful login, the system will ask to change the default password, please configure a new password.



- Use the initsrv command to modify the IP address, mask, gateway, and DNS. Pressing Y to save the configuration will automatically restart the olu server to

complete the configuration.

- Confirm the network card configuration and check the connectivity of the network.

```
Shell> ifconfig
ens18: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.250.0.10  netmask 255.255.255.0  broadcast 0.0.0.0
        inet6 fe80::fcfc:feff:fe2c:6a11  prefixlen 64  scopeid 0x20<link>
        ether fe:fc:fe:2c:6a:11  txqueuelen 1000  (Ethernet)
        RX packets 2792  bytes 171403 (167.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 54  bytes 2668 (2.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 66  bytes 6192 (6.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 66  bytes 6192 (6.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

Shell> ping 10.250.0.20
PING 10.250.0.20 (10.250.0.20) 56(84) bytes of data.
64 bytes from 10.250.0.20: icmp_seq=1 ttl=64 time=0.925 ms
64 bytes from 10.250.0.20: icmp_seq=2 ttl=64 time=1.38 ms
64 bytes from 10.250.0.20: icmp_seq=3 ttl=64 time=1.83 ms
```

- Enter the command moashell. Pop up the QR code, scan it with Sangfor Pocket Assistant (MOA), get the password in the Pocket Assistant "Little Assistant", and enter it into the command line. (Need Sangfor technical support processing).

```
Shell>
Shell>
Shell> moashell
```

- Create a user used by the olu server and set a password, and change the group of the olu user to root.

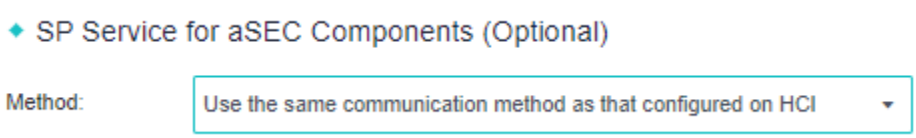
```
[root@localhost ~]# useradd olu
[root@localhost ~]# passwd olu
Changing password for user olu.
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]#
[root@localhost ~]# usermod -g root olu
[root@localhost ~]#
```

- Use the newly added olu account to log in to the patch server, upload the patch package of HCI and NFV devices to the /var/wwwroot directory through the sftp tool, and view it in the HCI patch list after decompression.

```
[olu@localhost wwwroot]$
[olu@localhost wwwroot]$
[olu@localhost wwwroot]$ pwd
/var/wwwroot
[olu@localhost wwwroot]$
```

- After configuring the Olu server, test the connectivity of the SP patch server on the HCI interface, fill in the address of the SP patch server, and click <test connectivity>.

6. Set the security component (aSEC) patch service (optional), select "The communication mode of the patch service is consistent with HCI".



7. Save the settings by clicking the Save button.

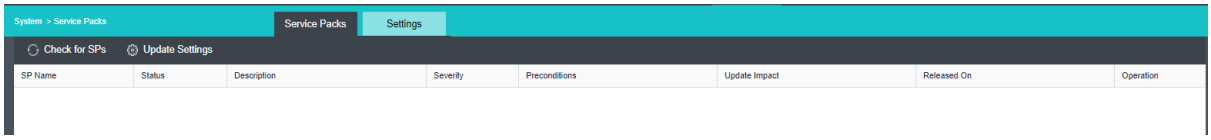
2.6.21.2 Patch information acquisition

Function Description

The patch information can be viewed in **Service Packs**, including:

- The name of the patch package, such as sp-xxx-xxx.
- Patch package status, such as: not downloaded, downloading, downloaded, upgrading, upgraded, etc.
- The description of the patch package, such as: the patch solves the xxx problem.
- The severity of the patch package, such as high, medium, and low.
- Preconditions for the patch, such as: None, and the virtual machine needs to be shut down.

- The impact of the patch upgrade, such as: none, the network will be interrupted for xx seconds.
- The patch release time, such as: 2020-10-20.
- Patch operations, such as upgrade, retry.



Precautions

1. If the platform can be connected to the Internet or through the network proxy virtual machine/third-party proxy, the online patch platform address can be accessed, which can be automatically obtained regularly or the user clicks to immediately obtain the patch information required by the platform.

2. If the communication mode setting is "Use the SP patch server built by the local data center", it will be automatically obtained from the patch server or click to obtain it now.

Steps

1. Navigate to **System** > **Service Packs**.

2. Click the **Update Settings** button to set the patch upgrade method.

SP without Update Impact:

- When the patch is upgraded, it has no impact on platform services and virtual machines.
- Patch upgrade options: automatic upgrade, manual upgrade. After the automatic upgrade is selected, the patch will be automatically upgraded from 01:00AM-06:00AM daily.

SP with Update impact:

- When a patch is upgraded, it may affect platform services or virtual machines. Therefore, the administrator must confirm the impact of the patch and choose a suitable time for manual upgrade.
- Patch upgrade option: manual upgrade.

3. After configuring the patch upgrade options, click <**OK**>.

4. Click the **Check for SPs** button to immediately obtain the patch information required by the platform.

Chapter 3 Case Study

Use Case: Sangfor HCI Storage

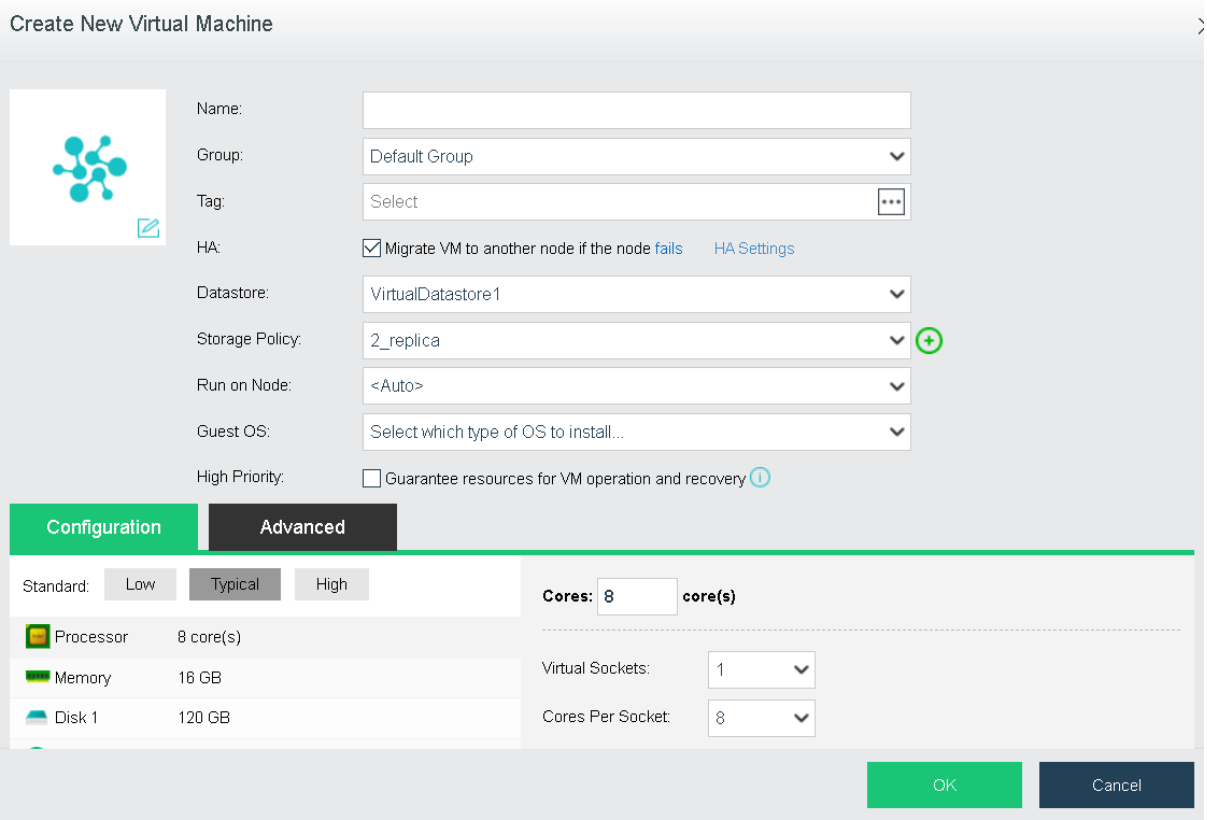
There are two types of storage: local storage and external storage. Disks that come with nodes having installed Sangfor HCI software are local storage, which cannot be accessed by other nodes. Only when external storage is added can clustered virtual machines be used. See Error! Reference source not found. section to add external storage.

Use Case: Virtual Machine

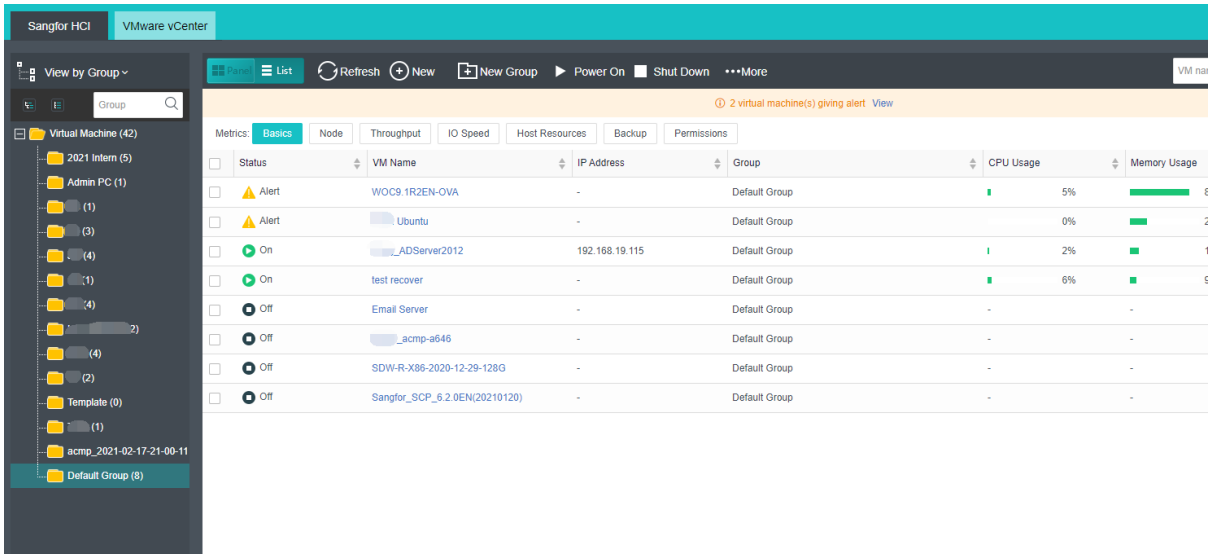
Creating VM

1. Go to **Compute,** click **New a**nd choose **Create New Virtual Machine** to create a new virtual machine running Windows Server 2008 OS. For details, refer to

2. 2.2 Compute section.



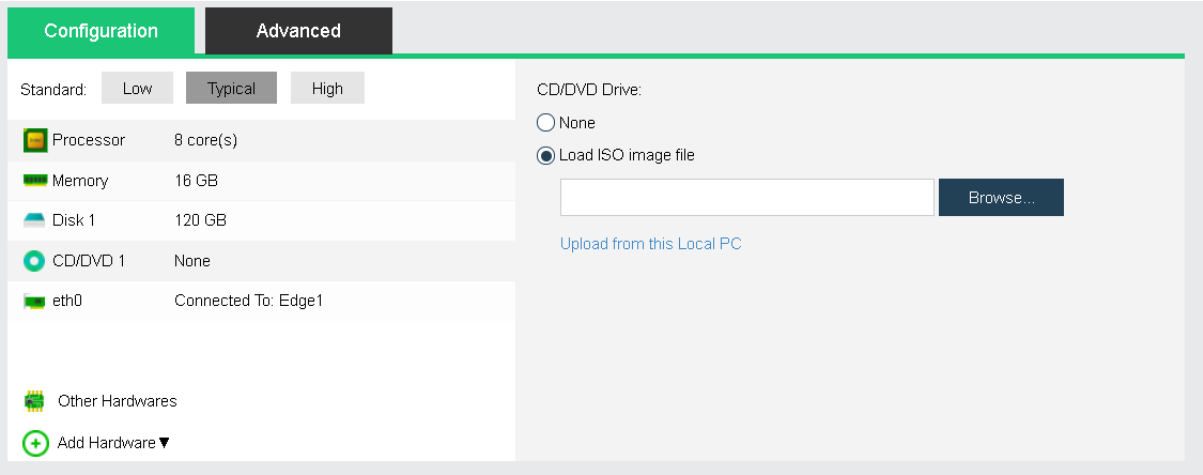
Information of the virtual machine that has been created will be displayed as follows:



3. Install guest OS.

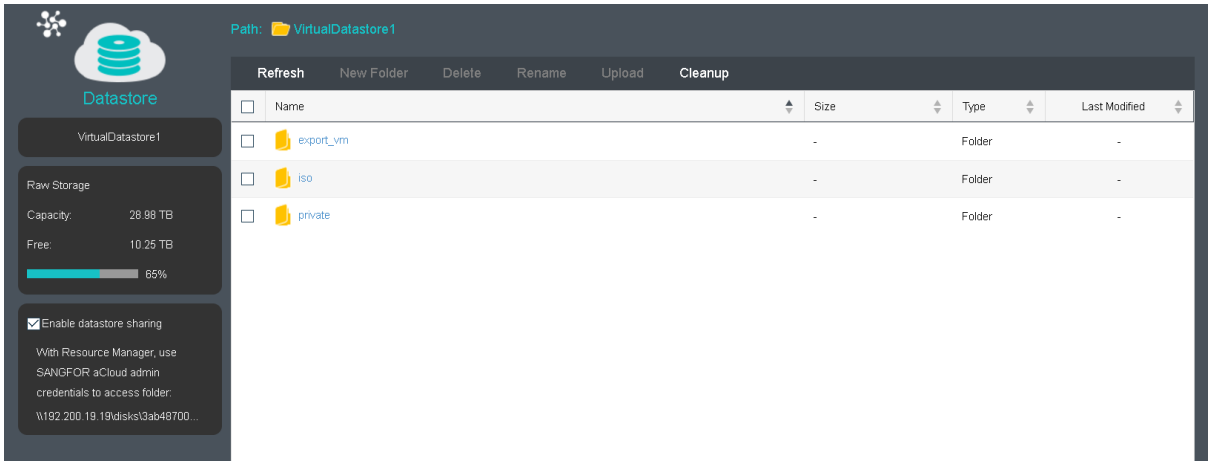
- Upload ISO Image

Method 1: Go to **Compute > New > Create New Virtual Machine,** click **Create New Virtual Machine**, and click **CD/DVD 1 > Upload from this Local Disk**, specify **Image File** and **Datastore** fields, and click **Upload from this Local PC** to start this operation.



Method 2: Go to **Nodes > Storage > Storage used to run VM(it may be virtual datastore, local storage, iSCSI storage or FC storage) > More > Manage,**

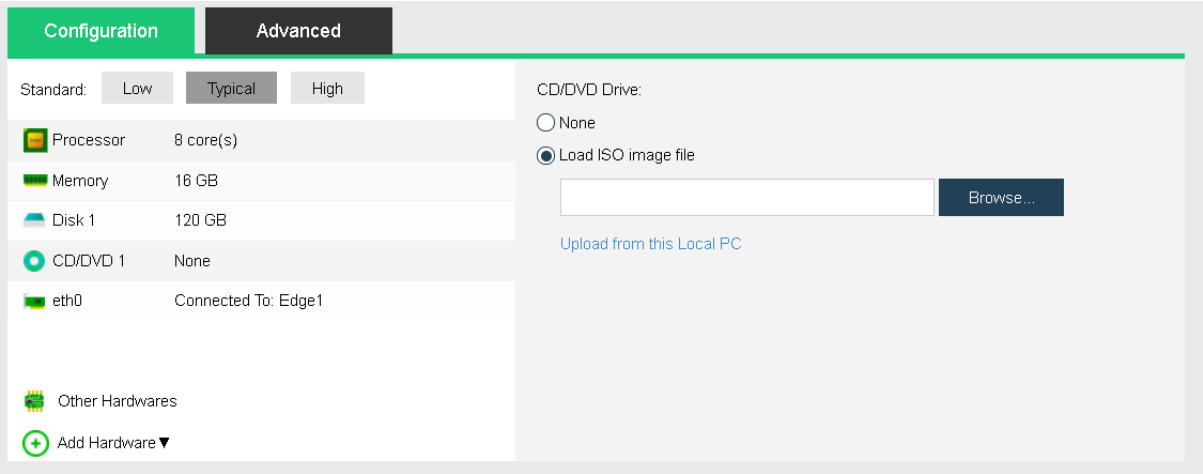
Click **Upload** to upload ISO image files to datastore.



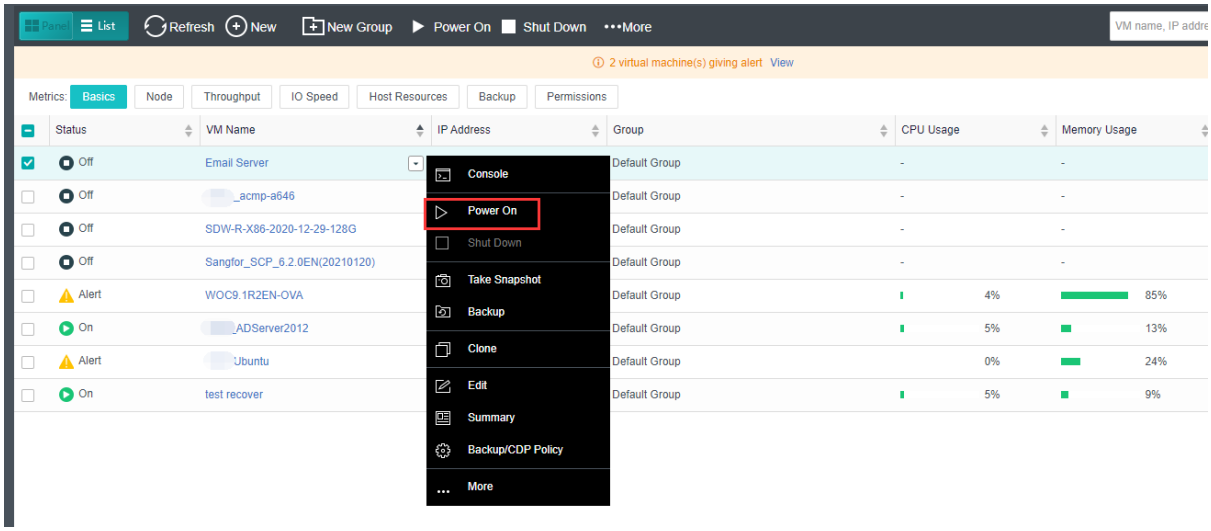
Method 3: Go to **Compute > New > Create New Virtual Machine**, click **CD/DVD 1**, and click **Browse** to enter the **Select ISO Image** page, and then click **Upload ISO Image** to enter the **Upload Image file from this local disk to datastore** page, click icon and enter **\\IP address of the host** in the address bar on the page that pops up and then you may be required to provide the admin account of that host. After entering the correct username and password, you get access to the files on that host, find the ISO image file and upload it to a specific datastore. Click **CD/DVD 1** to enter the ISO image file that has been uploaded in the **Load ISO image file** field.

Then go to edit VM configurations, click **CD/DVD 1** to enter the ISO image file that has

been uploaded in the **Load ISO image file** field, save the changes and go back to the **Compute**.



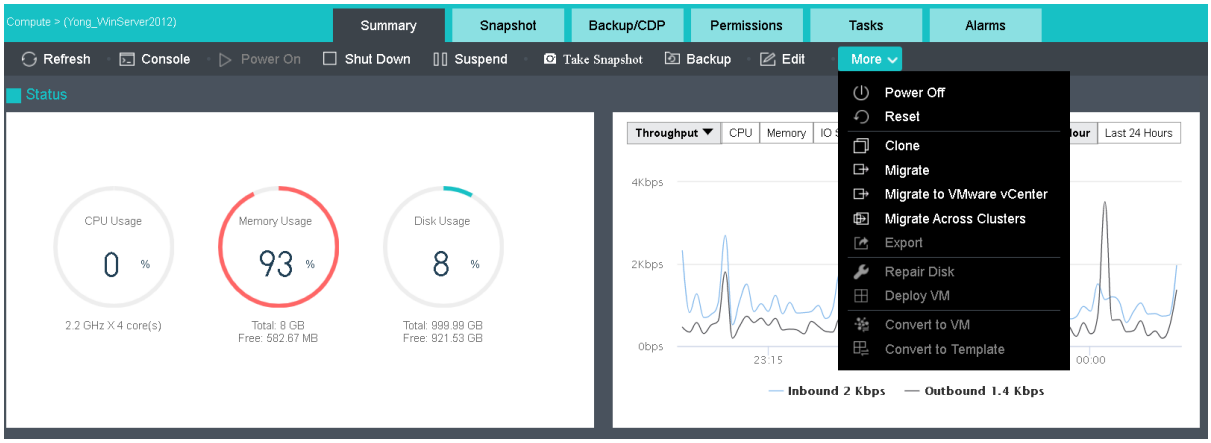
Click **Power On** to power on the virtual machine, as shown below:



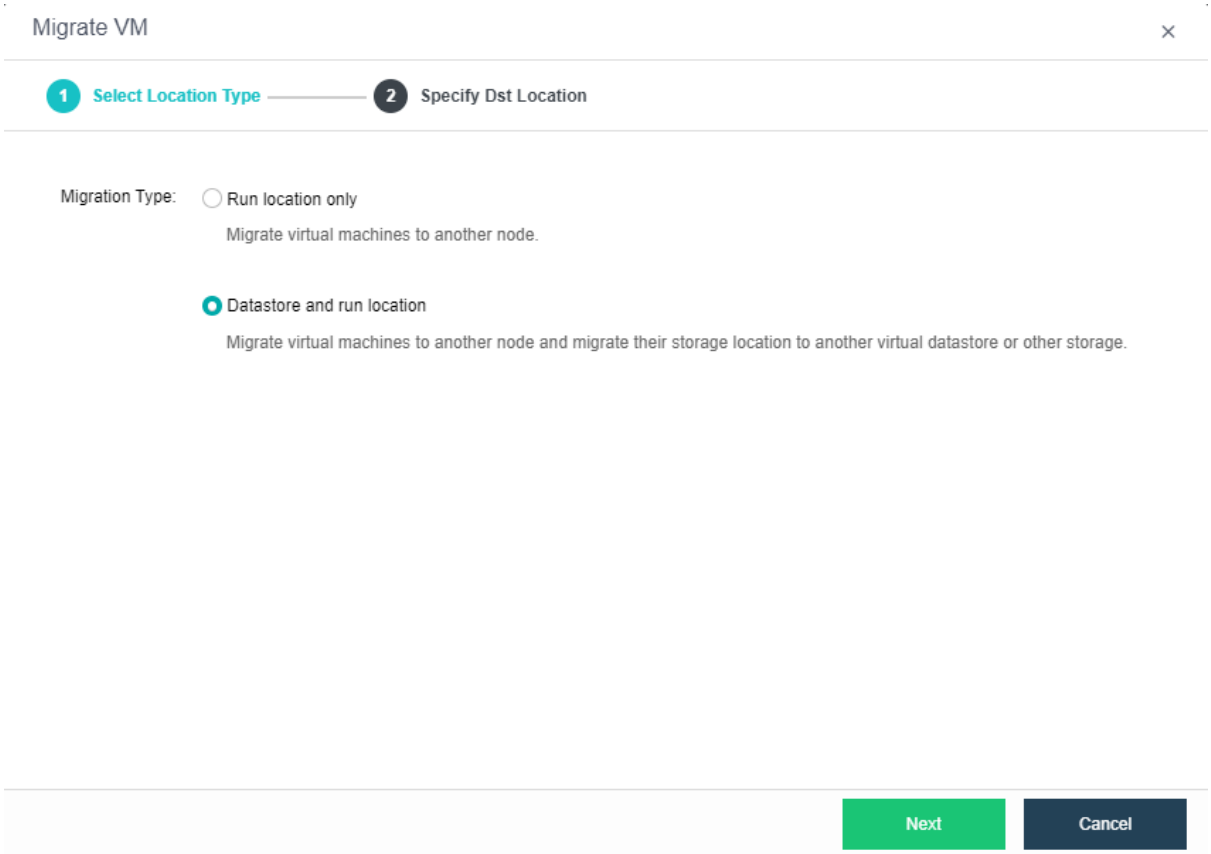
After powering on the virtual machine, click **Console** to enter VM console and install operating system and applications.

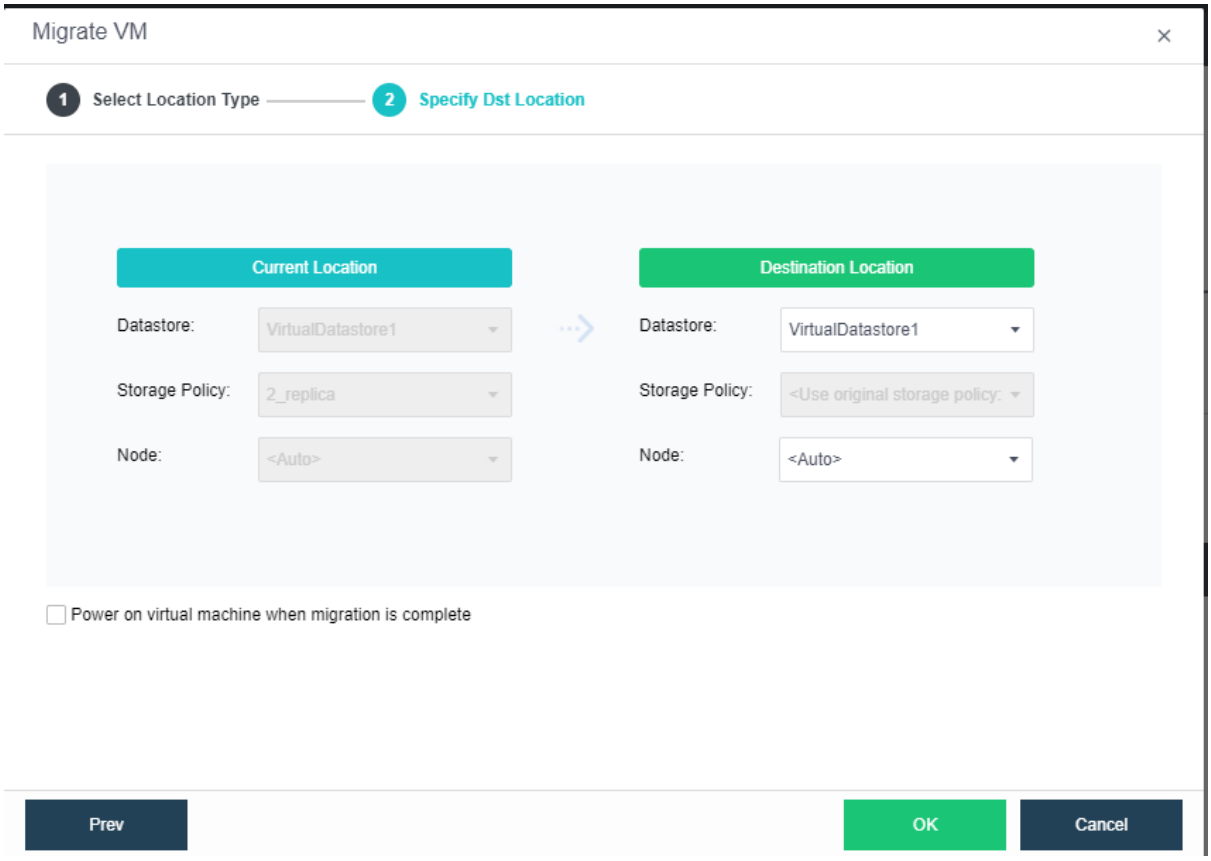
VM Migration

You may migrate the virtual machines to other nodes or other datastores.



Click **Migrate,** specify destination datastore and node, and click **OK** to start migration



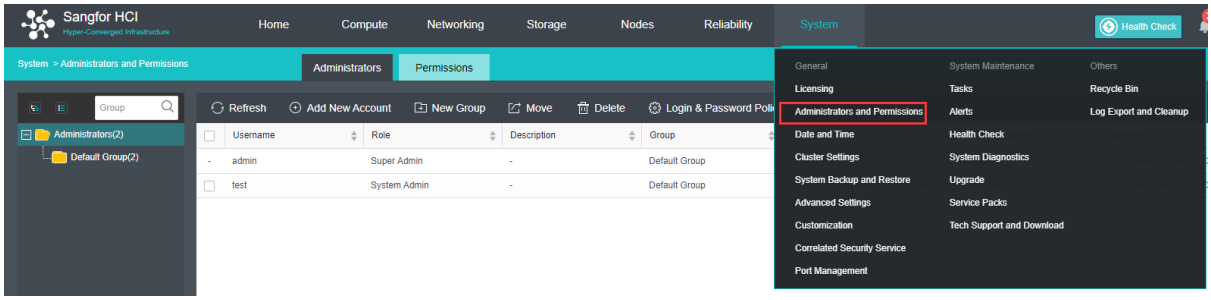


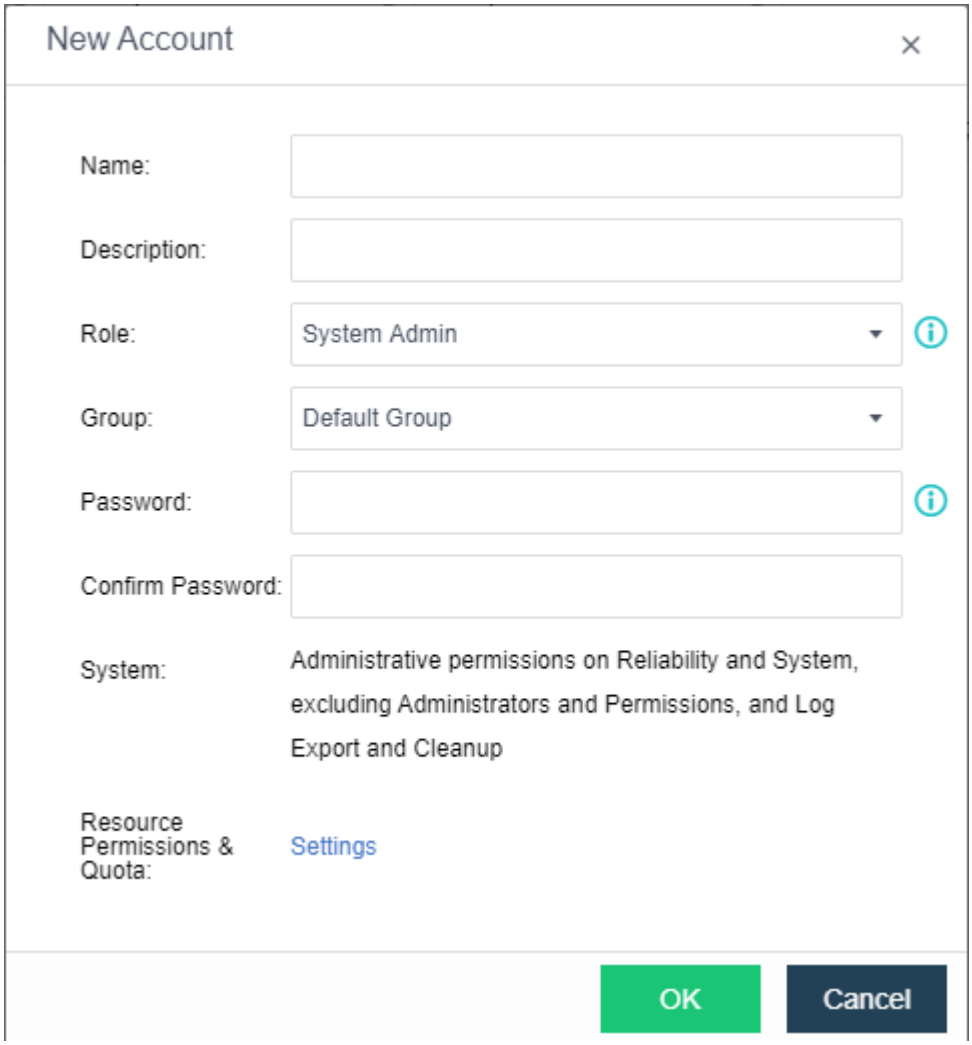
Use Case: Admin Permissions

Administrators are assigned with different permissions to manage virtual machines, virtual network, storage, etc. Meanwhile, administrators can also manage resources available to sub administrators.

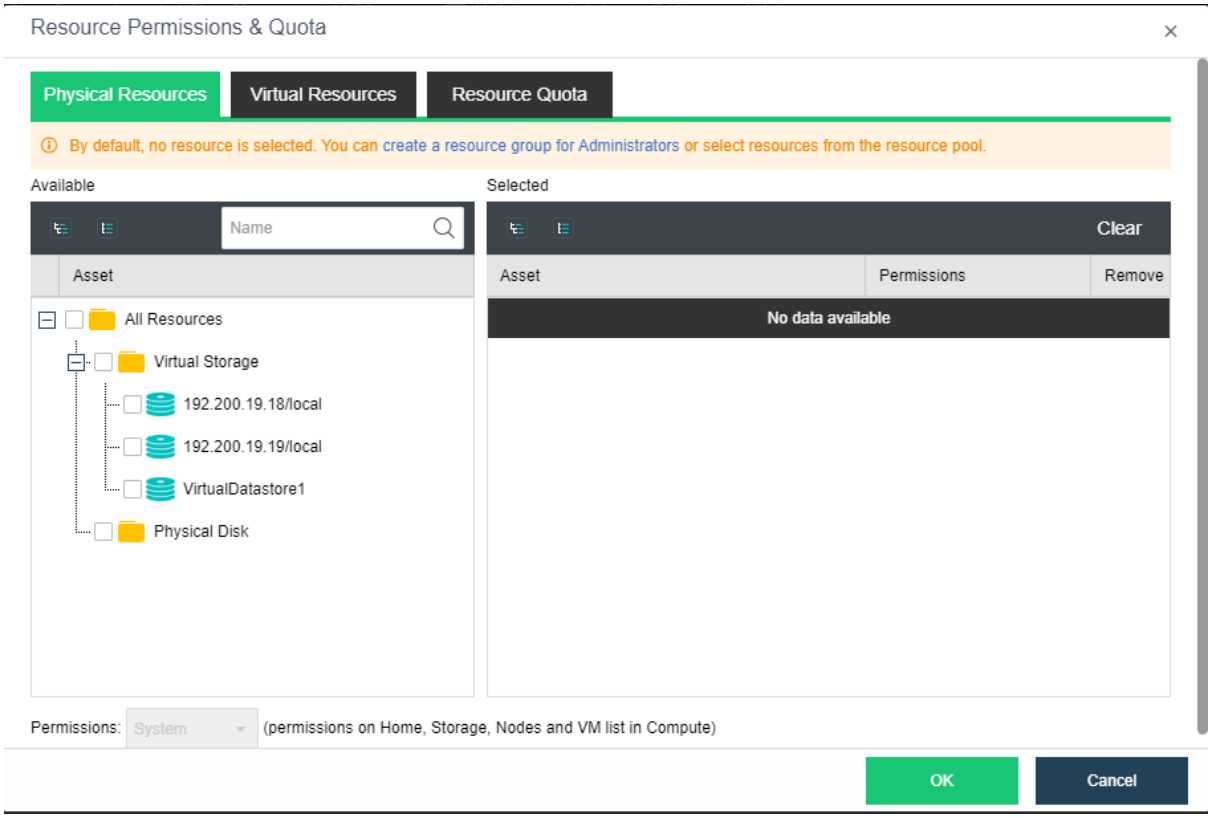
The following describes how to assign permissions:

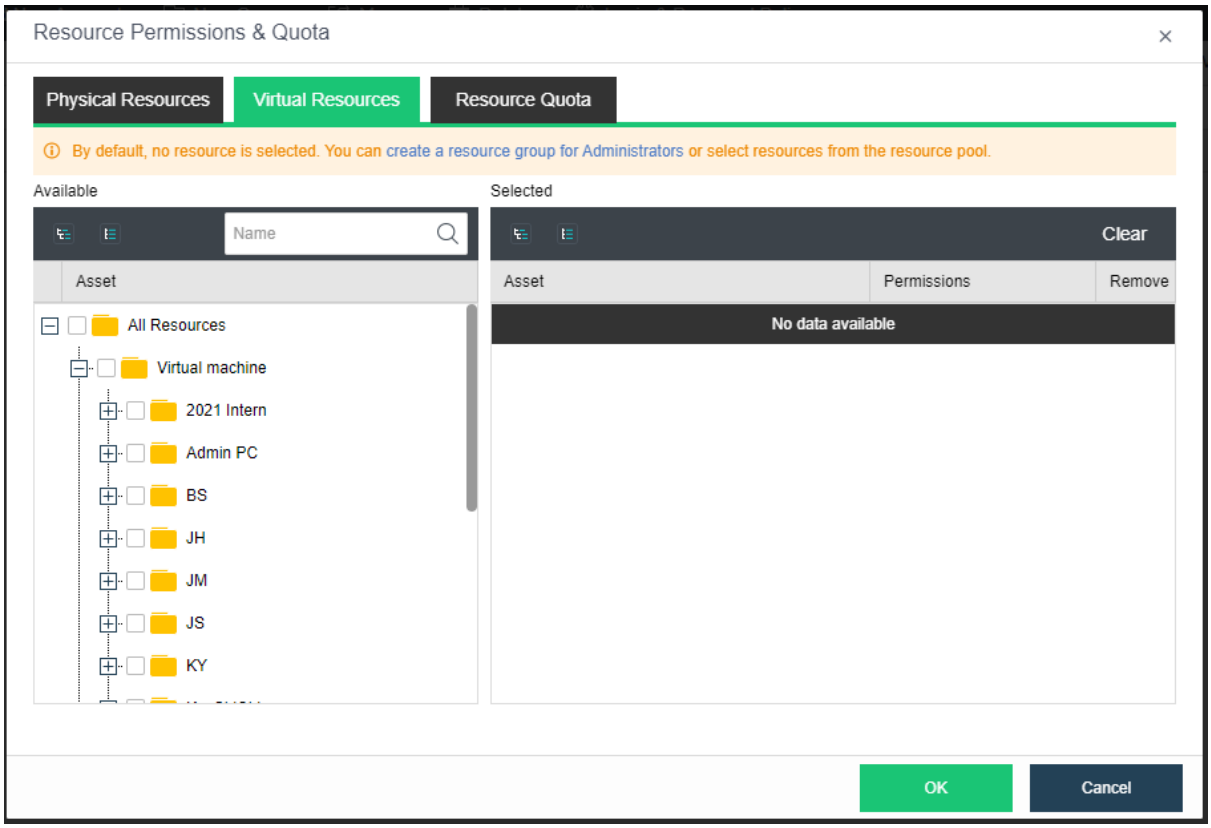
Go to **System > Administrators and Permissions > Administrators**, click **Add New Account** to add an administrator account first, as shown below:



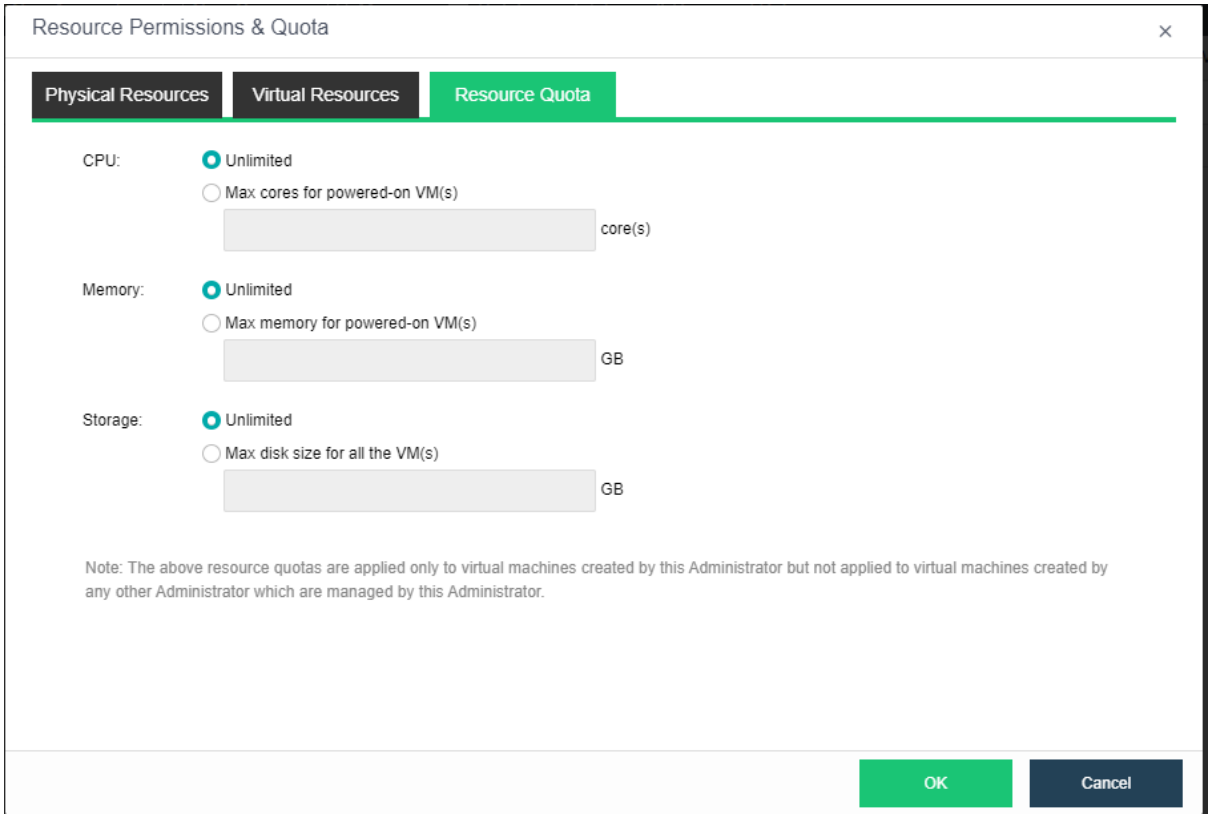


Click **Settings** to enter the following page as shown below. On the **Permissions** page, you may view resources available in the default group of virtual machines, virtual network, and resources available in virtual storage, then choose desired resource(s) under Available and assign the corresponding permission on under Selected.


Resource Permissions & Quota
Physical Resources
Virtual Resources
Resource Quota
By default, no resource is selected. You can create a resource group for Administrators or select resources from the resource pool.
Available
Selected
Name
Clear
Asset
Asset
Permissions
Remove
No data available
All Resources
Virtual Storage
192.200.19.18/local
192.200.19.19/local
VirtualDatastore1
Physical Disk
Permissions:
System
(permissions on Home, Storage, Nodes and VM list in Compute)
OK
Cancel


Resource Permissions & Quota
Physical Resources
Virtual Resources
Resource Quota
By default, no resource is selected. You can create a resource group for Administrators or select resources from the resource pool.
Available
Selected
Name
Clear
Asset
Asset
Permissions
Remove
No data available
All Resources
Virtual machine
2021 Intern
Admin PC
BS
JH
JM
JS
KY
OK
Cancel

Click **Resource Quota** to enter the following page, you may assign a maximum of 10 cores for powered-on VMs, allocate a maximum of 20GB memory for powered-on VMs, and specify 200GB as the maximum disk size for all the VMs.



Accounts can be assigned with different permissions on virtual machines and virtual network.