Sangfor SCP

User Manual

Product Version	6.11.1
Document Version	1.0
Released on	May. 24, 2025

Copyright © Sangfor Technologies 2025. All rights reserved.

Unless otherwise stated or authorized, Sangfor Technologies Inc. (hereinafter referred to as "Sangfor") and its affiliates reserve all intellectual property rights, including but not limited to copyrights, trademarks, patents, and trade secrets, and related rights to text, images, pictures, photographs, audio, videos, charts, colors, and layouts as presented in or concerning this document and content therein. Without prior written consent of Sangfor, this document and content therein must not be reproduced, forwarded, adapted, modified or displayed or distributed by any other means for any purpose.

Disclaimer

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

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

Technical Support

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

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

About This Document

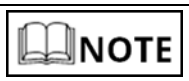
This document is the User Manual of Sangfor Cloud Platform (SCP), which describes the product architecture, key features, platform deployment, configuration instructions, and operation and maintenance management of SCP.

Intended Audience

This document is intended for:

- Technical Support Engineer
- O & M Engineer

Note Icons

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

Change Log

Date	Change Description

May. 24, 2025	This is the first release of this document.

Contents

Technical Support 2
Change Log 3
1 Product Description 10
1.1 Product Introduction 10
1.2 Product Features 11
1.3 Product Architecture 12
1.4 SCP Key Characteristics 13
2 Installation and Deployment 25
2.1 Introduction To Installation 25
2.2 Installation Procedure 25
2.3 Installation Preparation 26
2.4 Product Installation 27
2.4.1 Single Host installation 27
2.4.2 Cluster Deployment 35
2.4.3 Active/Standby Deployment (optional) 58
2.5 Platform License 61
2.5.1 USB Key License 61
2.5.2 vKEY License 62
2.6 Time Setting (Optional) 64
2.7 Platform Login Information 65
2.8 Use aDeploy Tool To Detect: 65
2.9 Patch Upgrade 65
3 Resource Initialization 76
3.1 Resource Initialization Process 76
3.2 Add Physical Resources 78
3.3 Dividing Resource Pools 81
3.3.1 Cluster License 82
3.3.2 Single Cluster License 82
3.3.3 Multi-Cluster License 84
3.4 Deploy Communication Domain 85
3.5 Security Resource License 85
3.6 Configure VPC Gateway 86

3.7 Configure Shared Services Gateway 87
3.8 Configure Direct Connect Gateway 89
3.9 DMP Environment Deployment (Optional) 90
4 Configuration Steps 92
4.1 Overview 94
4.1.1 Resource Overview 94
4.1.2 Big Screen 95
4.2 Resource Overview 95
4.2.1 Resource Center 95
4.2.2 Server Group Management 125
4.2.3 Cluster Management 126
4.2.4 Physical Machine Management 130
4.2.5 Third-Party Public Cloud 132
4.3 Compute 137
4.3.1 Virtual Machine Management 137
4.3.2 Image Management 164
4.3.3 aDesk VDI 172
4.3.4 aDesk VDI Configuration Guide 180
4.3.5 vGPU Management 236
4.4 Networking 251
4.4.1 Network Topology 251
4.4.2 Advanced Network Insight(aNI) 256
4.4.3 Traffic mirroring 269
4.4.4 Network Deployment 273
4.4.5 Shared Service Network 282
4.4.6 IP And Bandwidth 287
4.4.7 Enterprise Dedicated Line 293
4.5 Security Services 294
4.5.1 Distributed Firewall 294
4.5.2 VPC Boundary Firewall 302
4.6 aSEC Installation and Deployment 303
4.6.1 aSEC Cloud Security Center Platform Installation 305
4.6.2 VM security protection management platform installation 312
4.6.3 Virtual Machine Security Agent Installation 317
4.7 aSEC Configuration Guide 319
4.7.1 Dashboard 319
4.7.2 Virtual Machine Security 322

4.7.3 Security Capabilities 330
4.7.4 Security Logs 335
4.7.5 Security Settings 335
4.8 Hybrid Cloud Services 342
4.8.1 Third-Party Public Cloud 342
4.9 Reliability Center 347
4.9.1 Holistic View 347
4.9.2 Data Protection Overview 348
4.9.3 Backup and CDP 349
4.9.4 aDR (Cross-Site Disaster Recovery) 373
4.9.5 High Availability (HA) 397
4.9.6 Dynamic Resource Scheduling (DRS) 398
4.9.7 Resource Reservation 401
4.9.8 VM Resource Limit 402
4.9.9 VM Scheduling 403
4.9.10 Business Reliable Service 408
4.9.11 Platform Reliable Service 410
4.9.12 Hardware Reliability Service 414
4.9.13 Host Health Monitoring 415
4.10 Operations Center 420
4.10.1 User Management 420
4.10.2 Quota Management 435
4.10.3 Work Order Management 437
4.10.4 Billing Center 442
4.10.5 Federal Authentication 444
4.11 Storage 454
4.11.1 OSS 454
4.11.2 File Storage 464
4.12 Monitoring Center 464
4.12.1 Monitoring Dashboard 464
4.12.2 Reports 466
4.12.3 Monitor Center 467
4.13 Management 471
4.13.1 Operational Audit 471
4.13.2 Recycle Bin 471
4.13.3 Custom Attributes 473
4.13.4 Platform Customization 474

4.13.5 Security Management 475
4.13.6 System Configuration 488
4.14 Application Service 503
4.14.1 SCP Application Center 503
4.15 Chinese/English language switch 518
5 Tenant User Guide 519
5.1 Login Method 519
5.2 Overview 519
5.3 Compute 520
5.3.1 Virtual Machine 520
5.3.2 Image 530
5.4 Networking 531
5.4.1 Network Topology 531
5.4.2 IP And Bandwidth 535
5.4.3 Network Deployment 538
5.4.4 Application Delivery Controller (ADC) 549
5.5 Security 550
5.5.1 NFV Features 550
5.5.2 Distributed Firewall 554
5.6 Reliability 558
5.6.1 Scheduled Backup Policy 558
5.6.2 CDP Policy 559
5.6.3 Disaster Recovery 561
5.6.4 Auto Scaling 565
5.7 Monitor and Management 575
5.7.1 Monitoring Dashboard 575
5.7.2 Alert 576
5.7.3 Quota 577
5.7.4 Recycle Bin 577
5.8 Bills 578
5.9 Work Orders 579
5.10 Tenant And Tenant Users Management 581
5.10.1 Create User Account 581
5.10.2 Edit Tenant User Account 582
6 System Upgrade 583
7 Common Troubleshooting 584
8 Glossary 585

9 Abbreviations 591

1 Product Description

SCP (Sangfor Cloud Platform) is a comprehensive, safe and reliable cloud management platform that can manage HCI clusters and VMware clusters across regions and associate the managed clusters with resource pools to realize the management of multiple resource pools.

The platform provides basic services such as virtual machines, multi-tenant management, VPC, elastic IP, and enterprise private lines through products and services, reliability center, operation center, application center, and monitoring center. It also integrates reliability services such as backup, disaster recovery, and monitoring centers into the platform, reducing the difficulty of operation and maintenance and ensuring business continuity and reliability.

This chapter mainly introduces and explains the Sangfor SCP cloud computing platform in detail from the aspects of product introduction, product features, product architecture, and key features.

1.1 Product Introduction

Sangfor cloud platform SCP can provide rich management functions. In the resource creation stage, multiple data centers can be managed. These data centers can be cross-regional clusters or VMware data centers. In terms of Licensing, the unified license is supported. When multiple HCI clusters are managed, you only need to import the SCP license once, and all other managed clusters can be licensed through SCP licensing distribution. Through the platform's three role types of super admin, tenant, and tenant sub-account, hierarchical management can be realized between the head office, branches, companies, and departments. The platform supports custom work order approval procedures and billing functions, which greatly enhances the flexibility of platform resource management. The platform provides tenants with a VPC. The tenants are logically isolated to ensure user information and data security. It also innovatively integrates Sangfor NFV equipment (vAD, vAF,

SSL VPN) into the VPC to provide safe, reliable, and fully functional network surroundings.

1.2 Product Features

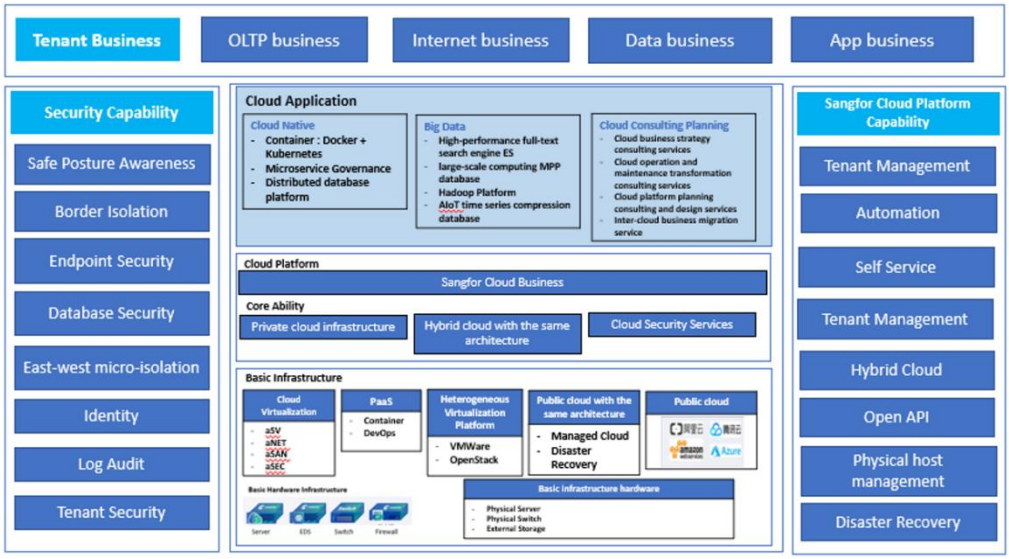
Sangfor Cloud Platform SCP integrates three centers: Reliability Center, Operation Center, and Monitoring Center.

The platform provides a comprehensive reliability mechanism in the Reliability Center, including business reliability, platform reliability, and hardware reliability. With hardware as the starting point, platform as the foundation, and business as the key. Business and data security is guaranteed in multiple dimensions.

In the operation center, through the platform's three role types of super admin, tenant, and tenant sub-account, hierarchical management between the head office and branch offices and between companies and departments can be realized. The platform supports custom work order approval procedures and billing functions, which significantly enhances the flexibility of platform resource management.

In the monitoring center, the platform provides a comprehensive monitoring mechanism that can monitor key services such as virtual machines and databases in real-time. Under the premise of ensuring business continuity and reliability greatly reduces the difficulty of operation and maintenance (O & M) for operation and maintenance personnel.

1.3 Product Architecture

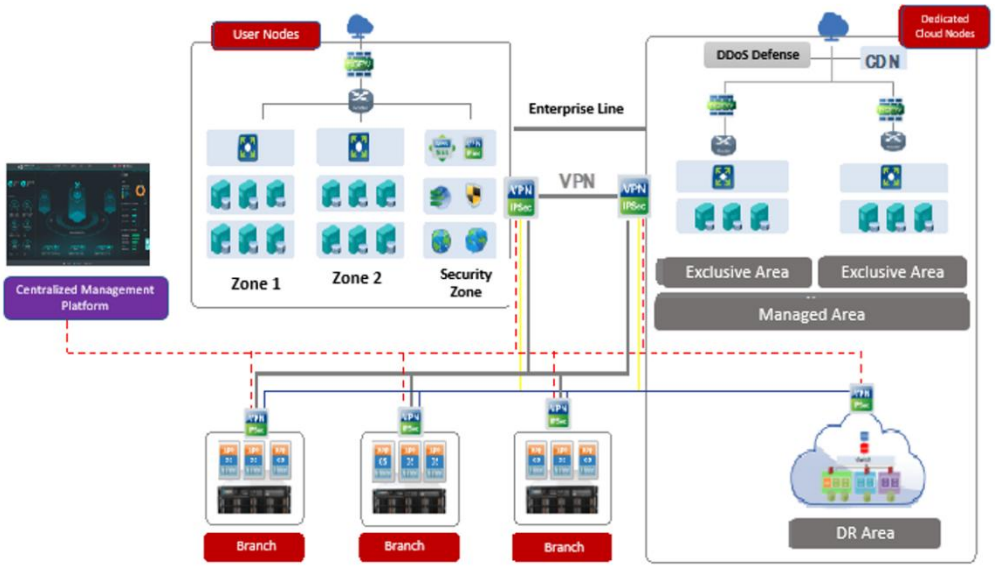


- Infrastructure hardware: Servers, storage devices, network, and security equipment needed to build a data center. According to different business needs, provide multiple types of hardware deployment architectures.
- Infrastructure layer (resource pool layer): The infrastructure layer is the computing, storage, network, and security resource pool based on physical facilities. It includes various resource pools such as Sangfor HCI, VMware, OpenStack, and public clouds.
- Cloud platform layer: Based on different resource pools, Sangfor can build cloud platforms such as private clouds and hybrid clouds with the same architecture.
- Cloud service layer: Sangfor Cloud can provide comprehensive cloud service capabilities, such as tenant management, automated operation, maintenance, etc. It can provide powerful security capabilities, such as security situation awareness, boundary isolation, etc. Based on traditional IaaS layer services, it can provide PaaS layer services, including cloud-native, big data, application store, etc., while carrying the core business, it helps the transformation and development of enterprise IT architecture.

1.4 SCP Key Characteristics

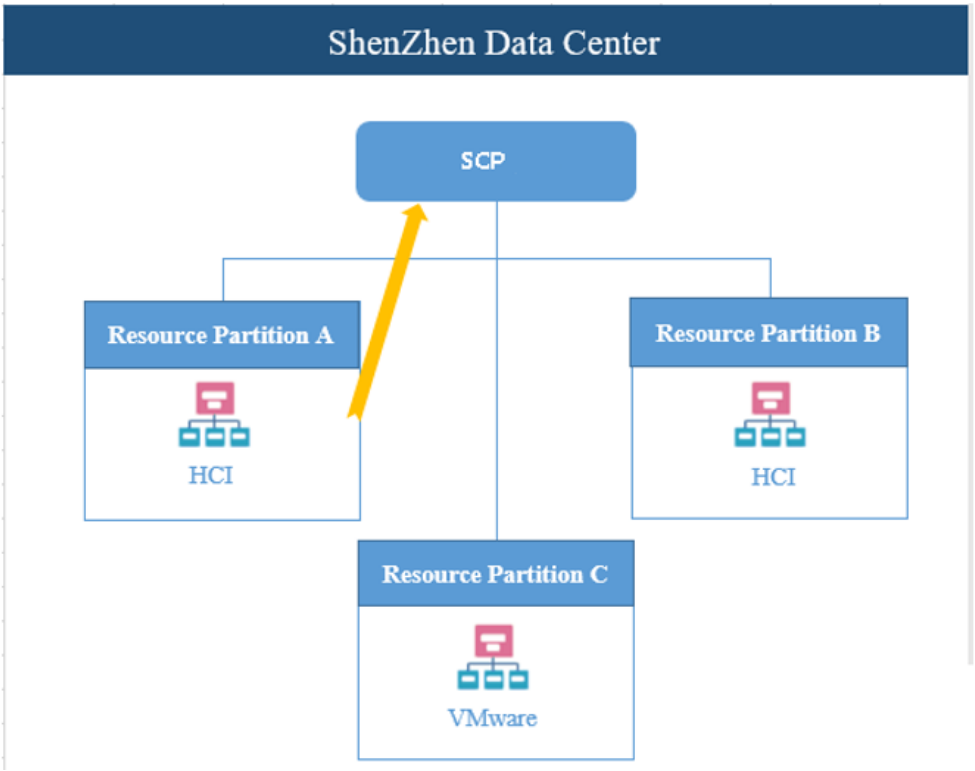
1. **Same architecture hybrid cloud management capabilities.**

   Sangfor Cloud's hybrid cloud with the same architecture based on the hyper-converged architecture supports the docking of private cloud data centers with managed cloud accounts to build a unified management cloud federation environment. Take the private cloud as the main body, trust the hosted cloud account through the IdP identity authentication mechanism, associate the platform administrator or tenant of the private cloud with the hosted cloud tenant account, trust and jump with one click so that the private cloud users can easily go to the cloud and experience Host the rich service catalog of the cloud and build a new blueprint for IT governance.

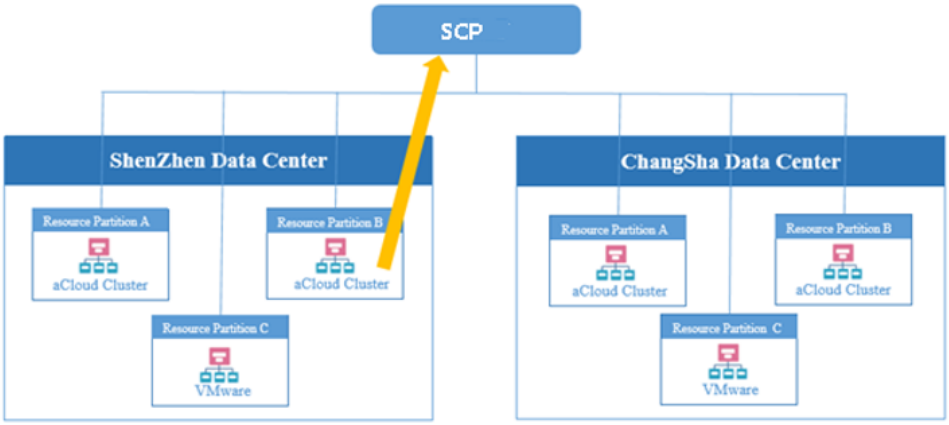


2. **Multi-cluster Management.**

   SCP unifies the management of resources such as infrastructure, Resource Pools, cloud services, and tenant applications. The deployment mode of SCP includes single data center and multi-cluster deployment, which is used to conduct heterogeneous management over multiple different clusters in the same data center. The logical topology of the deployment is shown in the figure below:



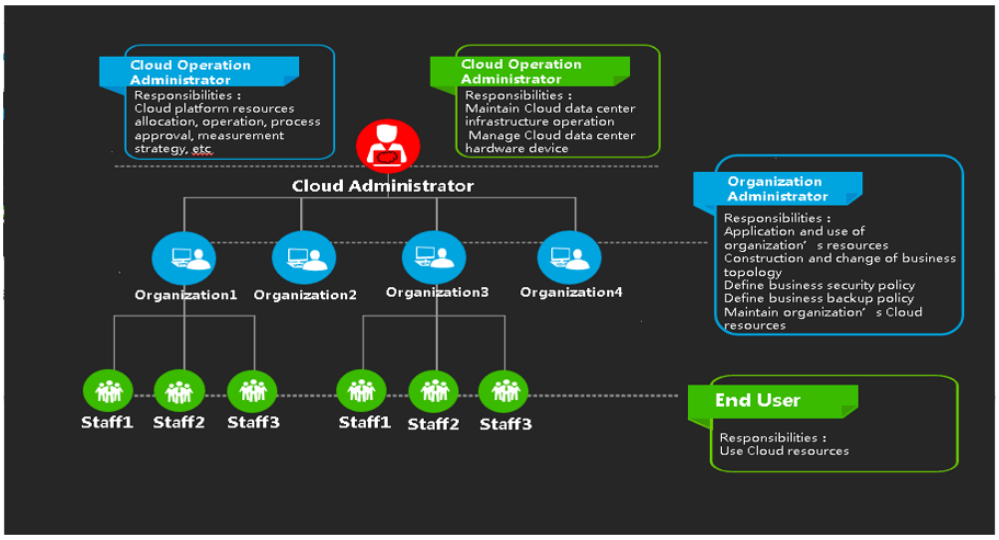
At the same time, SCP supports the cross-regional heterogeneous management of multiple clusters from multiple data centers. Its deployment logic topology is shown below:



3. Multi-tenant management

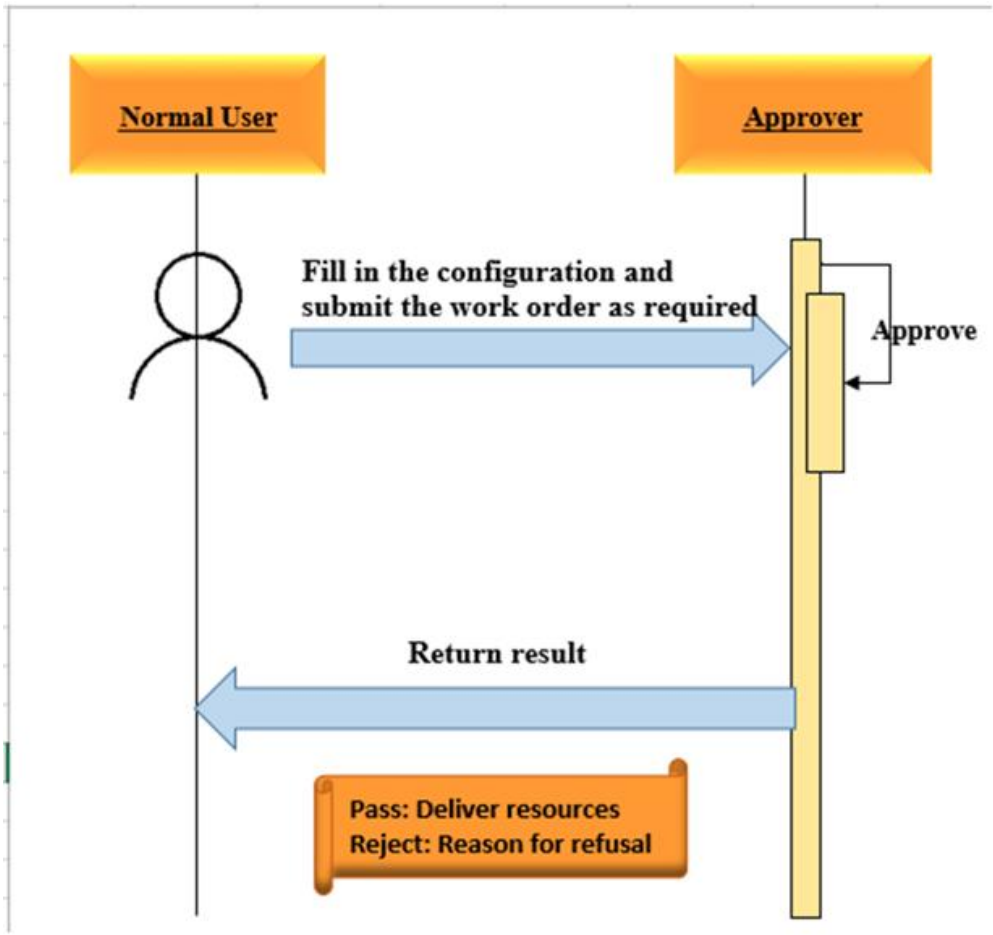
To meet the operational management requirements of the platform for the Tenant, SCP can set up a maximum of three user management levels, namely platform management, Tenant management, and end-user. The

relationship between management responsibilities and levels is shown in the figure below.



4. Self-service function

Work orders will be automatically generated after users apply for or manage cloud services, such as application for and deletion of work orders. The work order is submitted to the corresponding personnel for examination and approval. After approval, the system automatically executes the work order tasks. The application workflow is shown below.



5. VPC

The SCP cloud computing platform provides tenants with a VPC. The logical isolation between tenants ensures the security of user information and data. It also innovatively integrates Sangfor NFV equipment (vAD, vAF, SSL VPN) into the VPC network to provide security, reliability, and functionality. Comprehensive network environment.

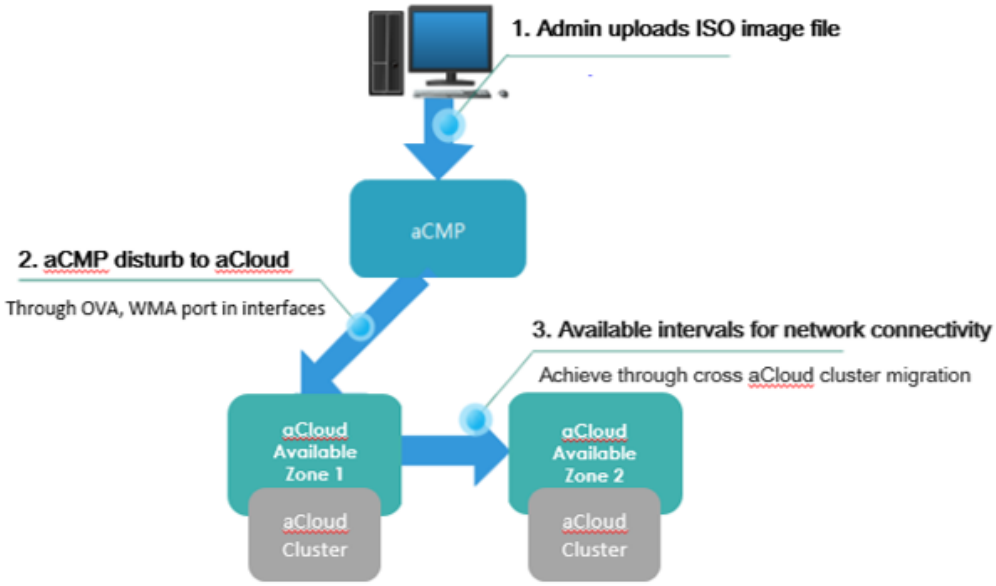
6. Image unified management

Provide unified image management functions to achieve unified creation and management of images on all HCI Resource Pools.

- In the multi-tenant mode, the administrators can customize the Tenant administrator. In the Tenant, the public image provided by the platform administrator can be used, or the customized private VM image can be used.

- By reducing the operation and maintenance pressure of platform administrators through a unified image management function

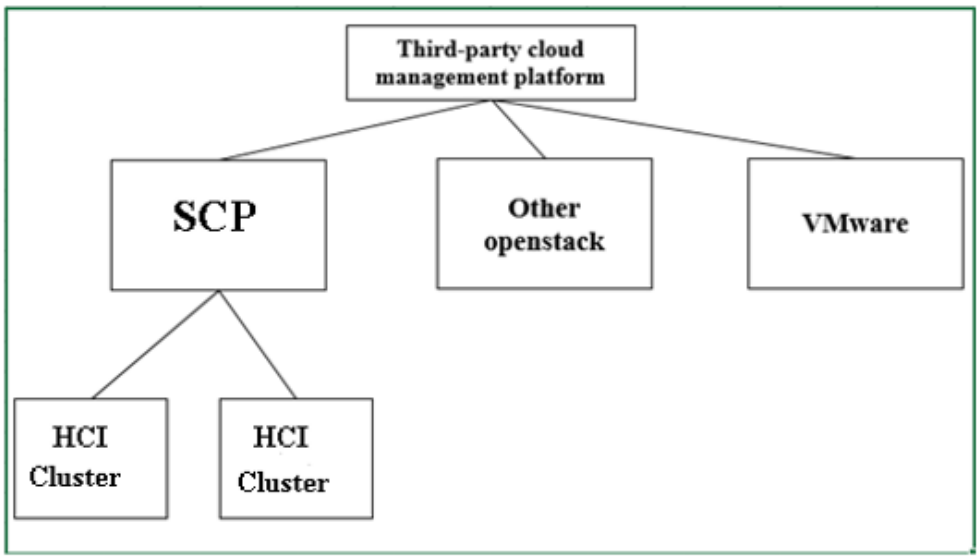
The process of image uploading and distribution is shown below:



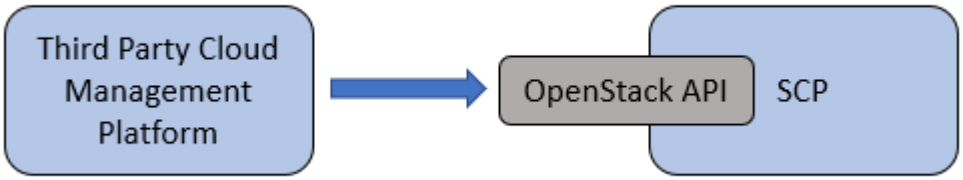
Connected aCloud can be uploaded by interval image, distribution process

7. Standard API Interface

SANGFOR SCP will provide industry-wide standard interfaces to the outside, and third parties will be able to customize docking according to their needs. Simple heterogeneous management logic is shown below:



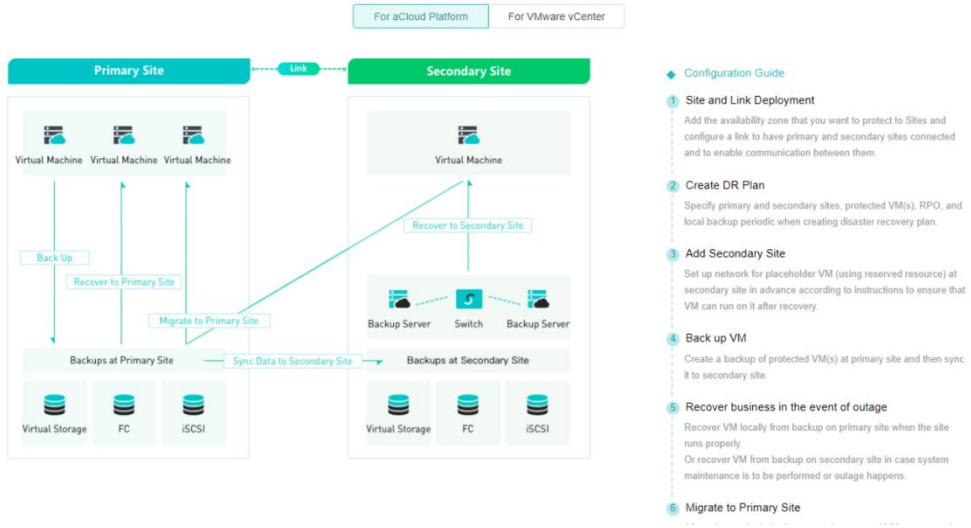
The simple management logic is shown in the following figure.



8. Billing and measurement management

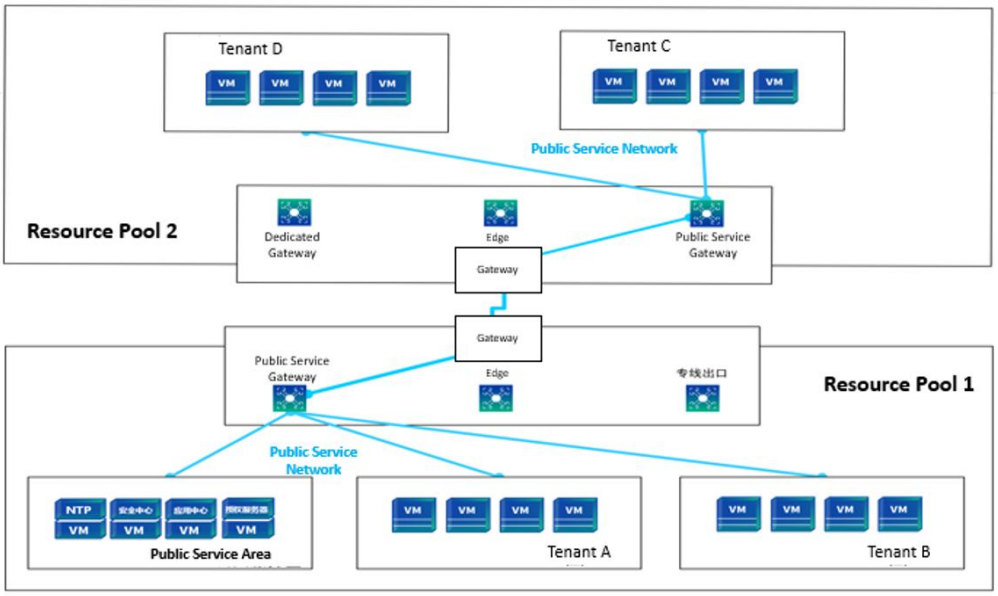
- Transparency and visualization of the usage of multi-tenant computing resources.
- Realize the conversion from data center billing center to profit center by charging the tenants and tenant sub-accounts based on the number of resources used.
- It is convenient for the industry cloud to charge for the resources used by each tenant, and it is convenient for them to realize resource settlement with the tenants.
- Provide exportable resource usage report

9. Disaster Recovery Services



Sangfor Disaster Recovery(DR) plans provide a **local backup - aDR (Cross-Site Disaster Recovery)**plan. The primary site configures a remote backup repository for a local backup repository, and the secondary site configures an HCI cluster as the disaster recovery center.

10. Public Services Network



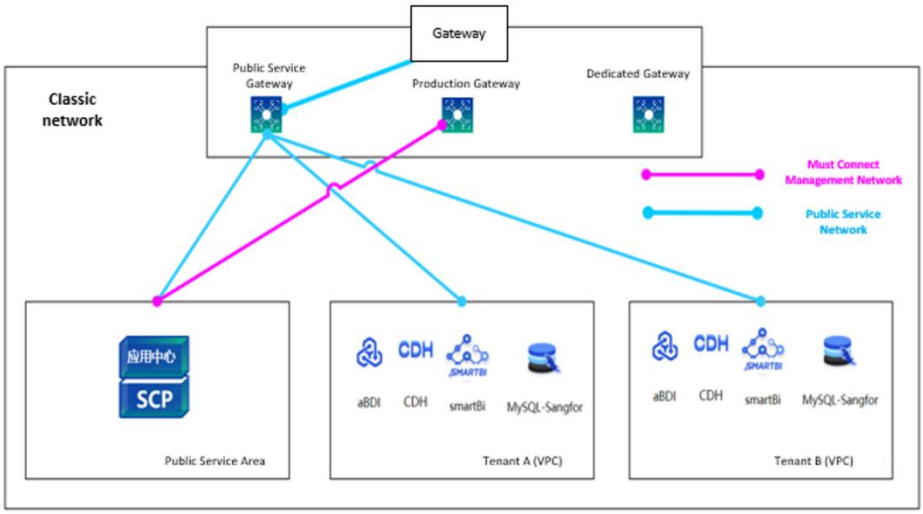
Sangfor SCP introduces public service regions, designates public service outlets for each resource pool, and builds a public service network as a dedicated channel between public service regions and resource pool tenants. NTP servers, licensing servers, NAS, security centers, application

centers, etc., can be deployed in public service regions to meet tenants' access requirements for public services.

11. Security Center

- Sangfor SCP joins the security center, supports the access of security devices on the cloud, realizes log reporting, single sign-on, security monitoring, and other functions, provides one-stop security solutions, and meets the security requirements of cloud platforms.
- The security center supports IAG, AF, ADC, and SSLVPN connected to the classic network and tenant VPC, allowing unified management, log collection, and risk reporting to meet the security requirements of tenants.

12. Application Center



- Sangfor SCP cloud computing platform introduces the application center function, supports one-click deployment of Mysql database, big data CDH/aBDI/SmartBI applications, Redis stand-alone version/Sentinel version/cluster version, Kafka stand-alone version/Sentinel version\cluster version, MongoDB stand-alone version/Sharded cluster version, RabbitMQ stand-alone version/cluster version of application middleware and other applications, realize the rapid launch of applications in development and test scenarios. The platform integrates application operation and maintenance methods, including monitoring, backup, alarms, configuration changes, custom deployment, and other management capabilities.

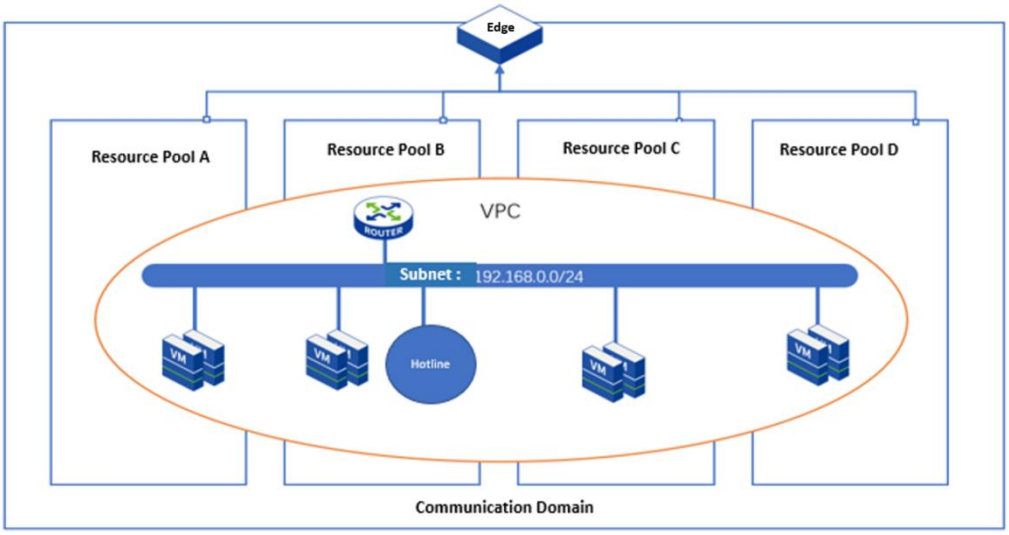
13. Security Compliance

- Sangfor SCP cloud computing platform supports OTP authentication and meets the security requirements of platform login.
- Support the active disabling and enabling of tenants, which is convenient for platform administrators to manage platform operations.
- Support binding new or existing key pairs to Linux virtual machines to avoid brute-force cracking of account passwords and have higher security.

14. Sangfor Database Management Platform (DMP)

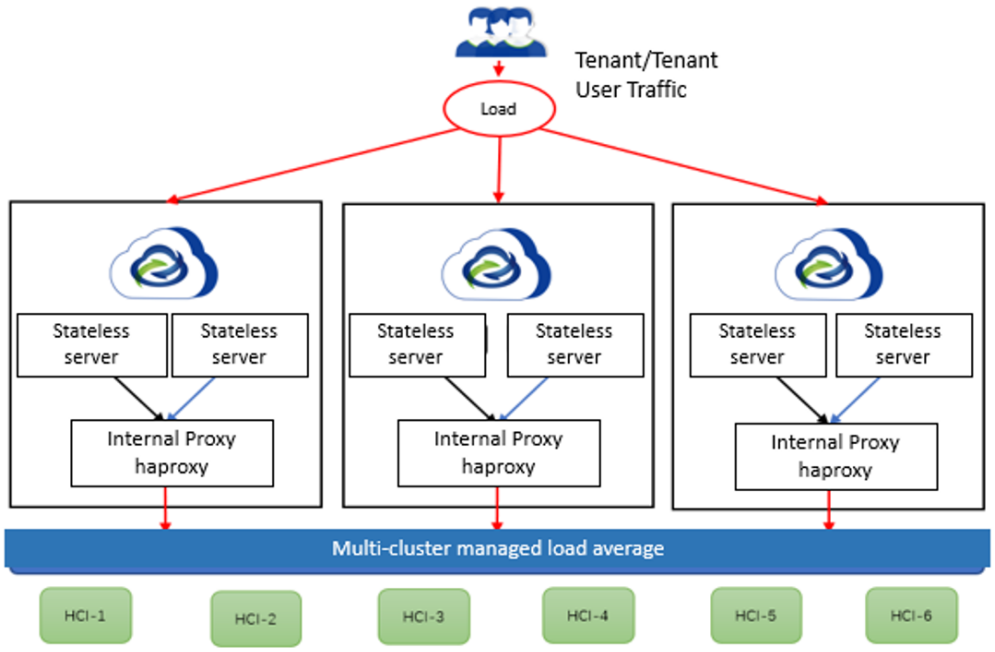
- Automatic deployment of MySQL stand-alone/master-slave, Oracle stand-alone/RAC.
- Cluster nodes can automatically switch between master and slave under failure conditions and combine cloud platform resource linkage to perform bottom-level repairs to achieve self-healing of failures and restore the cluster relationship.
- Provide database-level transaction-consistent backup capabilities, support full backup, incremental backup, and automatic cleanup. Support for restoring to a new database from any backup point.
- Monitor database resources, performance, and cluster master-slave relationships from multiple levels to support manual and automatic database inspections and realize daily operation, maintenance, and inspection automation.

15. Communication Domain



- Multi-site smooth connection, unified arrangement: It is not restricted by the physical environment level and software level of a single site and supports a total of 1024 nodes for multi-site Layer 2 connectivity at most.
- Isolated network fault domain: physical network level isolation between sites, a single site network failure (such as broadcast storm, loop) will not extend to other sites.
- Reliable SDN centralized management and control: The physical network equipment only forwards data, the aNET-SDN controller maintains the related configuration of the business network, the controller is deployed in clusters, and the high-reliability mechanism guarantees the robustness of the business network.

16. Cluster Mode



- SCP supports cluster mode to meet large-scale cluster management scenarios. It supports up to 128 clusters and scales horizontally to 1024 nodes.
- Support cluster load balancing. Tenants can access each node of the SCP cluster through the AD load function.
- Realize cluster high availability and real-time synchronous database backup to ensure data consistency.
- Supports automatic failover and automatic return of offline nodes.

17. Advanced Network Insight(aNI)

Network visualization (aNI, Advanced Network Insight) realizes automatic collection and sorting of virtual machine access relationships, automatic addition and display of new assets, and timely synchronization of asset status. From a business perspective, it provides an intuitive and clear access relationship topology diagram and access details between virtual machines. It is convenient for optimizing policy configuration, discovering business access risks, and reducing risk port exposure.

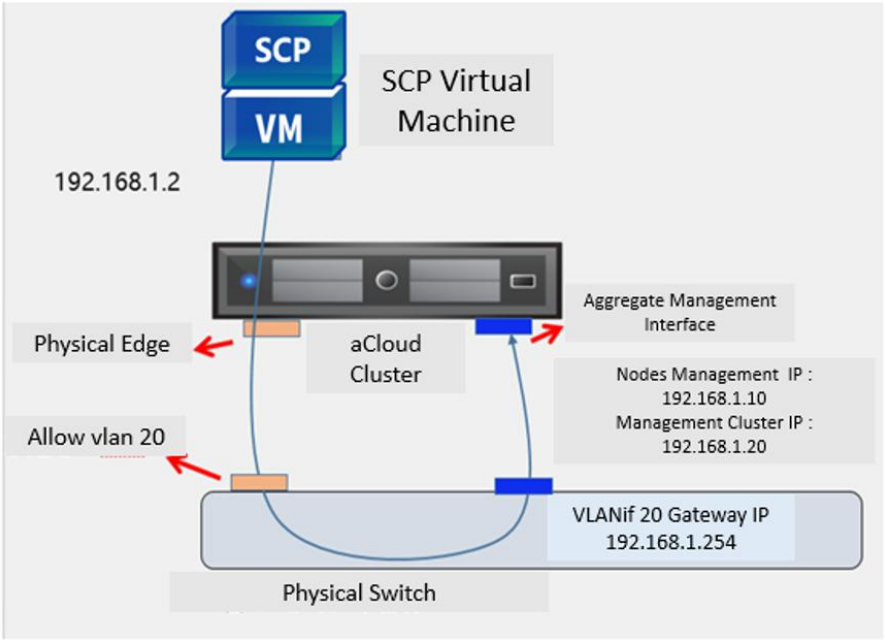
18. Network Traffic Mirroring

Sangfor HCI supports copying and forwarding the network card traffic of virtual machines/network devices to the hyper-converged egress. In the operation and maintenance scenario, the network traffic of business virtual machines can be mirrored to the security auditing device to realize traffic filtering and monitoring.

2 Installation and Deployment

2.1 Introduction To Installation

Sangfor SCP cloud computing platform currently only supports virtualization deployment on the HCI platform and deploys by importing VMA format virtual machines. An example deployment topology is shown in the figure below.

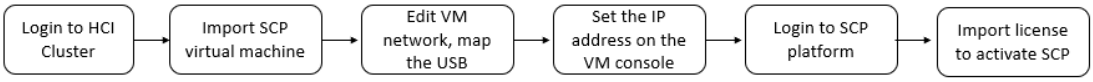


NOTE

SCP currently does not support deployment on VMware platforms and physical machines.

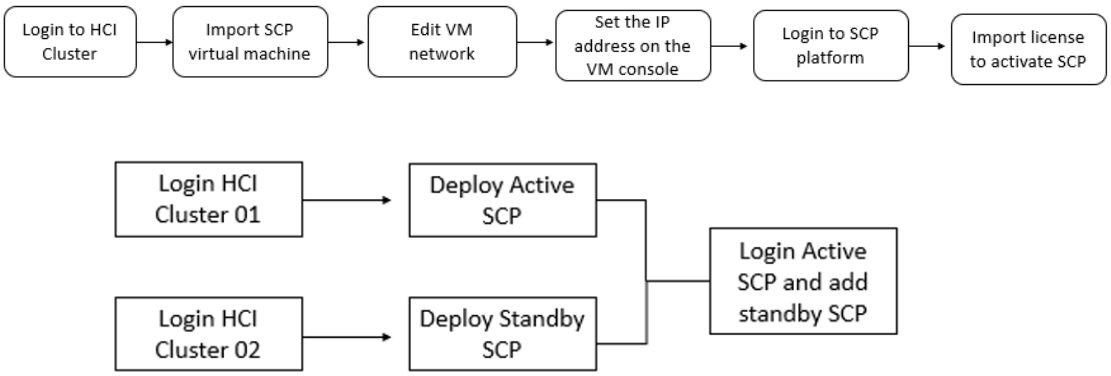
2.2 Installation Procedure

USB Key installation:



vKey installation:

Active-Standby SCP:



2.3 Installation Preparation

Software package preparation:

Installation Procedure	Function	Source
SCP 6.8.0 installation package	Support the whole new deployment of SCP platform	https://community.sangfor.com/plugin.php?id=service:download
NFV image	Used to deploy NFV	

Document preparation:

Document Name	Function	Source
HCI 6.8.0 user manual	HCI platform basic operation, maintenance and configuration operations	https://community.sangfor.com/plugin.php?id=sangfor_databases:index
SCP 6.8.0 user manual	SCP platform basic operation, maintenance and configuration operations	

Tools Preparation:

Tools	Function	Source
Authorized key	Hardware license key, used for SCP licensing	Contact Sales representative to get it
Authorized license	A lic document based on the authorized key used for SCP licensing	
Chrome	Browser software installed on the PC	Self-download
Putty	SSH tools	Self-download
MD5	Verify the integrity of the software package	Self-download

Migration Preparation:

1. HCI platform networking information and login information.
2. When SCP is deployed in active and standby mode, you need to prepare one IP address for the active and standby cluster management network segments.

2.4 Product Installation

2.4.1 Single Host installation

Function Description:

Sangfor SCP was newly deployed on the HCI platform.

Precautions:

Please ensure that the IP configured for SCP does not conflict with the IP addresses of other nodes.

Recommended configuration:

Many factors affect SCP performance, including the number of tenants, users, concurrent users (the number of users who log in to the SCP simultaneously), managed clusters, physical nodes, and virtual machines, depending on the scale of the cloud platform. Therefore, it is recommended to use the following

configuration for SCP virtual machine.

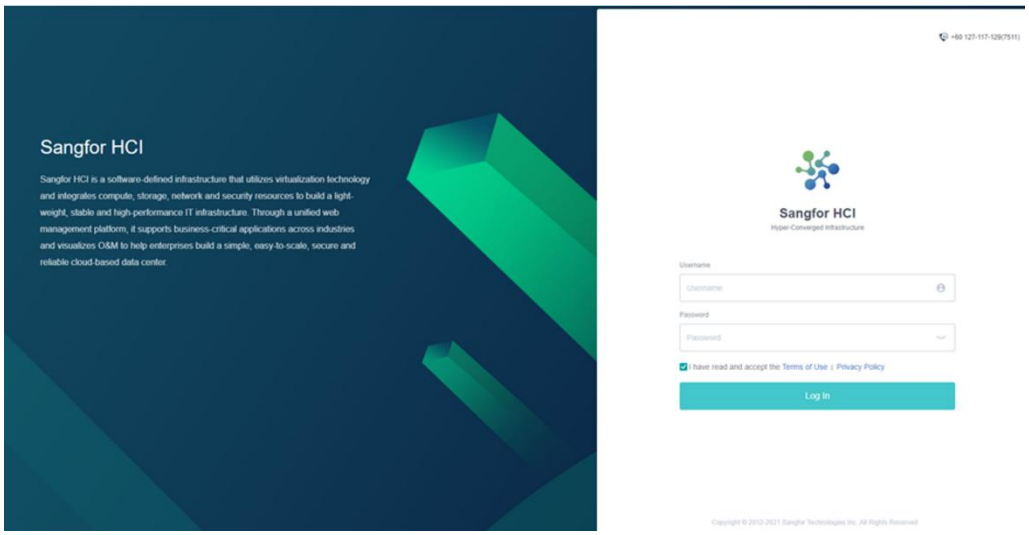
SCP Configuration	Number of Tenant	Number of Tenants User	Concurrency Number of accounts	Number of HCI Cluster	Number of Physical Nodes	Number of Virtual Machine
16 Core 26G	32	200	64	4	32	0-3000
22 Core26G	64	500	128	8	64	3000 - 5000
22 Core 42G	128	1000	256	16	128	5000 - 10000
30 Core 42G	128	1000	256	25	256	10000 - 30000

Prerequisites:

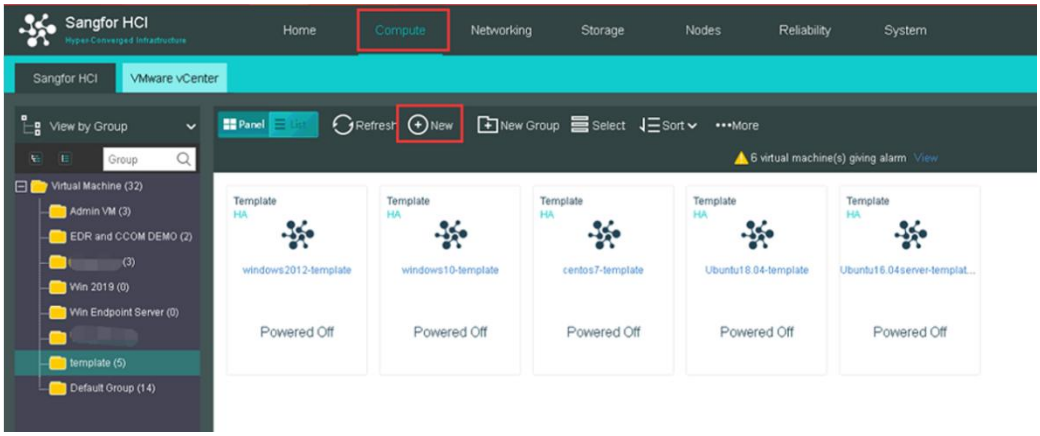
1. Sangfor HCI platform has been correctly deployed.
2. Prepare the IP address of the SCP on the same network segment as the HCI management interface.
3. Prepare Sangfor SCP cloud computing platform image package.

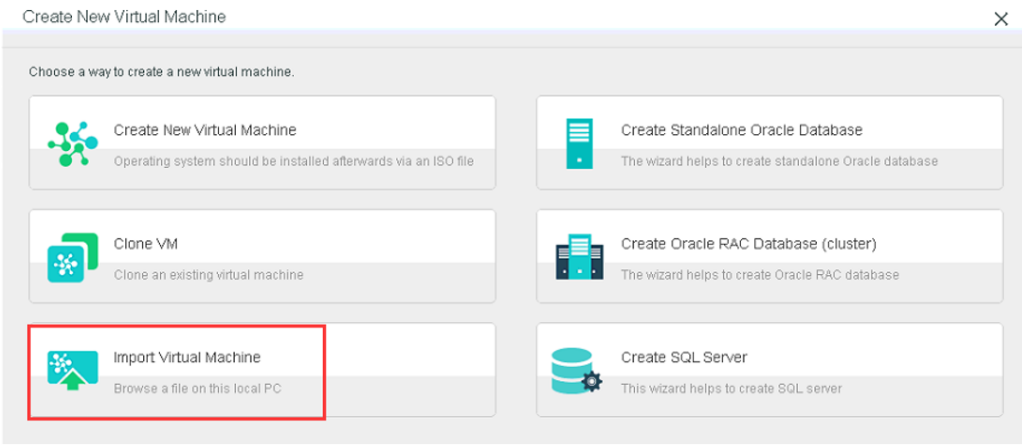
Steps:

Step 1. Log in to the HCI platform console.

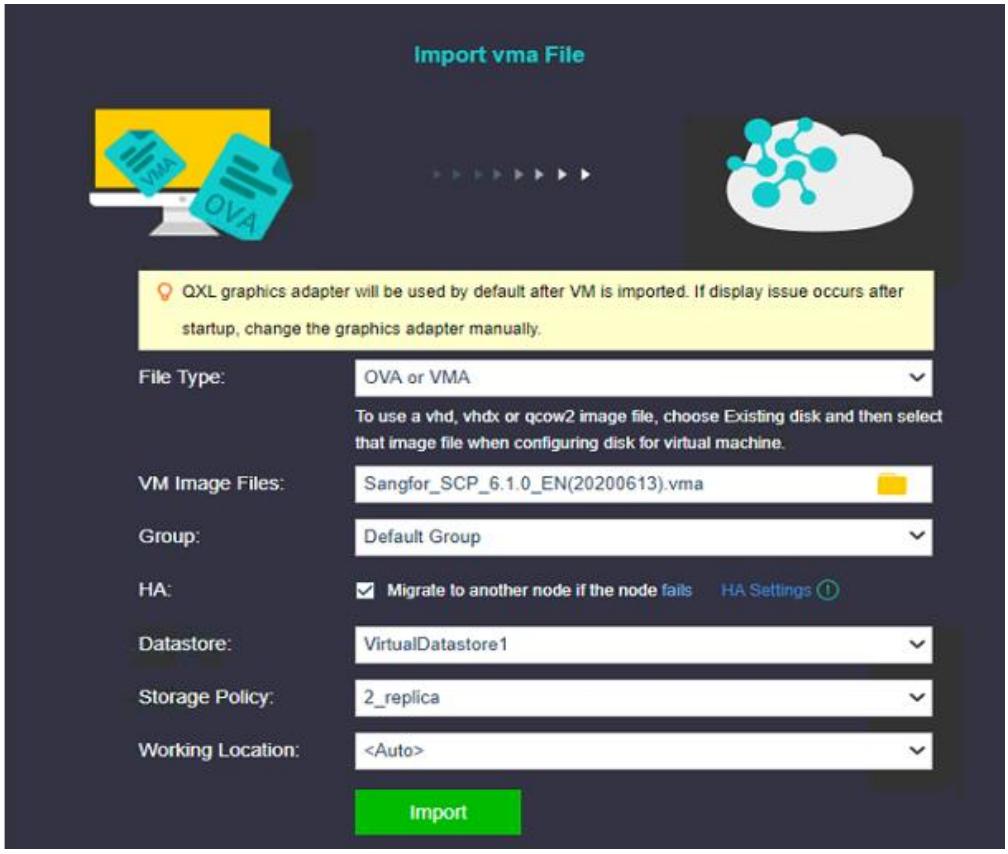


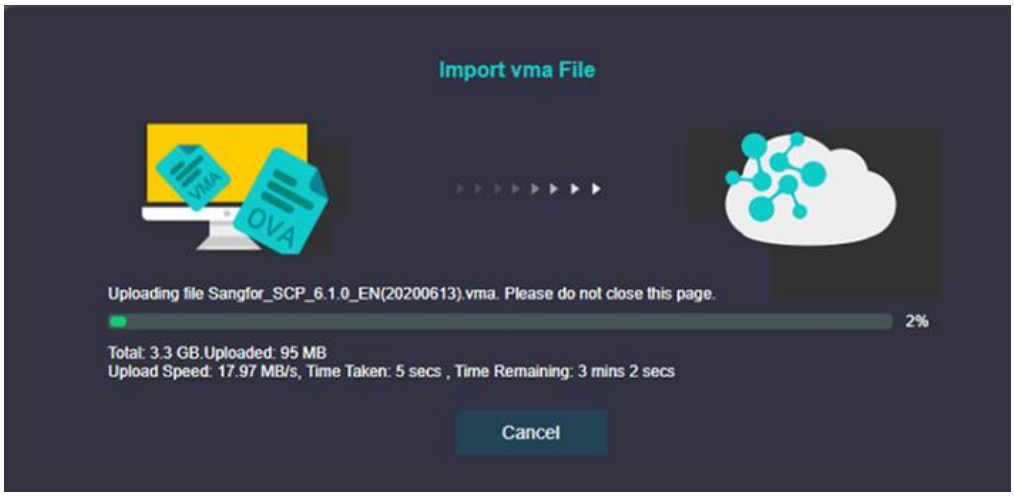
Step 2. Click **Compute** > **New** > **Import Virtual Machine:**



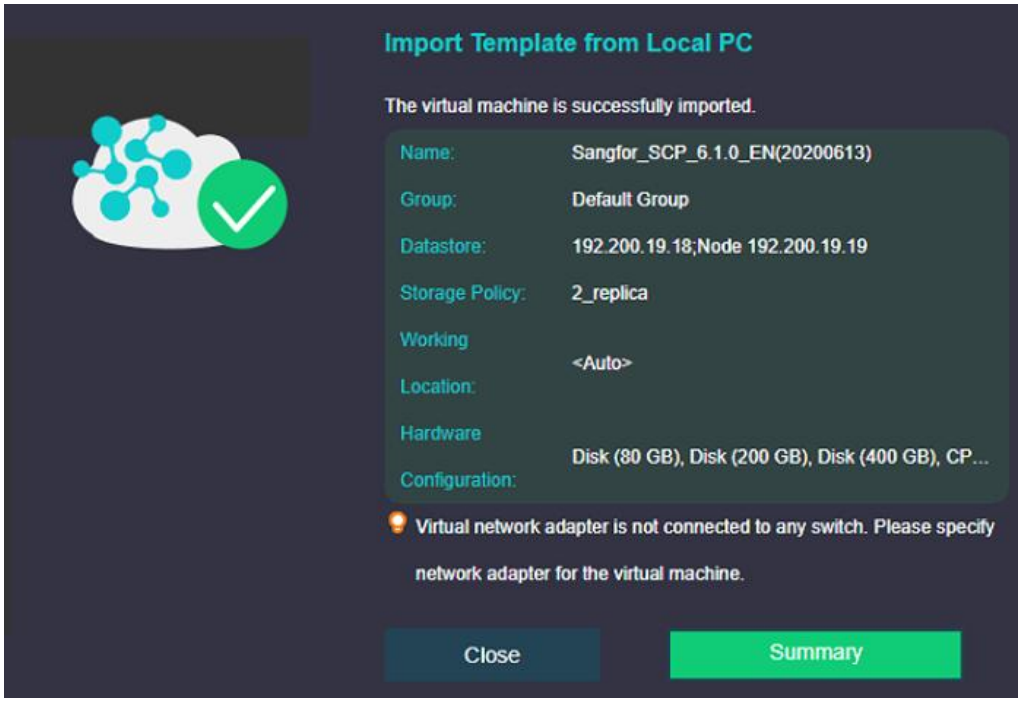


Step 3. Select the corresponding **VM Image File**, **Group**, **Datastore,** and **Run-on Node**. After that, click **Import** to display the upload interface.

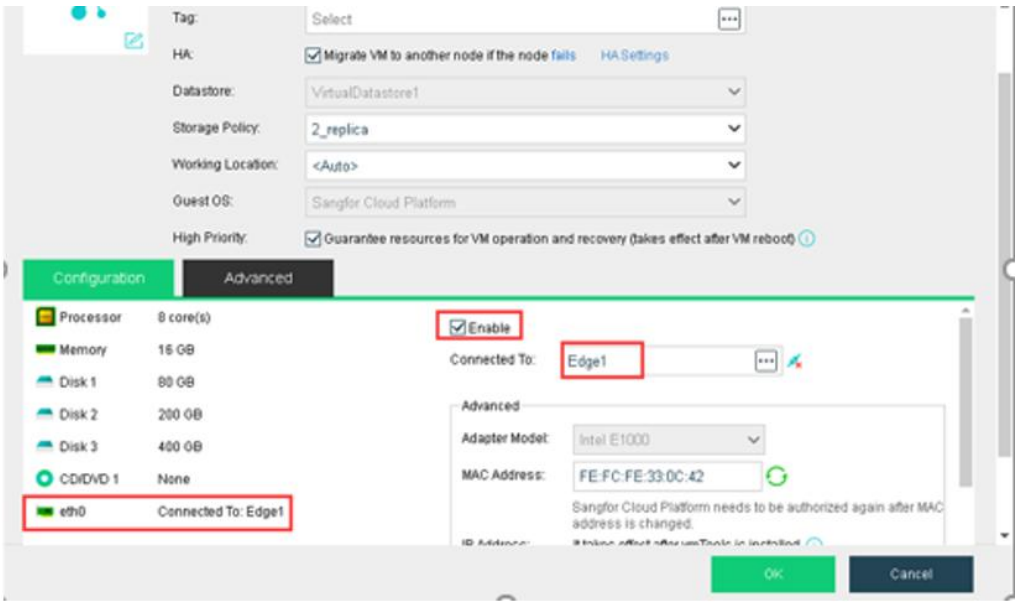




Step 4. After successfully uploading, select the newly imported SCP virtual machine and click **More** > **Edit** to map the USB key.

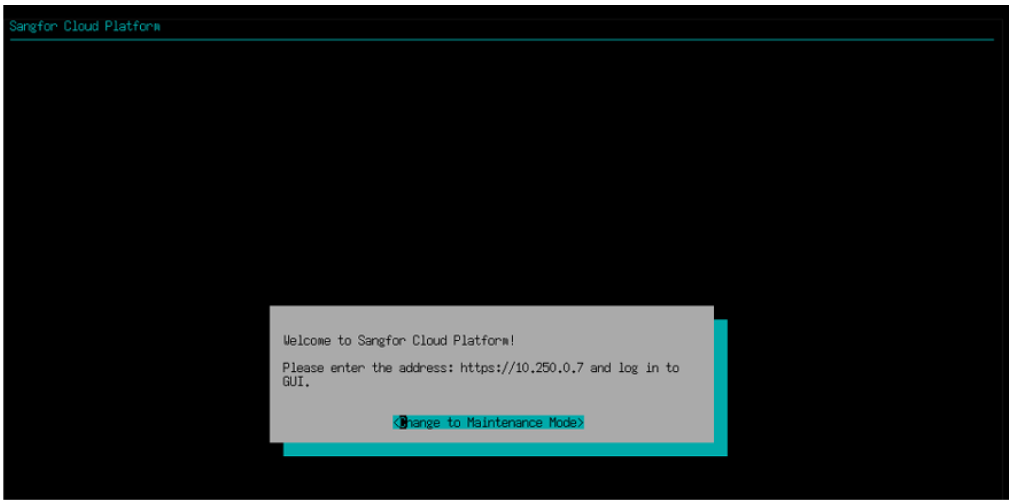


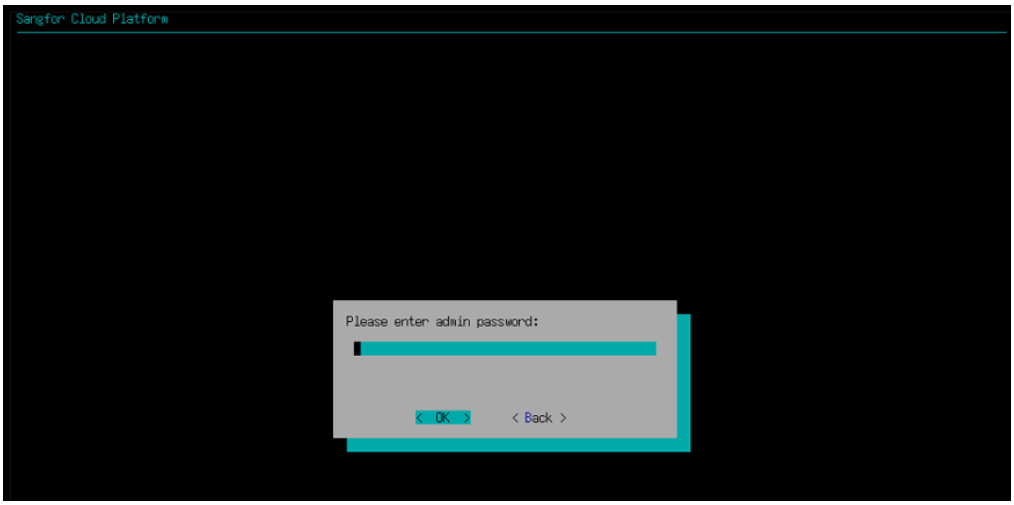
Step 5. Select the newly imported SCP virtual machine, click **More** > **Edit** to edit the NIC, connect the network with the second/third layer management network, and click **OK**.



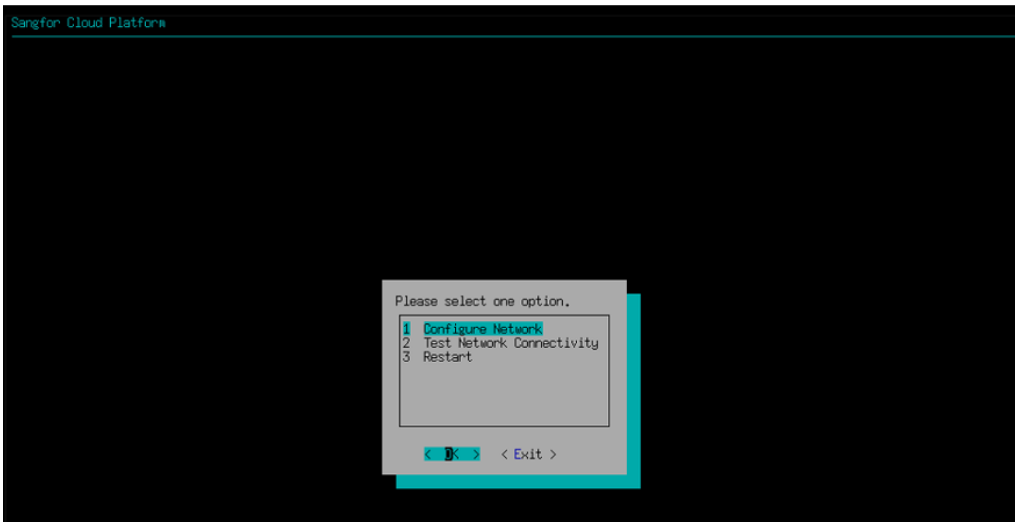
Step 6. Powered on the imported SCP virtual machine, have a random click on the virtual machine's console, press **Enter** to enter into the maintenance mode, and then enter the password (the initial password is admin). After the password is entered, click **OK** and press Enter to **enter** the configuration

interface.

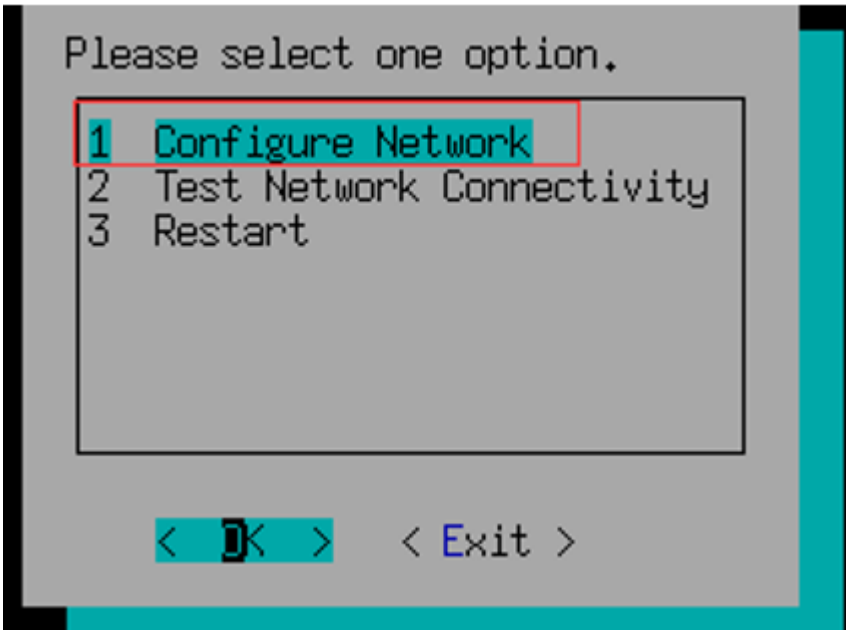


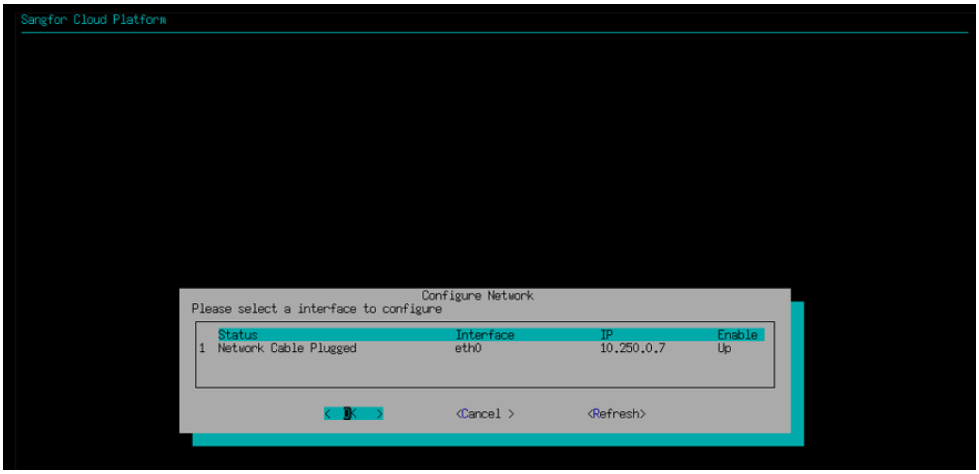


Click **OK** to enter the following interface:

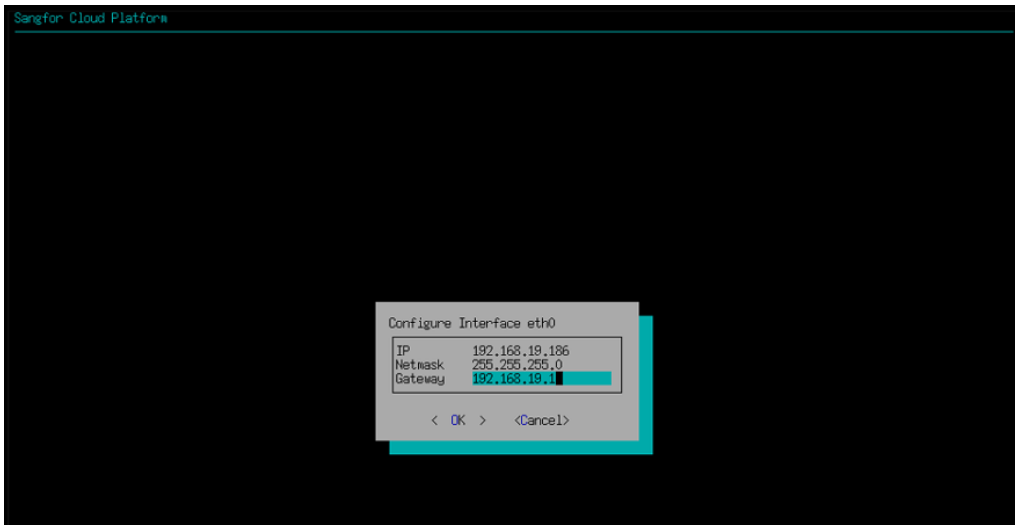


Step 7. Click the key ↑↓ on the keyboard to select **Configure Network** and press **enter**.



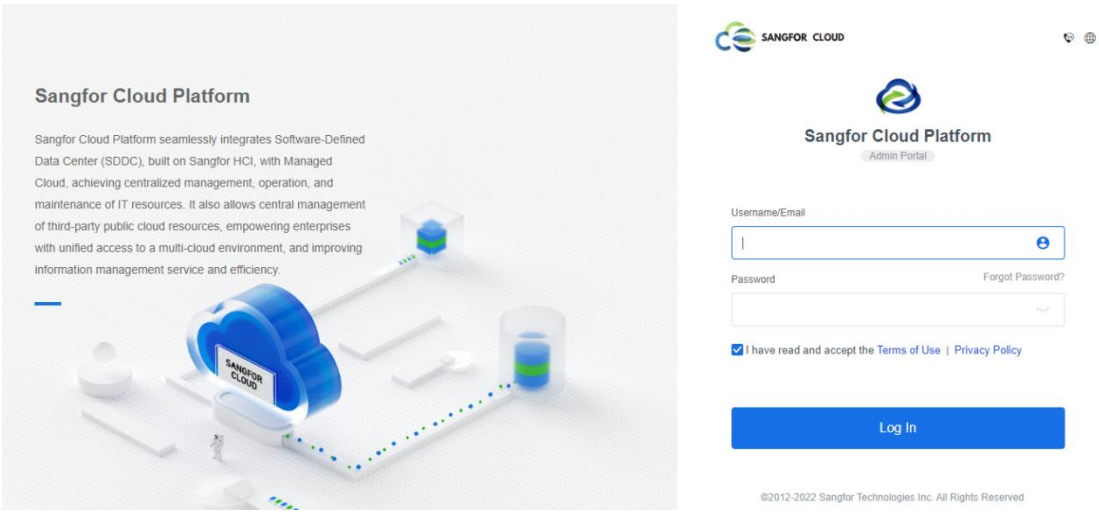


Step 8. Set the IP address, netmask, gateway and click **OK**.





Step 9. Open a browser, browse https://SCP IP:4430 and click **enter**.



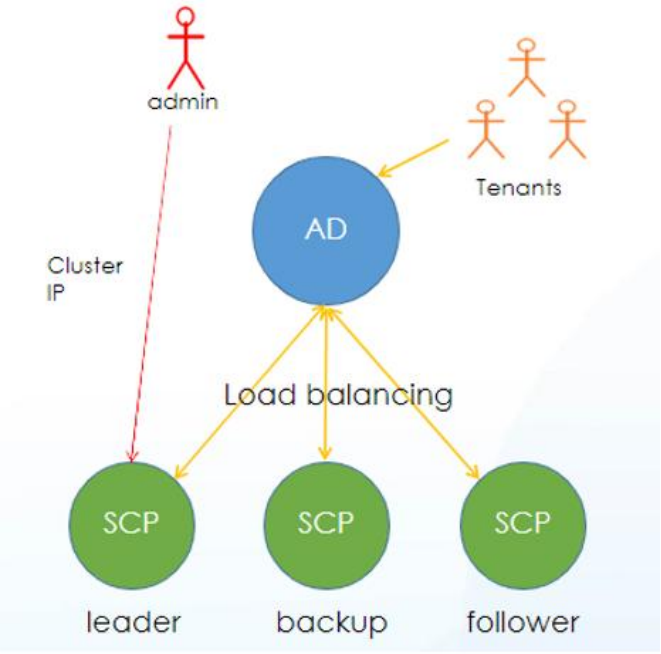
NOTE

1. The super administrator (admin) login needs to add port 4430, and the tenant and tenant sub-account user login can directly log in through the IP address, such as the IP set by HTTPS://.
2. The default account password is admin/admin. For your account security, please change the password.

2.4.2 Cluster Deployment

Function Description:

Sangfor SCP supports cluster mode deployment, switching SCP from stand-alone mode to cluster mode, providing horizontal expansion and high availability capabilities. After switching to the cluster mode, tenants are supported to access each node of the SCP cluster through the load function of AD, and the admin logs in to the controller node through the cluster IP to manage the SCP cluster.



Precautions:

1. Currently, only three-node SCP cluster deployment is supported, and only one node is allowed to fail in the cluster.
2. The SCP to form a cluster needs to be of the same version, and the added SCP has no information such as resource pools and users.
3. The node configuration to be added to the cluster needs to be greater than or equal to the configuration of the active node in the cluster.
4. When the active node is offline and the backup node needs to be switched to the active node, if the database of the active node and the backup node is not kept in real-time consistency, they will not automatically switch. You need to manually restore the active node before the business can be automatically restored. The identity remains unchanged at this time.
5. After a node fails and goes offline, if you need to return automatically, you need to keep the version of the offline node and the patch package version consistent with the active node.
6. Only offline nodes can be deleted.
7. Switching SCP from cluster mode to stand-alone mode is not supported.
8. When deploying the cluster mode, it does not support SCP deployment to multiple units through cloning, and it must be deployed by importing the SCP template multiple times.

Recommended configuration

The SCP cluster deployed with three nodes significantly improves the transaction processing capabilities of the cloud computing platform and provides high concurrency and high availability features for large-scale delivery scenarios. In cluster mode, it is recommended to use three nodes for deployment. The configuration specifications are as follows:

SCP Configuration	Number of Tenants	Number of Tenant Users	Concurrency Number of HCI Cluster	Number of Managed Cluster	Number of Physical Node	Number of Virtual Machine

32 Core 64G *3	2000	4000	4000	128	1024	60000

2.4.2.1 Single NIC Scenario

Function Description:

For the SCP single network card scenario, the situation where the management network and the business network are integrated, small-scale delivery scenarios are recommended.

Precautions:

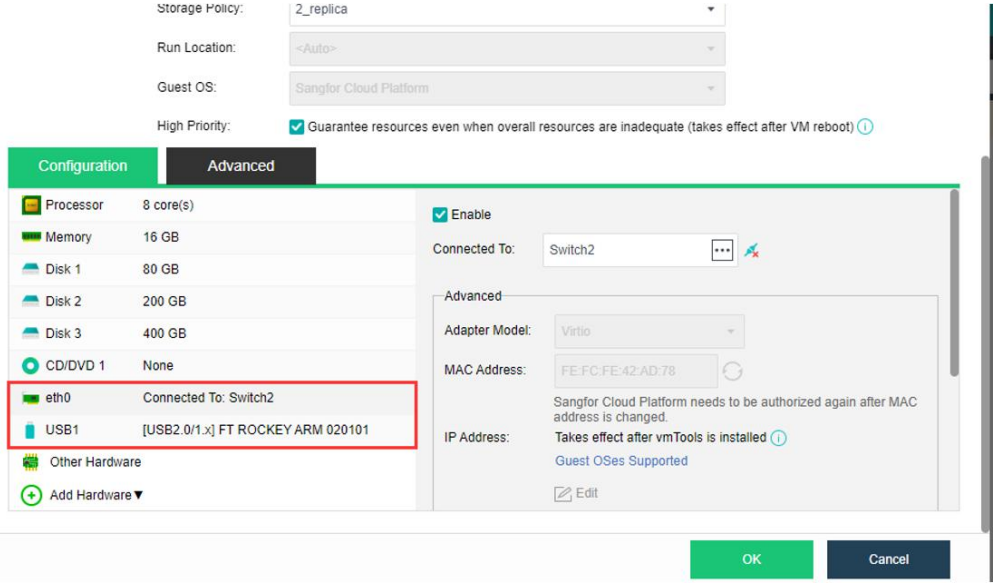
Load balancing cannot be done in a single network card scenario.

Prerequisites:

Ports 4480 and 443 can be accessed.

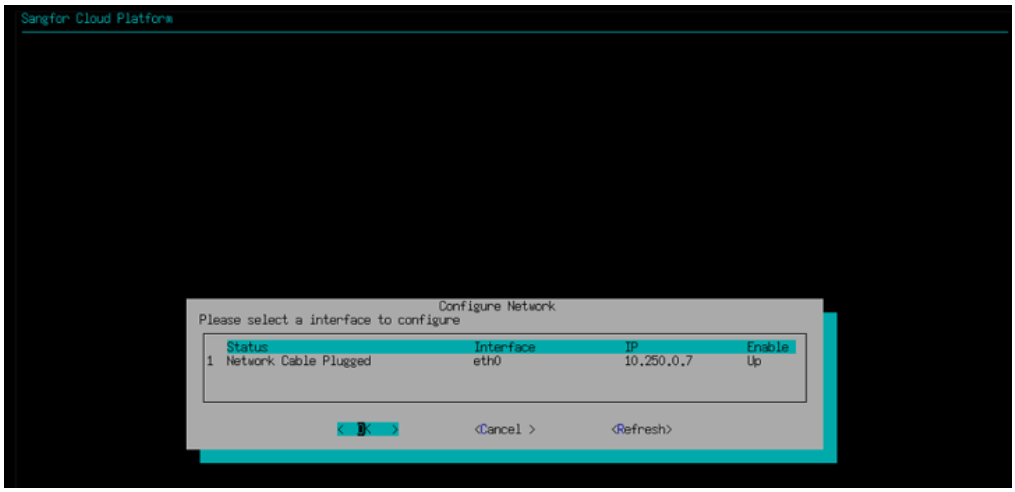
Steps:

Step 1. Log in to the HCI platform console, select the SCP virtual machine, click **Edit**, add USB hardware, and map the license key to the virtual machine. (Only the SCP active node needs to be added, the other two nodes can skip). Edit the network card, so it is reachable between the second-and third-layer network. After this, click **OK**.



Step 2. SCP single network card configuration: log in to the SCP console, click on any part of the virtual machine console, type **enter** on the keyboard, enter

the maintenance mode, and enter the password (the initial password is admin). Use the keyboard ↑↓ key to select **Setup Network**, press **enter** key on the keyboard, configure the IP address, netmask, and gateway, and click the **OK** button.

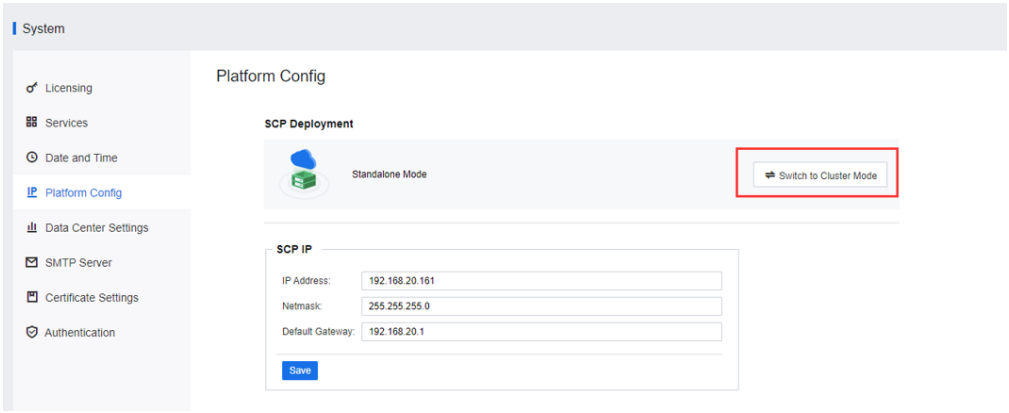


Step 3. Follow the above steps to complete the deployment and network card configuration of the other two SCP nodes in sequence.

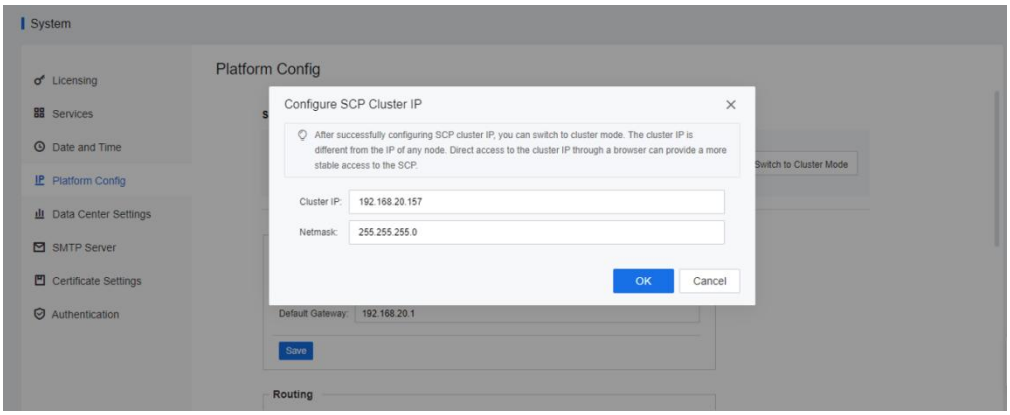
Step 4. Log in to the main SCP console, navigate to **System > Platform Config**, and click the **Switch to Cluster Mode** button to switch the SCP platform deployment mode to cluster mode.

NOTE

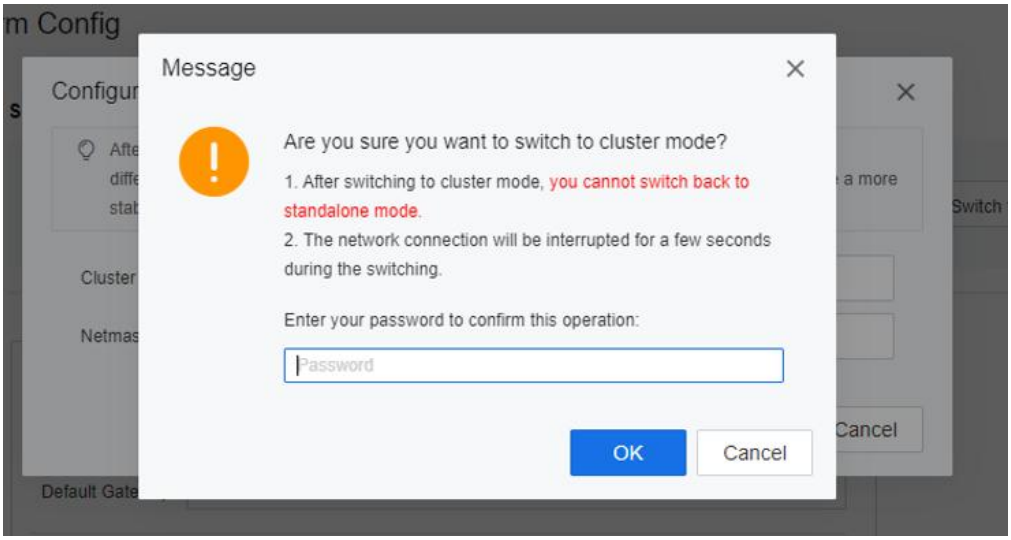
After the SCP is switched to the cluster mode, it cannot be switched back to the stand-alone mode.

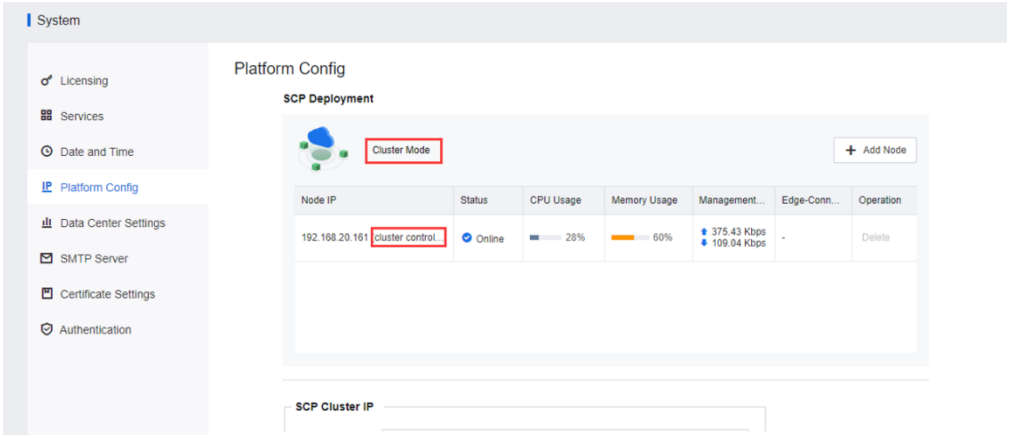


Step 5. Enter the **Cluster IP** and **Netmask** in the pop-up dialog box. You must ensure it is in the same network segment as the platform IP.

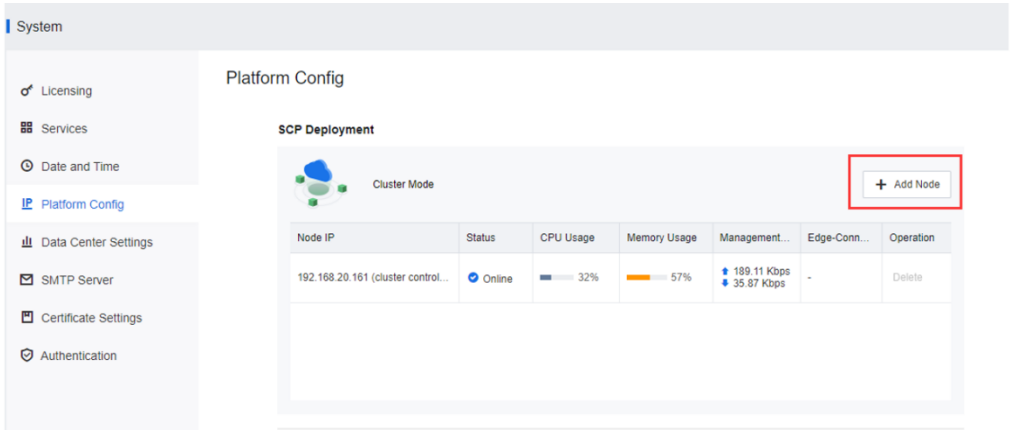


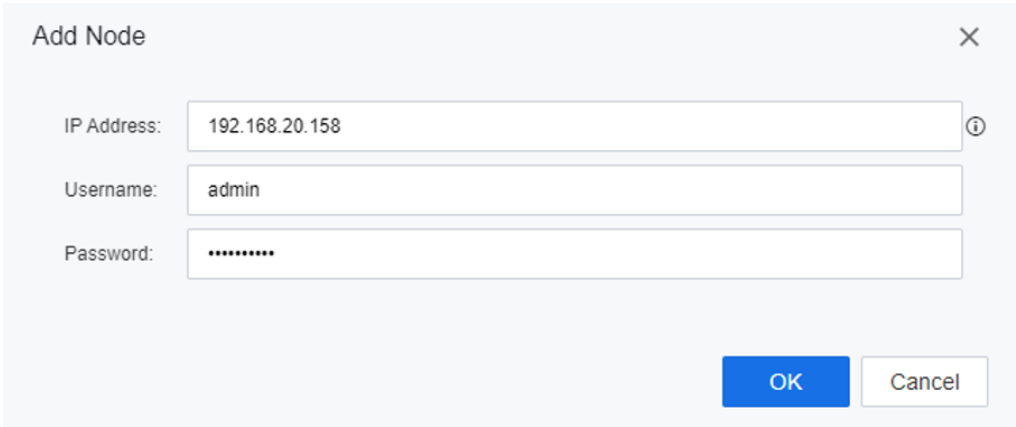
Step 6. Click **OK** to switch to cluster mode, and the current node is switched to the cluster controller node of the cluster.

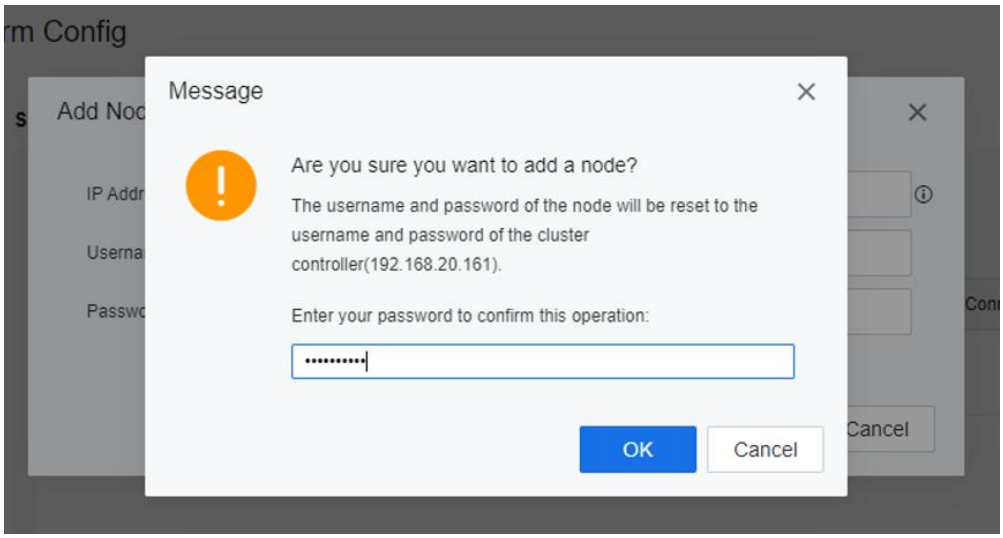


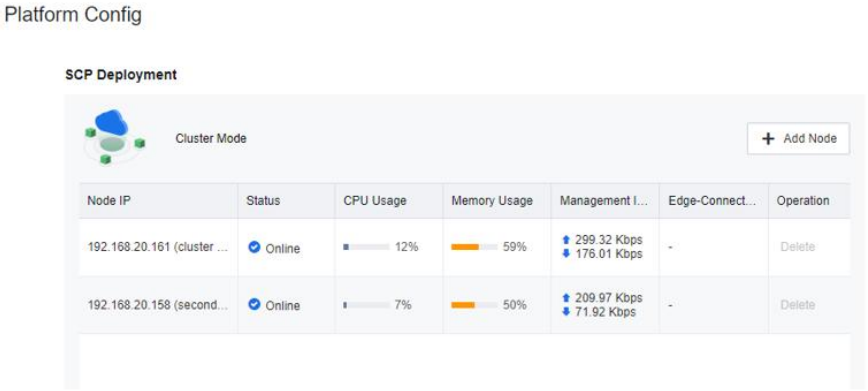


Step 7. Continue to add the standby node, click **Add Node**, enter the standby node IP address, username, and password, click **OK**, enter the current admin password, and complete the addition of the standby node.

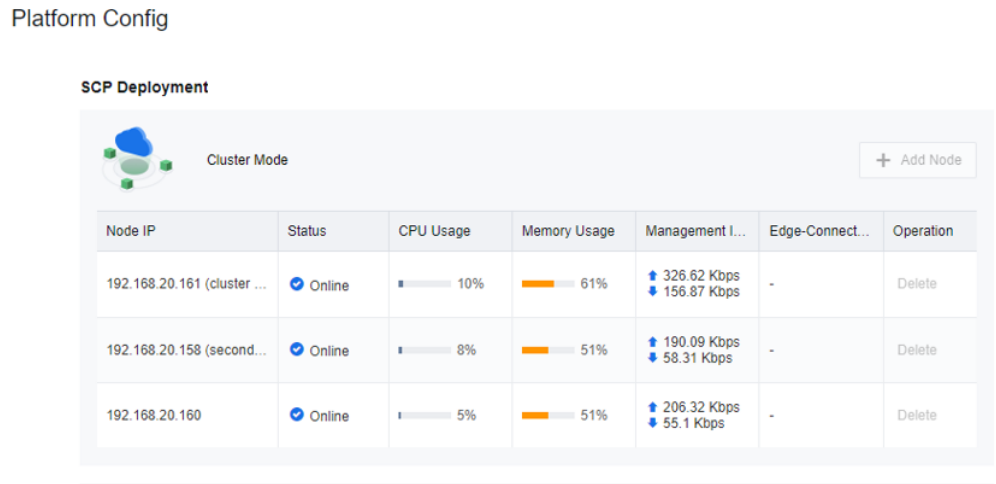






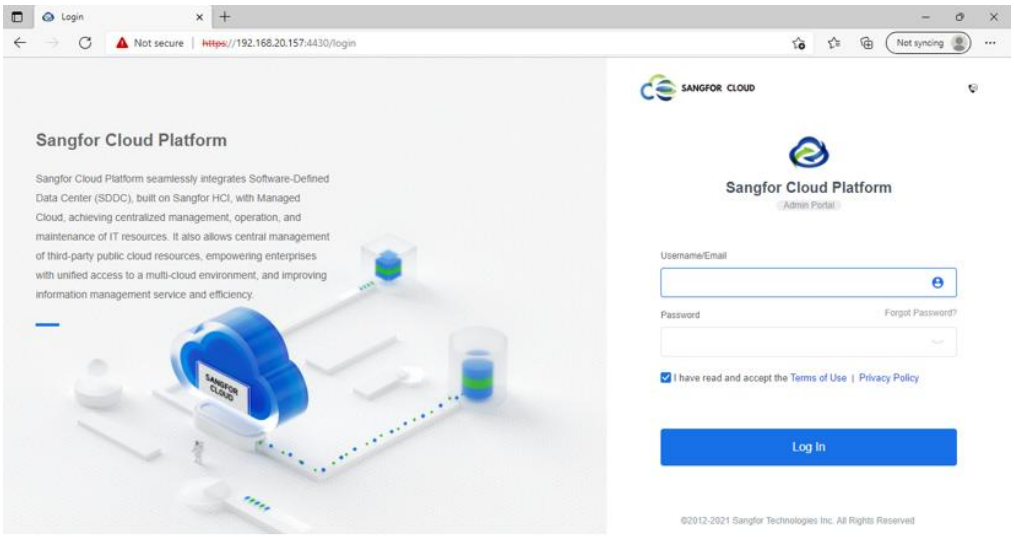


Step 8. Continue to add cluster nodes until SCP Cluster is successfully formed.



Step 9. After the deployment is complete, open the browser, the

administrator logs in at https://{cluster IP}:4430, and the tenant logs in at https://{cluster IP}:443.

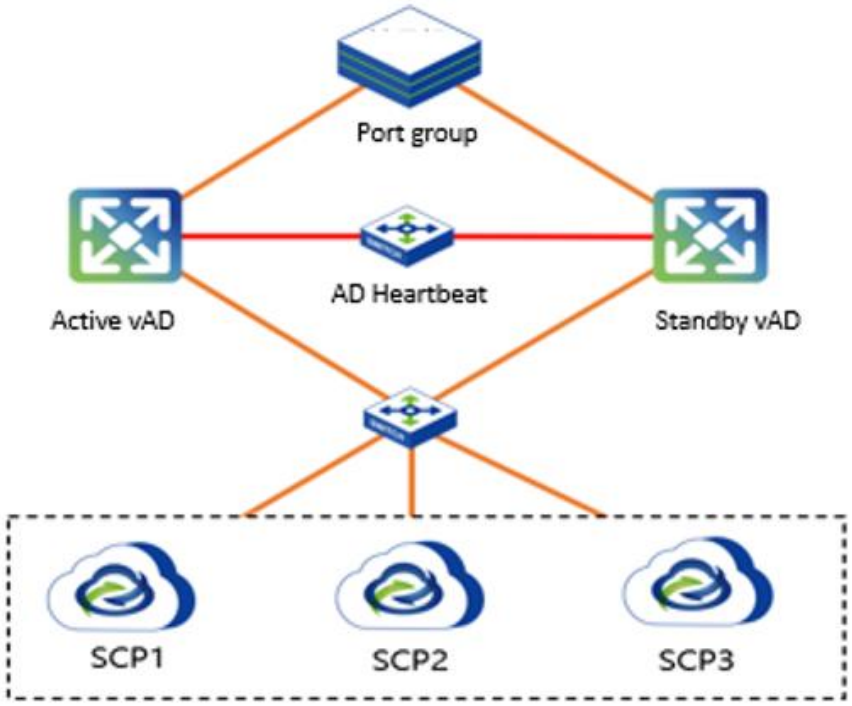


2.4.2.2 Multiple NIC Scenario

Function Description:

For the SCP multiple network card scenario, which separates the management network and the business network, it is recommended to use it in a large-scale delivery scenario.

Topology Overview



Precautions:

The SCP multiple network card scenario needs to be configured with load balancing. There is no mandatory requirement for the vAD version. It is recommended to use vAD7.0.8R4, and the AD High Availability deployment is recommended.

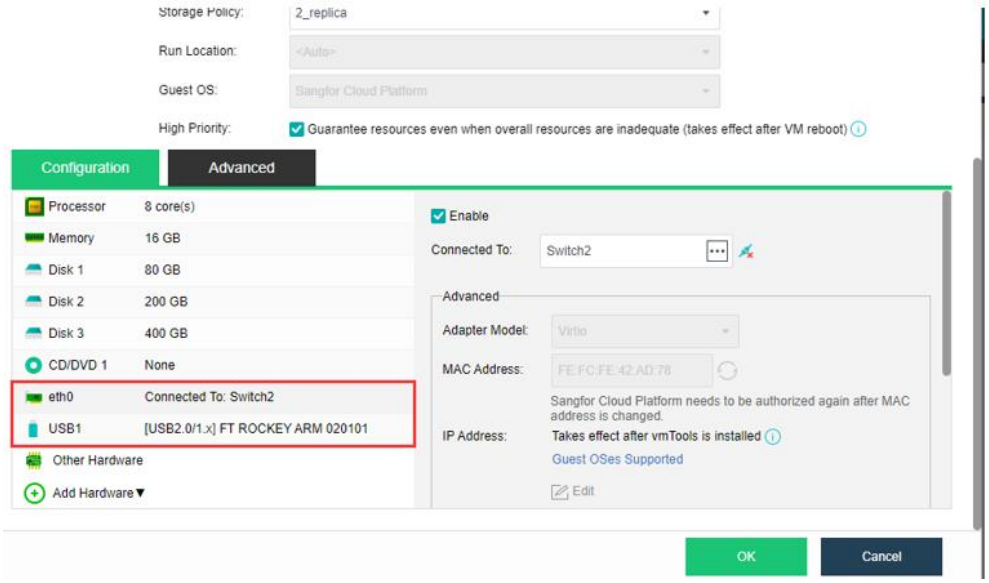
Prerequisites:

Ports 4480 and 443 can be accessed.

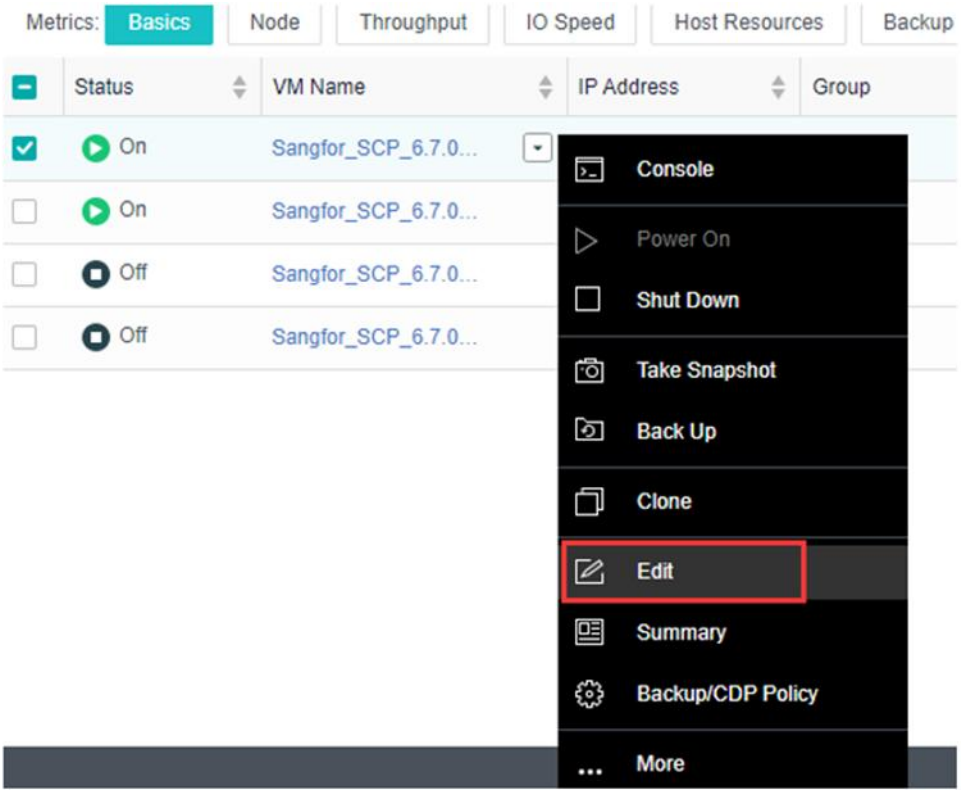
Steps:

1. SCP Multiple NIC configuration

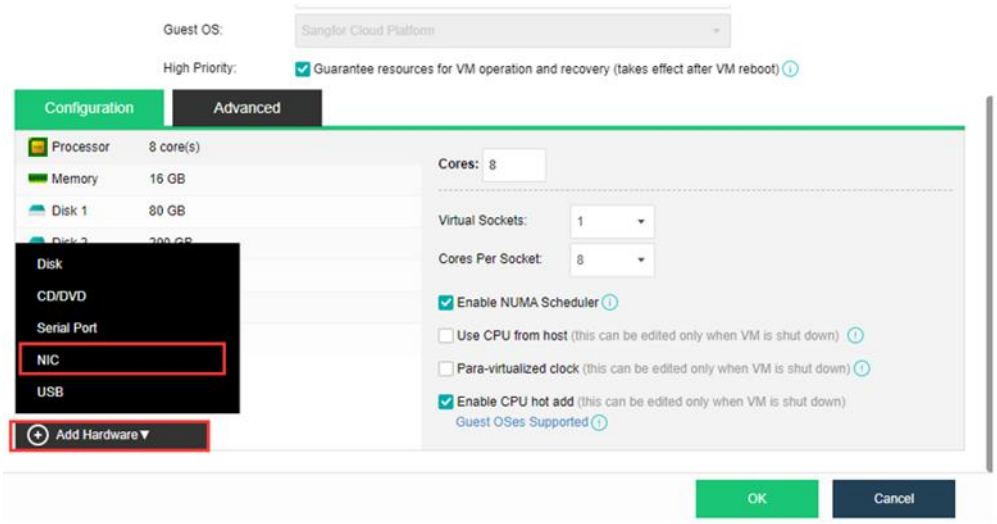
Step 1. Log in to the HCI platform console, select the SCP virtual machine, click **Edit**, add USB hardware, and map the license key to the virtual machine. (Only the SCP active node needs to be added, the other two nodes can skip). Edit the network card, so it is reachable between the second-and third-layer network. After this, click **OK**.



Step 2. Enter the HCI virtual machine list, find the SCP virtual machine, right-click the **Edit** button, and enter the Edit virtual machine page.



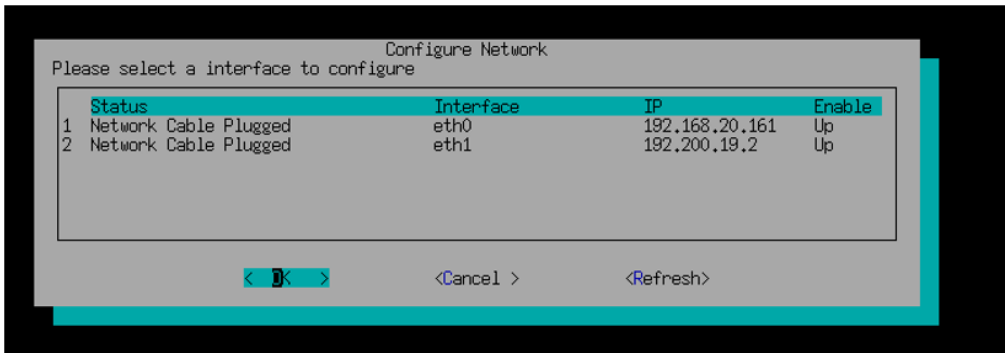
Step 2. Click **Add Hardware** to add second network cards for SCP. Then, edit the network card to connect to the tenant's business network.



Step 3. Log in to the SCP console, click on any part of the virtual machine console, type **Enter** on the keyboard, enter the maintenance mode, and enter the password (the initial password is admin). Use the keyboard ↑↓ key to select **Configure Network** and type the **enter** key on the keyboard to configure the IP address, netmask, and gateway for the SCP multiple network card, and click the **OK** button.

NOTE

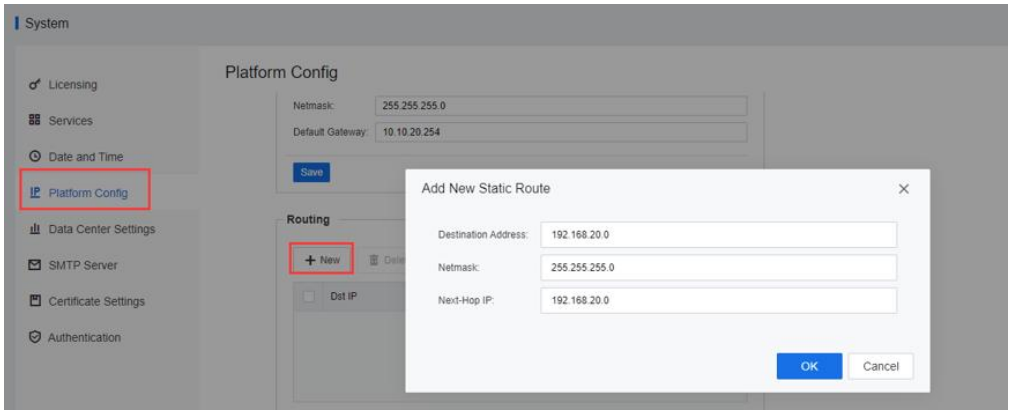
1. The network card configuration is as follows: eth0 is configured as the management login IP, and eth1 is configured as the tenant login IP.
2. The SCP gateway is recommended to be configured on eth1.



Step 4. Follow the above steps to complete the dual network card configuration for the other two SCP nodes.

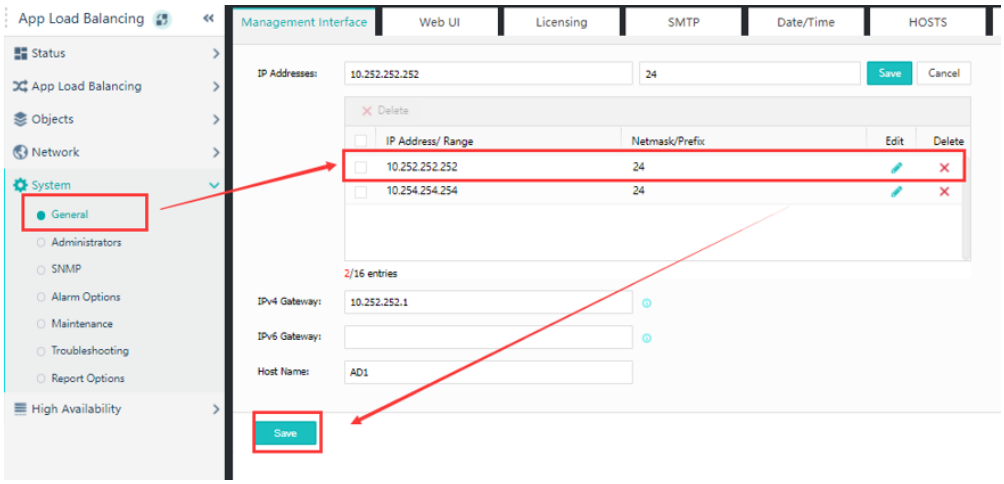
Step 5. Log in to the main SCP console and switch to cluster mode. For switching the cluster mode and adding nodes in the cluster, please refer to chapter **2.3.2.1 SCP Single NIC Scenario, steps 4-7**.

Step 6. Navigate to **System** > **Platform Config > Routing**, and click the **New** button. The **Destination Address** is the gateway of the local PC, and the **Next-hop IP** is the gateway of the cluster management network.

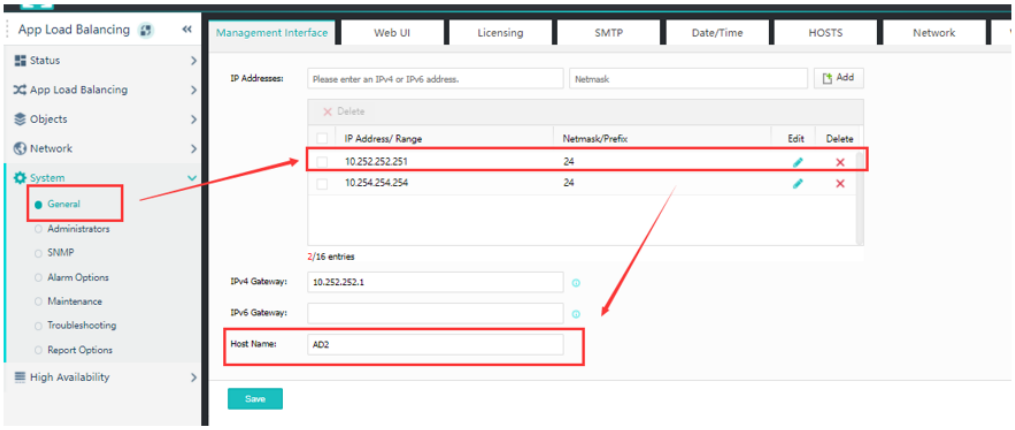


2. vAD (Virtual Application Delivery) High Availability Configuration

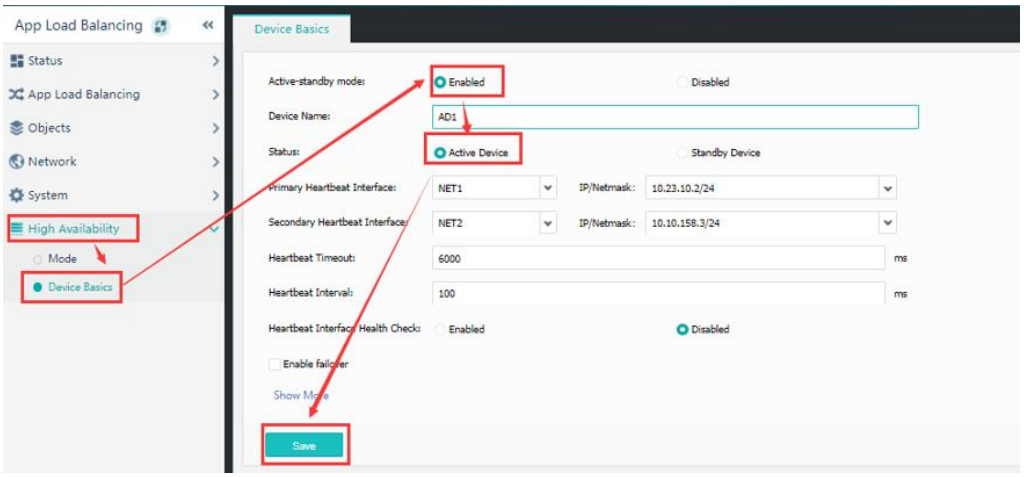
Step 1. Configure the management interface IP address. Log in to the console of the main AD1, navigate to **System > General > Management Interface**, and configure the management IP of the main AD1.



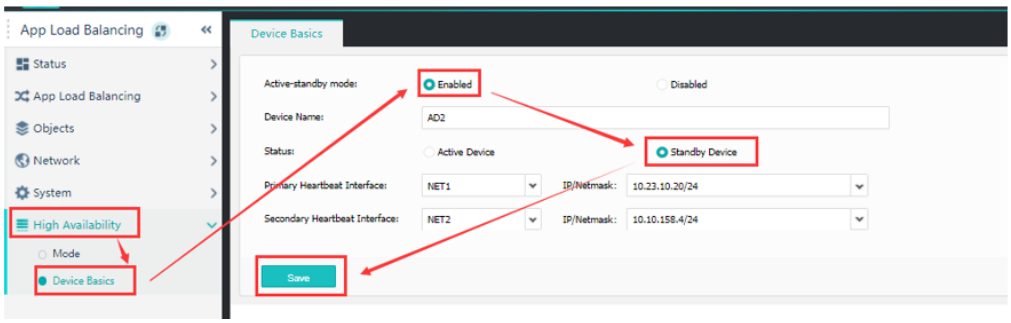
Step 2. After this, log in to the standby AD2 console to complete the configuration of the management IP.



Step 3. Configure high availability for both vAD. **Navigate to High Availability > Device Basics of** the main AD1, select **Enable** for **Active-standby mode**, and **Active Device** for **Status**.



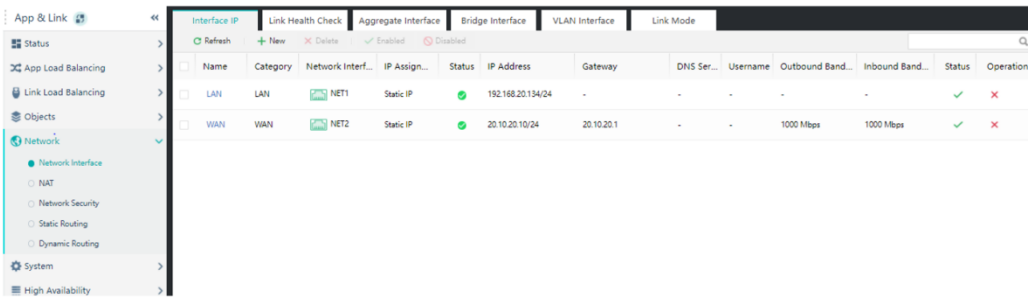
Step 4. Perform the same steps above for AD2.



Step 5. After completing the high-availability configuration, enter **the High**

Availability > **Device Basics** page of the active and standby ADs to check whether the active or standby status is normal.

Step 6. Navigate to the **Network** > **Network Interface** page and configure the



NOTE

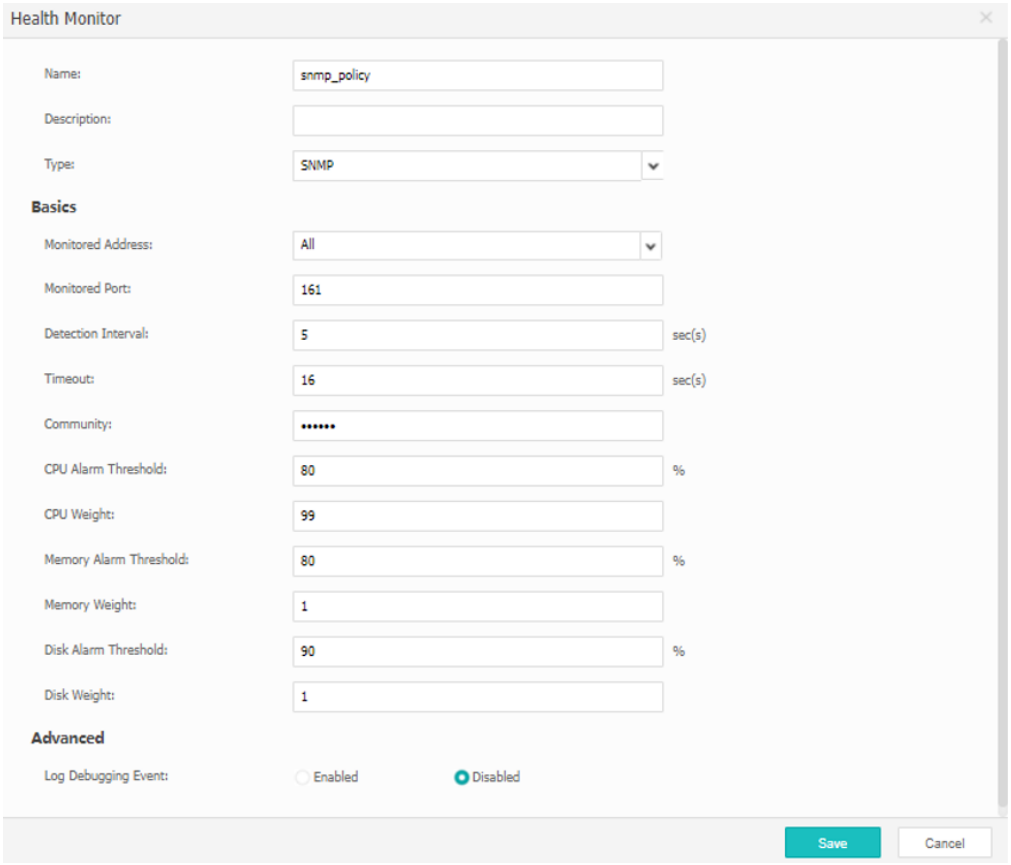
Here you only need to configure on the active device, and the backup will automatically synchronize the configuration in the standby device.

The configuration parameter description is shown in the following table.

Network Interface	Description
Network Interface - LAN	Connect the production port of the SCP node to communicate with the SCP node.
	There is no need to configure the gateway, DNS, name, inbound bandwidth, and outbound bandwidth.
	Status: Enabled.
Network Interface - WAN	By connecting to the external network, the tenant can access the AD through this IP address and then access the SCP through the SCP production port.
	Outbound Bandwidth and **Inbound Bandwidth**: 1000Mbps is recommended.

Step 7. Navigate to the **App Load Balancing** > **Node Pool** > **Health Monitor** page, configure the business health check policy, and configure the SNMP

policy.



The configuration description is shown in the following table.

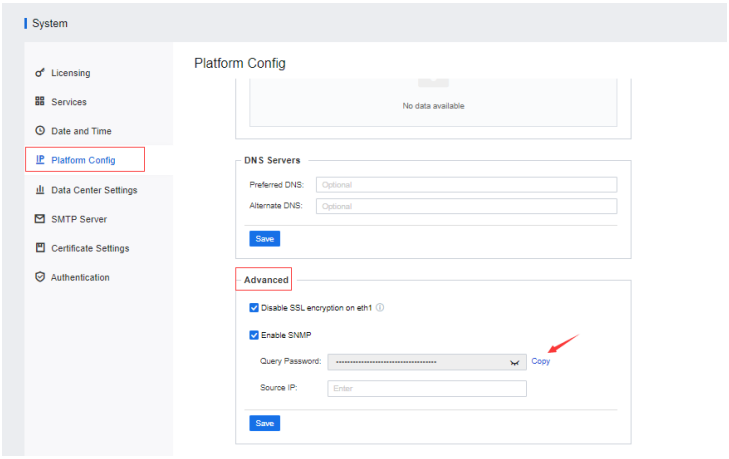
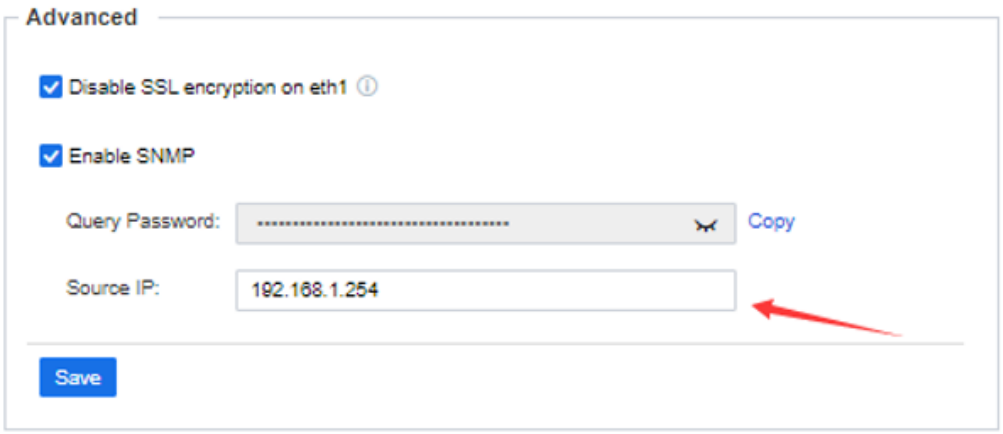
Attributes	Description
Name	Configure Policy Name
Type	Choose **SNMP**
Password Enquiry	Enter the SNMP query password. You can get the query password by logging into the SCP platform. Then, navigate to **System > Platform Config > Advanced**, and click the **Copy** button beside **Query Password**. 
CPU weight	Set as 99.
Memory Weight	Set as 1.
Memory alarm threshold	Set as 80.
Disk weight	Set as 1.
Other configurations	Use the default settings.

Table 1: SNMP Configuration Specification

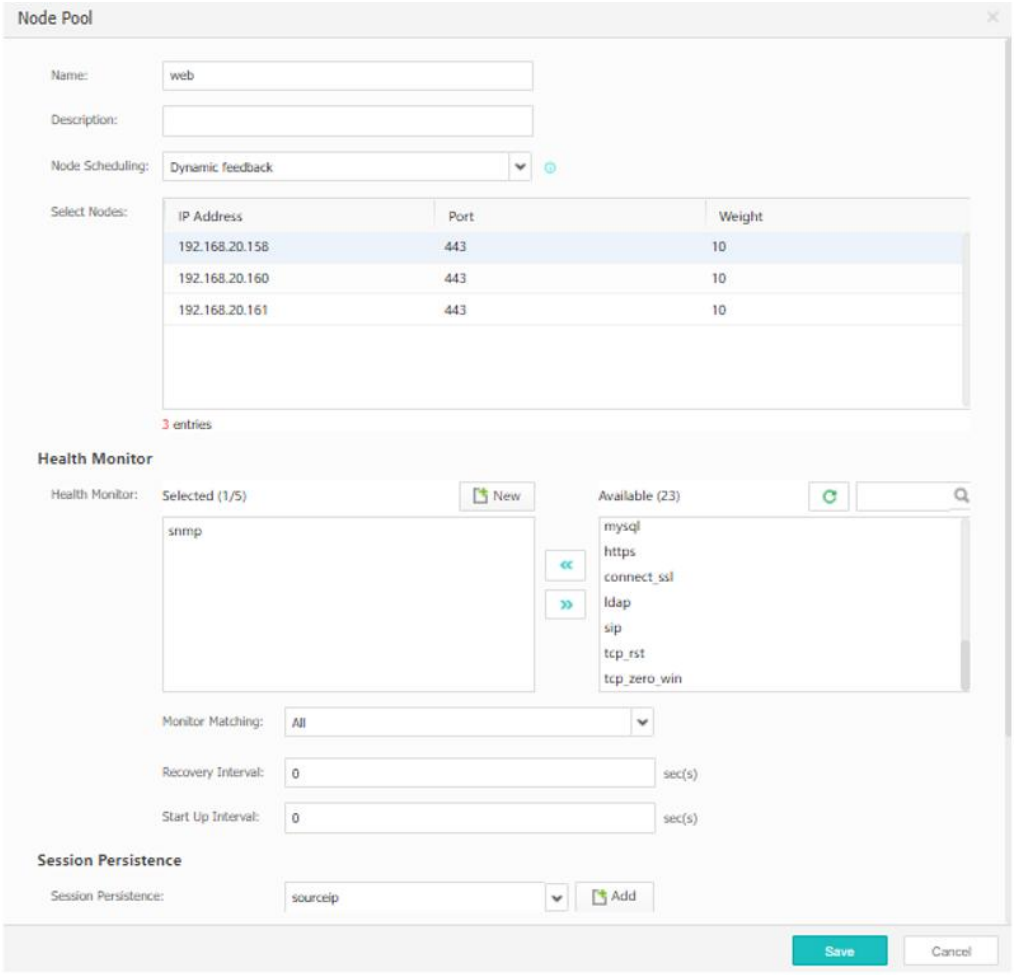
Back to the SCP platform, navigate to **System** > **Platform Config** > **Advanced** to configure the **Source IP.** Fill in the business IP address used to interconnect with SCP on vAD.



Step 8. Configure the **Node Pool**. Create two address pools. The ports are 443 and 4480, respectively, the addresses must be the service addresses of the SCP, and the SNMP policy in the previous step is used for detection. Navigate to the **App Load Balancing** > **Node Pool** page:



- Web node pool configuration



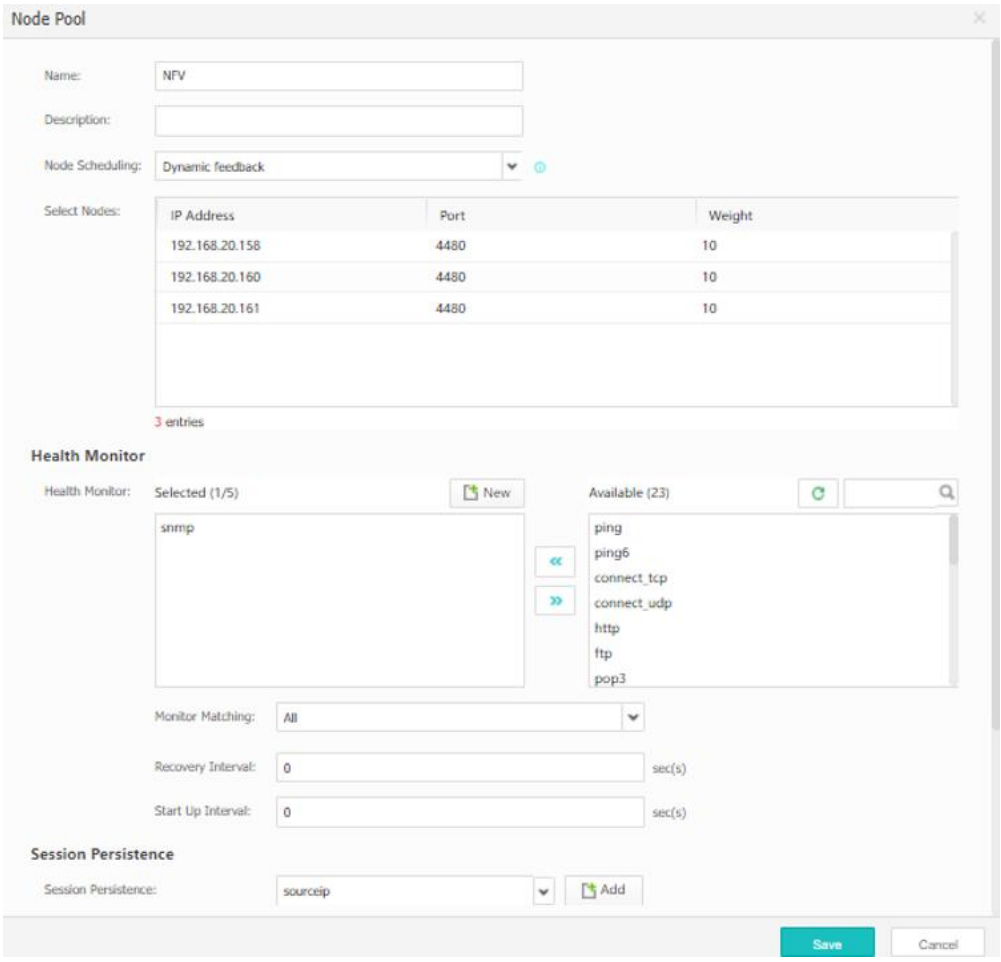
The configuration description is shown in the following table.

Attributes	Description
Node Scheduling	Select “Dynamic Feedback”
Select Node	Add the service IP of the SCP node. The port number is 443, the weight is 10, and the priority is 1.
Health Monitor	Select custom SNMP Policy created previously.
Others	For **Heavy Load**, select **Set to Scheduling**. For **Connections**, select **All in any status**.
Session Persistence	Select **sourceip**

Other configurations	Use the default settings.

Table 2: Node Pool Configuration Specification

- NFV node pool configuration



The configuration description is shown in the following table.

Attributes	Description
Node Scheduling	Select “Dynamic Feedback”
Select Node	Add the service IP of the SCP node. The port number is 443, the weight is 10, and the priority is 1.
Health Monitor	Select custom SNMP Policy created previously.
Others	For **Heavy Load**, select **Set to Scheduling**. For **Connections**, select **All in any status**.
Session Persistence	Select **sourceip**
Other	Use the default settings.

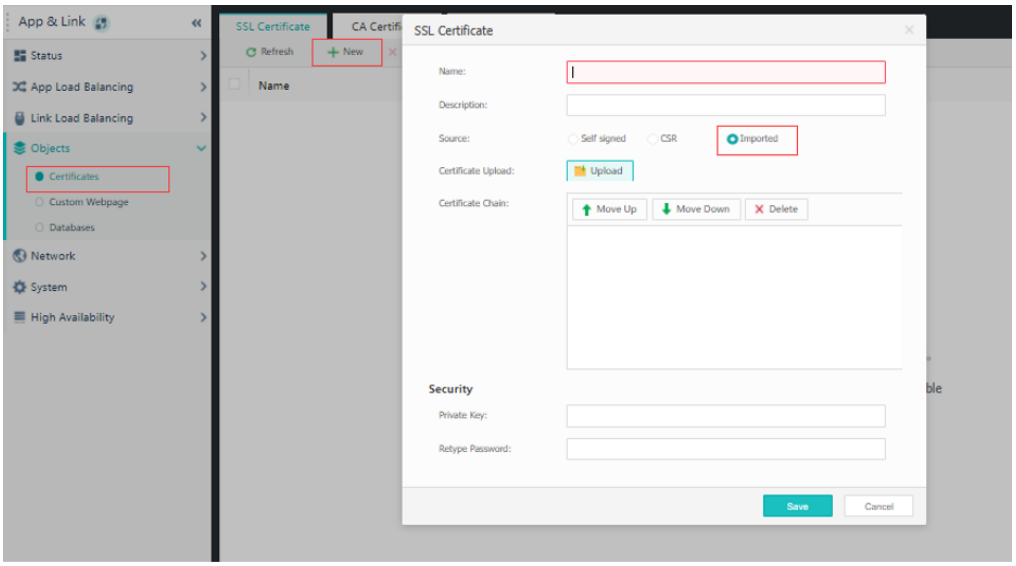
configurations	

Table 3: NFV Node Pool Configuration Specification

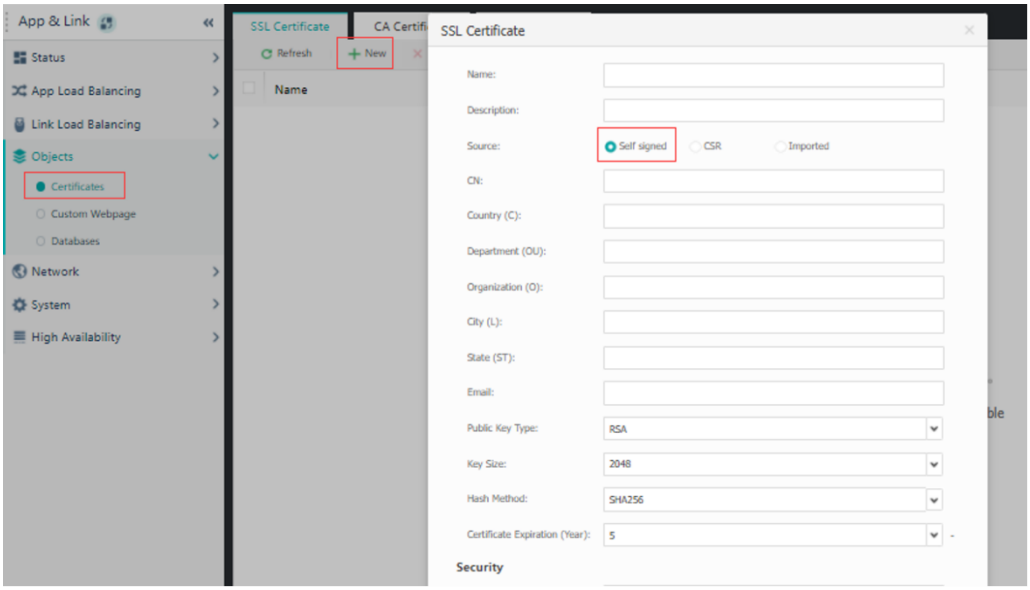
Step 9. Configure certificate offload and apply payload.

Add Certificate: There are two ways to add a certificate here. You can choose to import a certificate or manually add a certificate.

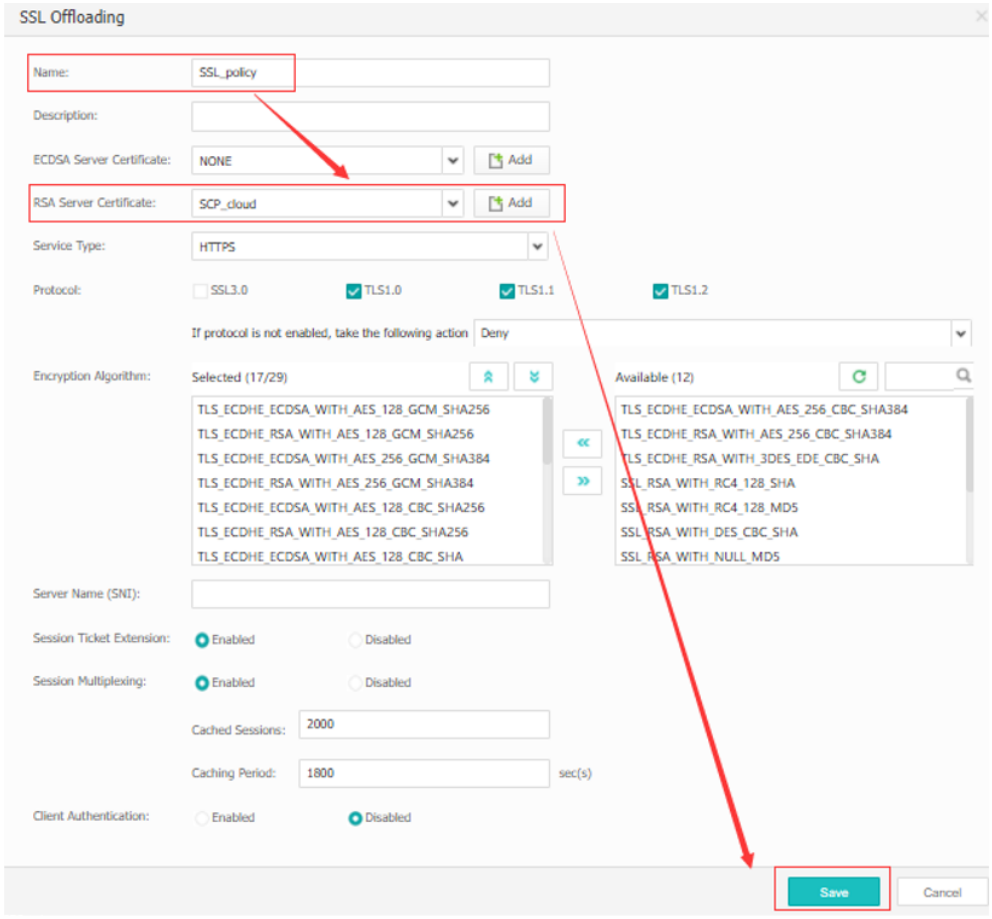
a. Import Certificate: Navigate to Objects > Certificates > SSL Certificate, click New, and select Imported for the Source. Then, import the certificate.



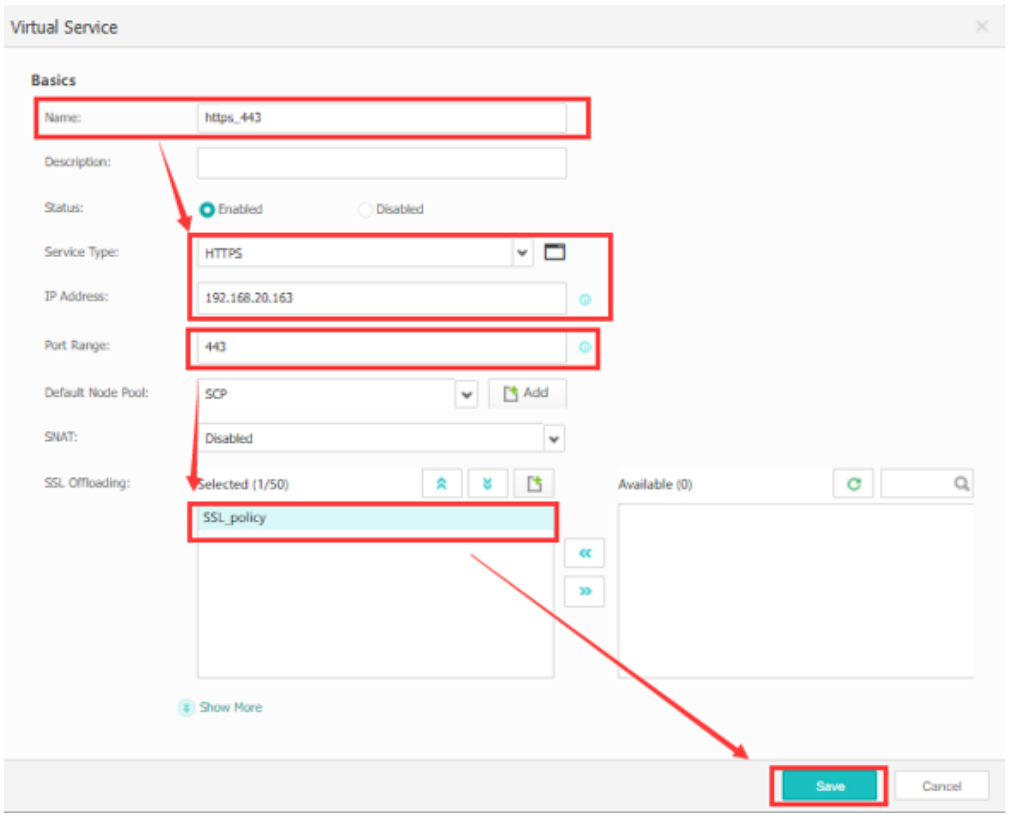
b. Add A New Certificate: Navigate to Objects > Certificates > SSL Certificate, click New, select Self signed for the Source, and customize the new certificate.

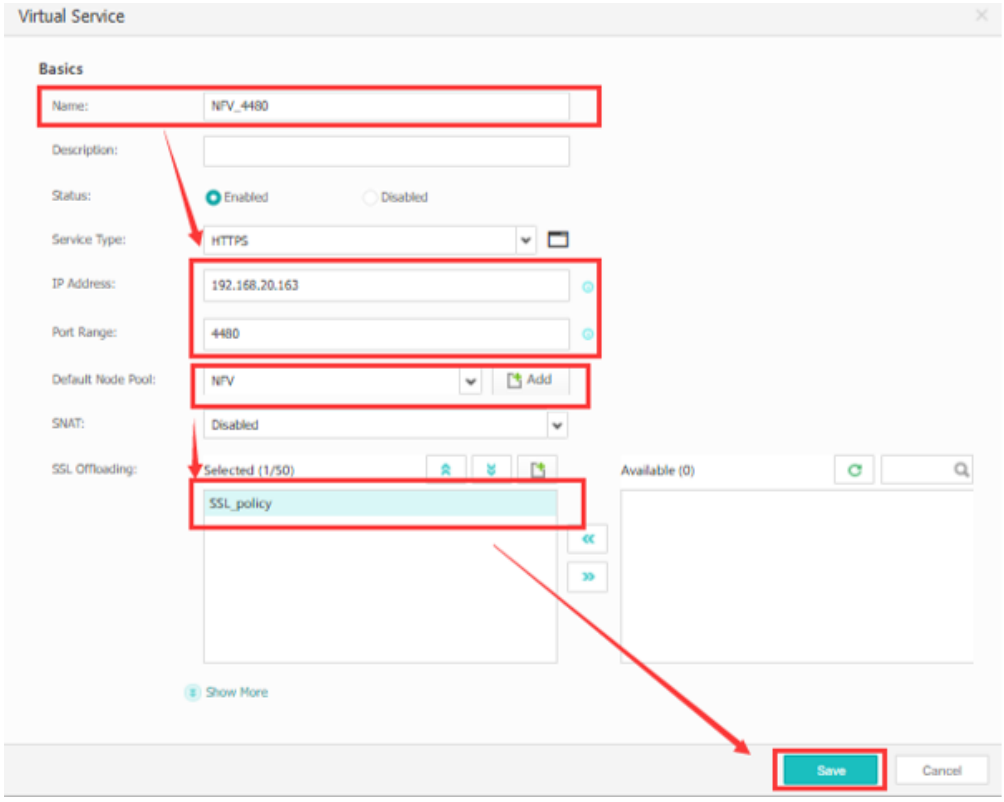


Next, navigate to **App Load Balancing** > **SSL Policy** > **SSL Offloading** and click **New** to create an SSL offload policy.



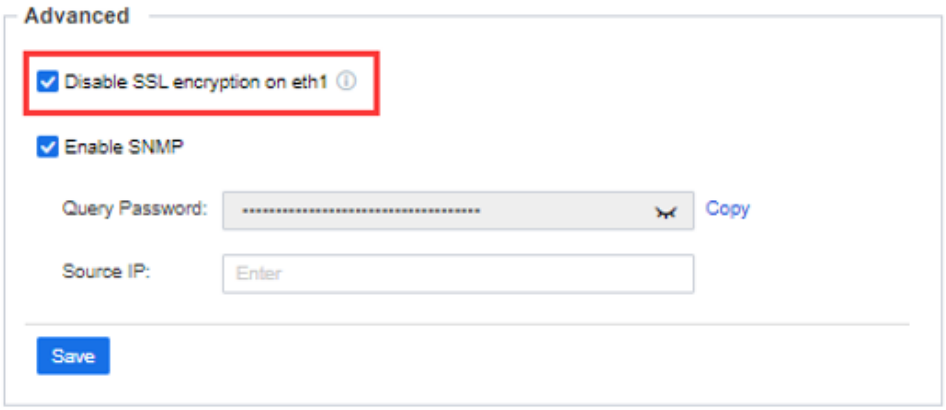
c. Configure virtual services for ports 443 and 4480.





Step 10. Turn off HTTP offloading for WAF

Log in to the SCP console, go to the **System** > **Platform Config** > **Advanced** page, and check **the Disable SSL encryption on eth1** checkbox.

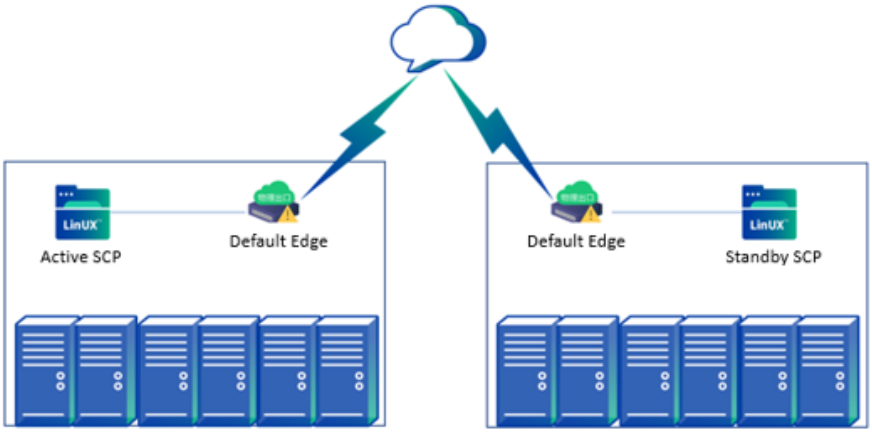


Step 11. After the deployment is complete, open a browser, the administrator logs in via https://{eth0IP}, and the tenant logs in via https://{eth1IP}.

2.4.3 Active/Standby Deployment (optional)

Product Description:

Sangfor SCP supports the deployment of active and standby, which improves reliability and can be used in the aDR (Cross-Site Disaster Recovery) scenarios. The main SCP is deployed in the node room cluster, and the standby SCP is deployed in the disaster recovery computer room cluster. When the node room fails and the primary SCP node is unavailable, the standby SCP node can be manually switched to the primary node to ensure the high availability of the management platform. The standby node can only be manually switched when the primary node is unavailable. In other cases, it cannot be switched at will.



Precautions:

1. Please ensure that the IP configured for SCP does not conflict with the IP addresses of other nodes. The network between the active and standby SCPs is reachable.
2. After the active/standby switchover, the standby SCP node becomes the active SCP node after restarting.
3. After switching, accessing the new main SCP will prompt that the USB-KEY has been removed and the licensing will expire soon. **Processing method**: The USB-KEY must be mapped to the new primary SCP after the switch within 30 days, and then the SCP virtual machine must be redeployed at the primary site, and the newly deployed SCP must be added as a standby SCP node.
4. If SCP is deployed in active/standby mode, and the active SCP is in cluster mode, the original SCP cluster will no longer be enabled if the remote backup node is switched to the primary. Otherwise, dual-active may occur, and the remote backup node will be restored in stand-alone mode.

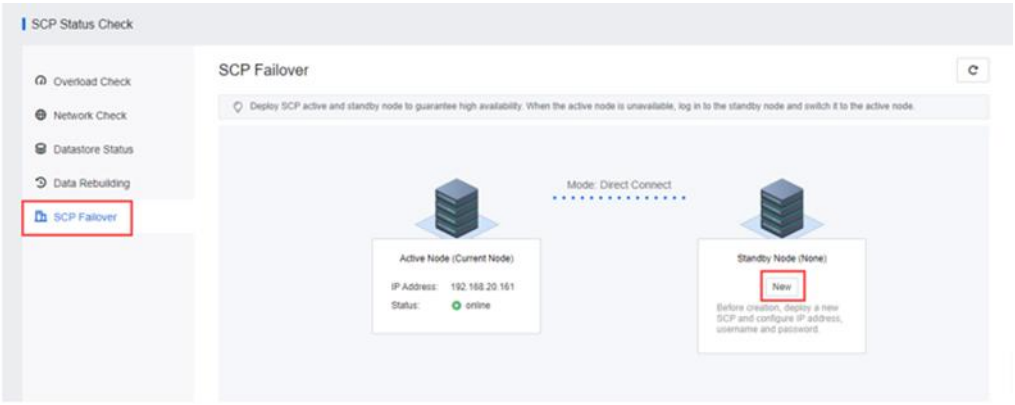
Prerequisites:

Sangfor HCI platform and SCP have been correctly deployed.

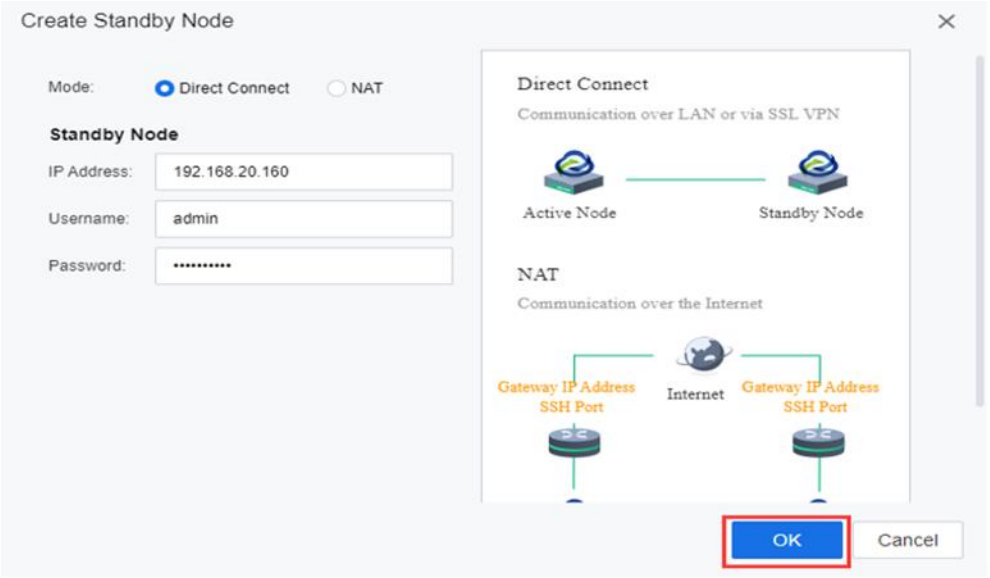
Steps:

Step 1. Deploy the standby SCP according to **Chapter 2.3.1 Single Host Installation**.

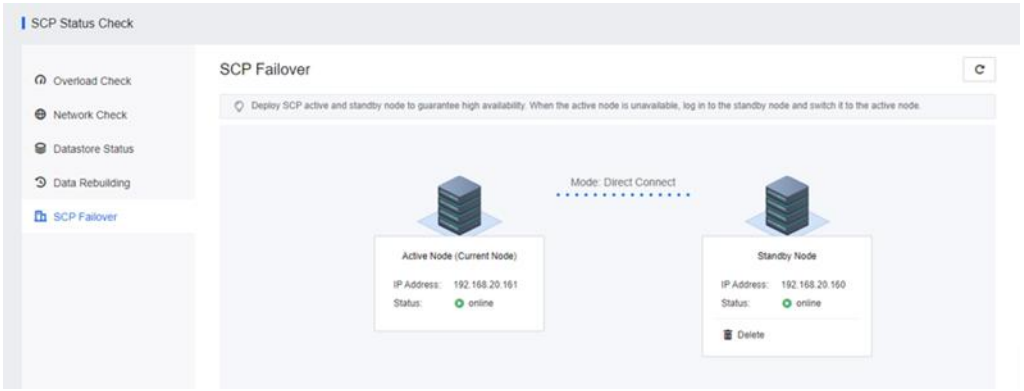
Step 2. Log in to the active SCP and navigate to **Resources > SCP Status Check > SCP Failover**.



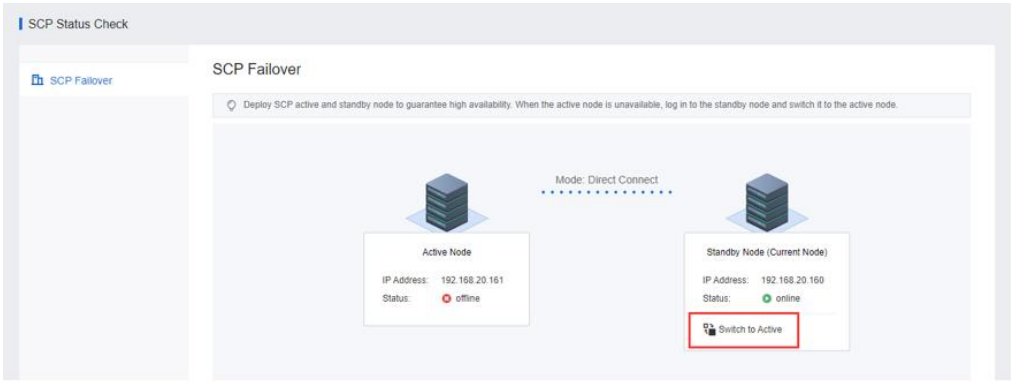
Step 3. Click the **New** button, enter the **IP address** and **Password** of the SCP standby machine, and click **OK**.



Step 4. After the successful addition, you can see the active and standby SCP status.



Step 5. When the primary SCP is offline, you can log in to the standby SCP to switch the standby to the primary.



2.5 Platform License

2.5.1 USB Key License

Function Description:

Use the authorization and license keys to authorize the SCP cloud management platform.

Precautions:

None.

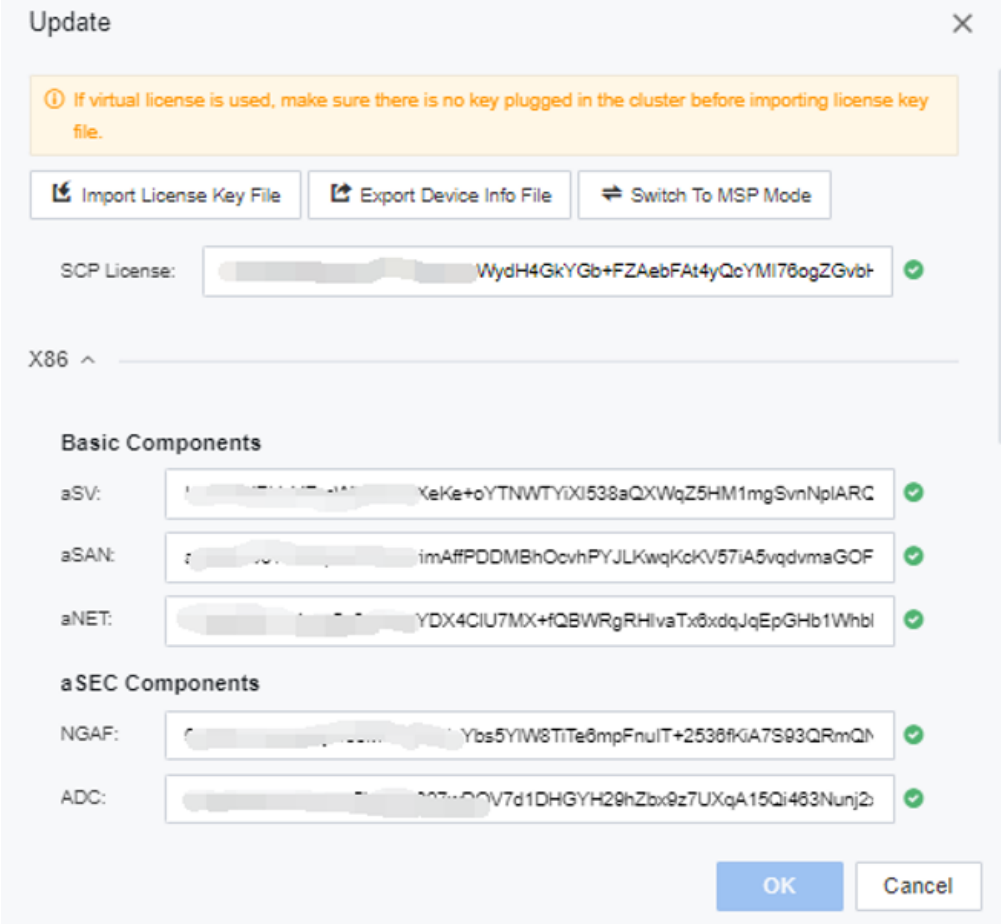
Prerequisites:

1. Sangfor HCI platform and SCP have been correctly deployed.
2. The license key has been correctly mapped to the SCP virtual machine, and the corresponding license key has been provided (.lic file).

Steps:

Step 1. Log in to SCP, click **System** > **Licensing** to enter SCP's licensing management page.

Step 2. Click **Update** and select the prepared License file (.lic file). After the import is successful, you can view the corresponding license key information.



2.5.2 vKEY License

Function Description:

SCP supports KEY-less licensing. In case of hardware KEY loss and failure, it will not affect cluster usage. By using vKEY, the user does not need to send back and re-apply for the USB KEY in the license change scenario, improving the work efficiency.

Precautions:

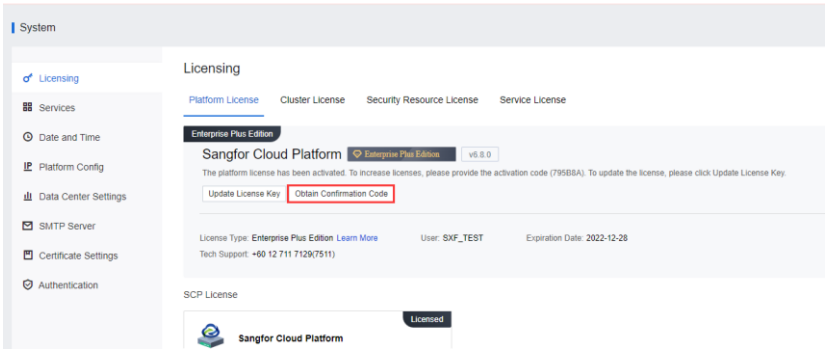
1. Only SCP6.8.0 and later versions support the vKEY licensing mode.
3. USB KEY and vKEY licensing cannot exist at the same time.
4. For the upgrade scenarios of SCP6.8.0 and earlier versions, the USB KEY mode is used by default, and the licensing mode can be switched after the upgrade. When replacing, you need to contact Sangfor technical support for the licensing file and send the USB KEY back to Sangfor.
5. After switching the licensing mode, the original USB KEY will be invalid.
6. vKEY licensing only supports offline licensing, and online licensing is currently not supported.
7. When SCP6.8.0 uses the vKEY licensing mode, the HCI cluster where the SCP runs should be HCI6.1.0 and later versions.
8. When SCP failover is configured, if the active/standby switchover occurs, you need to re-apply for licensing to import to the standby node according to the licensing application process.

Prerequisite:

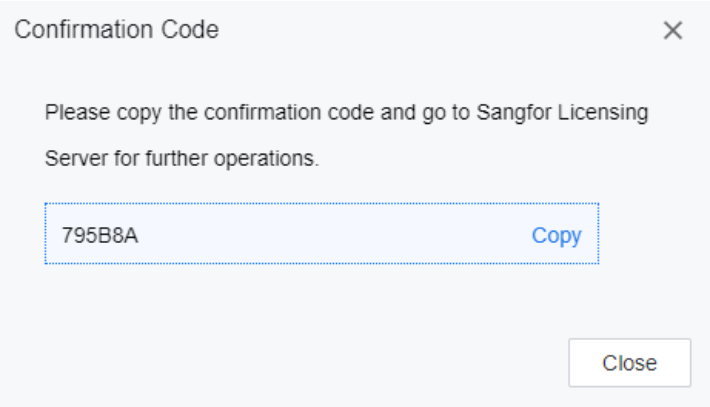
None.

Steps:

Step 1. Go to **System > Licensing > Platform License**, and click **Update License Key** to get the Confirmation Code.



Step 2. Copy the confirmation code.



Step 3. Go to the **Sangfor Licensing Server**, log in to the platform to import device information, and obtain the licensing file. You can click **Help Information** in the upper right corner to obtain detailed operation instructions for the licensing file.

Step 4. Import the obtained licensing file into the platform to complete the licensing activation.

2.6 Time Setting (Optional)

Function Description:

Set the time of the Sangfor SCP cloud computing platform. The platform supports custom time and the automatic acquisition of NTP time.

Precautions:

None.

Prerequisites:

Sangfor HCI platform and SCP have been correctly deployed. If you need to obtain NTP time, you need to ensure that the SCP and the NTP server network are reachable.

Steps:

Step 1. Log in to the SCP platform and select **System > Date and Time**.

Step 2. You can set the system time or **Sync with Local Time**. Then, click **Save**.

Step 3. When the SCP platform needs to synchronize time with the NTP

server, you can check the **Sync with NTP Server** checkbox, enter the NTP time server address, and click **Save**.

2.7 Platform Login Information

Instruct users to log in to the SCP platform in different roles.

Roles	Login Address	Default username and password
Super admin	https://SCP IP:4430	admin/admin
Tenant	https://SCP IP	Self-defined
Tenant User	https://SCP IP	Self-defined

2.8 Use aDeploy Tool To Detect:

After the platform is deployed, you need to check whether there are available patches for the current version that needs to be upgraded. According to the test results, please use the aDeploy tool to check and upgrade the corresponding patch package.

aDeploy tool can be found in Sangfor Community:

https://community.sangfor.com/plugin.php?id=service:download&action=tool

2.9 Patch Upgrade

Function Description:

Sangfor SCP platform supports online patch upgrades and can obtain the latest patch information regularly to ensure the stability and security of the equipment.

Precautions:

1. When the SCP manages the HCI cluster, you only need to enable the online SP service on the SCP, and the HCI does not need to be configured.
2. It is not recommended that the management network directly access the online SP service, which is not conducive to its security.

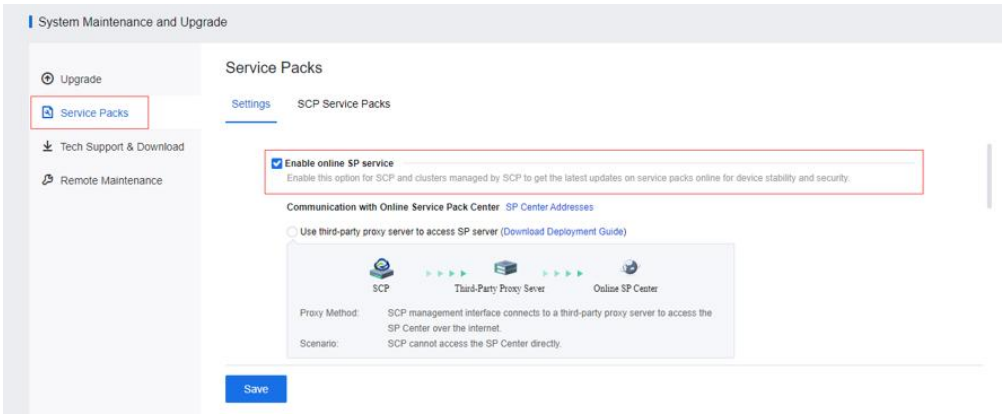
3. After the online SP service is configured, the connectivity must be tested to ensure that the platform can connect to the patch server.
4. Use the Sangfor network proxy virtual machine to access the Online SP Center mode. Do not modify the virtual machine name after importing the network proxy virtual machine (the default name is _SangforaOperation_VM_WorkStation_). Otherwise, the proxy service will become invalid.
5. SCP cannot be connected to the on-premises Sangfor SP server.

Prerequisites:

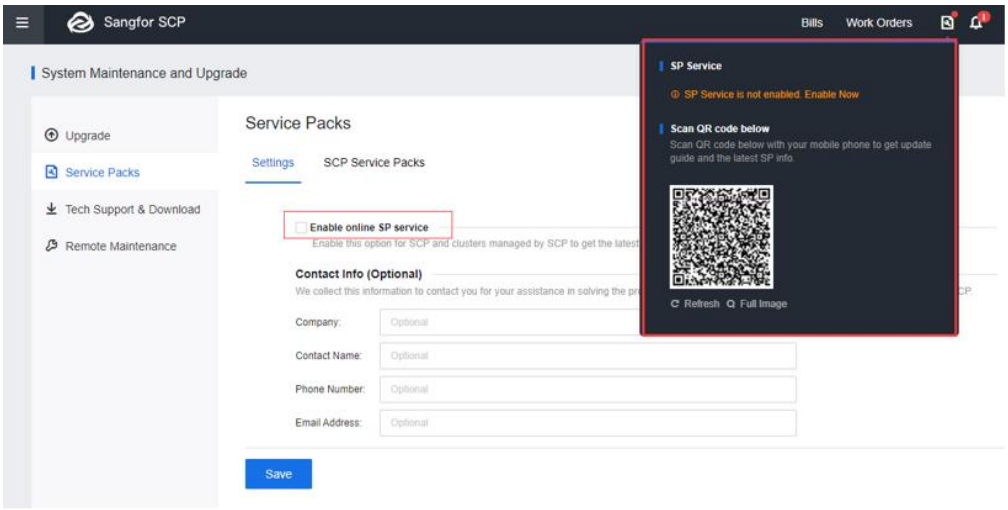
The customer network needs to allow the address **update1.sangfor.net** of Sangfor's patch server to ensure that the platform can access the patch server.

Steps:

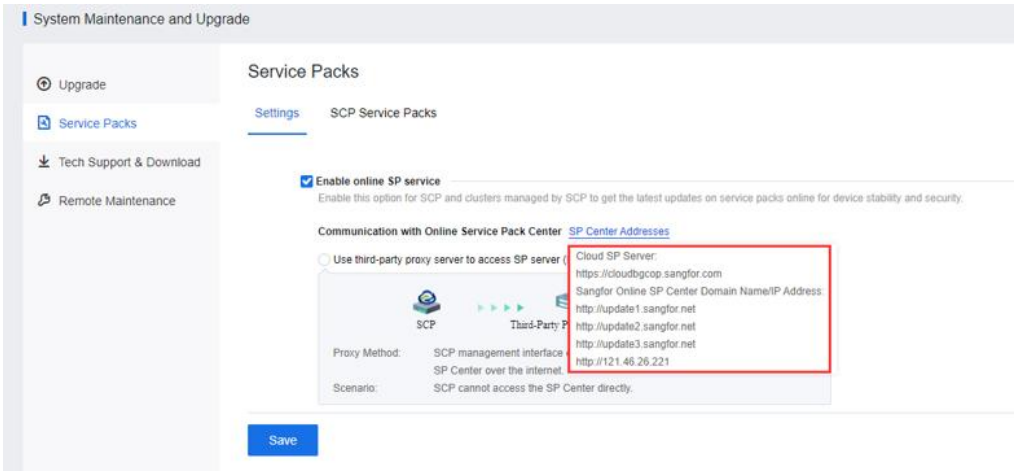
Step 1. Navigate to **Resources > Management > System Maintenance and Upgrade** > **Service Packs** > Settings, and check **the Enable online SP service** checkbox.



When the Online SP Service is not turned on or the patch platform is not connected, the Patch Alert icon will appear in the upper right corner of the platform, click to view the reminder, and you can scan the SCP or the QR code of each cluster to obtain the corresponding patch information, according to the provided download link, completes the patch download.



Step 2. Click **SP Central Addresses** to obtain the access address of the online patch platform.

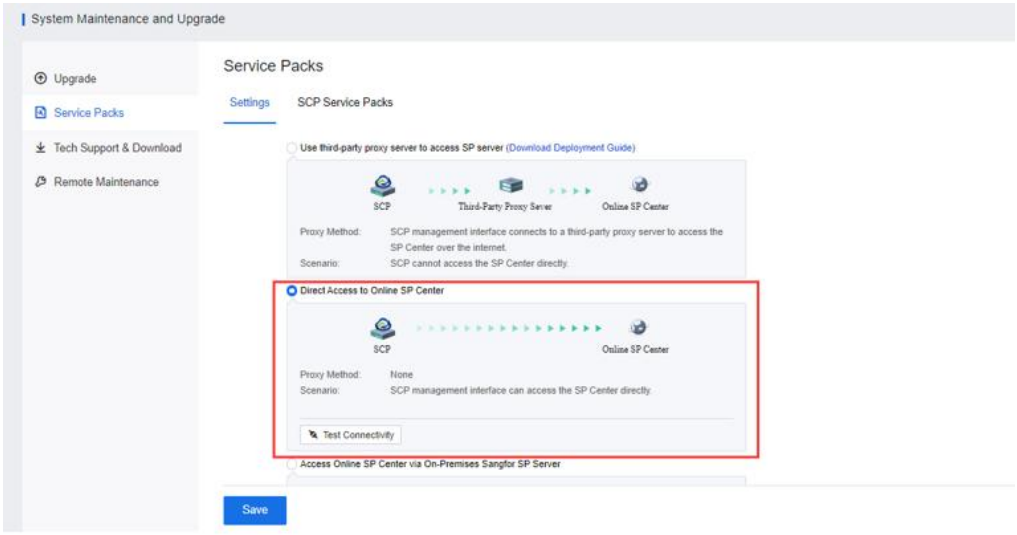


Users need to allow the address shown in the table below in the corresponding gateway device to ensure that the SCP or proxy can access it.

Server IP Address	Description	Requirement
https://cloudbgcop.sangfor.com	Cloud Server IP Address.	Must be allowed.
http://update1.sangfor.net	Online SP center IP Address.	Allow at least one of the IPs. It is recommended to allow multiple.
http://update2.sangfor.net		
http://update3.sangfor.net		
http://121.46.26.221		

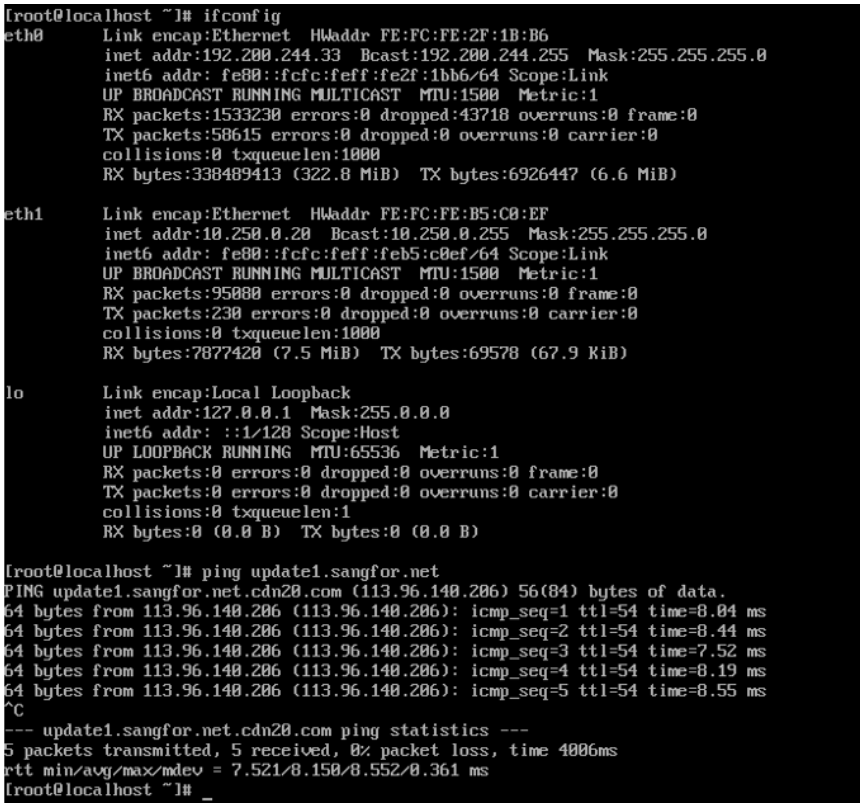
Step 3. Configure the communication method with the online SP center.

Scenario 1: Directly access to an online SP center.

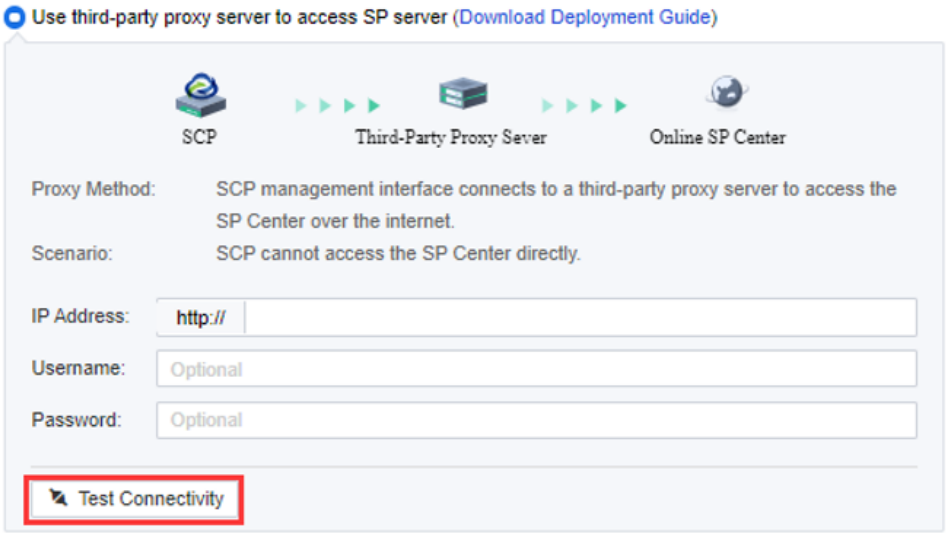


Scenario 2: Use a third-party proxy server to access the SP server.

Click **Download Deployment Guide**. Refer to the **Deployment Guide for Third-Party Proxy Server** document to install and configure the third-party agent program and confirm that the agent server can access the online patch server address in **Step 2.** Deploy two incoming interfaces as shown in the figure below, one can access the Internet to connect to the Sangfor patch server, and the other can access the HCI platform of the intranet.

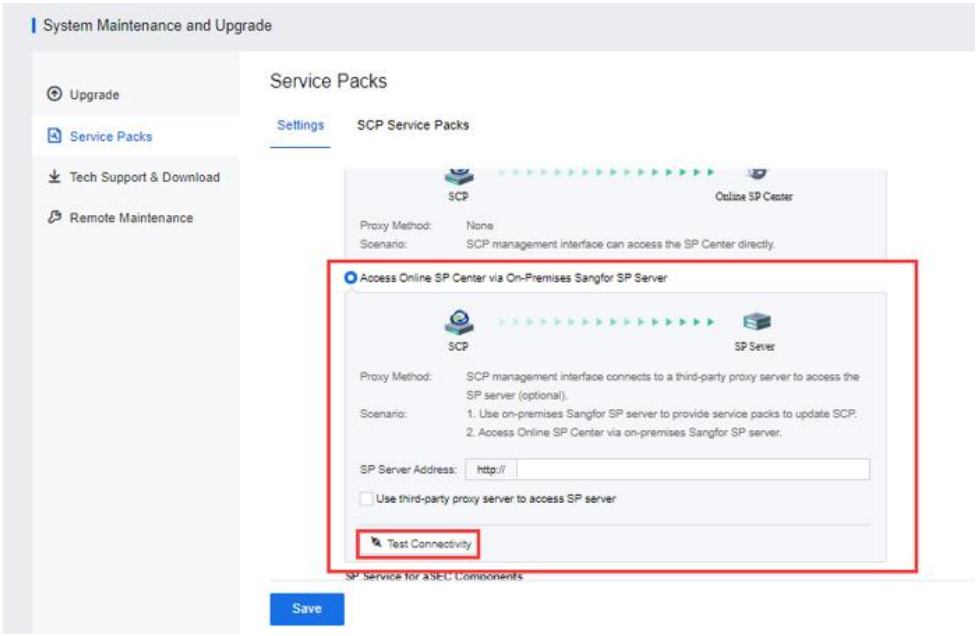


- Fill in the proxy address (IP + port, example: 10.250.0.20:3128) set above on the SCP platform. And the proxy authentication username and password are set during the deployment of the proxy server.
- The IP address is the IP of the internal incoming interface of the proxy server.
- The port is the publishing port of the proxy service, and the default is 3128.
- Click the **Test Connectivity** button to confirm that the network is connected.



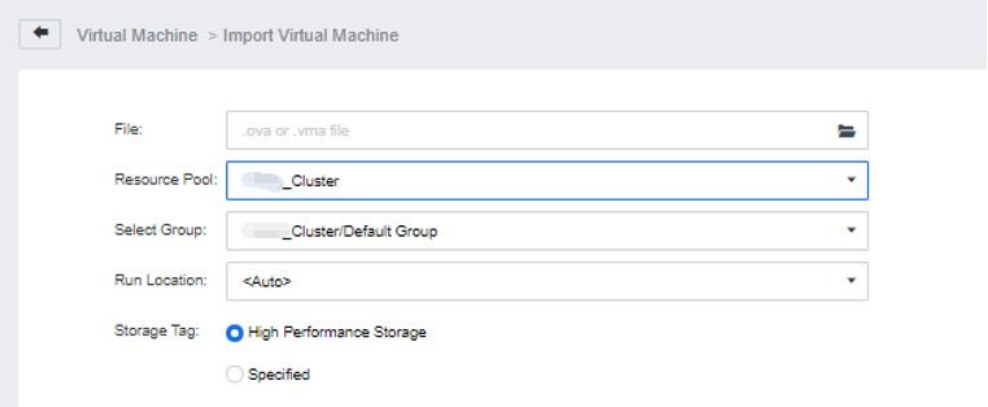
Scenario 3: The SCP platform cannot be connected to the Internet, and the SP server has been set up in the local data center.

- Select **Access Online SP Center via On-Premises Sangfor SP Server**.

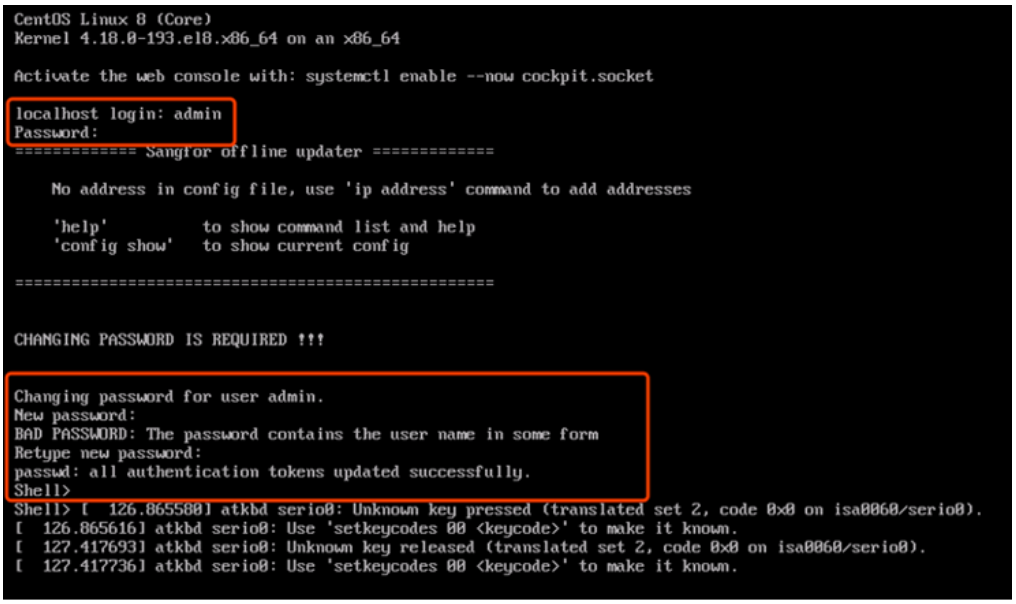


- Contact Sangfor Technical Support to obtain the vma template of the offline patch server.
- Import the virtual machine of the offline patch server under **Virtual Machine > New > Import Virtual Machine**.

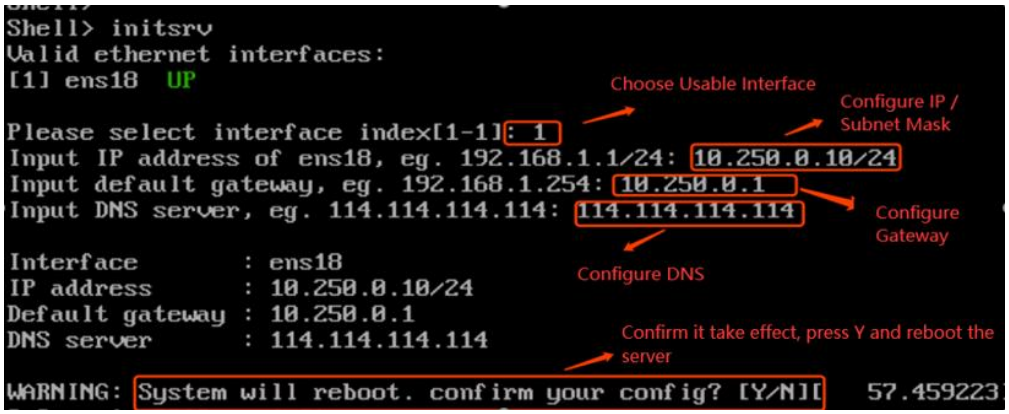
- After importing, click **More** >**Edit** on the specified virtual machine. Edit the network card and connect to the planned network.



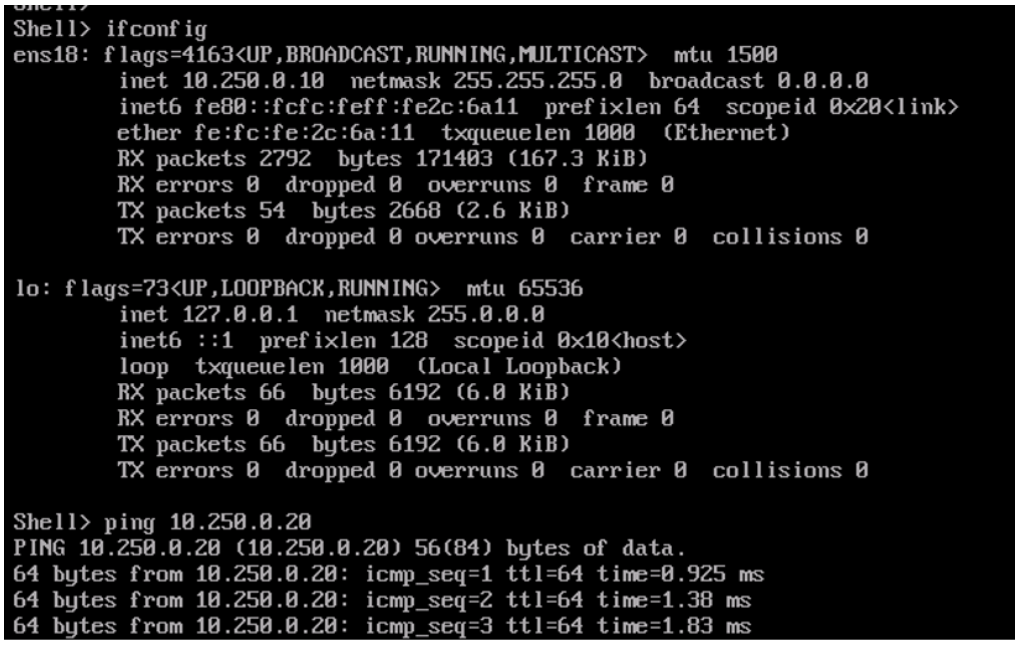
Open the VM console and enter the default username and password: **admin/Sangforupdater**. After successful login, the system will ask to change the default password. Please configure a new password.



- Use the **initsrv** command to modify the IP address, netmask, 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.



- Confirm the network card configuration and check the connectivity of the network.

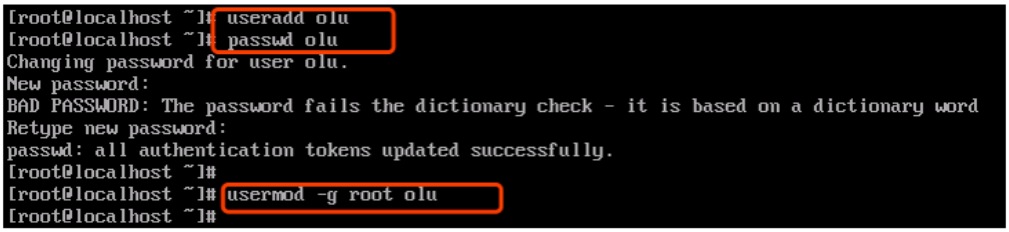


- Enter the command **moashell**. The QR code pop up. The QR code pop up. Scan it with Sangfor Pocket Assistant (MOA), get the password from the Pocket Assistant **Little Assistant**, and enter it into the command line. (Need Sangfor technical support processing).





- Create a user used by the olu server, set a password, and change the group of the olu user to root.



- Use the newly added olu account to log in to the patch server, upload the patch package of the SCP and NFV device to the **/var/wwwroot** directory through the sftp tool, and view it in the SCP patch list after decompression.

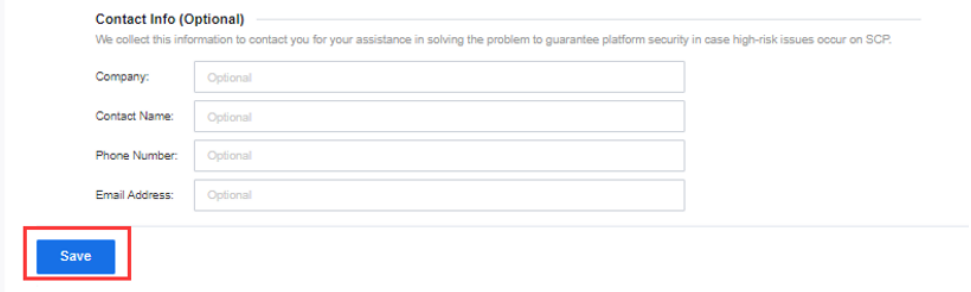


- After configuring the Olu server, test the connectivity of the SP patch server on the SCP interface, fill in the address of the SP patch server, and click **Test Connectivity**.



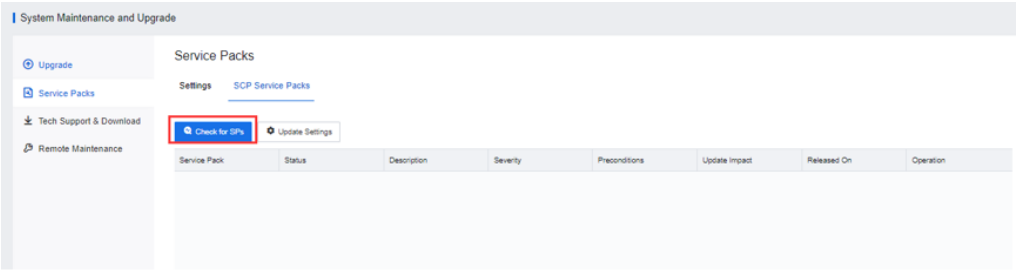
Step 4. NFV patch upgrade settings need to log in to a single cluster and go to **System Maintenance and Upgrade** > **Upgrade** to edit. For details, please refer to **Sangfor Hyper-Converged HCI Version 6.7.0 User Manual.**

Step 5. Set emergency contacts (Optional) and click **Save** after confirming the correct information.

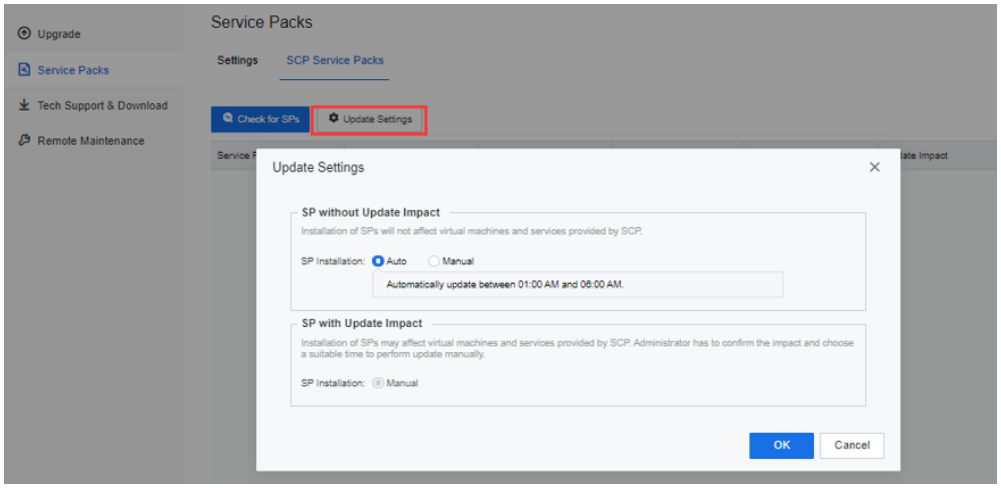


Step 6. **Navigate to the System Maintenance and Upgrade** > **Service Packs > SCP Service Packs**. You can make patch upgrade-related settings.

- Click **Check for SPs,** and the platform will immediately initiate a patch request.



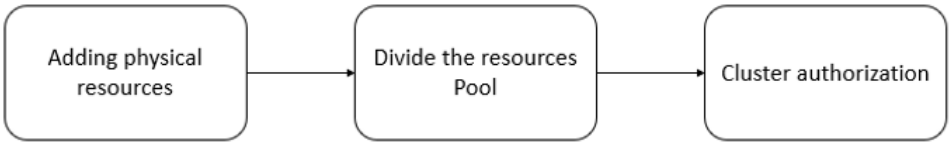
- Click **Update Settings**. **Auto** has been selected by default under **SP installation**. After the patch is obtained online, it will be automatically downloaded and upgraded from 1:00 to 6:00 in the morning. It is recommended to keep the default selection of **automatic upgrade**, and also support **manual upgrade**. If you choose to download manually, click **OK** for the un-upgraded patch in the patch list to start downloading and upgrading.



- SP patches only support **manual upgrade**, which requires the user to display the pre-conditions and upgrade impact according to the patch list. When the impact is acceptable, the user clicks to execute **Upgrade**.

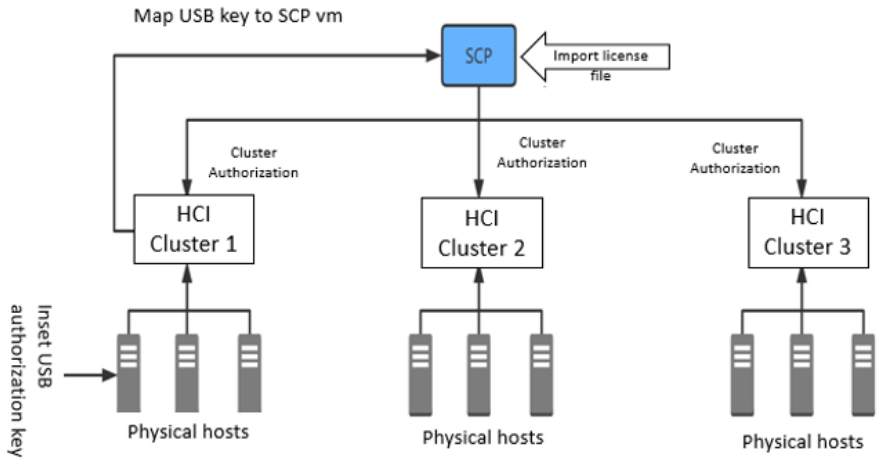
3 Resource Initialization

3.1 Resource Initialization Process

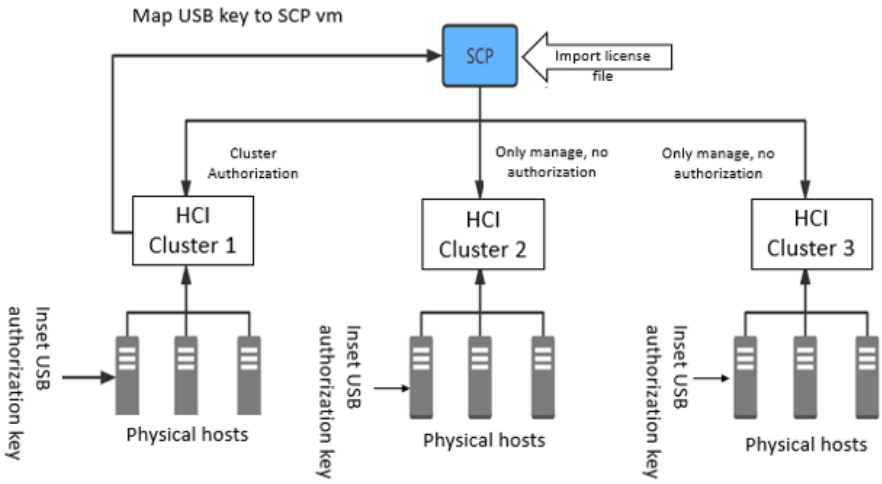


1. **Adding physical resources:** Add the prepared physical resources to the SCP platform in clusters and tag the storage.
2. **Divide the resource pool:** Associate the added cluster to the resource pool.
3. **Cluster license:** The current SCP cloud computing platform has two licensing modes for hyper-converged resource pools: Centralized and standalone.

- **Centralized mode:** Through the SCP, the clusters associated with the resource pool are licensed, and the clusters occupy the centralized mode. (This licensing mode requires a license key and license file. For example, the SCP platform is deployed on hyper-converged cluster 1, and hyper-converged cluster 2 and cluster 3 need to be managed. Both clusters 2 and 3 are licensed through cloud management authorization. Only one license key and matching authorization file are required).



- **Standalone mode:** After the HCI cluster uses its license key authorization, it is managed by the cloud platform, and the cluster does not occupy the centralized mode license. At this time, the SCP platform only manages independently licensed clusters and does not issue authorizations. (This licensing mode requires 1+n keys, and n is the number of independently licensed clusters. For example, if the SCP platform is deployed on hyper-converged cluster 1, hyper-converged cluster 2 and cluster 3 need to be managed, and clusters 2 and 3 are standalone mode Authorization. At this time, 1+2 license keys are required, and each key has a matching license file).



NOTE

1. Since only one license key can be inserted into an HCI cluster, the cluster where the SCP platform is deployed must be authorized for centralized mode.
2. When SCP is deployed in active/standby mode, to avoid the licensing of the standby SCP is lost after 30 days after switching to the active SCP. You are advised to use centralized mode for both the active and standby clusters when deploying the active/standby SCP.

3.2 Add Physical Resources

Function Description:

Sangfor SCP supports the management of multiple HCI clusters and VMware clusters and realizes unified management of multiple resource pools through the SCP platform.

This section will Instruct the administrator to add the prepared physical resources to the SCP platform in a cluster and tag the storage resources.

Prerequisite

1. Sangfor SCP and HCI resource pools or VMware resource pool networks are reachable.
2. According to the management and authorization plan, prepare sufficient license keys and licensing documents.

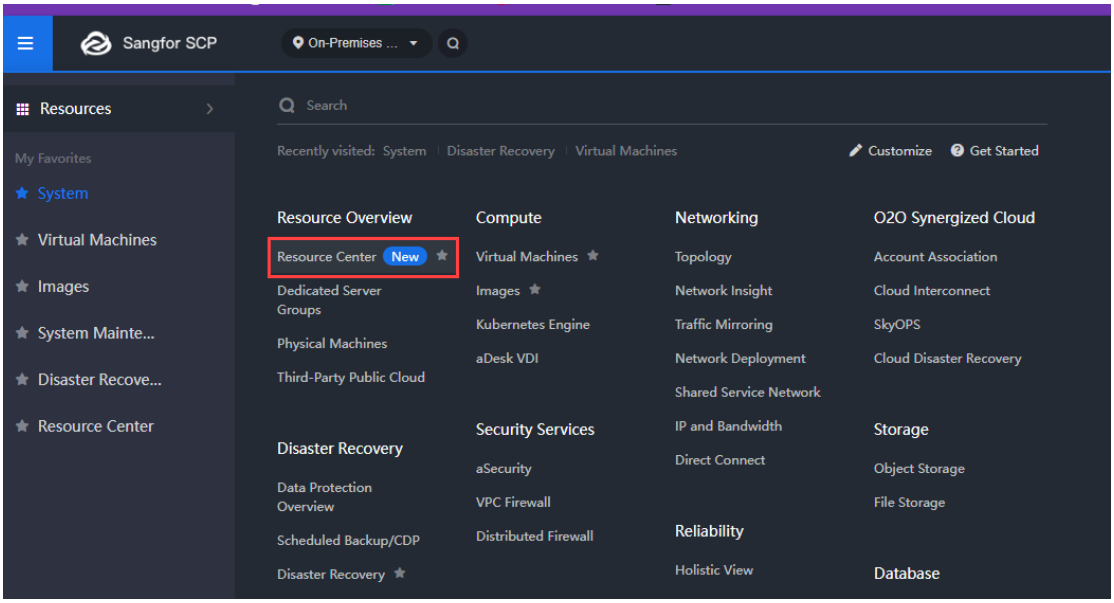
Precautions:

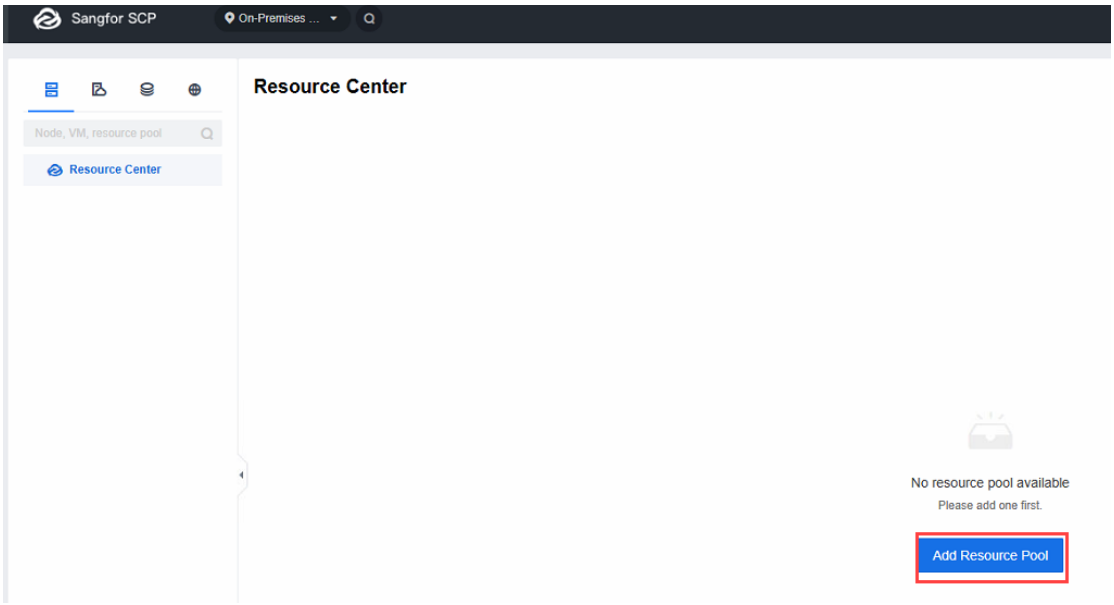
1. The SCP cloud computing platform supports managing different versions of hyper-converged resource pools. For details of the hyper-converged versions that support management, please log in to **Sangfor Community** for inquiries.
2. The SCP cloud computing platform supports ARM's hyper-converged clusters and resource management.

3. Disaster recovery between X86 and ARM resource pools is not supported.
4. Only one security center (ARM or X86 architecture) is supported on SCP, and NFV access security centers with different architectures are not supported.
5. The SCP cloud computing platform supports managing different versions of VMware clusters. The supported VMware versions are as follows: VMware 5.0 、VMware 5.1、VMware 5.5、VMware 6.0、VMware 6.5. Versions after aCloud 5.8.7 R1 support VMware 6.7.
6. Some functions of the SCP rely on the underlying HCI resource pool. When the underlying hyper-converged resource pool does not support a function, the corresponding function button on the SCP platform will be grayed out.
7. The NFV version supported by the SCP cloud platform depends on whether the underlying hyper-converged resource pool supports it. When the hyper-converged resource pool does not support a certain NFV version, it cannot be used in SCP. (Please refer to the specific support list: HCI and NFV version correspondence table)
8. When the versions of multiple managed resource pools are inconsistent, virtual machine migration between resource pools of different versions is not supported.
9. When the versions of multiple resource pools managed are inconsistent, the Sangfor aDR (Cross-Site Disaster Recovery solution between resource pools of different versions is temporarily not supported.

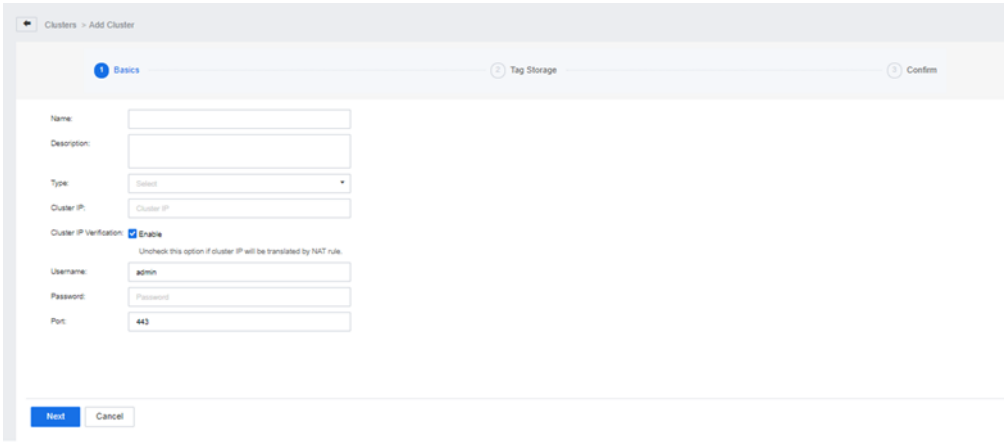
Steps:

Step 1. Log in to SCP as an administrator and go to **Resources** > **Resources Overview** > **Resource Center** > **Resource Pools** > **New**.





Step 2. Enter the cluster Name and Description, and after selecting the cluster Type, enter the Cluster IP and admin Password. If the port has not been changed, keep the default setting (if the cluster IP has been mapped by NAT, please uncheck Cluster IP verification), select the appropriate licensing mode, and click the Next button.



Step 3. According to the actual situation of the cluster, different tags can be set for different storage volumes. The default includes high performance, performance, and capacity.

- High-performance storage: Strong read and write performance, used to create high-performance virtual machines, generally gives this tag to the SSD storage category.
- Performance storage: Strong read and write performance, but relatively aging, generally old storage.
- Capacity storage: Average read and write performance, but large capacity, high security, and high-cost performance.

Step 4. After confirming that the information is correct, click the Confirm button.

3.3 Dividing Resource Pools

Product Description:

After managing the cluster, you need to associate the cluster with the resource pool. The resource pool is a collection of computing, storage, network, and other resources and is the basic unit of SCP cloud computing platform management. The managed cluster can only be licensed and used after it is associated with the resource pool.

Prerequisite

SCP has successfully added clusters.

Precautions:

1. In the current version, a resource pool can only be associated with one cluster.
2. Resource pool attributes are divided into two types: Dedicated and Shared. Shared resource pools can be allocated to multiple tenants. Dedicated resource pools can only be provided to one tenant. VMware resource pools can only choose shared attributes.

Steps:

Step 1. Log in to SCP as an administrator and go to **Resources** > **Resources Overview** > **Resource Center** > **Resource Pools** > **New**.

Step 2. Fill in the name and description of the resource pool, select the resource type and attributes, and click the **Next** button.

Step 3. Select the cluster that needs to be associated. You can click the **Add Cluster** button if the target cluster is not found. Please refer to chapter **3.2 Add Physical Resources,** for the detailed operation process. After the configuration is complete, click the **Next** button.

Step 4. Confirm that the information is correct and click the **Confirm** button.

Step 5. Upon completion, you can view the created resource pool.

3.3.1 Cluster License

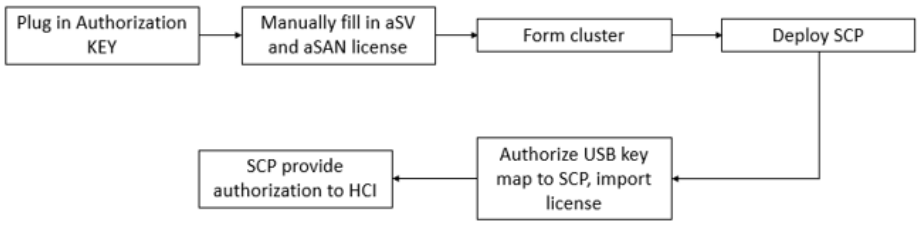
3.3.2 Single Cluster License

Function Description:

After the SCP platform manages the HCI cluster and associates the cluster with the resource pool, the HCI cluster needs to be licensed to ensure that the HCI cluster service is available.

Precautions:

The workflow of creating SCP in the HCI cluster and activating the HCI license by SCP is shown in the figure below.



1. When activating HCI with SCP licensing, you must manually fill in the aSV and aSAN license keys. If you import the entire file, the activation will fail and cause the cluster to be abnormal, and subsequent manual filling will not activate.
2. HCI5.8.5 and later versions require manual input of aSV and aSAN licenses.

Prerequisite

1. The SCP has been activated by importing the license key, and the licensed resources are sufficient to license the HCI cluster of the associated resource pool.
2. The cluster has been associated with the resource pool. If it is not yet associated, the cluster cannot be licensed.

Steps:

Step 1. Log in to the SCP platform and select **System** > **Licensing** > **Cluster License** to view the not licensed clusters.

Step 2. Click **Licensing** on the right side of the cluster with abnormal status and click the **Confirm** button.

Step 3. After the licensing is successful, cluster licensing can be viewed, edited, and recycled on the licensing interface.

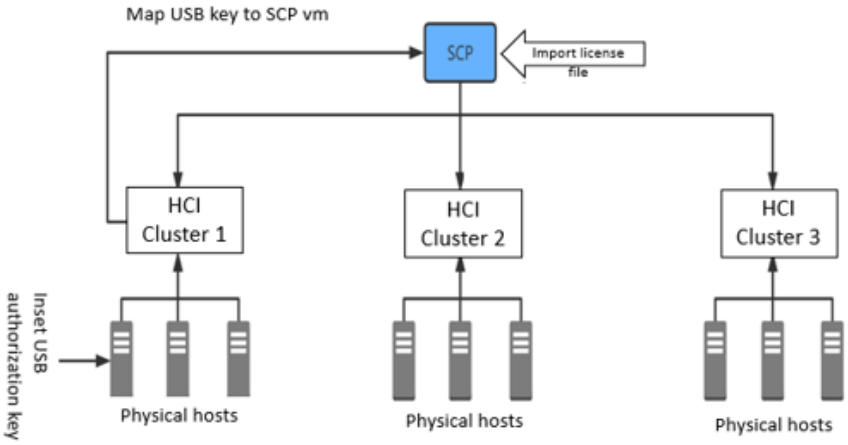
Please note when performing licensed revoke:

- Revoking the licensing may affect the related functions of the cluster. Please operate with caution. If all the licensing is recovered, the licensing of the NFV devices in the cluster will also be recovered.
- Except for CDP, aHM, aSC, aSI, aGPU, the licensing of other components does not support separate revoking for the time being.

3.3.3 Multi-Cluster License

Function Description:

Instruct users to license nodes that have not yet formed a cluster, as shown in the figure below: SCP has managed cluster 1 and licensed cluster 1. At this time, cluster 2 has not yet formed a cluster.



Precautions:

None.

Prerequisite

SCP has been activated by importing the license key, and licensed resources are sufficient to license all clusters.

Steps:

Step 1. Set the cluster IP on node 1 of cluster 2 to ensure that this cluster IP can communicate with SCP to form a single-node cluster.

Step 2. The platform administrator logs in to the SCP platform, manages the single-node cluster established in **Step 1,** and selects **Centralized mode** after associating the resource pool and licensing the single-node cluster.

Step 3. Log in to a single-node cluster. The cluster has been licensed, and you can add nodes to form a multi-node cluster.

Step 4. Cluster 3 can be licensed as well.

3.4 Deploy Communication Domain

If you need to configure connected domains, please refer to the **Communication Domains** chapter.

3.5 Security Resource License

Function Description:

After the HCI cluster is managed by the SCP and associated with the resource pool, the NFV equipment can only be deployed on the SCP. At the same time, the NFV equipment needs to be licensed on the SCP before the NFV equipment can be used.

Precautions:

1. Two new fields, **Resource Pool** and **Tenant,** have been added to the **Security Resource License** page, which distinguishes the ownership of NFV resources. When the NFV resource belongs to the admin, it displays "-", and when it belongs to the tenant, it displays the tenant's name.



2. For Tenants' NFV equipment, the supported operation is **Edit**. **Power On** or **Shut Down** are not supported.

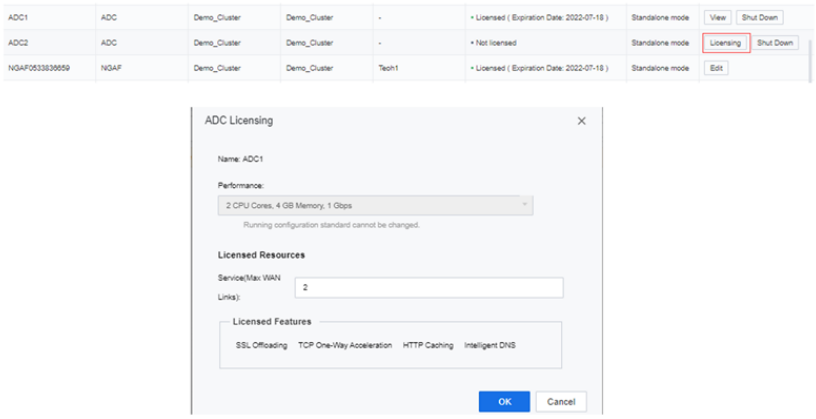
Prerequisite

Sangfor SCP has imported licensing activation, and authorization resources are sufficient to license NFV equipment.

Steps:

Step 1. Log in to the SCP platform and select **System** > **Licensing** > **Security Resource License**.

Step 2. Select the NFV device that needs to be licensed, click **Licensing** on the right, and click the **OK** button after assigning the corresponding licensing.



Step 3. After the licensing is successful, you can view and edit the licensing of the NFV device on the licensing interface.

3.6 Configure VPC Gateway

Function Description:

The VPC is to assign a fixed VPC subnet to each resource pool. After the setting is successful, a VPC is generated when the tenant is created, and the interface will be connected by default. Please specify a fixed VPC outgoing interface for each resource pool if you need to create a tenant.

Prerequisite

1. The SCP has managed the HCI cluster and created a resource pool.
2. The SCP platform has licensed the cluster.

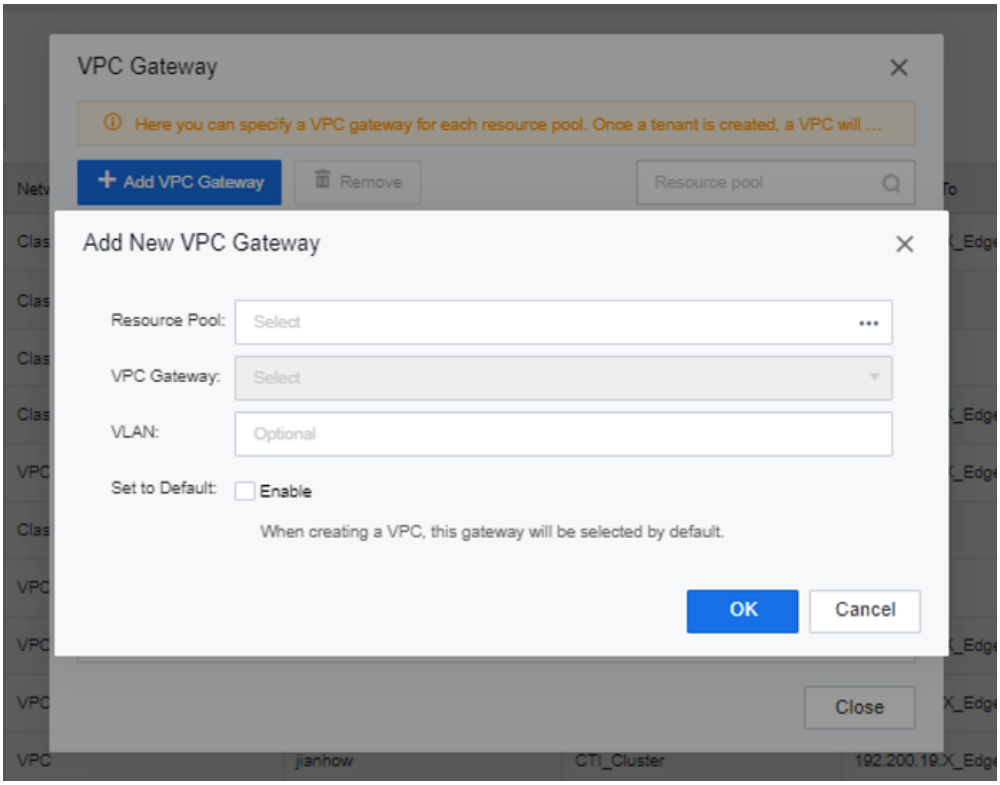
Precautions:

After setting the VPC, please delete all tenants in the resource pool first if you need to modify it.

Steps:

Step 1. Select **Networking** > **Network Deployment** and click **VPC Gateway**.

Step 2. Click **Add VPC Gateway** to select the VPC outgoing interface corresponding to each resource pool, enter the password of the admin administrator for confirmation, and complete the creation of the VPC Gateway.



3.7 Configure Shared Services Gateway

Function Description:

The shared service is to assign a fixed public service network gateway to each resource pool. After the setting is successful, the interface is connected by default when creating a public service, which is used for resource pool tenants to access resources in the public service area.

Prerequisite

1. The SCP cloud computing platform has managed the HCI cluster and created a resource pool.
2. The SCP cloud computing platform has been licensed for the cluster.

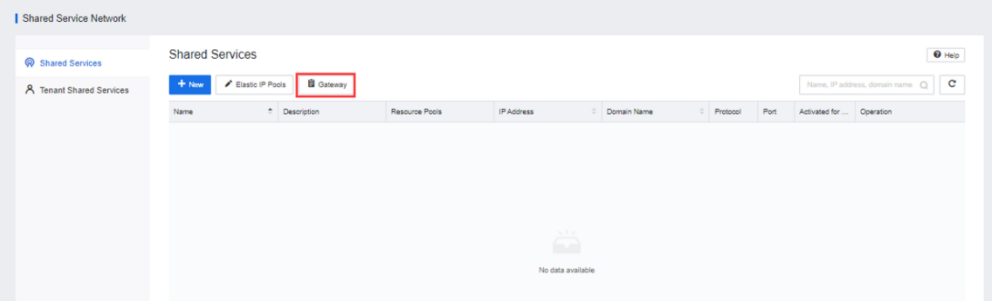
Precautions:

After the public service gateway is set, if you need to modify it, please delete all public services under the exit first.

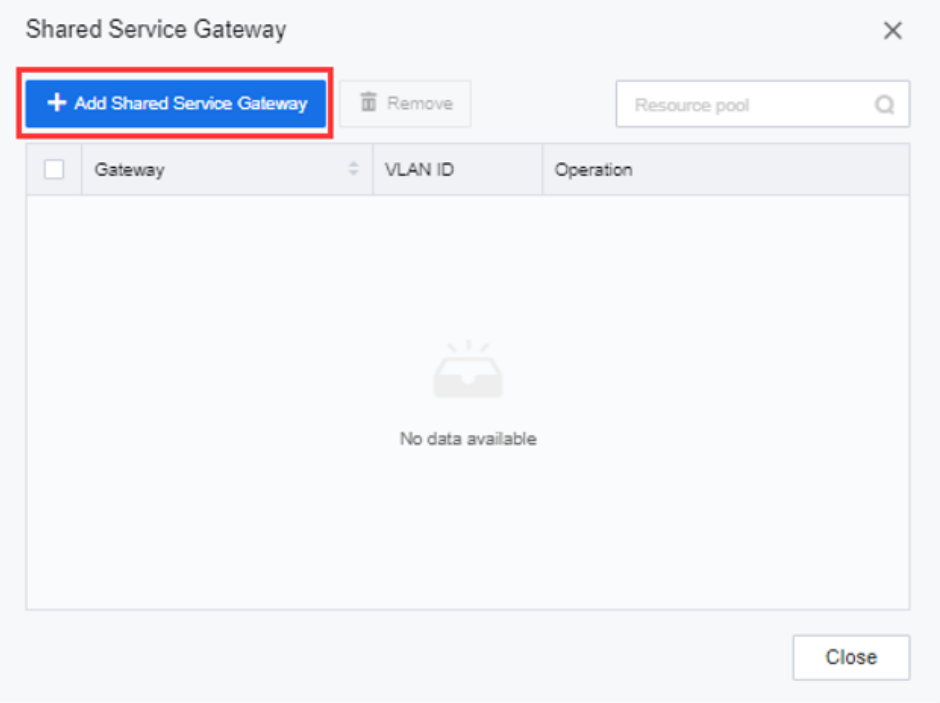
Steps:

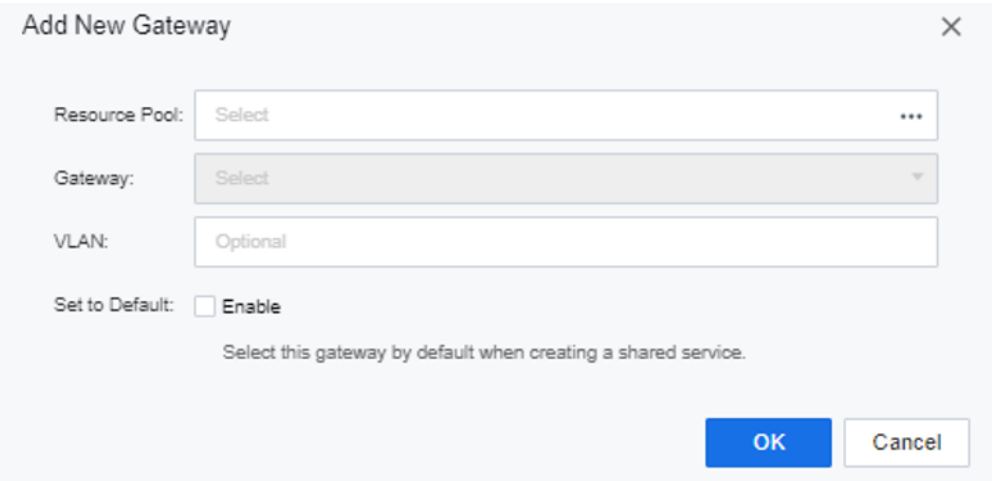
Step 1. Select **Networking > Shared Service Network > Shared Services**,

and click Gateway.

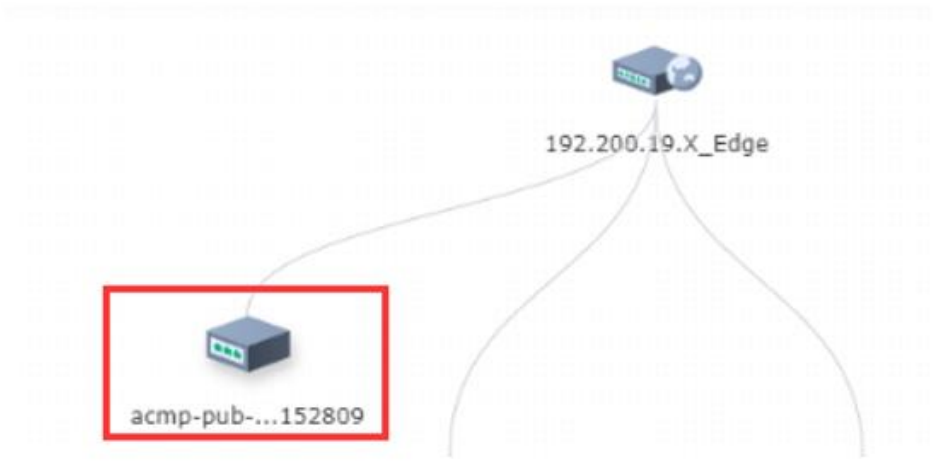


Step 2. Click **Add Gateway** to plan shared service exits for each resource pool.





Step 3. After the deployment is complete, you can see the newly added public service outlet **acmp-pub-trunk** under the corresponding outlet in the network topology.



3.8 Configure Direct Connect Gateway

Function Description:

The VPC of tenants can communicate with the external environment of the VPC through the enterprise's private line at the second and third layers. If you need to use the corporate's private line function, you need to specify a direct connect gateway for each resource pool.

Prerequisite

1. The SCP has managed the HCI cluster and created a resource pool.
2. The SCP platform has licensed the cluster.

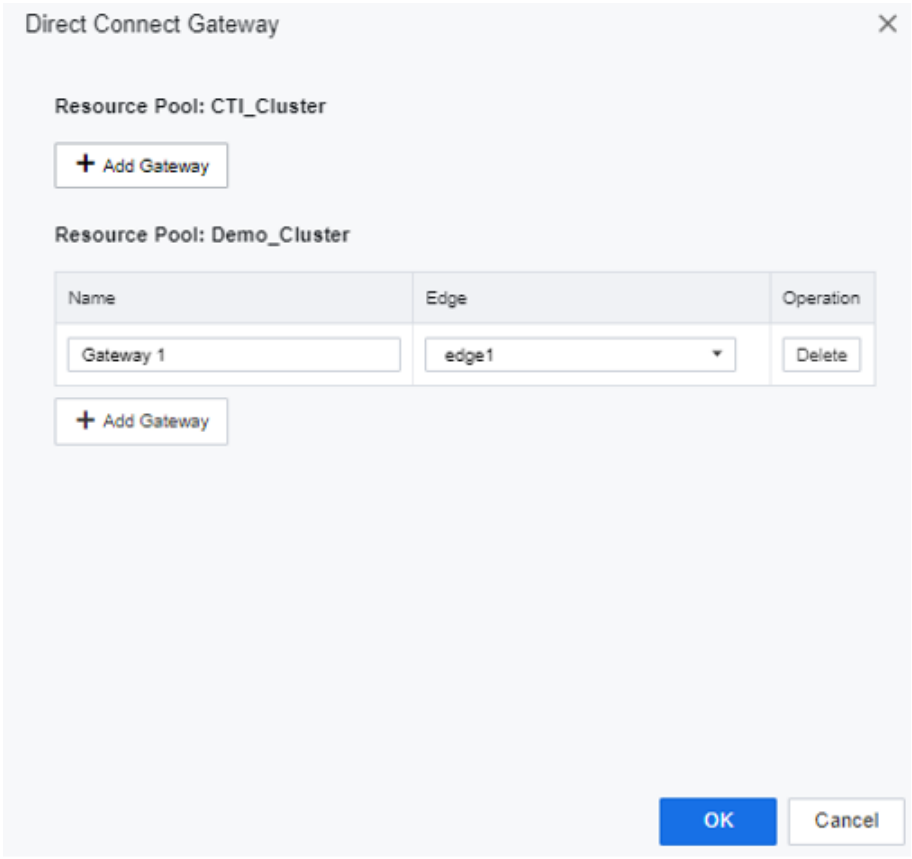
Precautions:

After the direct connect gateway is set, please delete all the dedicated direct lines under the direct line gateway if you need to modify it.

Steps:

Step 1. Select **Network** > **Direct Connect** and click **Direct Connect Gateway**.

Step 2. Configure the dedicated line outlet name and associated physical gateway of each resource pool, and each resource pool can create multiple dedicated line gateways.



3.9 DMP Environment Deployment (Optional)

Sangfor Database Management Platform (DMP) is a database service product that provides Relational Database Service (RDS) capabilities for private clouds and graphical management.

Make sure that DMP is deployed after the deployment of HCI and SCP so that the IP address configured for DMP does not conflict with those of other hosts.

For detailed instructions, see Sangfor DMP Implementation Guide.

Prerequisites

1. HCI and SCP of the correct versions have been properly deployed.
2. IP addresses prepared for DMP are on the same network segment as (or are connected to) the SCP management interface.

3. The DMP image package, database image package, and database load balancing image package are prepared.

Procedure

1. Log in to the SCP console by using the admin account.
2. Go to **Resources** > **Compute** > **Images**. Select **Network Device Images** and upload the database load balancing image. Select **Advanced Service Images** and upload the database platform image and database image.
3. Go to **Networking** > **Shared Service Network** and click **Gateway** to specify a shared service gateway.
4. Go to **Networking** > **IP and Bandwidth** and click **New**. In the **Create Elastic IP Pool** pop-up window, specify the information and select **Shared Network Service** for **Line Type**.
5. Go to **Networking** > **Network Deployment** and select **VPC Gateway** to configure a VPC gateway as required.
6. Go to **Resources** > **Database** > **MySQL** and click **Activate Now** to activate the DMP service. Enter the information as well as the management IP address and internal communication IP address.
7. Log in to the DMP console and apply for a license.
8. Go to **Users and Access Management** > **Users** > **Tenants** in the SCP console, click **New**, and configure a VPC.
9. Go to **Edit Resource Quota** > **Tenant Quota** in the SCP console and allocate quotas to the tenant. If no quota is specified in the resource pool, go to **Edit Resource Quota** > **Quota Overview** and specify quotas.

NOTE

DMP can only be deployed on SCP as an uploaded image. It cannot be deployed independently.

For more information about DMP functions, see Sangfor Database Management Platform Manual V2.1.0

4 Configuration Steps

The list of super administrator functions of the Sangfor SCP is shown as follows.

Role Name	Function permissions	Description
Platform Administrator (admin)	Resource pool management	Manage clusters and associated resource pools
	Virtual machine management	Virtual machine life cycle management, virtual machine group management, virtual machine migration and cloning, image management
	Network management	Plan VPC Gateway, manage elastic IP pool, edit network topology, manage subnet, NFV equipment management.
	Business reliability management	Backup & CDP, aDR(Cross-Site Disaster Recovery), high-availability (HA), dynamic resource scheduling (DRS), and platform resource reservation.
	Platform reliability management	Resource overload status, network configuration status, storage volume status, data reconstruction status, SCP active/standby management, hardware health detection
	User Management	Tenant management, tenant sub-account management
	Quota management	Overview of the basic resource quotas and NFV resource quotas.
	Work Order Management	Work order approval, custom work order workflow template.
	Billing management	View consumption overview, view tenant bill details, and set billing unit price.

	Monitoring and management	Set monitoring overview, deploy aMC monitoring center, view platform alarm logs, and set alarm rules.
	System Management	License authorization management, system configuration (date and time, platform IP, mailbox), system maintenance (operation audit, upgrade), and business maintenance (recycle bin).

Table 4: Platform administrator (admin) function list

The list of SCP platform tenant functions is as follows.

Role Name	Function permissions	Description
Tenants	Virtual machine management	Virtual machine life cycle management, virtual machine group management.
	Network management	VPC, edit network topology, use elastic IP, NFV device management.
	Business reliability	Virtual machine backup.
	Monitoring and management	Set monitoring overview, and view log alarms.
	Tenant sub-account management	Add, modify, and edit tenant sub-accounts.
	Quota management	View basic resource quotas and NFV equipment quotas.
	Work Order Management	Approve work orders, and apply for resource quota work orders.
	Billing management	View tenant consumption overview.
	System Management	Manage tenant recycle bins and view operation logs.

Table 5: Tenant function list

The list of functions of SCP platform tenant user accounts is as follows.

Role Name	Function permissions	Description
Tenants user	Virtual machine management	Apply for virtual machines, virtual machine management
	Billing management	View ticket process and results.
	Monitoring management	View monitoring log.
	System Management	Personal settings: view operation logs.

Table 6: Tenant user function list

4.1 Overview

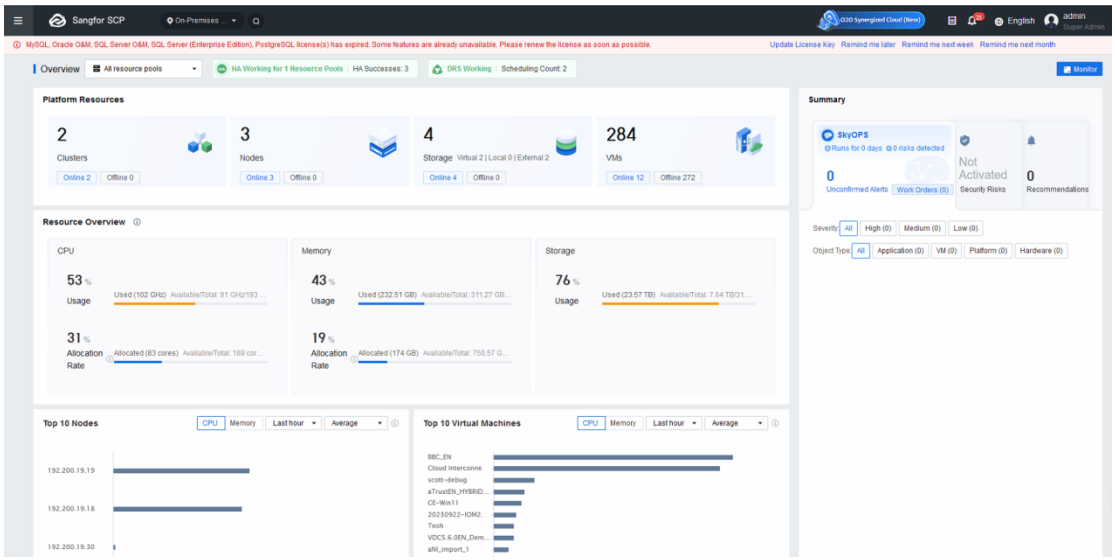
4.1.1 Resource Overview

Function Description:

Supports viewing resource usage of a single resource pool or all resource pools, such as CPU and memory usage, total disk capacity, total number of hosts, VMs, and clusters, as well as their running status.

Supports viewing O&M and monitoring information, such as unread alerts, security risks, and recommendations.

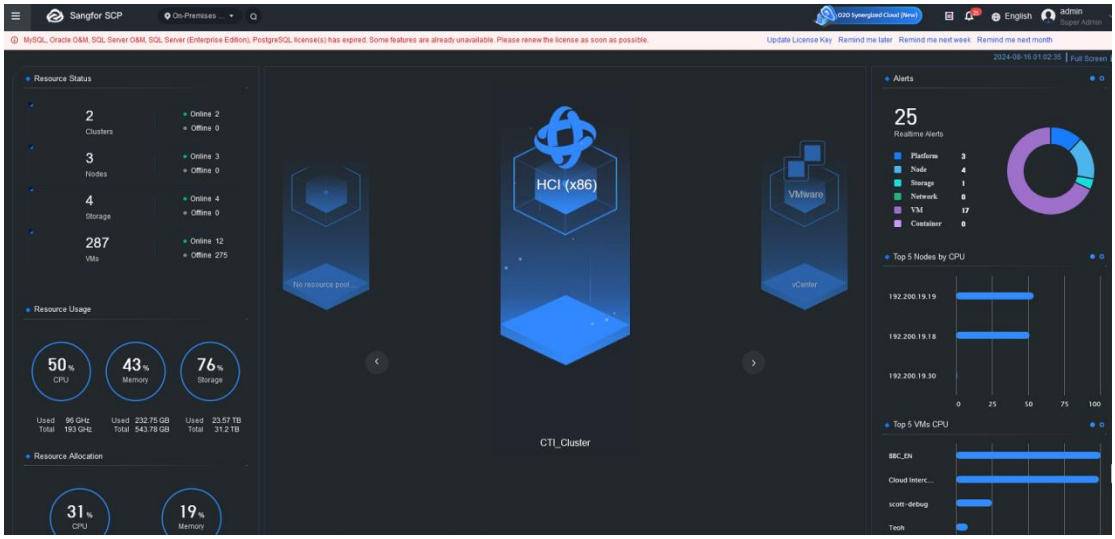
Supports viewing real-time alerts and quickly filtering them by severity and object.



4.1.2 Big Screen

Function Description:

Supports viewing the HA and DRS status of managed resource pools as well as resource metrics for hosts and VMs in the pools.

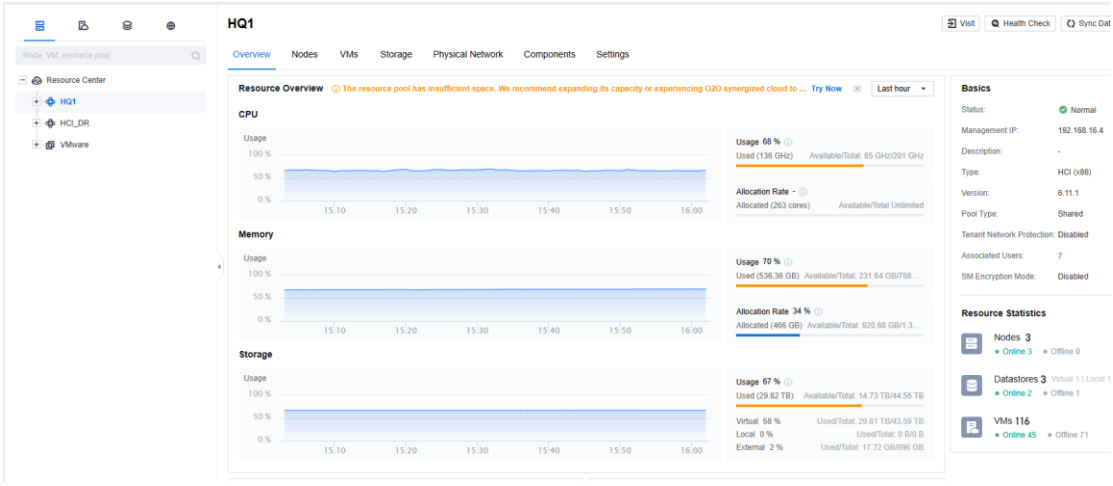


4.2 Resource Overview

4.2.1 Resource Center

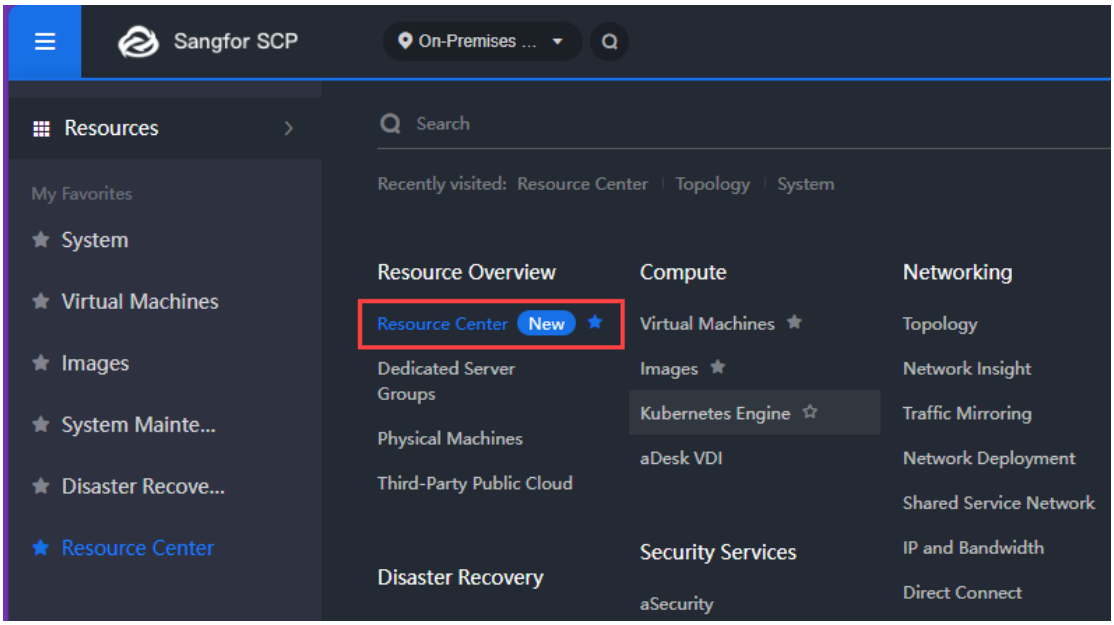
Function Description:

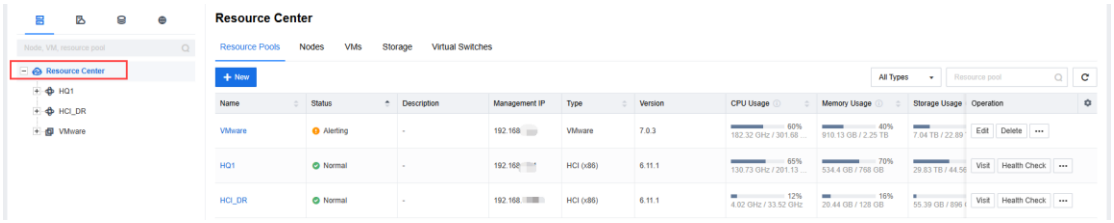
In SCP 6.11.1 and higher versions, resources including resource pools, nodes, VMs, storage, and virtual switches are managed in the **Resource Center**, which can be viewed by node, VM, storage, and network.



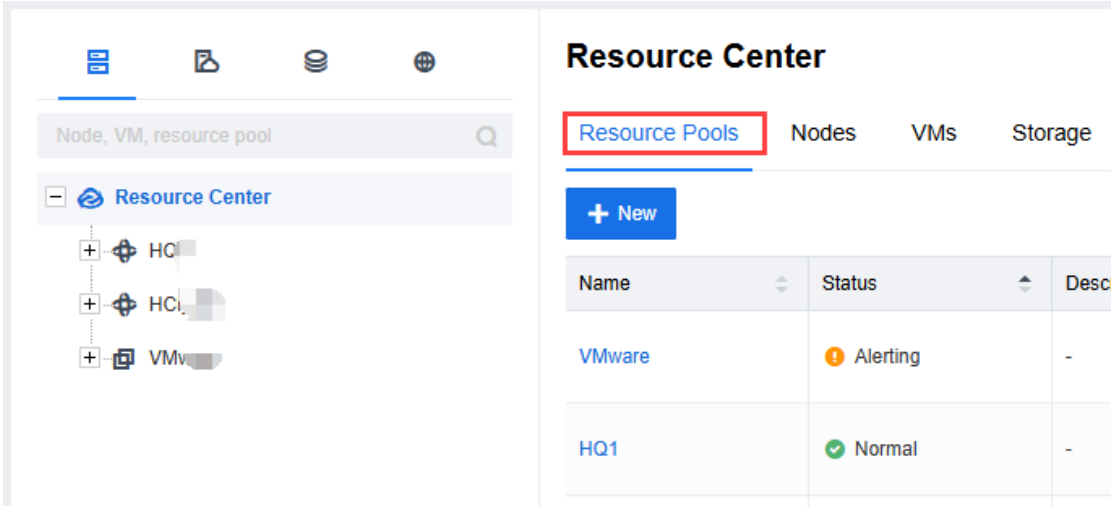
Steps:

Step 1. Log in to SCP and go to **Resources** > **Resource Overview** > **Resource Center**.

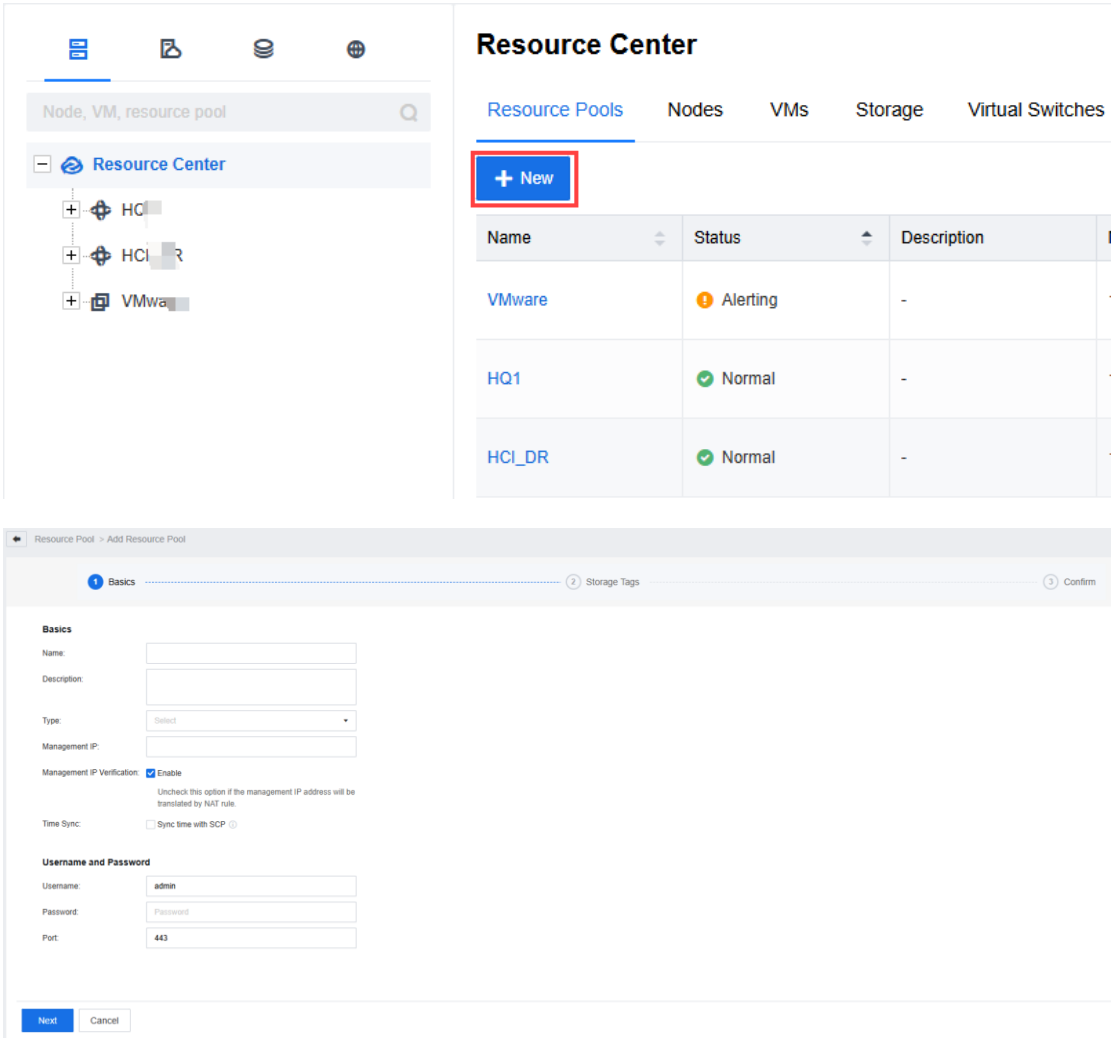




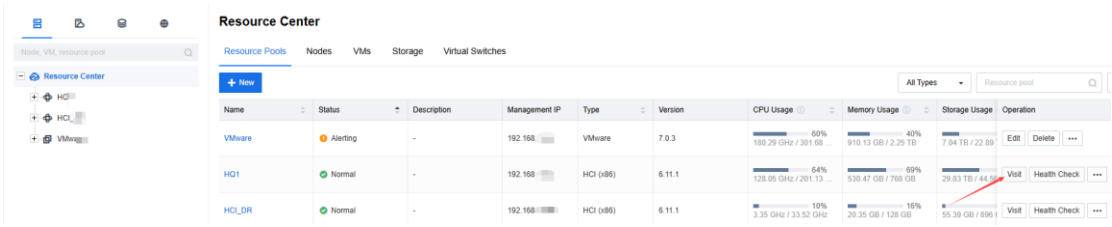
Step 2. Go to the **Resource Pools** page.



1. Click **New**, complete the basic information, and tag the storage to create a resource pool.

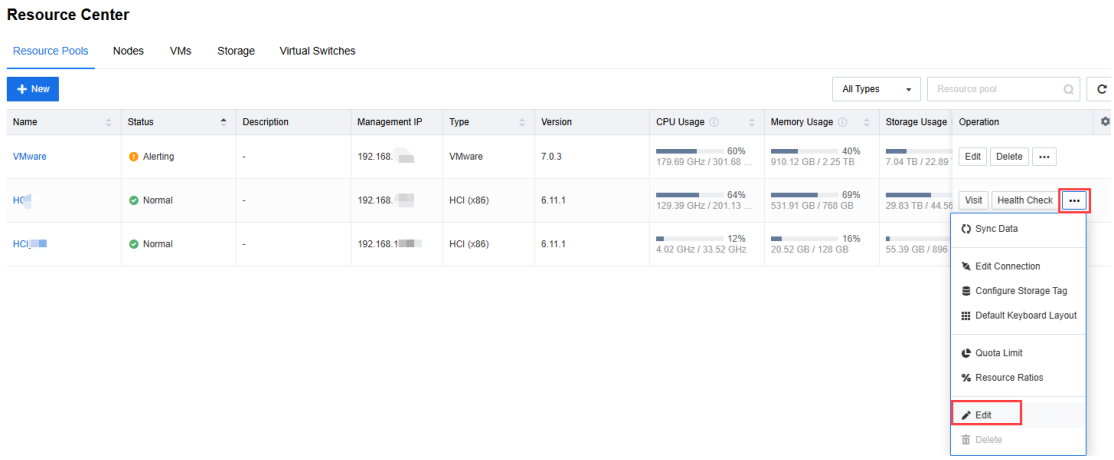


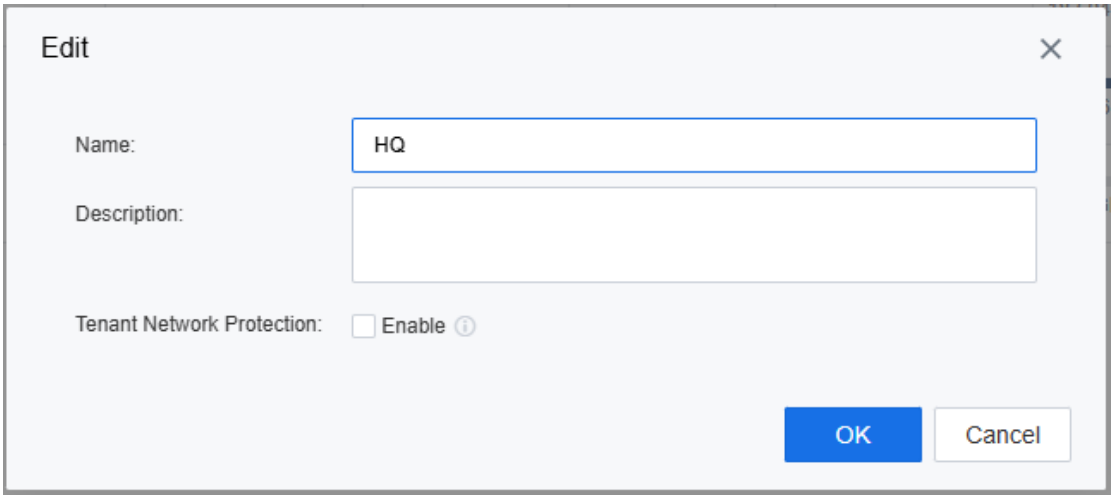
2. Click **Visit** of the created resource pool (HCI) to log in to it.





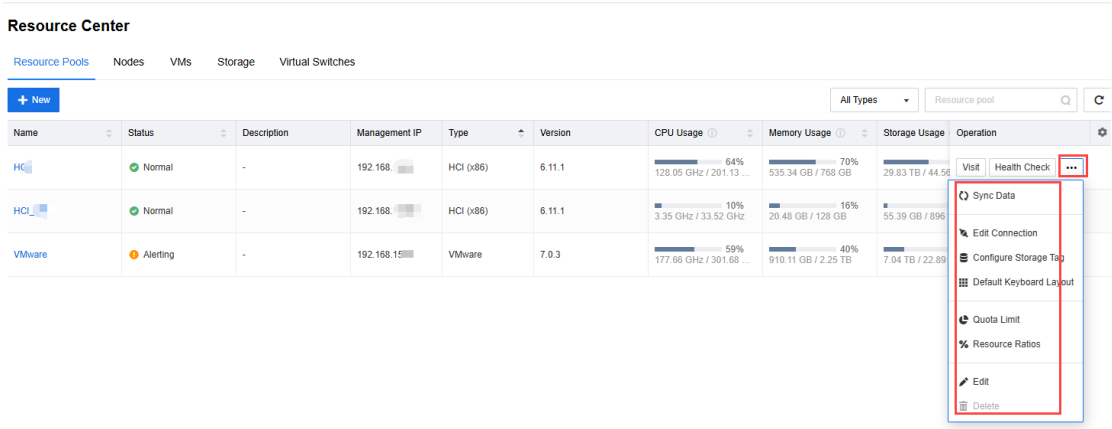
3. Click its **Edit** to modify the **Name** and **Description**, and enable or disable **Tenant Network Protection**.





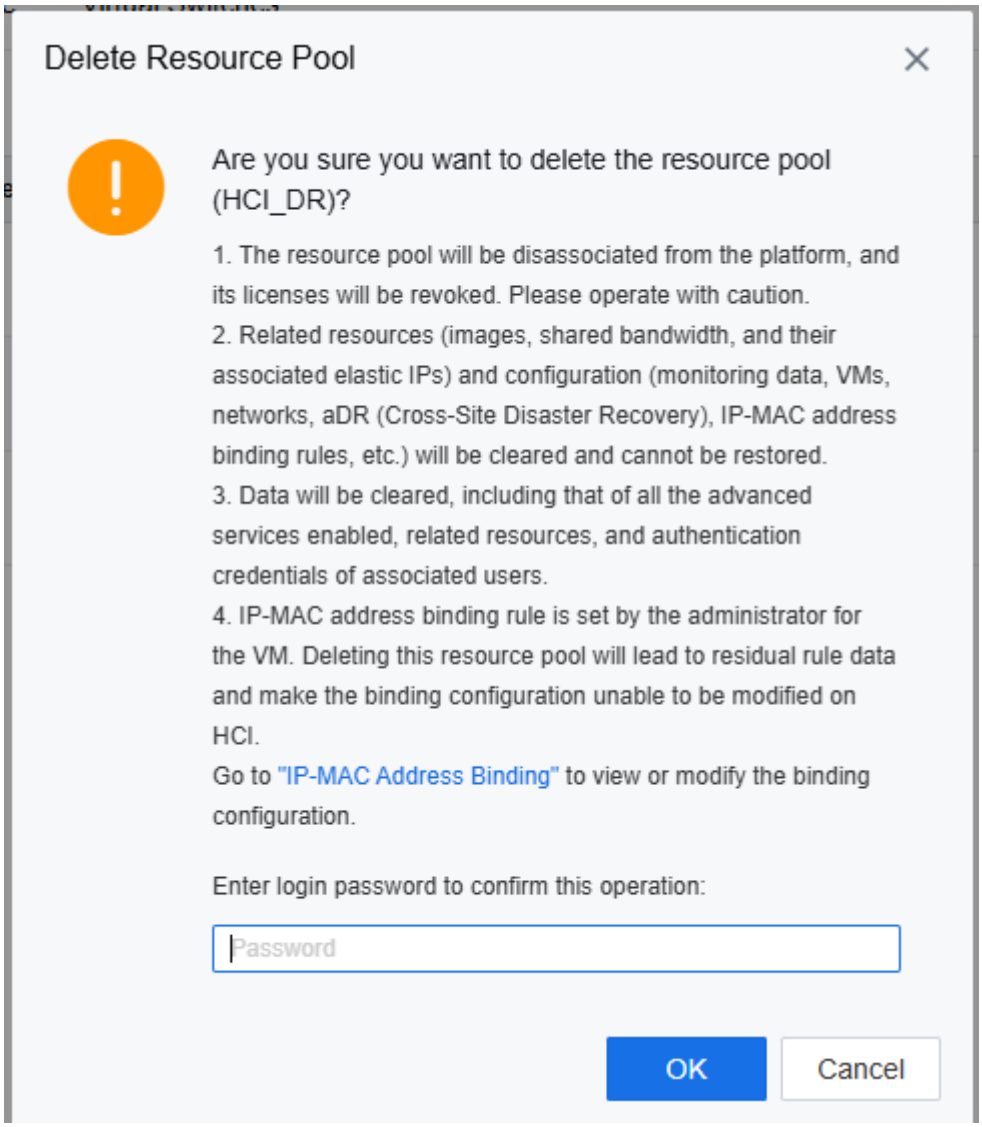
4. Click its **More** to configure the connection, storage tag, default keyboard

layout, quota limit, and resource ratios.

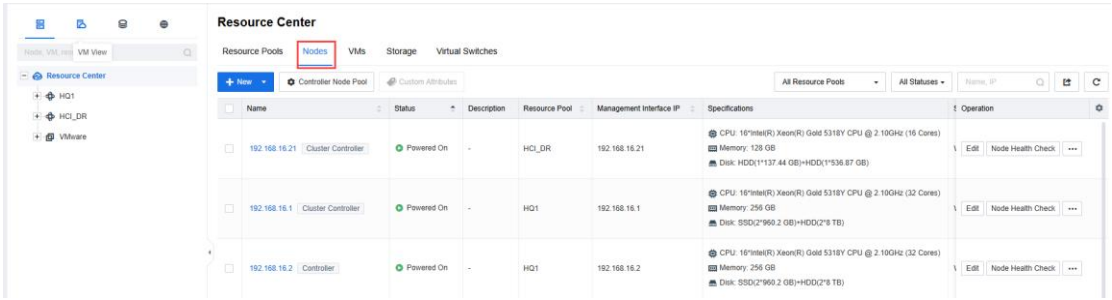


5. Click its **More** then **Delete**, and enter the administrator password to delete it (high risk).

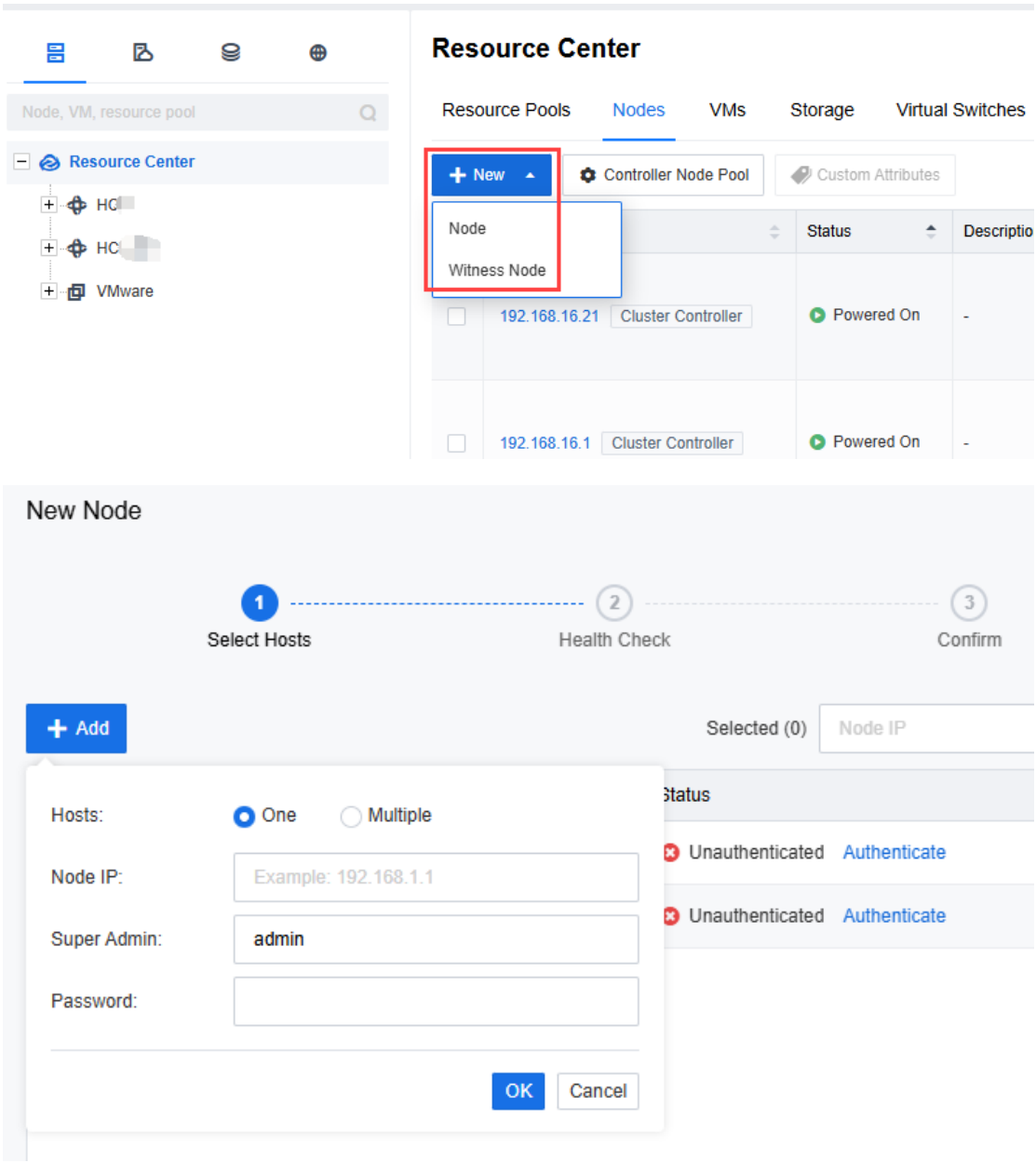




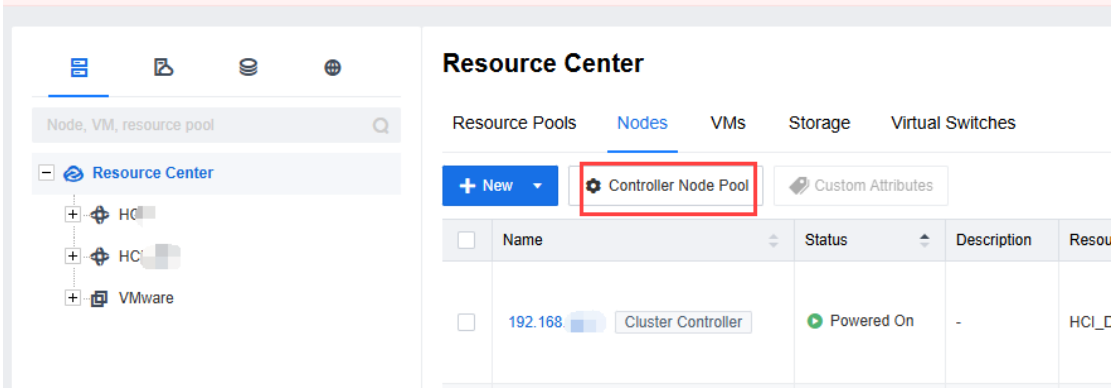
Step 3. Go to the **Nodes** page.

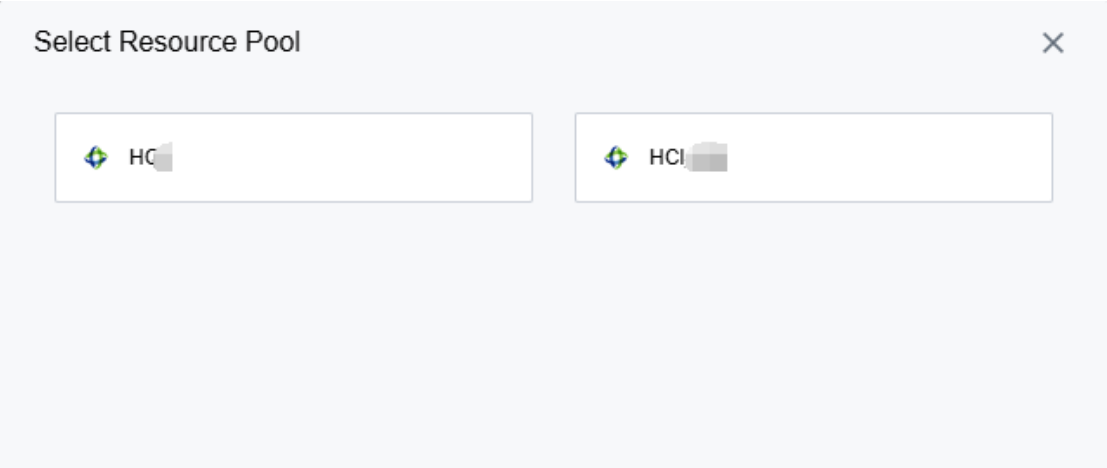


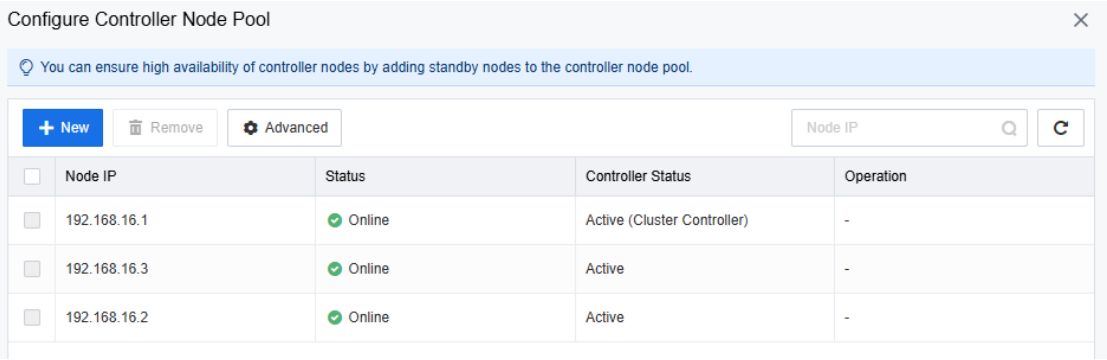
1. Click **New**, select **Node** or **Witness Node** and the resource pool to which nodes belong, and check the environment to add them.



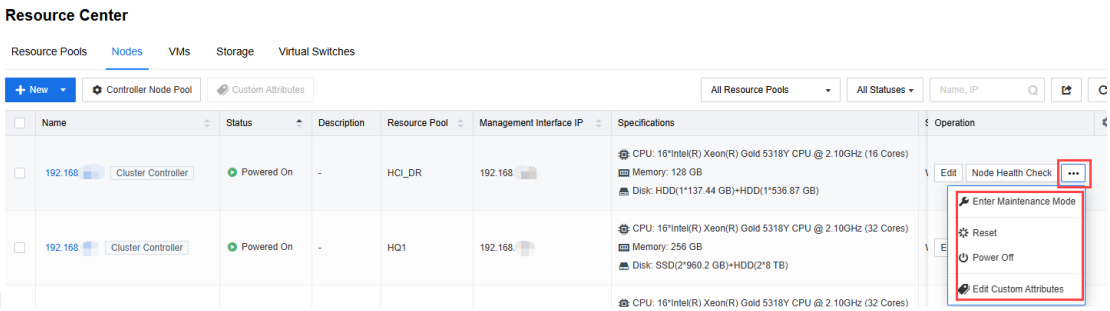
2. Click **Controller Node Pool**, select the corresponding resource pool, and add or remove controller nodes.



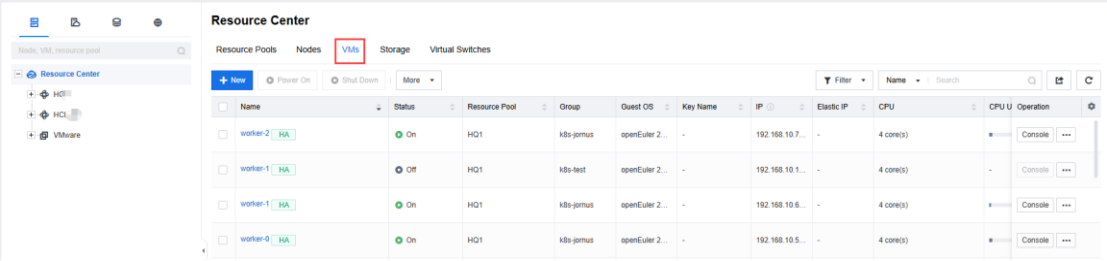




3. Click **Edit** of an added node to modify the **Name** and **Description**, and click its **More** to set it as cluster controller, enable Maintenance Mode, edit custom attributes, and replace, reset, or power off it.

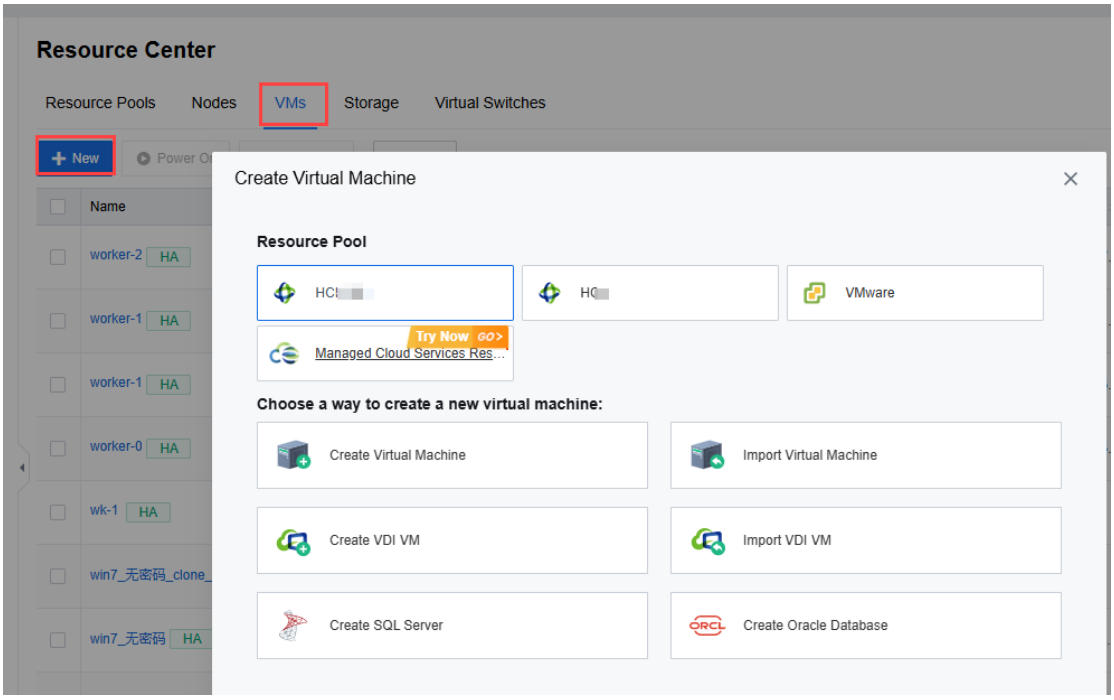


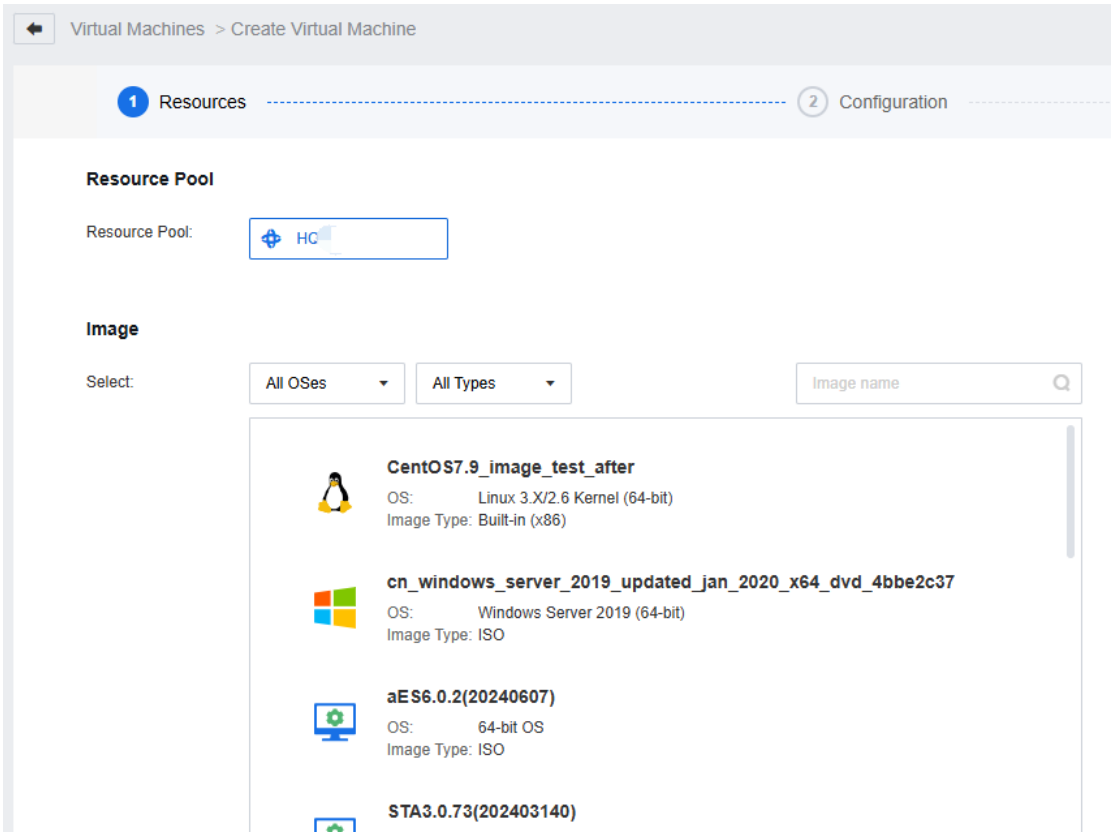
Step 4. Go to the **VMs** page.

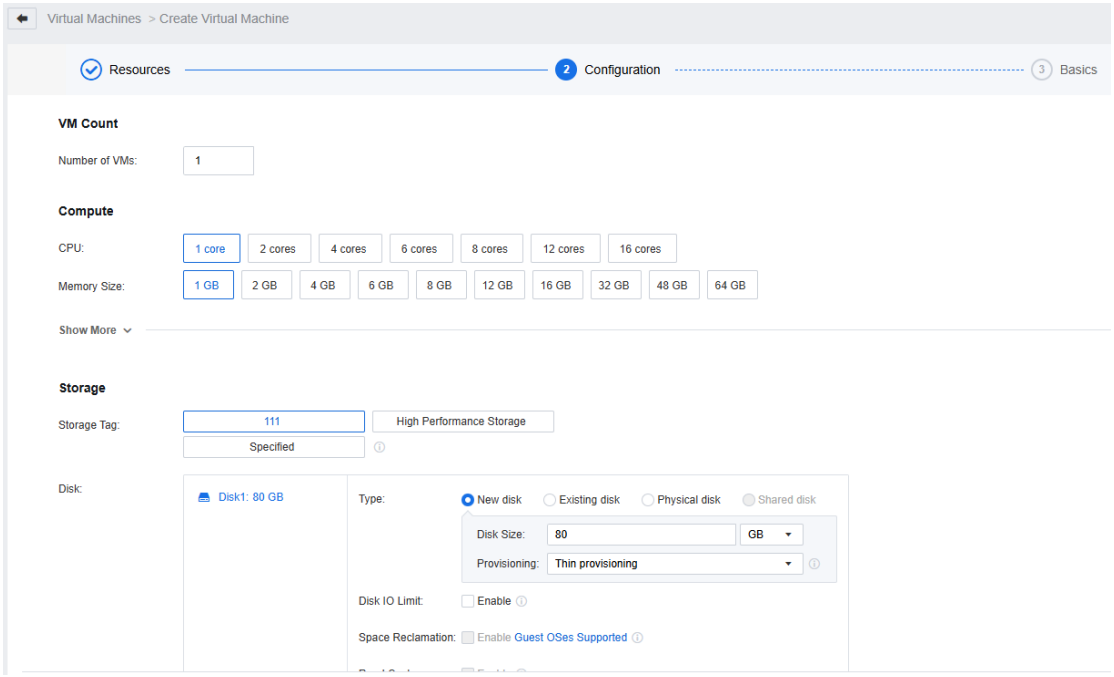


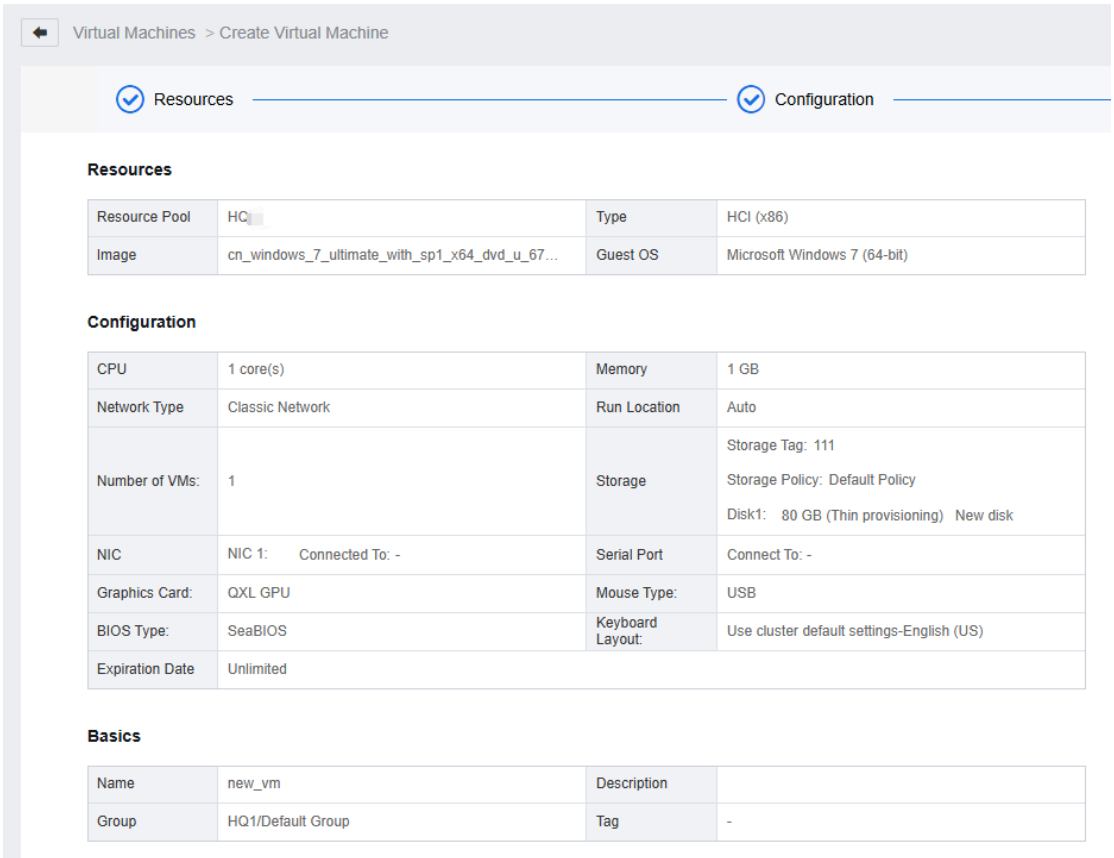
1. Click **New**, select the resource pool to which VMs belong and the creation

method, and follow the instructions to create them as needed.

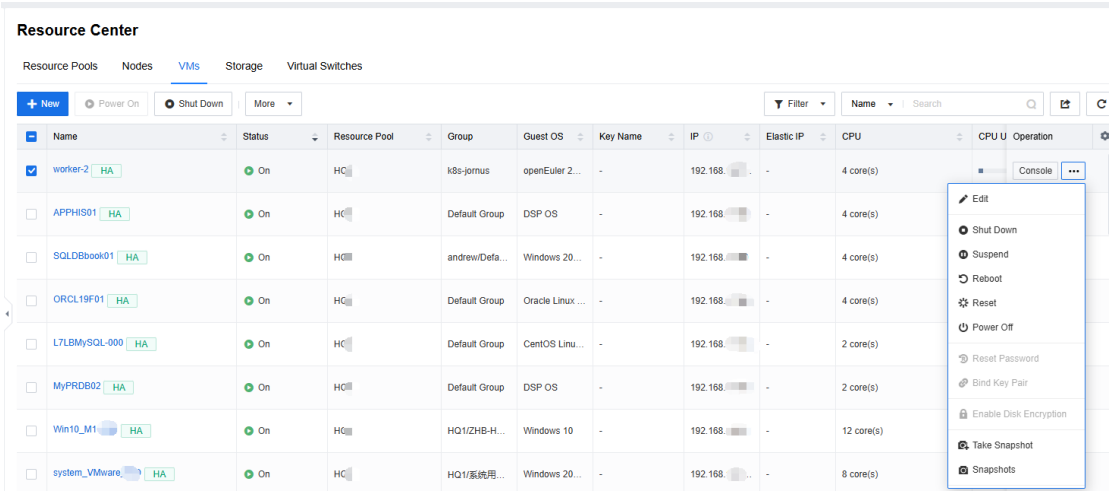




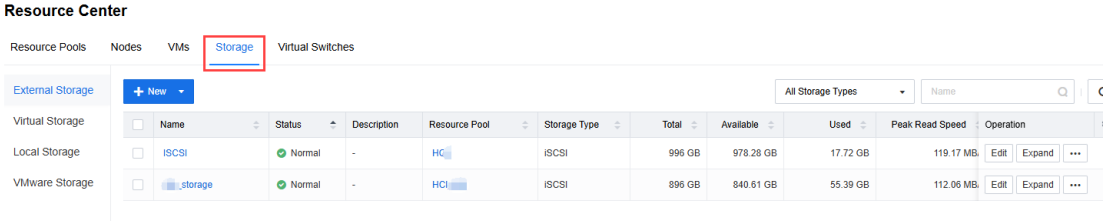




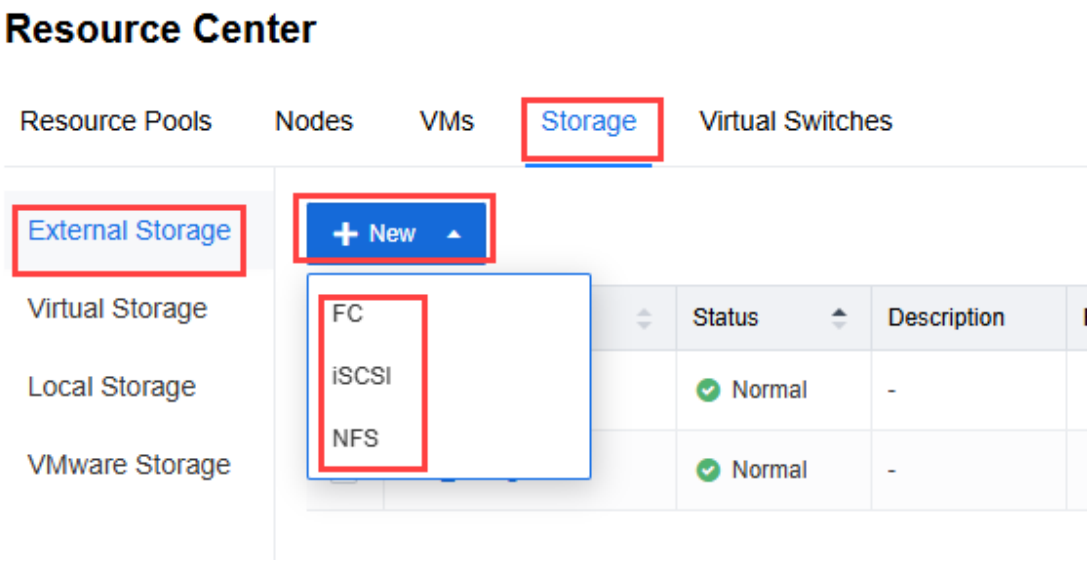
2. Click **Console** of a created VM to access the console, and click its **More** to edit, shut down, suspend, restart, reset, or power off it, and take and manage snapshots.

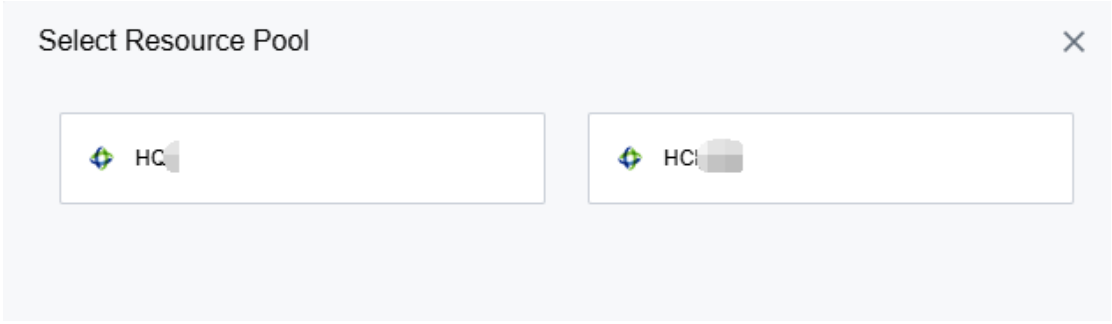


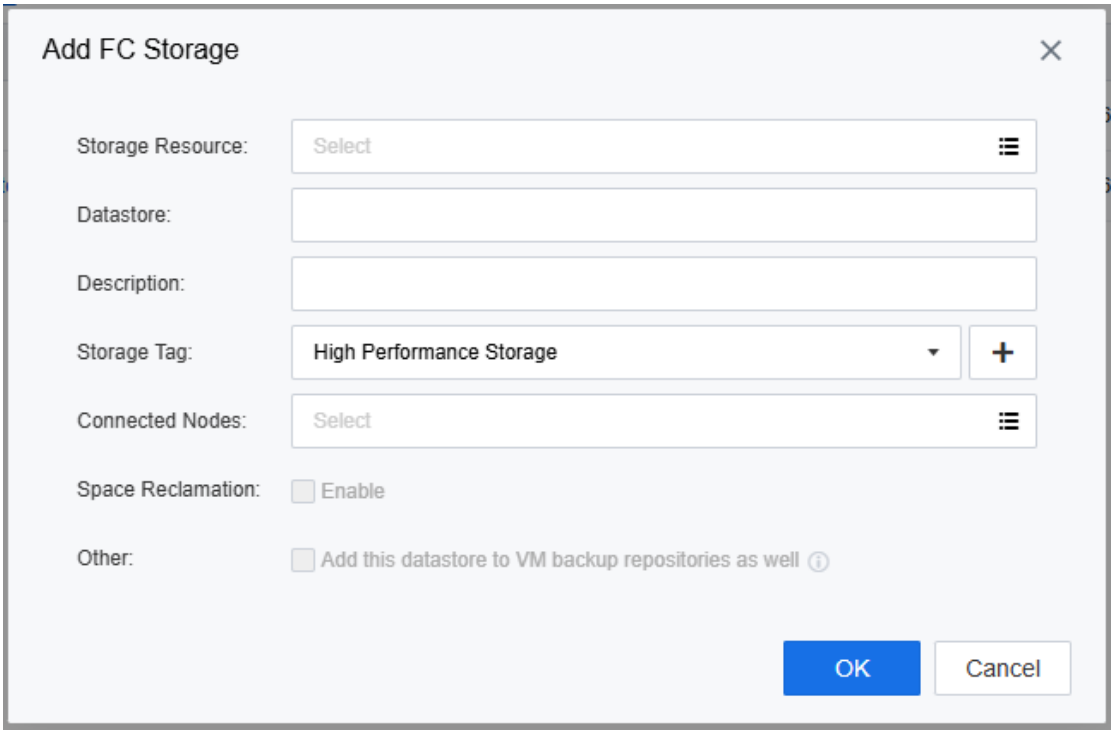
Step 5. Go to the **Storage** page.

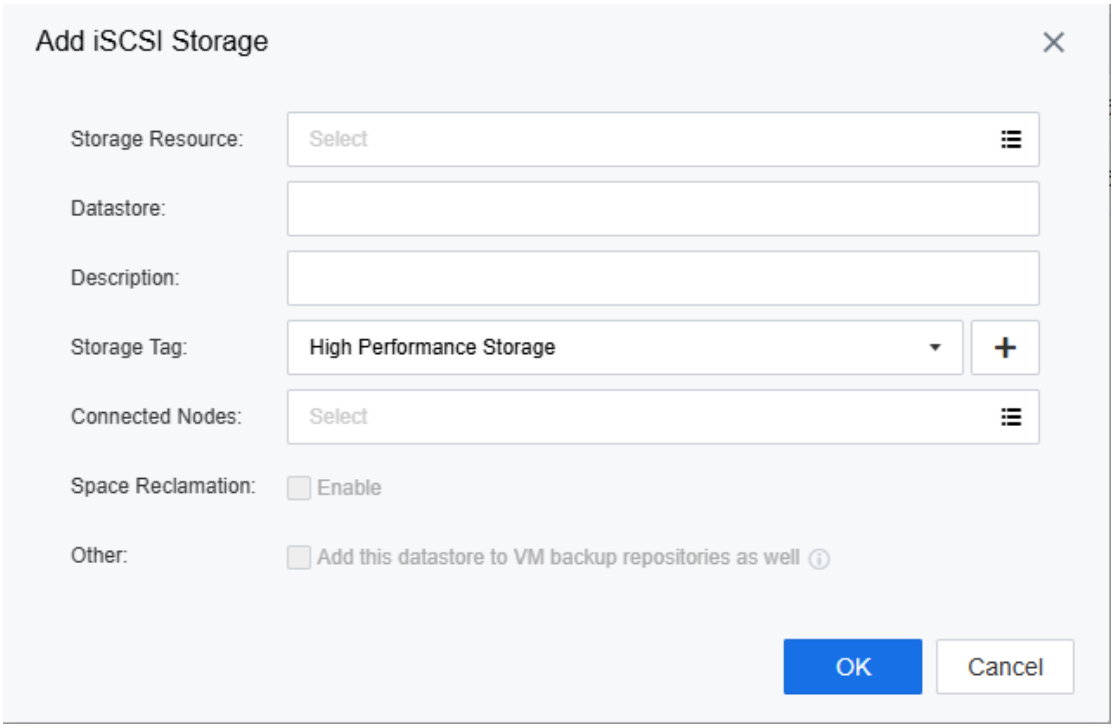


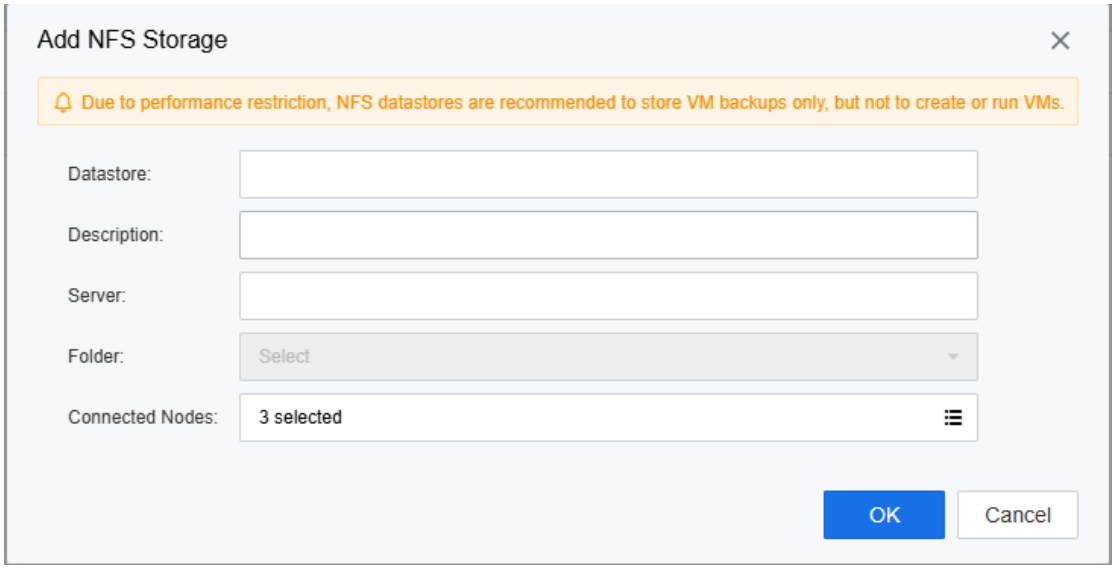
1. Go to **External Storage** > **New**, select **FC**, **iSCSI**, or **NFS** and the resource pool to which the storage belongs, and complete the configuration to add it.



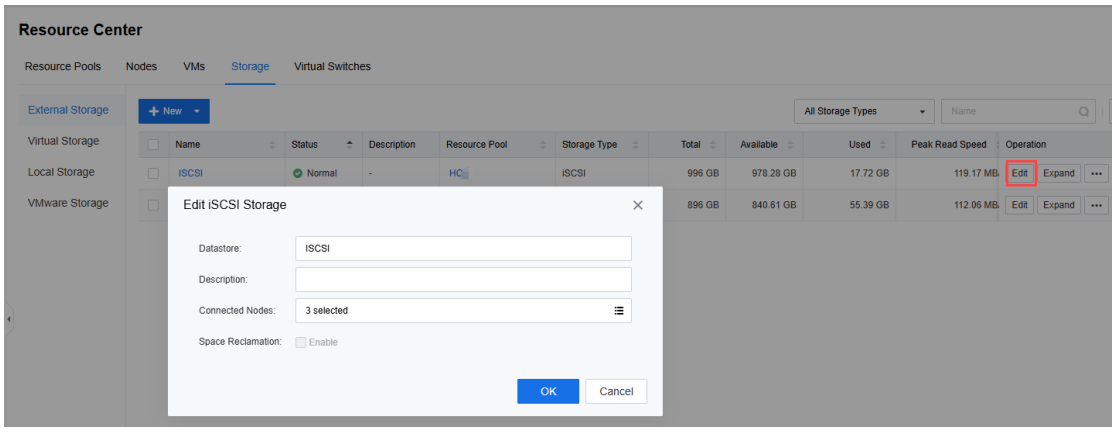

Select Resource Pool
HC
HCI


Add FC Storage
Storage Resource:
Select
Datastore:
Description:
Storage Tag:
High Performance Storage
Connected Nodes:
Select
Space Reclamation:
Enable
Other:
Add this datastore to VM backup repositories as well
OK
Cancel

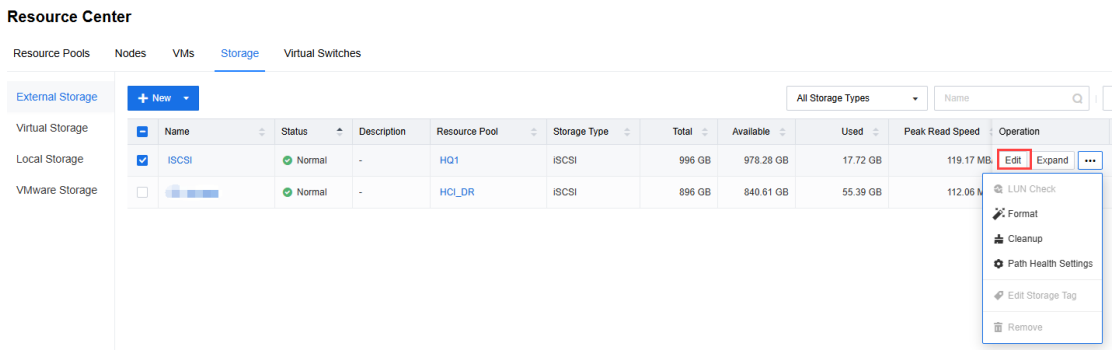

Add iSCSI Storage
Storage Resource:
Select
Datastore:
Description:
Storage Tag:
High Performance Storage
Connected Nodes:
Select
Space Reclamation:
Enable
Other:
Add this datastore to VM backup repositories as well
OK
Cancel



2. Click **Edit** of the added external storage to modify the **Datastore**, **Description**, and **Connected Nodes**, and enable or disable **Space Reclamation**.

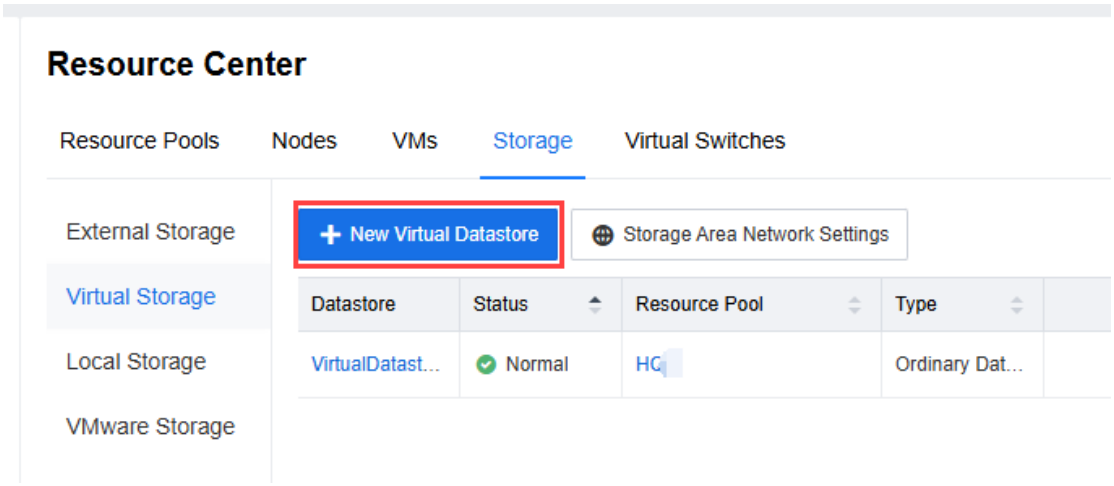


3. Click its **More** to format, clean up, or remove it, edit the storage tag, and configure the path health monitoring policy.

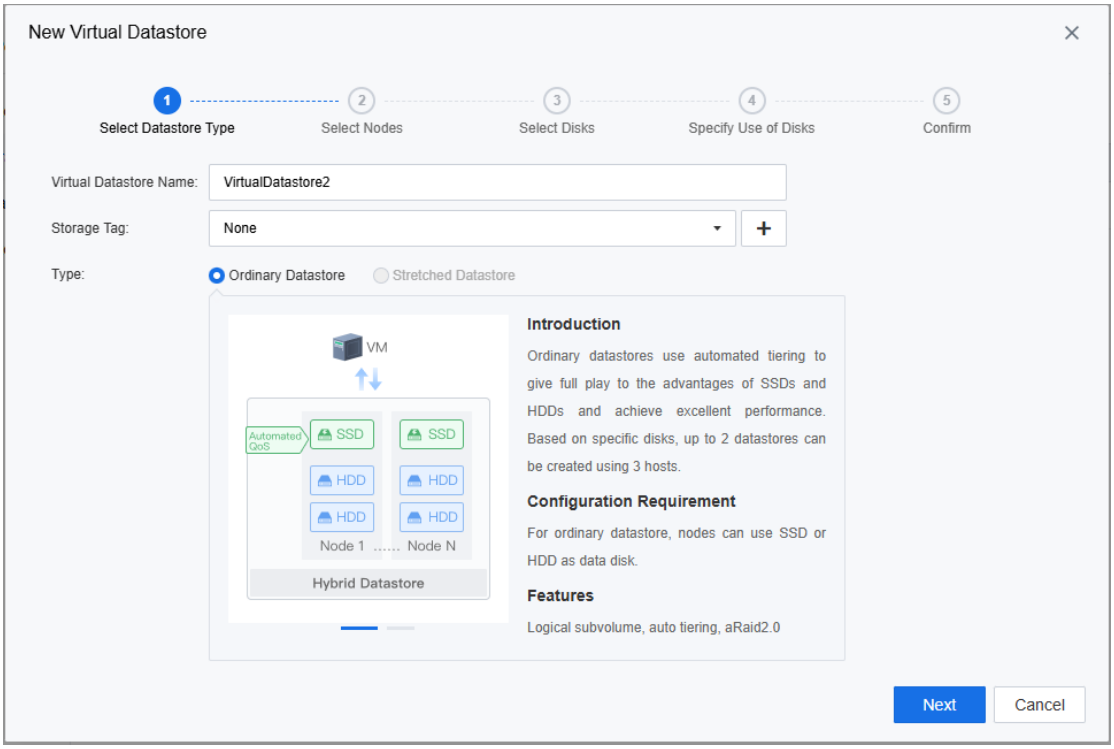


4. Go to **Virtual Storage** > **New**, select the resource pool to which the virtual datastore belongs, and follow the instructions to complete the configuration

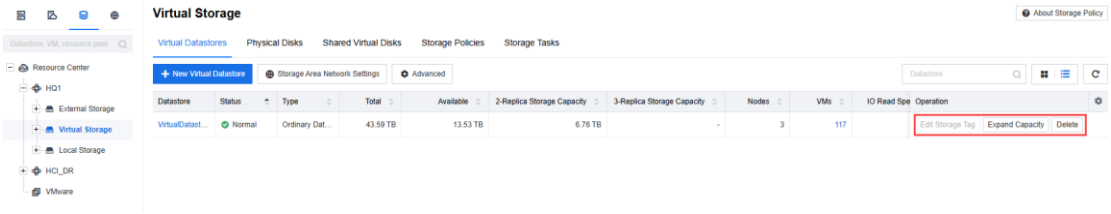
to create it.


Resource Center
Resource Pools
Nodes
VMs
Storage
Virtual Switches
External Storage
Virtual Storage
Local Storage
VMware Storage
New Virtual Datastore
Storage Area Network Settings
Datastore
Status
Resource Pool
Type
VirtualDatast...
Normal
Ordinary Dat...

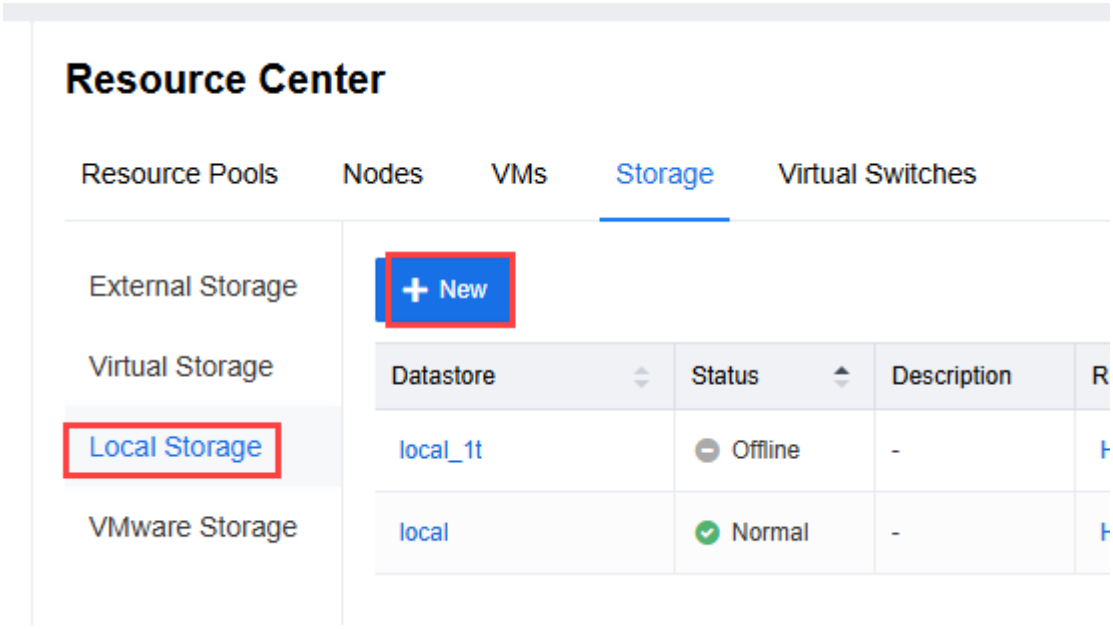

Select Resource Pool

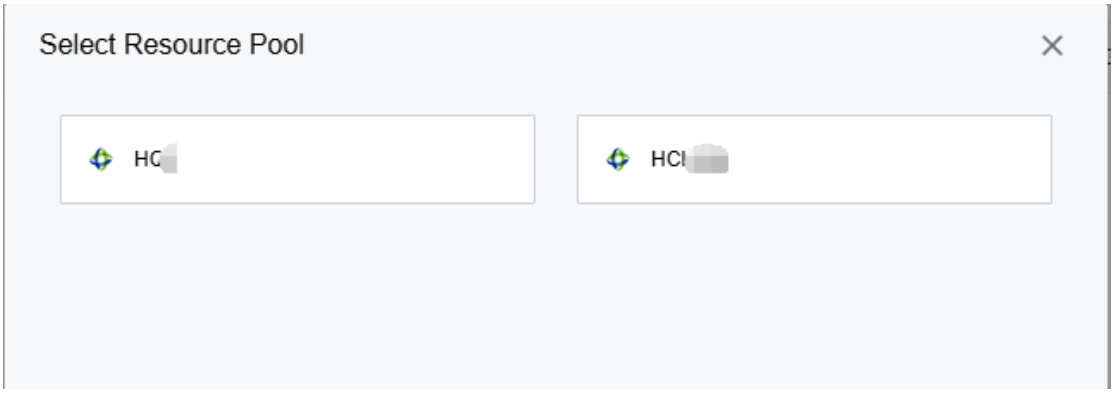

New Virtual Datastore
Select Datastore Type
Select Nodes
Select Disks
Specify Use of Disks
Confirm
Virtual Datastore Name:
VirtualDatastore2
Storage Tag:
None
Type:
Ordinary Datastore
Stretched Datastore
VM
Automated QoS
SSD
HDD
Node 1
Node N
Hybrid Datastore
Introduction
Ordinary datastores use automated tiering to give full play to the advantages of SSDs and HDDs and achieve excellent performance. Based on specific disks, up to 2 datastores can be created using 3 hosts.
Configuration Requirement
For ordinary datastore, nodes can use SSD or HDD as data disk.
Features
Logical subvolume, auto tiering, aRaid2.0
Next
Cancel

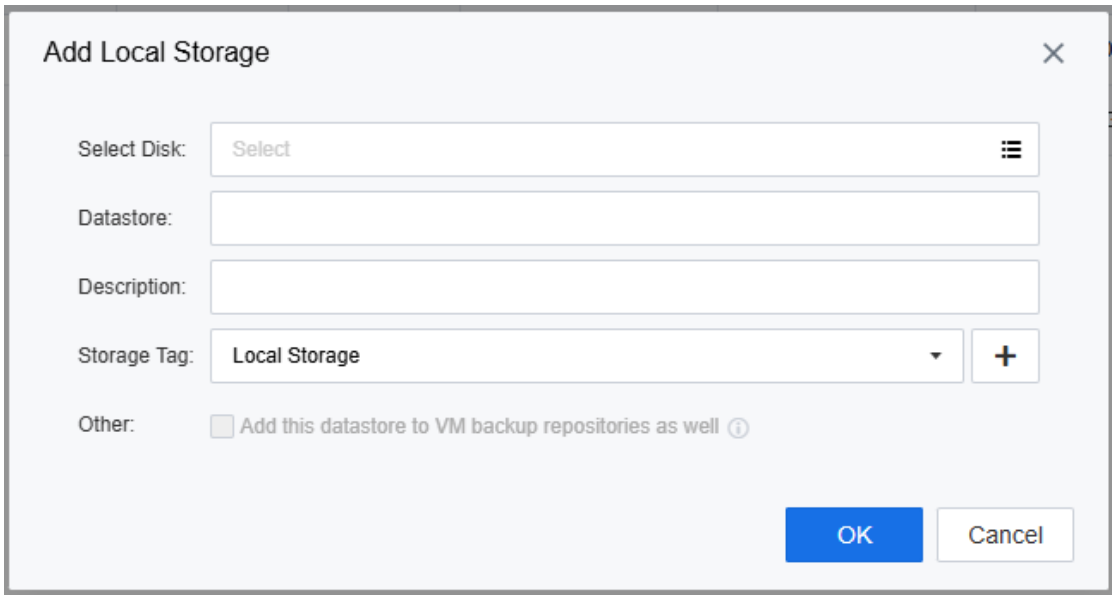
5. Edit the storage tag of the created virtual datastore, expand its capacity, or remove it.



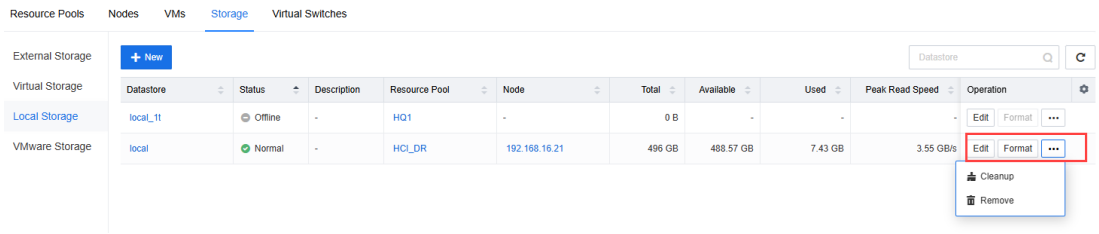
6. Go to **Local Storage** > **New**, select the resource pool to which the storage belongs, and complete the configuration to add it.





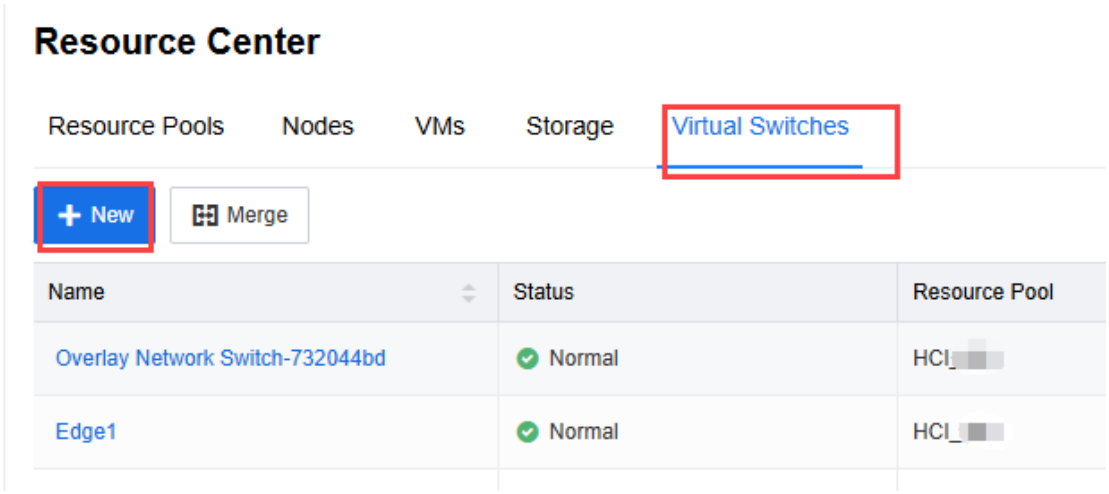


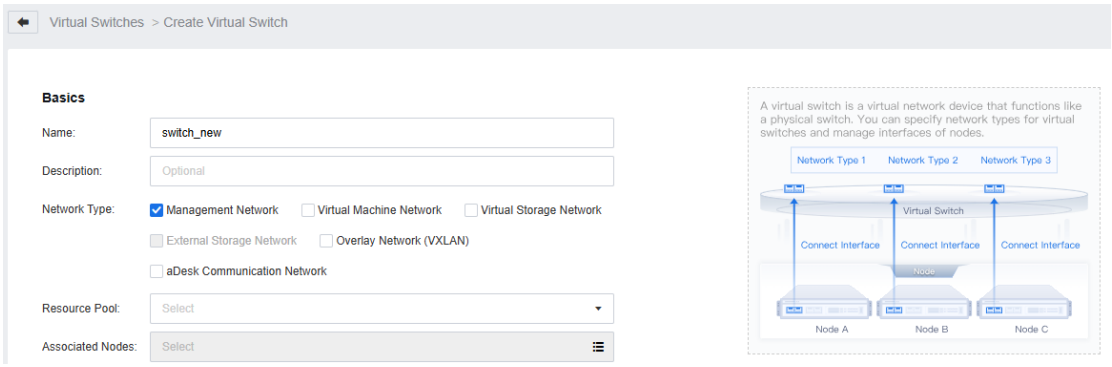
7. Modify the name of the added local storage, edit its storage tag, and format, clean up, or remove it.



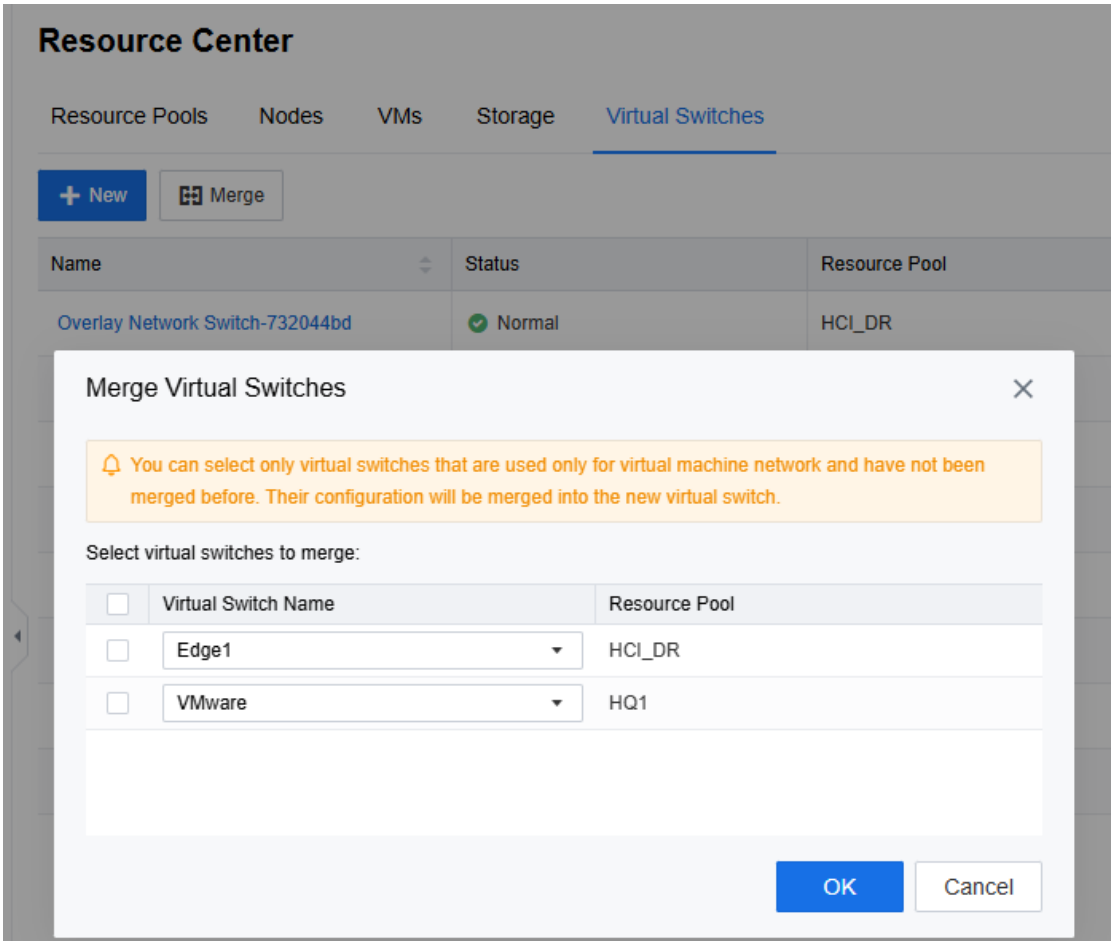
Step 6. Go to the **Virtual Switches** page.

1. Click **New**, specify the **Name** and **Description**, and select the **Network Type**, **Resource Pool**, and **Connected Nodes** to create a virtual switch.

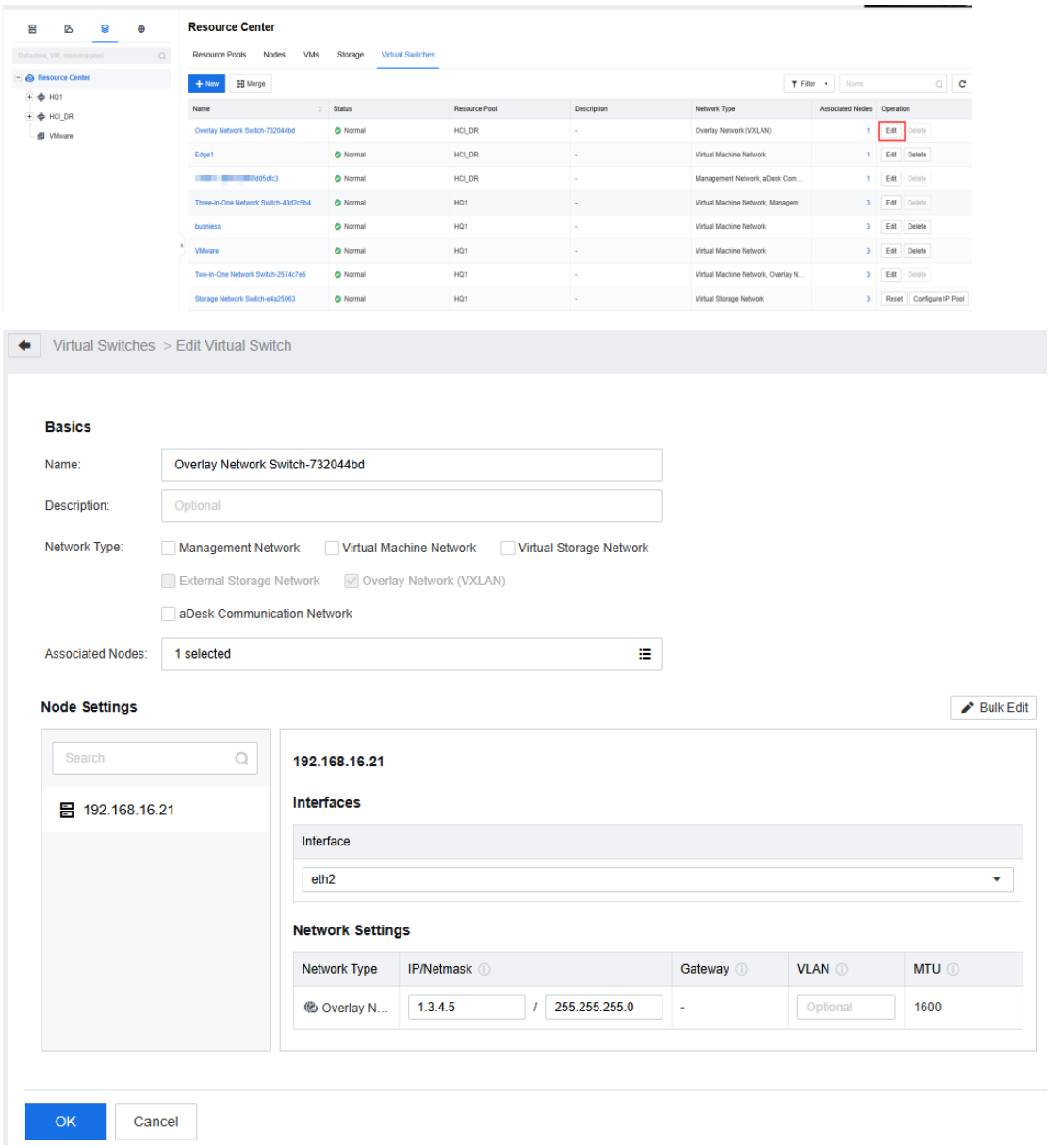




2. Click **Merge** and select virtual switches to merge their configuration into the new virtual switch.



3. Click **Edit** of a virtual switch to modify the **Name**, **Description**, **Network Type**, **Connected Nodes**, and **Interfaces**, **Network Settings**, and **Max Bandwidth Limit** for each node.



4.2.1.1 View by Node

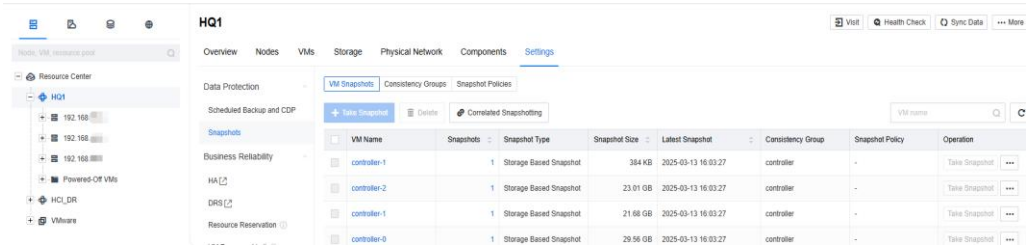
Function Description:

Resources such as resource pools, nodes, VMs, and storage can be viewed and managed by node.

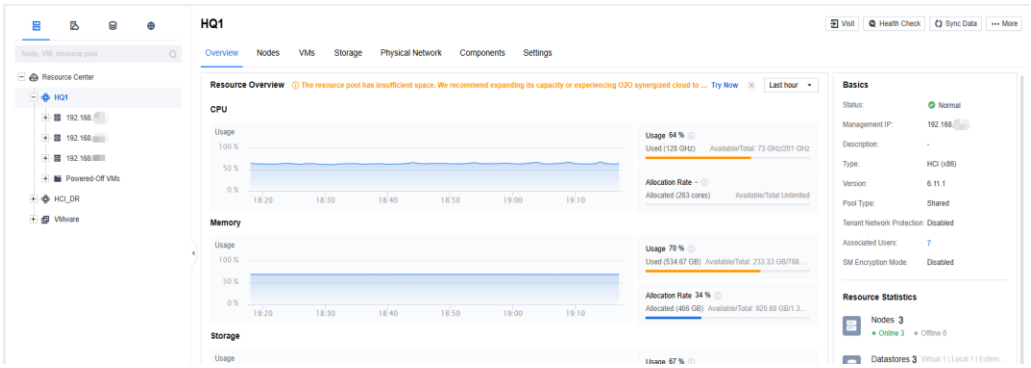
Steps:

Step 1. Click **View by Node** on the left to display resource pools by node.

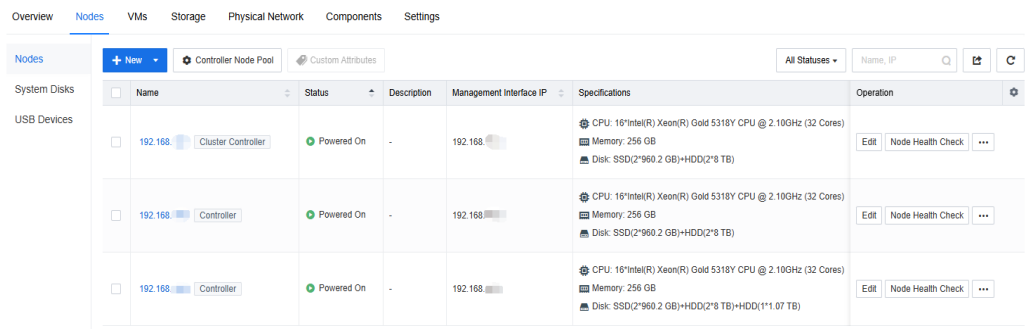
Step 2. Click a resource pool to view the nodes in it and the VMs on the nodes.

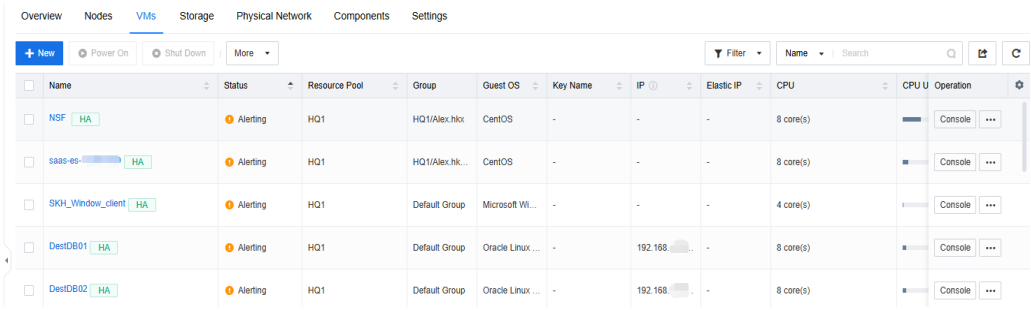


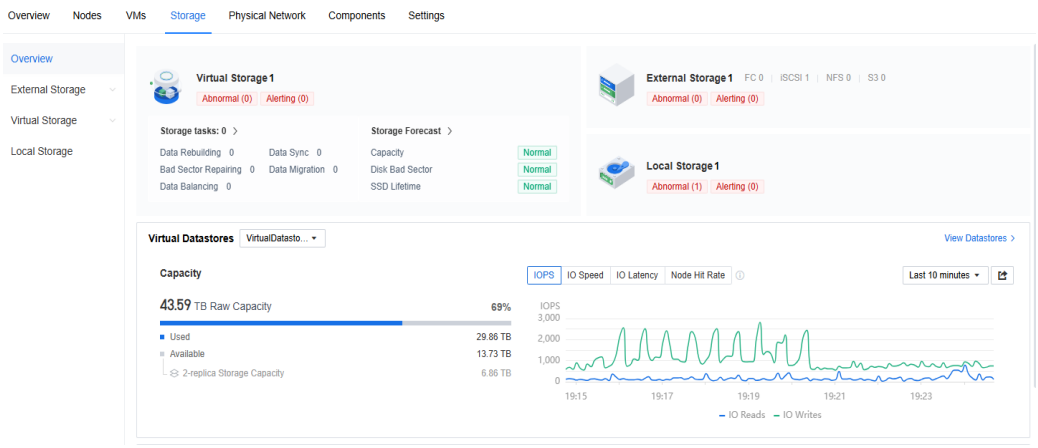
1. View the **Overview**.

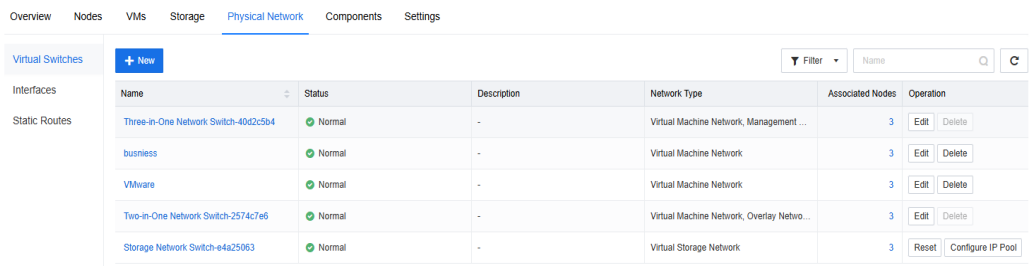


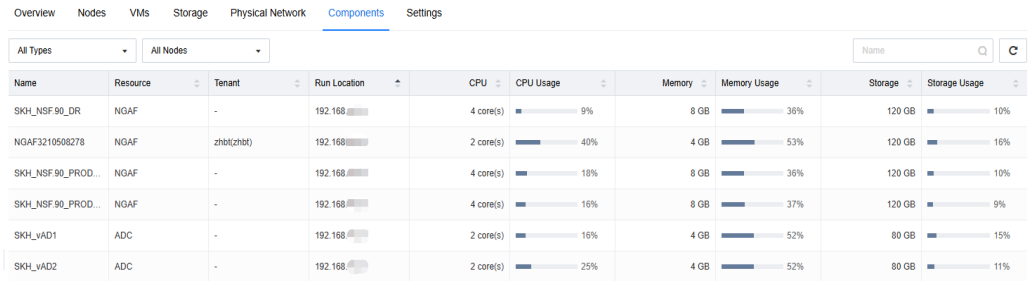
2. View and manage nodes, VMs, storage, physical network, and components.



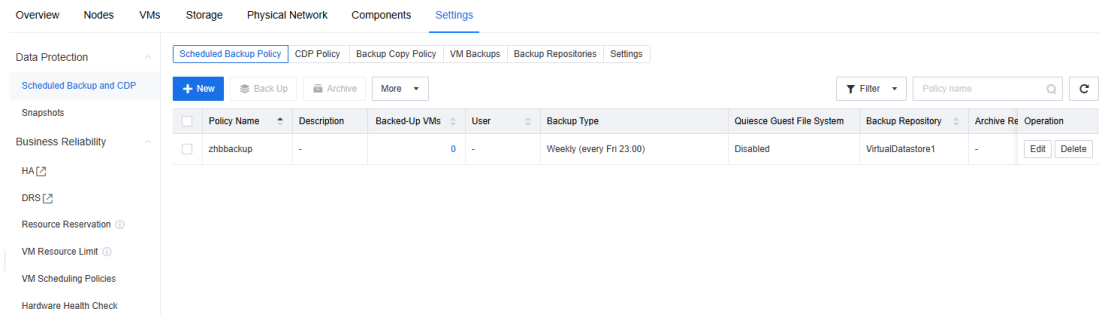


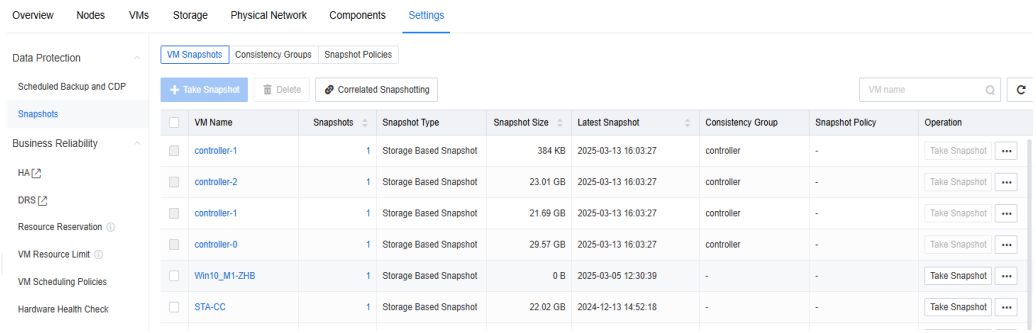




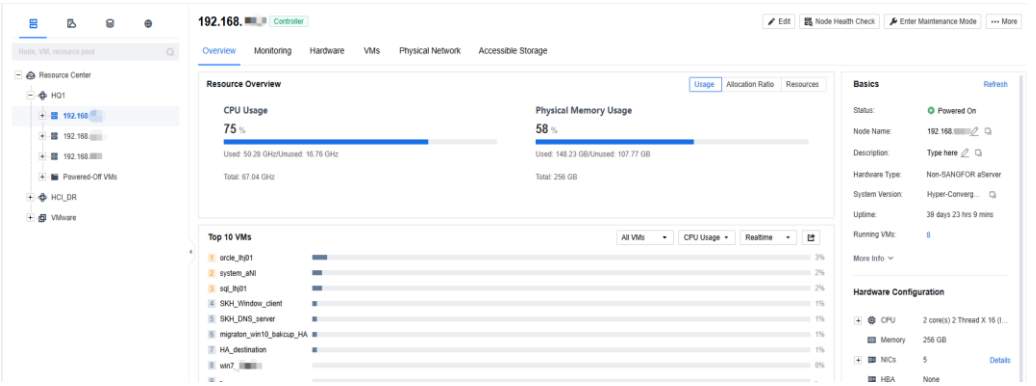


3. Click **Settings** to configure data protection, business reliability, resource ratios, and system.

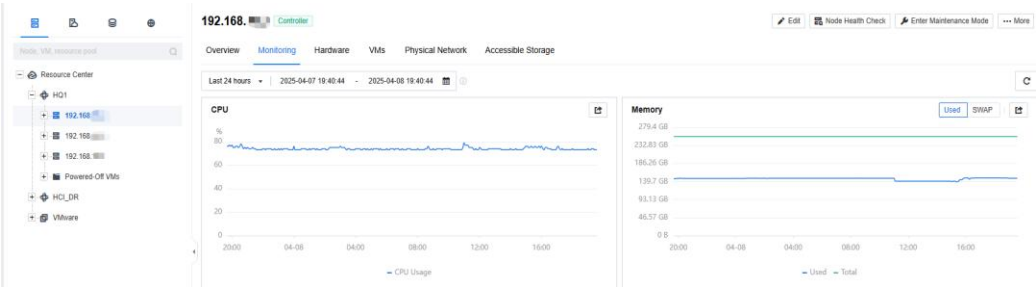




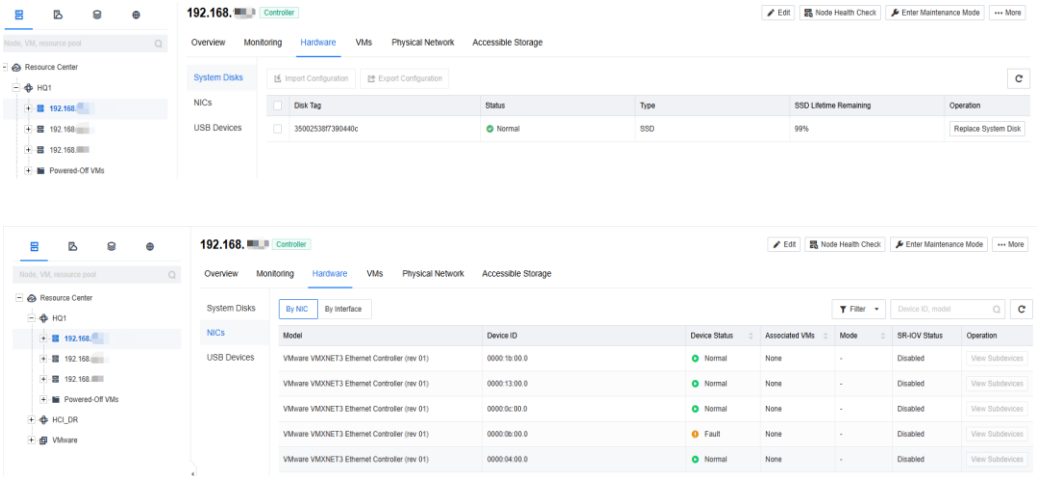
Step 3. Click a node to view the **Overview**.



1. Click **Monitoring** to view CPU and memory usage, interface throughput, and disk I/O.

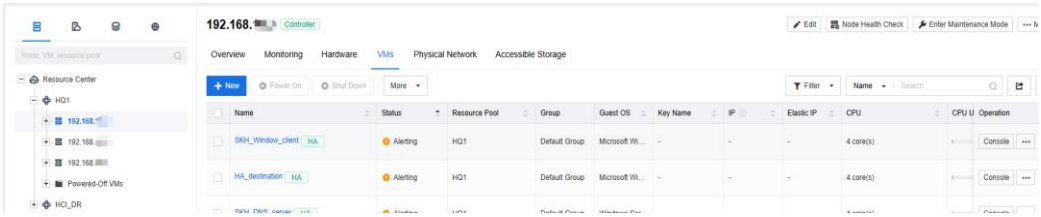


2. Click **Hardware** to view and manage system disks, PCI-e devices, and USB.

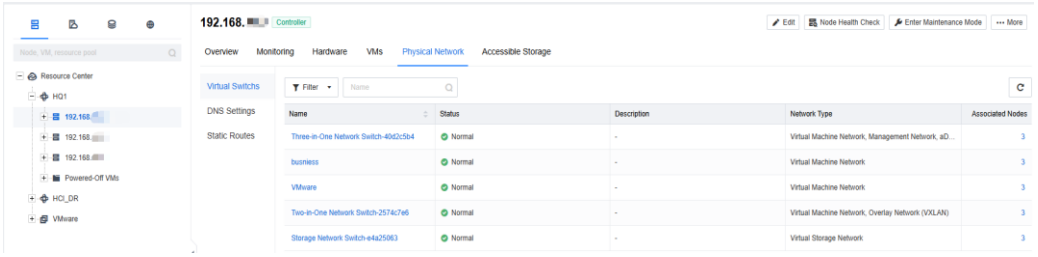


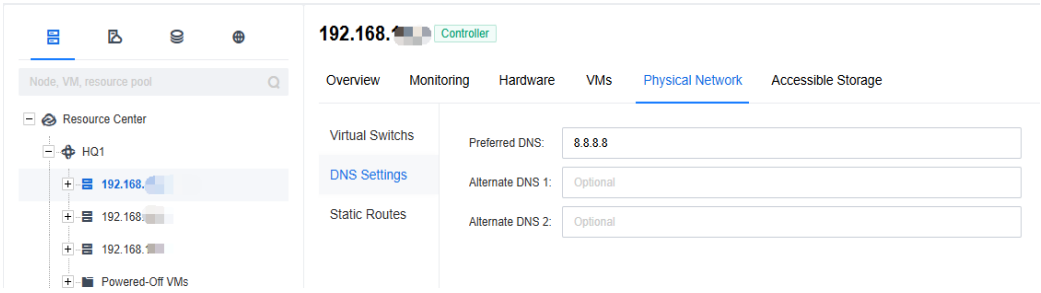


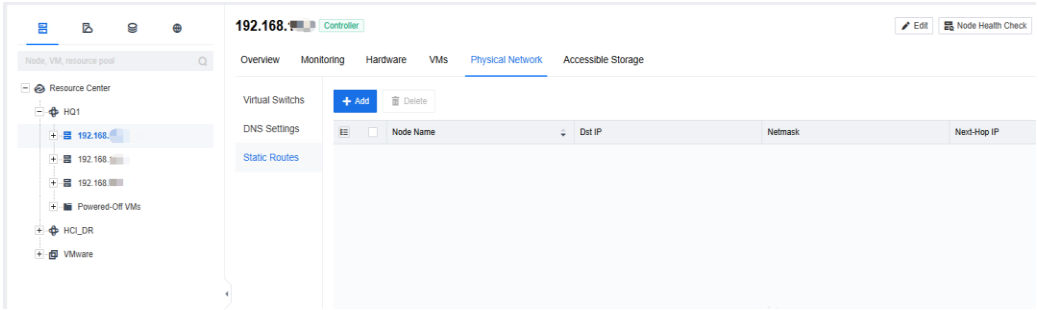
3. Click **VMs** to create and manage VMs.



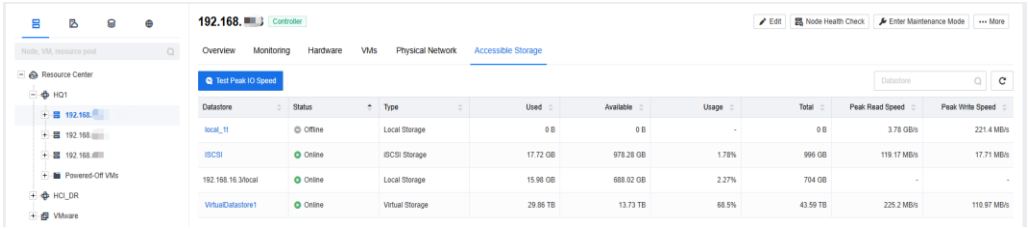
4. Click **Physical Network** to configure virtual switches, DNS, and static routes.



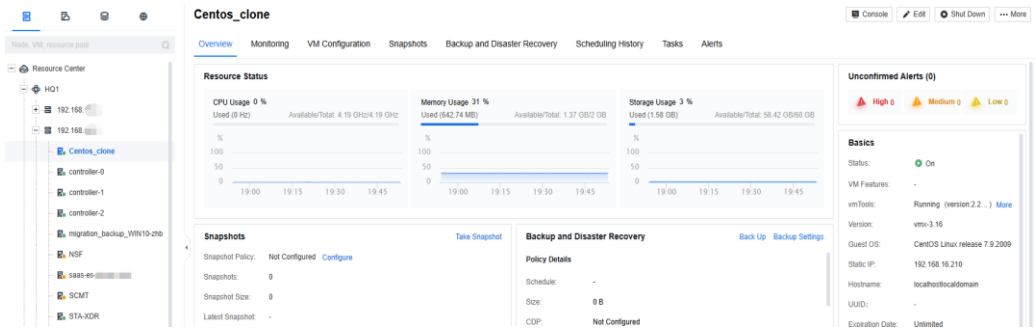




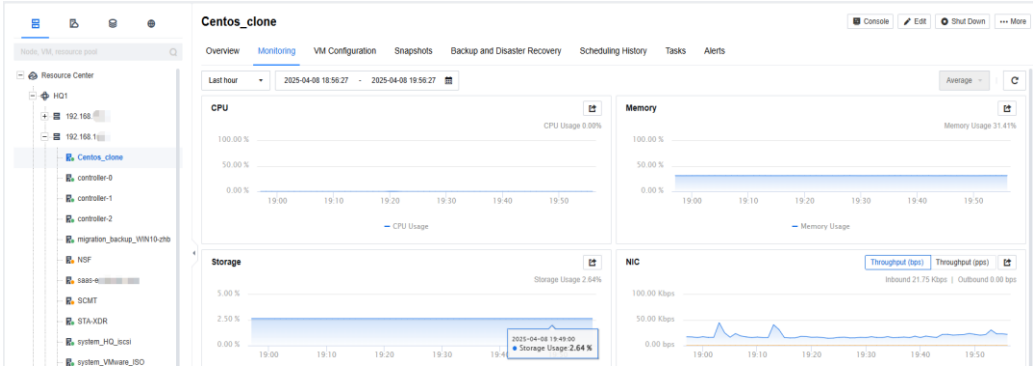
5. Click **Accessible Storage** to view accessible storage and test peak I/O speeds.



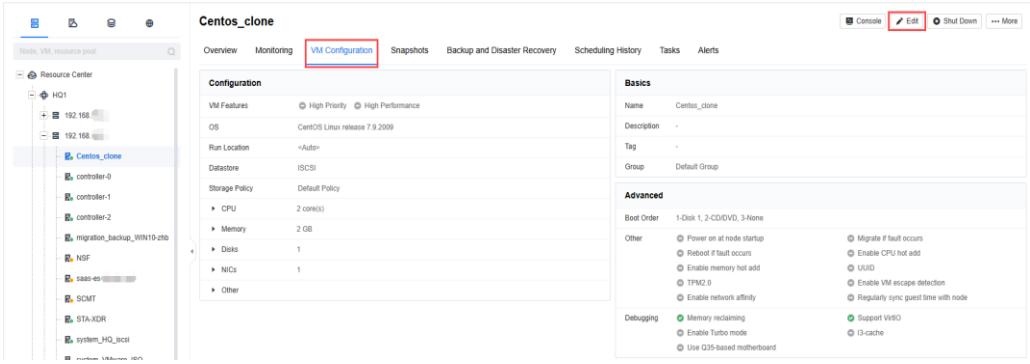
Step 4. Click a VM to view the **Overview**.



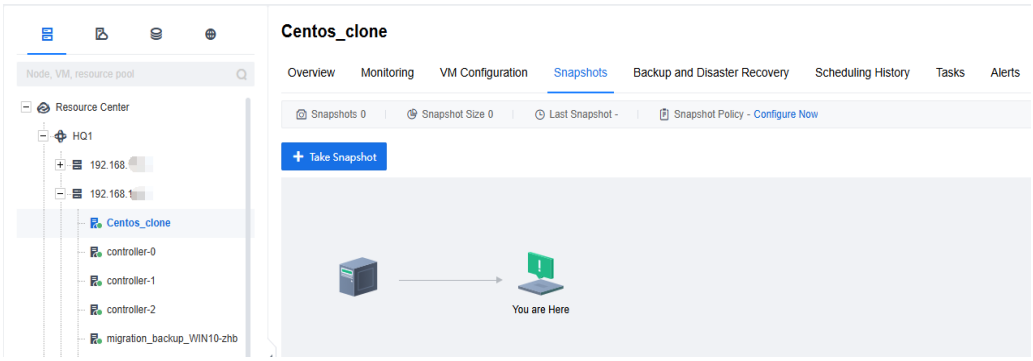
1. Click **Monitoring** to view CPU, memory, and storage usage, and NIC throughput.

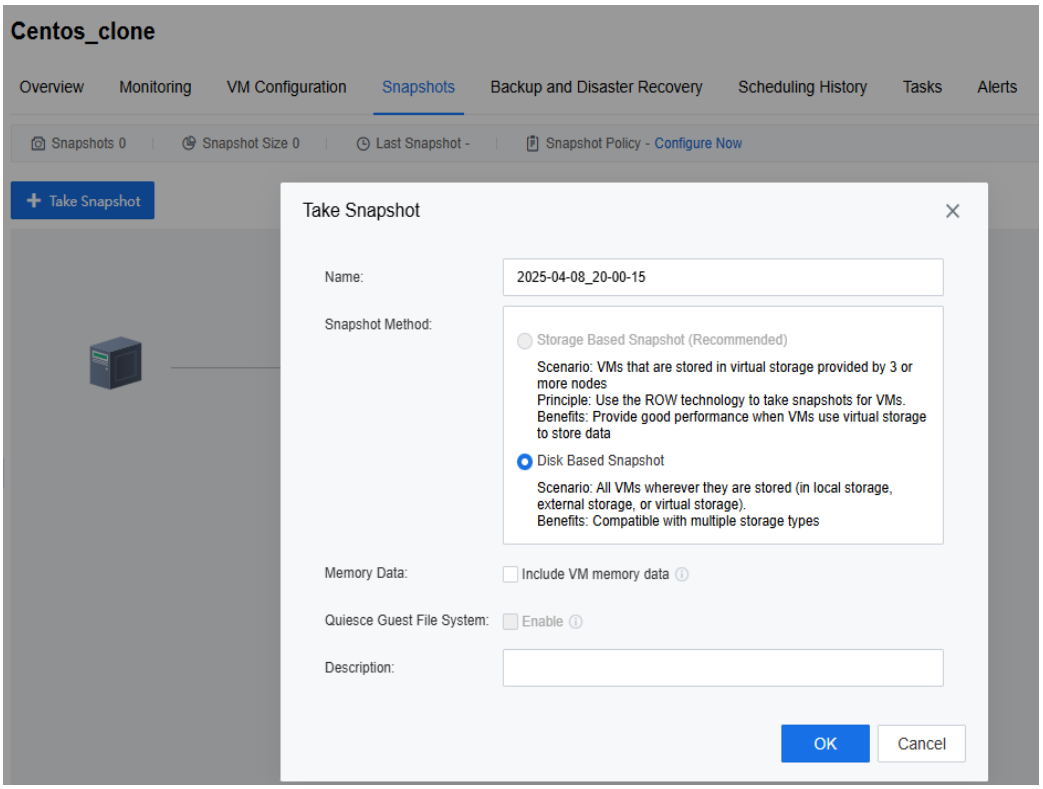


2. Click **Configuration** to view the configuration and click **Edit** to modify it.

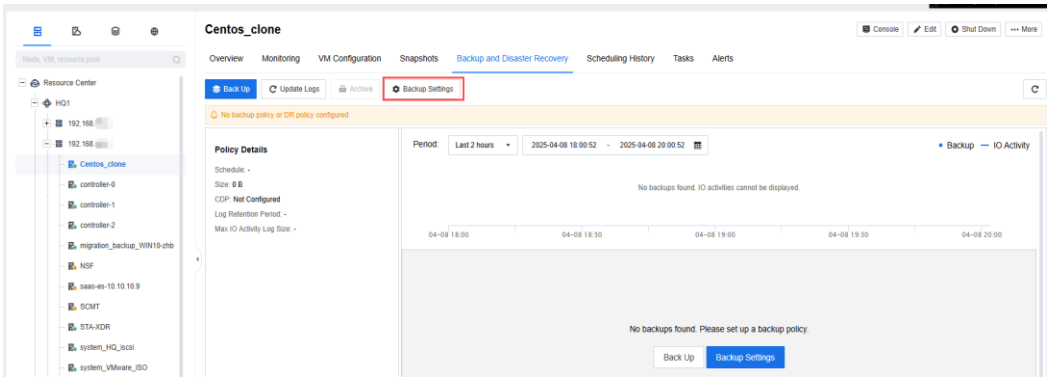


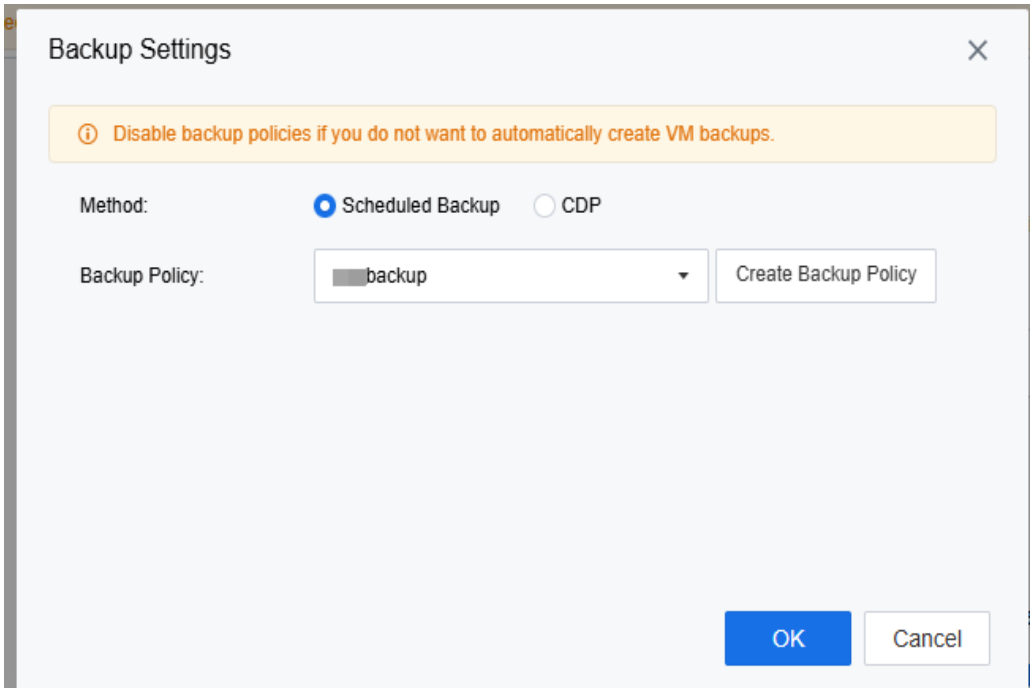
3. Click **Snapshots** to view and take snapshots.



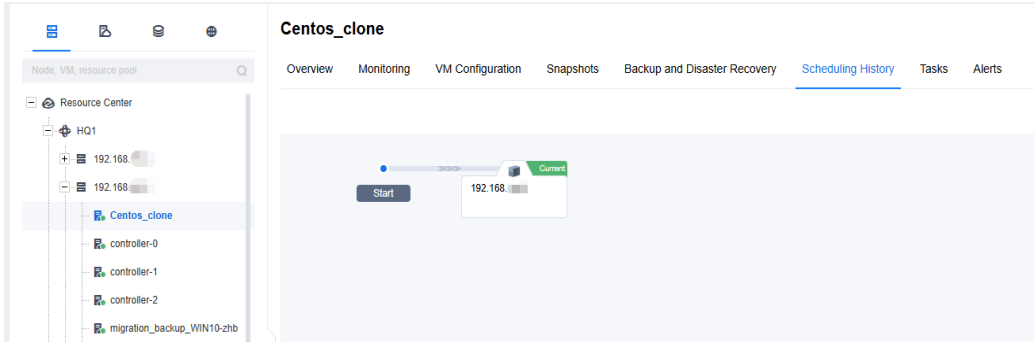


4. Click **Backup and Disaster Recovery** to perform backups and configure backup settings.

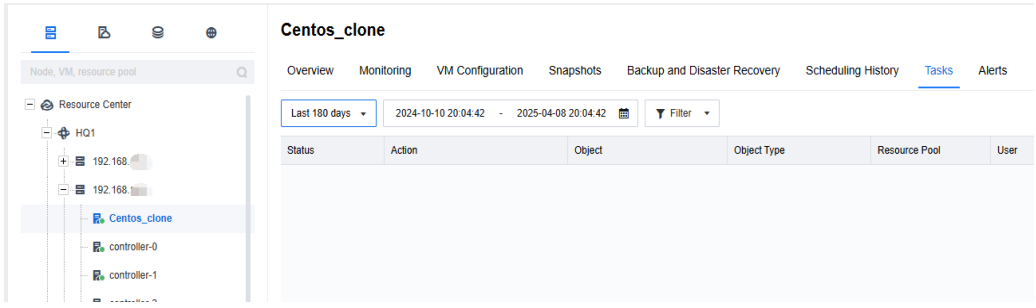




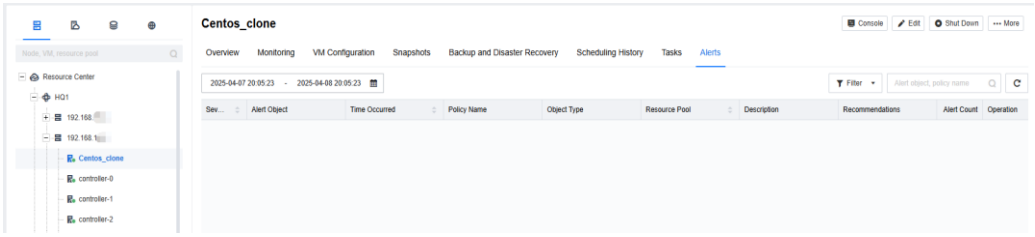
5. Click **Scheduling History** to view the scheduling history.



6. Click **Tasks** to view tasks.



7. Click **Alerts** to view alerts.



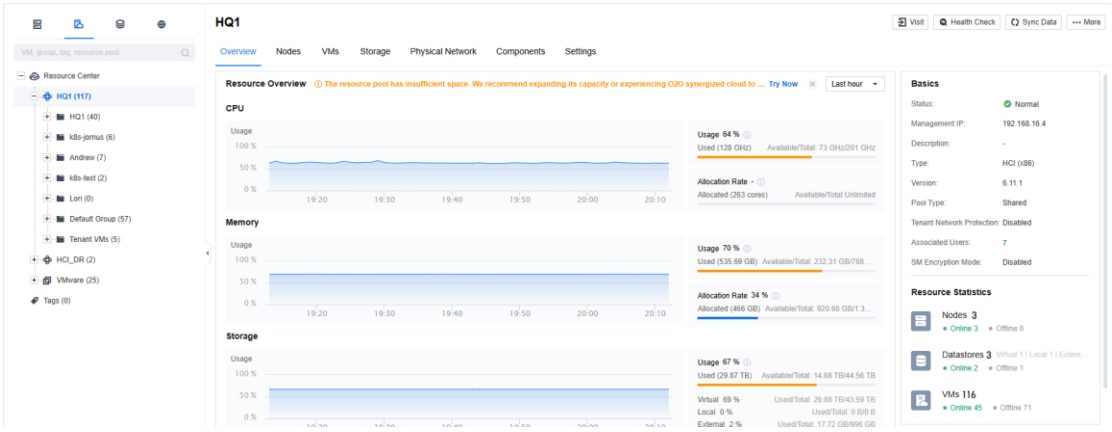
4.2.1.2 View by VM

Function Description:

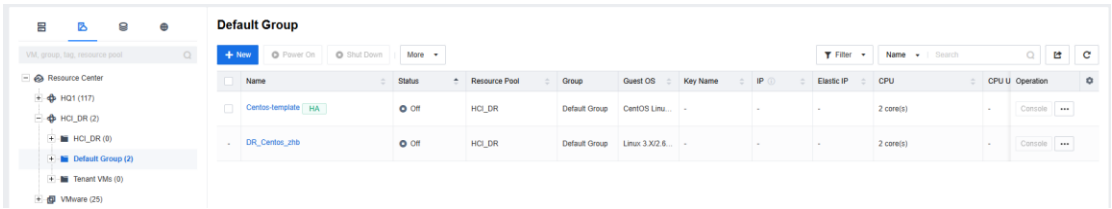
Resources can be viewed and managed by VM.

Steps:

Step 1. Click **View by VM** on the left to display resource pools by VM group.



Step 2. Click a VM group to view, create, and manage the VMs in it.



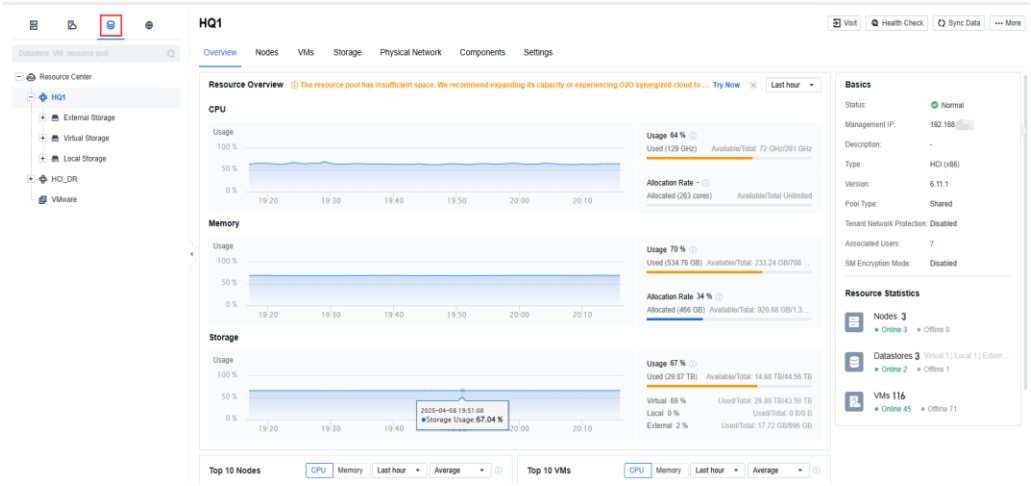
4.2.1.3 View by Storage

Function Description:

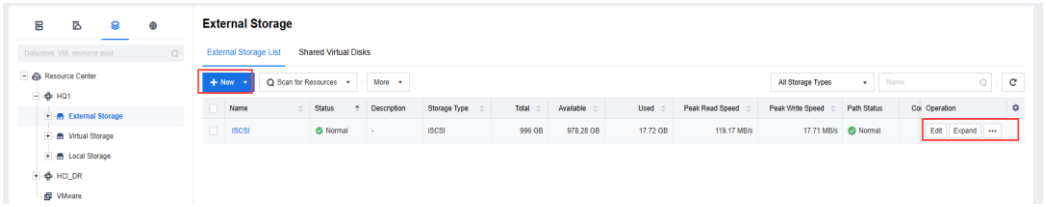
Resources can be viewed and managed by storage.

Steps:

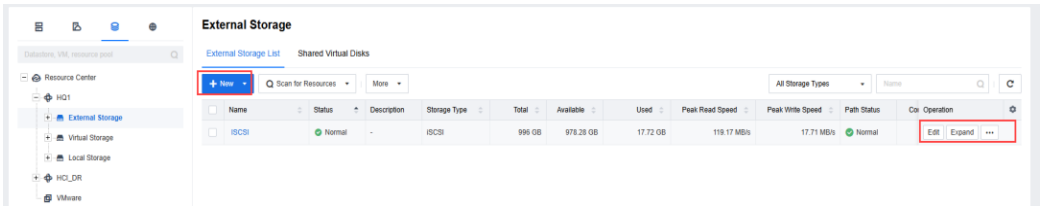
Step 1. Click **View by Storage** on the left to display resource pools by storage type.



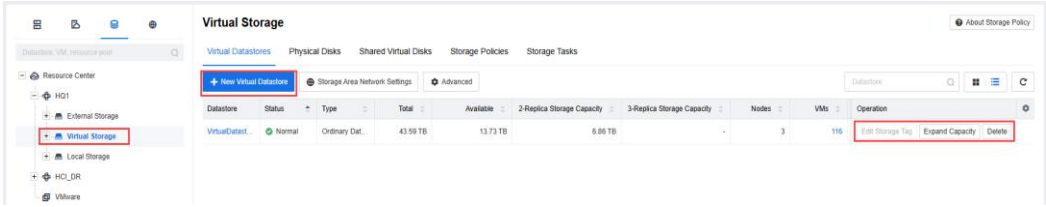
Step 2. Click an **External Storage** to view, create, edit, or delete the external storage in the corresponding resource pool and view their shared virtual disks.



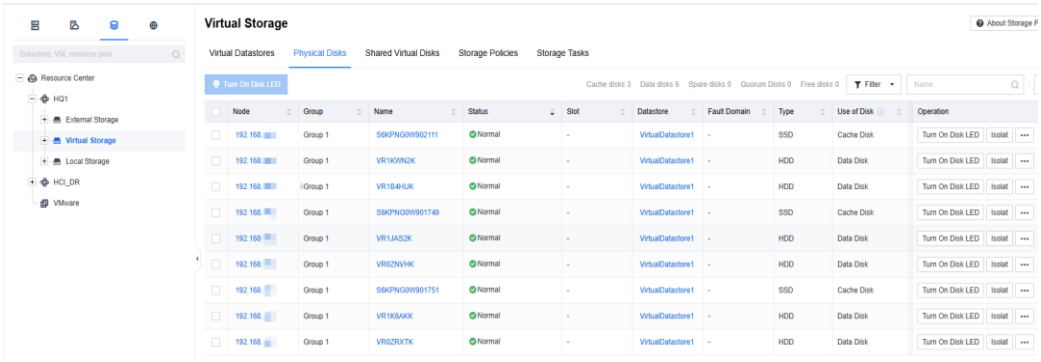
Step 3. Click a **Virtual Storage** to view the **Basics**, **Capacity**, and **Storage Forecast** of the datastores in the corresponding resource pool.



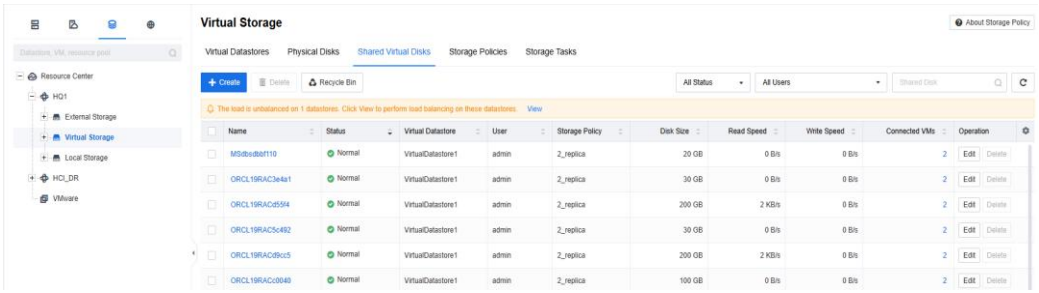
1. Create virtual datastores, modify storage network settings, configure storage policies, expand the capacity of existing datastores, edit their storage tags, or delete them (high risk).



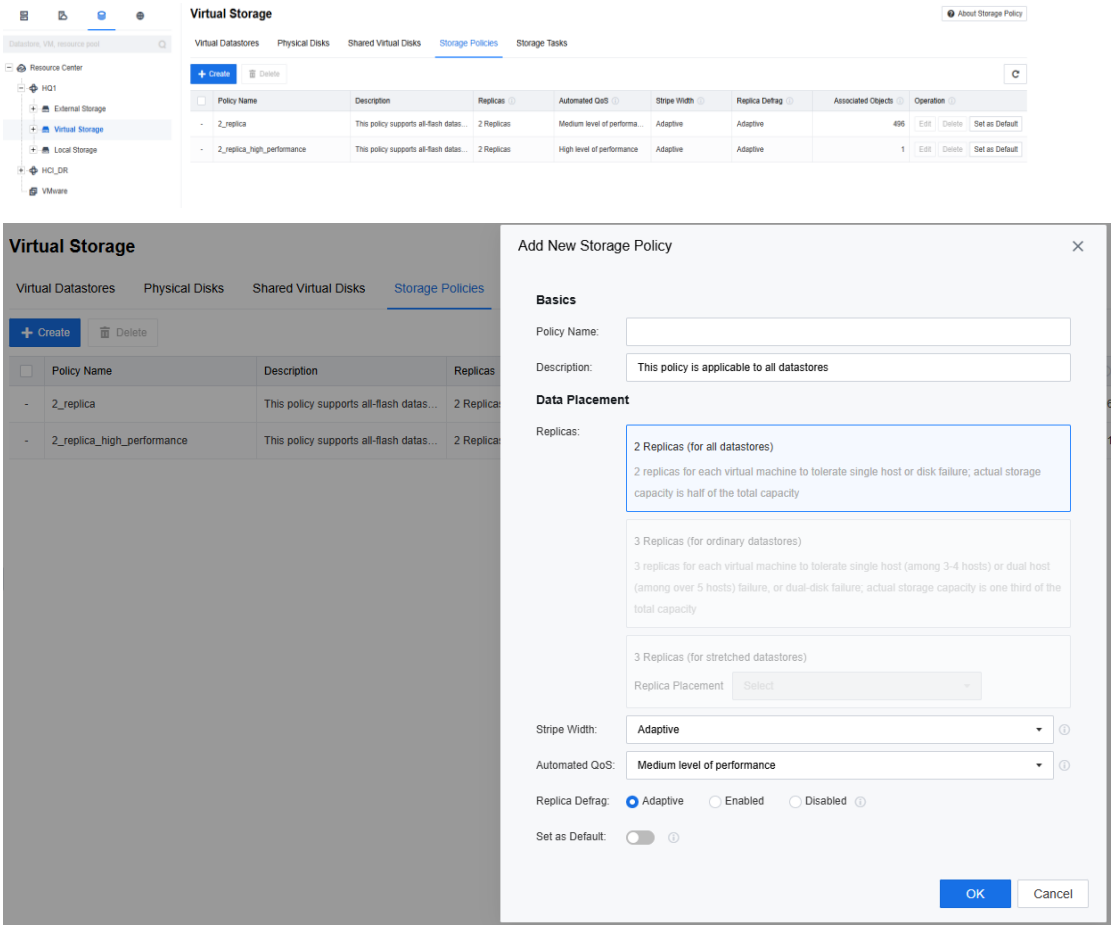
2. Click **Physical Disks** to view the disks on datastores and isolate, replace, or remove them based on O&M requirements.



3. Click **Shared Virtual Disks** to view, create, edit, or remove shared virtual disks on datastores.

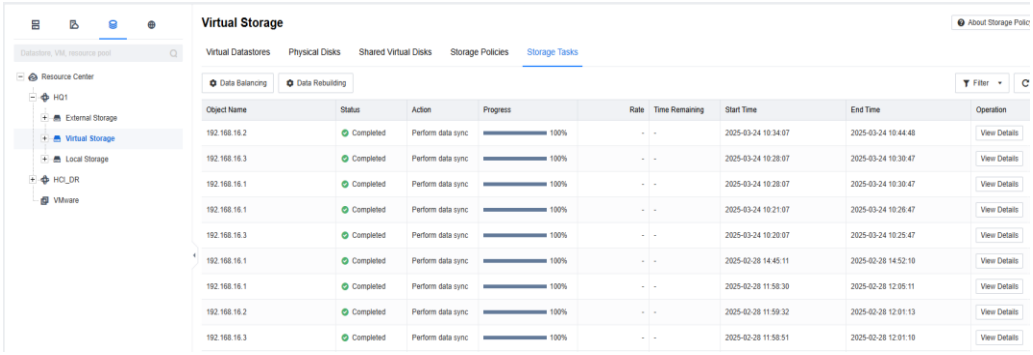


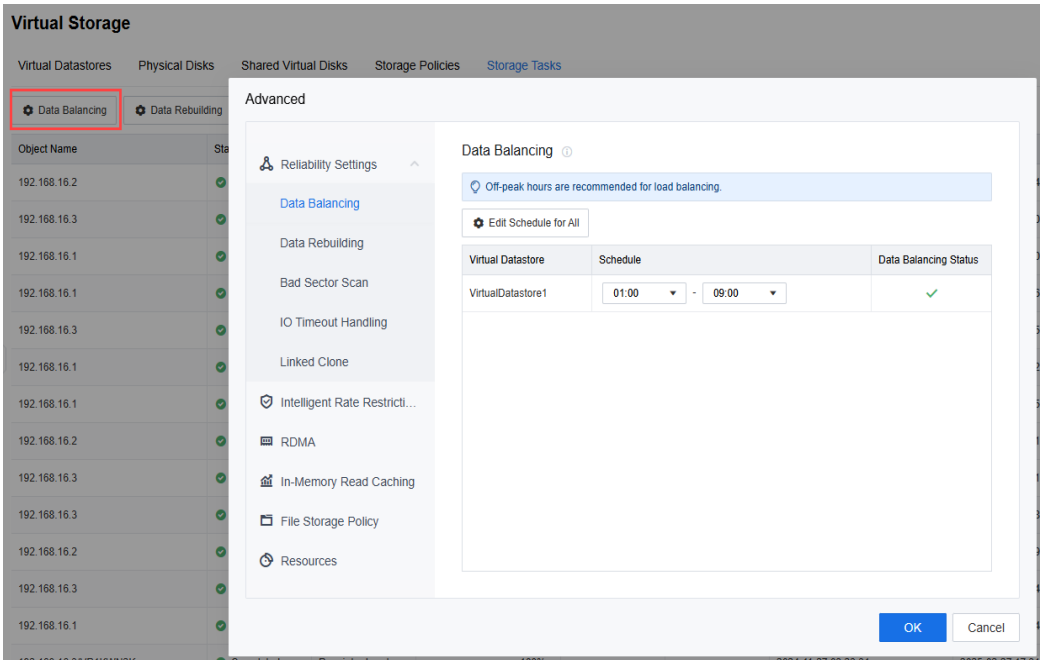
4. Click **Storage Policies** to create storage policies for datastores.

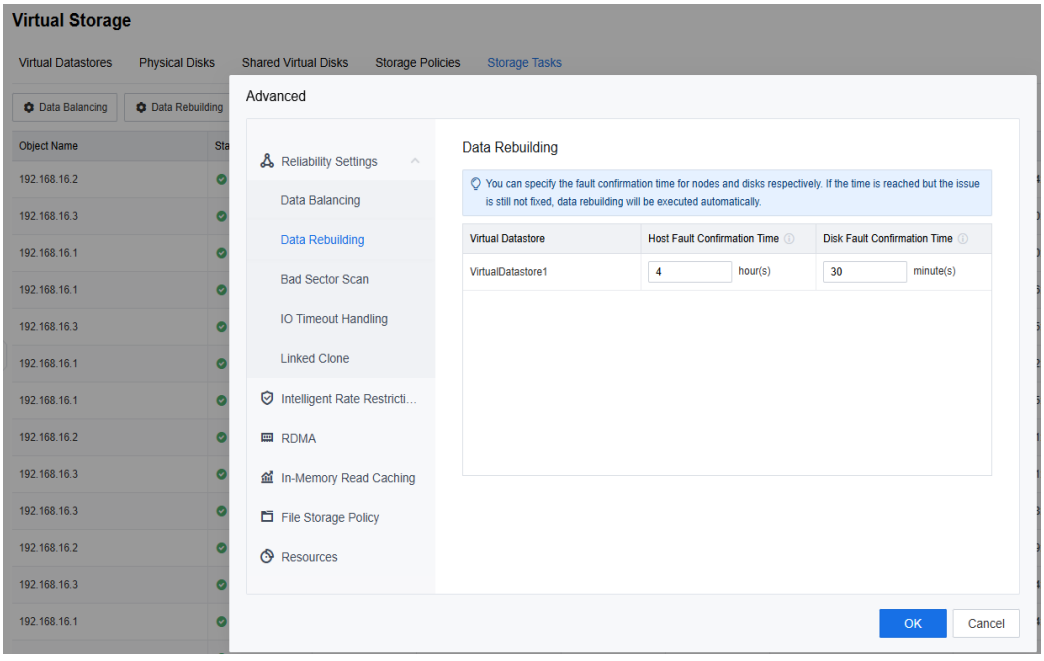


5. Click **Storage Tasks** to view the progress of storage tasks and configure data

balancing and data rebuilding for datastores.







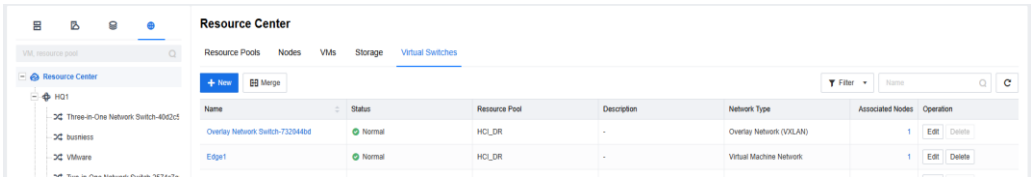
4.2.1.4 View by Network

Function Description:

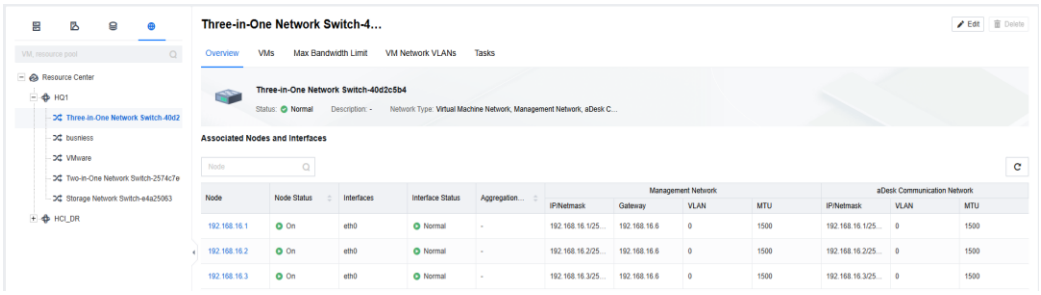
Resources can be viewed and managed by network.

Steps:

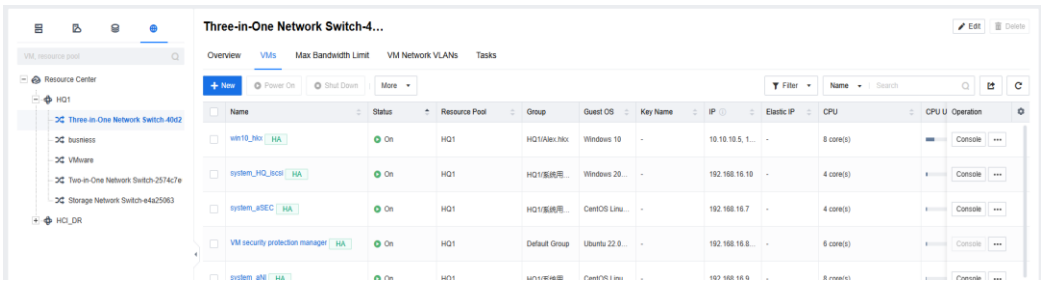
Step 1. Click **View by Network** on the left to display resource pools by virtual switch.



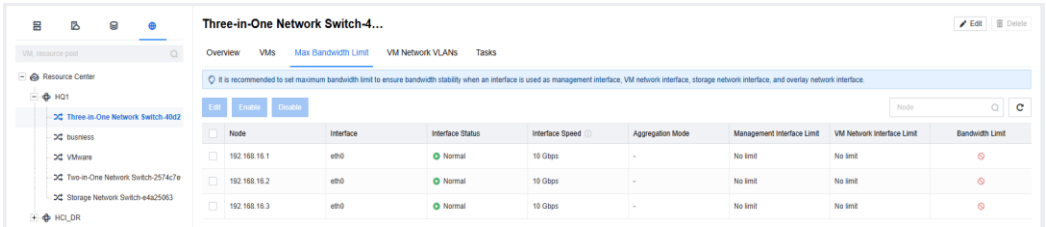
Step 2. Click a virtual switch to view the **Overview**, including the **Network Type** and **Connected Nodes and Interfaces**.



Step 3. Click **VMs** to view, create, edit, or delete connected VMs.

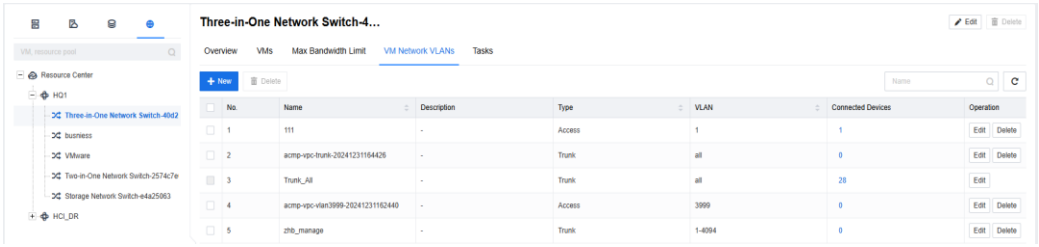


Step 4. Click **Max Bandwidth Limit** to view the status and bandwidth limit of the connected nodes' interfaces.

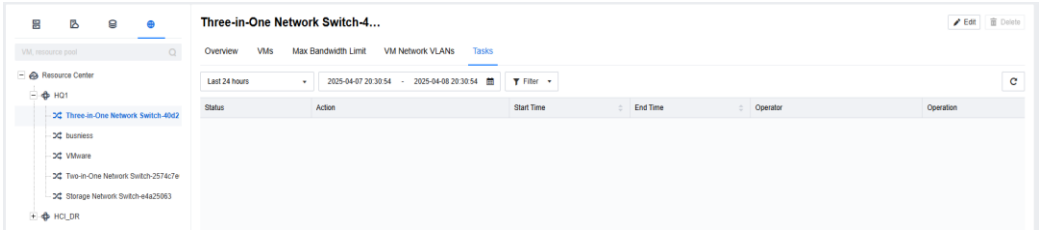


Step 5. If the virtual switch has the network type of VM network, click **VLANs**

in VM Network to view VLAN information.



Step 6. Click **Tasks** to view tasks.



4.2.2 Server Group Management

Function Description:

Sangfor SCP supports the division of multiple hosts into dedicated server groups. The dedicated server group combines designated physical hosts in the cluster. It supports single or multiple computers. Computing resources between groups are isolated, and storage resources are shared within the cluster. It can be allocated to tenants or operation administrators, who exclusively share the computing resources in the group.

Precautions:

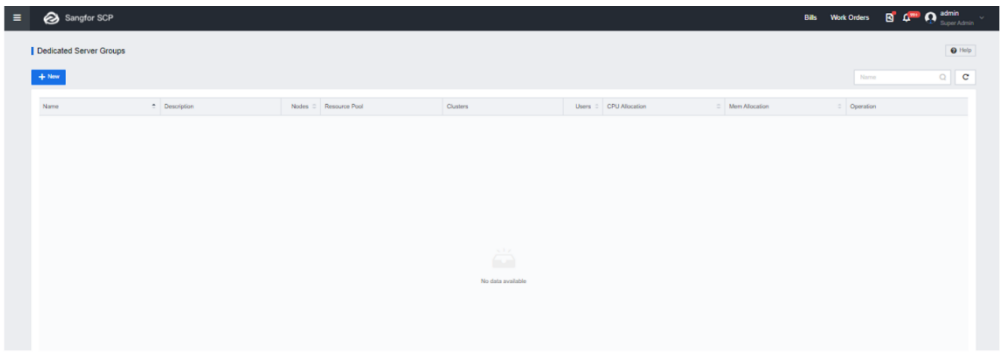
Suppose all the resource pools currently managed by SCP have been assigned to tenants or operation administrators. In that case, a new dedicated server group cannot be created, and a new resource pool needs to be expanded. If you need to allocate a dedicated server group in the private cloud scenario, please create a dedicated server group after initializing the resource pool.

Prerequisite

SCP has a brand-new resource pool that has not been allocated to tenants or operation administrators and is not running virtual machines.

Steps:

Enter the **Resources Overview** > **Dedicated Server Groups** interface and follow the process prompts to create a new server group.



4.2.3 Cluster Management

4.2.3.1 Add Cluster

For detailed operation steps, please refer to the **Adding Physical Resources** chapter.

4.2.3.2 Login Cluster

Function Description:

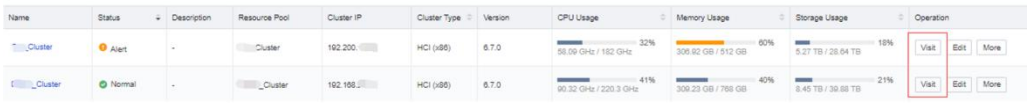
The platform administrator can log in to the managed HCI cluster from the SCP platform to perform more fine-grained cluster management.

Prerequisite

The SCP platform has successfully managed the cluster.

Steps:

Step 1. The platform administrator logs in to the SCP platform selects **Resources Overview** > **Cluster**, enters the cluster list interface, and clicks the **Visit** button to log in to the corresponding cluster.



4.2.3.3 Edit Cluster

Function Description:

The platform administrator can log in to the managed HCI cluster from the SCP platform to perform more fine-grained cluster management.

Prerequisite

1. After a cluster is associated with a resource pool, the storage tag of the cluster cannot be modified.
2. After the cluster is associated with the resource pool, the cluster cannot be deleted.

Precautions:

The SCP platform has successfully managed the cluster.

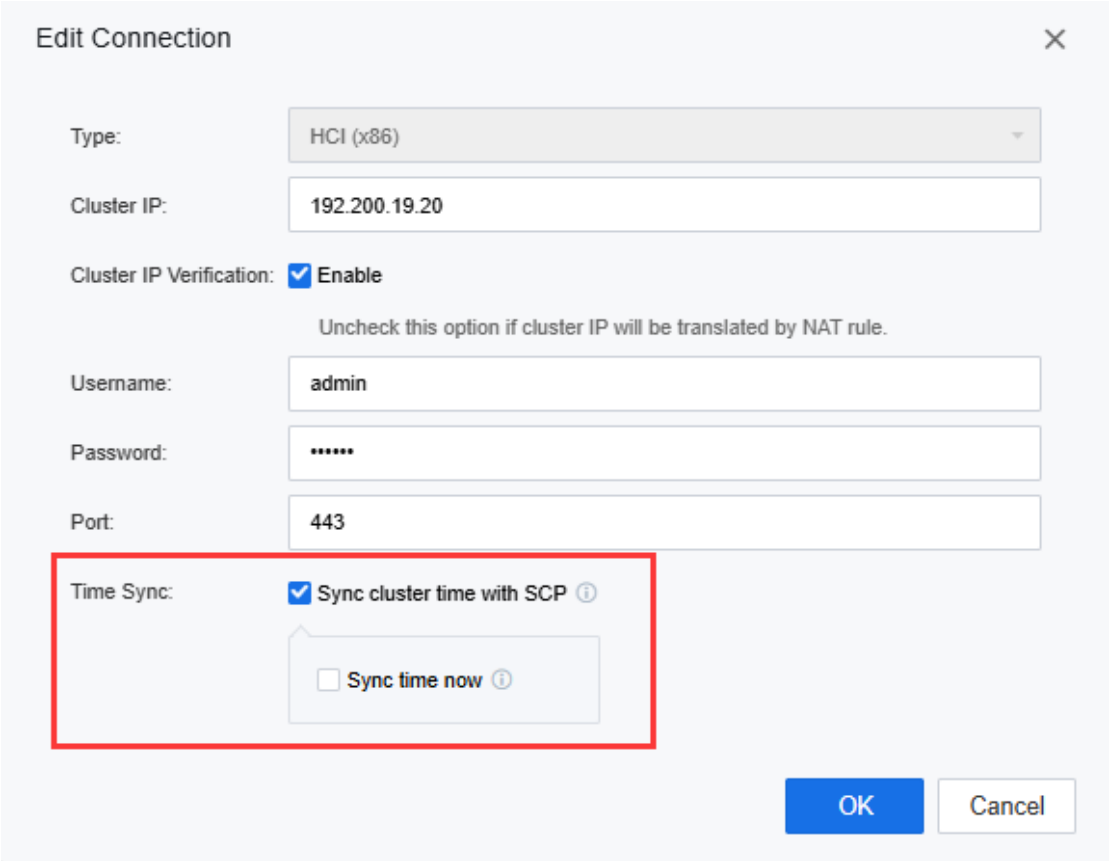
Steps:

Step 1. Platform administrator login to the SCP platform selects **Resources Overview** > **Cluster**, enters the cluster list interface, and clicks **Edit** to modify the name and description of the cluster.

Step 2. Click **More** to **Edit Connection**, **Configure storage tag**, **Configure Default keyboard layout**, and **Delete cluster** operations.



- **Configure Connection Information:** you can modify the cluster connection information. Note: Supports enabling **Time Sync Between Cluster and SCP**.



- **Tag Storage:** you can modify or customize the storage performance.
- **Configure The Default Keyboard Layout:** Currently supports six keyboard layout modes: **English (United States), English (Ireland), German, Spanish, French**, and **Italian**. After the configuration, new virtual machines under the cluster will use this configuration by default. After the configuration is changed, the original virtual machine that inherits the default configuration of the cluster will use the new keyboard configuration after the restart.
- **Delete Cluster:** When the cluster is not associated with the resource pool, you only can delete the cluster.

4.2.3.4 Delete Cluster

Function Description:

Due to certain requirements, the SCP platform is no longer required to manage a certain cluster, and the cluster can be deleted in the SCP.

Precautions:

This operation will delete related data and cannot be recovered. Please operate

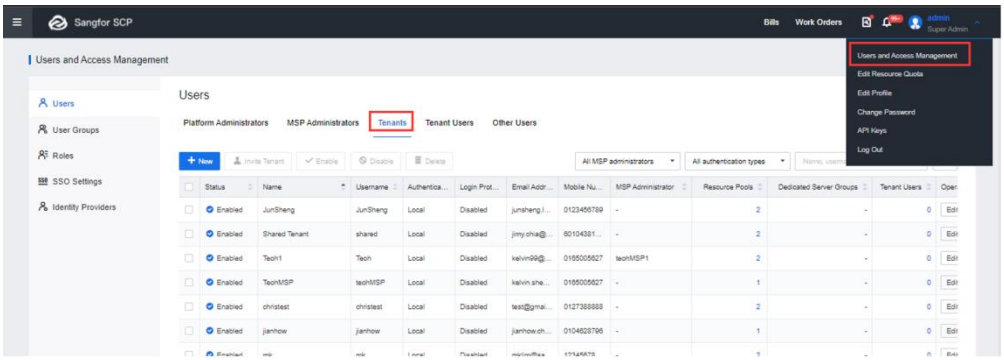
with caution.

Prerequisite

1. To delete a cluster, you must first delete the associated resource pool.
2. If you want to delete a resource pool, you need to delete the tenants created under the resource pool first.
3. Deleting a cluster will reclaim the license of the corresponding cluster.

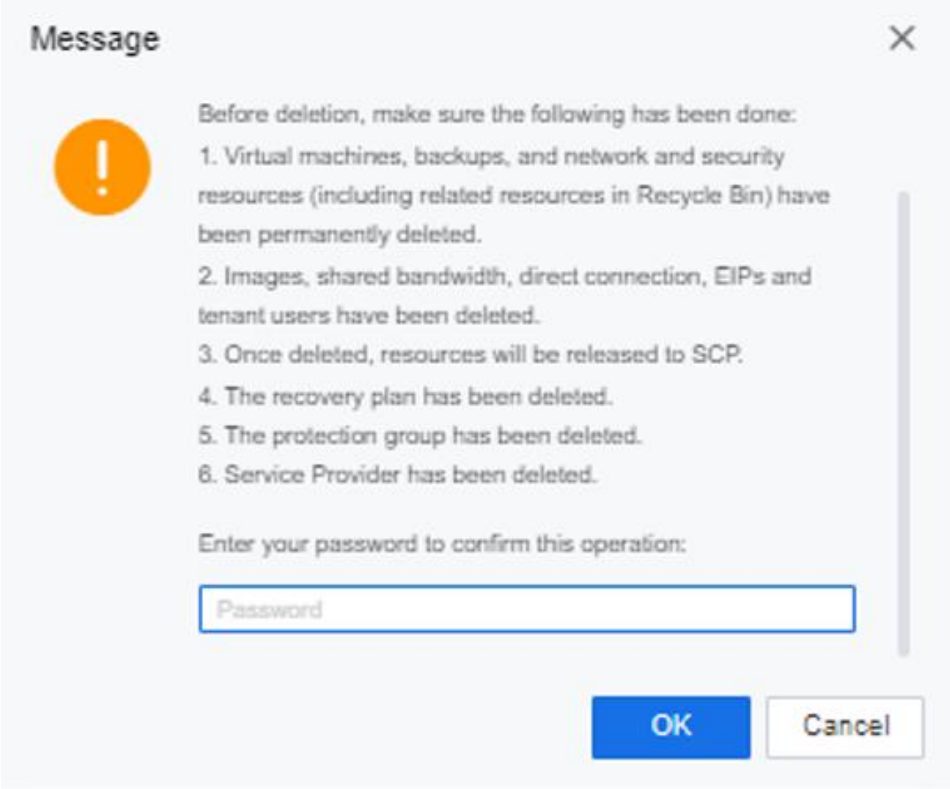
Steps:

Step 1. Login to the SCP platform and clicks **User and Access Management** > **Tenant** to enter the tenant management interface.

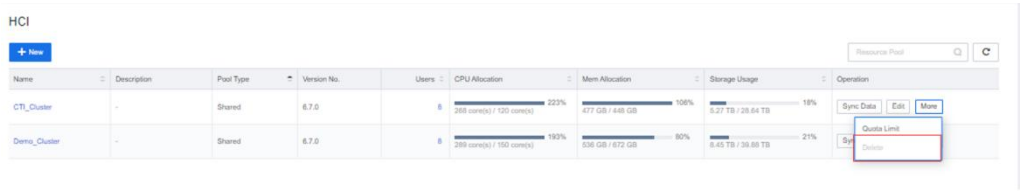


Step 2. Delete the tenant and tenant users created under the resource pool, enter the password and click the **OK** button once you confirm the operation.





Step 3. After the tenants and tenant users under the resource pool are deleted, proceed to **Resource Overview** > **Resource Pools**, click the **Delete** button, and click **Confirm** in the pop-up window.



Step 4. Under **Resource Overview** > **Cluster**, find the cluster you want to delete, click **More** > **Delete**, and click the **OK** button in the pop-up window to delete the cluster.



4.2.4 Physical Machine Management

Function Description:

Some applications with extremely high-performance requirements are generally deployed on physical servers, such as core databases and high-

performance computing applications. Sangfor Cloud Platform (SCP) provides the function of managing physical machines and provides dedicated physical servers for applications to ensure the high performance of core applications and stability. By setting the IPMI port of the physical server, SCP can realize the management, monitoring, alarming and other operations of the physical server.

Precautions:

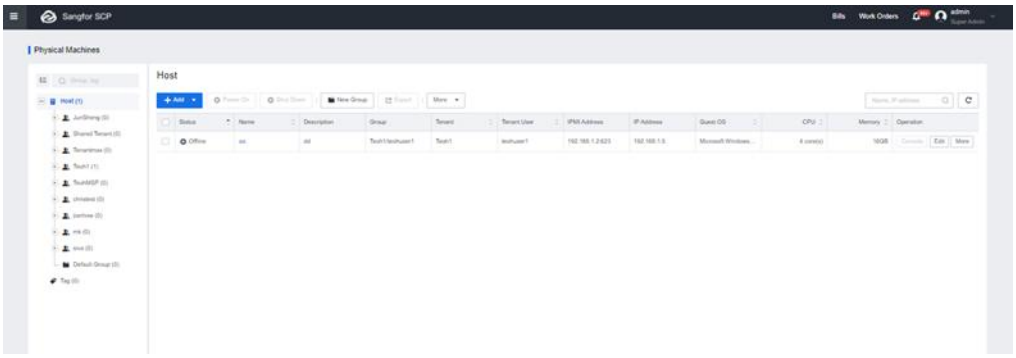
None.

Prerequisite

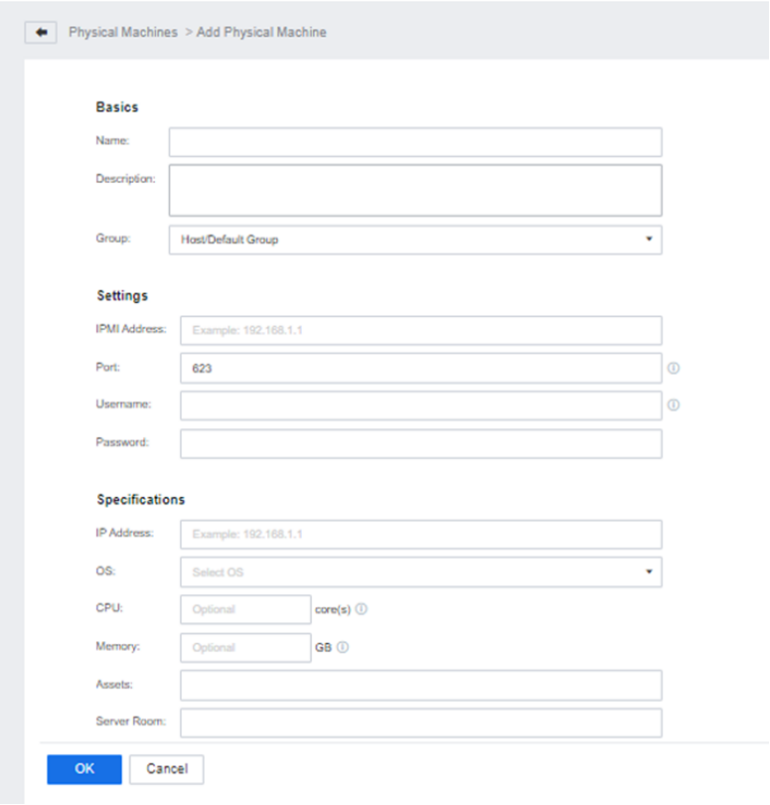
The SCP needs to communicate with the IPMI port of the physical server.

Steps:

Step 1. Log in to the SCP platform as the admin administrator, select **Resource** > **Physical Machine**, and enter the physical machines management interface.



Step 2. Click **Add** to add physical machines, which support single addition and batch addition.



Step 3. After completing the addition, you can view the added physical machines in the physical machine list.

Step 4. Click **Console** to redirect to the server BMC login page.

Step 5. Click **More** to power on, shut down the physical machine, and assign the physical machine to the tenant.

4.2.5 Third-Party Public Cloud

4.2.5.1 Cloud Account

4.2.5.1.1 Add Cloud Account

Refer to **Section 4.2.5.2.1 Create Cloud Environment**.

4.2.5.1.2 Delete Cloud Account

Function Description:

Administrators can delete cloud accounts.

Precautions:

After a cloud account is deleted, the associated cloud environment and resources will be cleared and cannot be restored, without affecting resources on the third-party cloud platform.

Prerequisite:

A cloud agent has been added.

Steps:

Step 1. Log in to SCP as an administrator.

Step 2. Go to **Resources** > **Resource Overview** > **Third-Party Public Cloud** > **Cloud Environment** > **Account Management**.

Step 3. Click **Delete** of an account.

4.2.5.2 Cloud Environment

4.2.5.2.1 Create Cloud Environment

Function Description:

SCP supports managing Alibaba Cloud and adding its regions as cloud environments. The created cloud environments can be allocated to tenants to use the Elastic Compute Service (ECS) of Alibaba Cloud directly on SCP.

Precautions:

1. It is not supported to manage the same cloud environment with different access keys of an Alibaba Cloud account.
2. Adding more than 10 cloud environments to an Alibaba Cloud account requires payment due to Alibaba Cloud's monthly free API query limit.
3. Please recharge overdue Alibaba Cloud accounts on the Alibaba Cloud console; otherwise, service unavailable will be reported when collecting cloud environment data.

Prerequisite:

1. The SCP IP address can communicate with the internet.
2. An access key ID and secret access key of an Alibaba Cloud account have been obtained, which are unique credentials for accessing Alibaba Cloud APIs. The secret access key works like a login password and serves to sign the access parameters to prevent them from being tampered with. You can

log in to the Alibaba Cloud console, place the cursor on your profile in the upper right corner, and click **Access Keys** to obtain them.

Steps:

Step 1. Go to **Cloud Environment** > **New**.

Step 2. Add an account as follows:

- **Type**: Alibaba Cloud.
- **Add Account**: Select **Create one** (**Use existing one** can be selected subsequently).
- **Account Name**: Custom Cloud Account.
- **Access Key ID**: Obtain from the customer.
- **Secret Access Key**: Obtain from the customer.
- **Sync Interval**: Resources allocated to the account by Alibaba Cloud will be synced to SCP at a specified interval, which is 60 minutes by default. The shorter the interval is, the more SCP resources will be occupied.

Step 3. Click **Next** and select the region where the customer's VMs on Alibaba Cloud are located to create the cloud environment.

4.2.5.2.2 Allocate Cloud Environment

Function Description:

Administrators can allocate cloud environments to tenants as dedicated resource pools unavailable to other tenants.

Precautions:

After a cloud environment is allocated to a tenant, the VMs in it cannot be allocated to other tenants.

Prerequisite:

A cloud environment has been created.

Steps:

Step 1. Go to the **Cloud Environment** page.

Step 2. Click **More** of the cloud environment then **Allocate**, select a tenant, and click **OK**.

4.2.5.2.3 Deallocate Cloud Environment

Function Description:

Administrators can deallocate cloud environments.

Precautions:

After a cloud environment is deallocated, it will be unavailable to the tenant.

Prerequisite:

A cloud environment has been allocated to a tenant.

Steps:

Step 1. Go to the **Cloud Environment** page.

Step 2. Click **More** of the cloud environment then **Deallocate**, and click **OK**.

4.2.5.2.4 Delete Cloud Environment

Function Description:

Administrators can delete cloud environments.

Precautions:

After a cloud environment is deleted, local synced data of resources from it will be cleared, without affecting resources on the third-party cloud platform.

Prerequisite:

A cloud environment has been created.

Steps:

Step 1. Go to the **Cloud Environment** page.

Step 2. Click **More** of the cloud environment then **Delete**, and click **OK**.

4.2.5.3 Virtual Machine

4.2.5.3.1 Create Virtual Machine

Function Description:

Administrators can create and use VMs on managed Alibaba Cloud directly on SCP for unified O&M.

Precautions:

None.

Prerequisite:

The Alibaba Cloud account balance is sufficient.

Steps:

Step 1. Go to **Third-Party Public Cloud** > **Alibaba Cloud** > **New**.

Step 2. Select a cloud environment and availability zone and click **Next**.

Step 3. Select the payment type and complete the configuration information such as the VM count and specifications to create elastic VMs.

Step 4. Click **Remote Connection** of a created VM and enter the VNC password to access its console. If you forget the password, click **More** to reset it.

4.2.5.3.2 Allocate and Deallocate Virtual Machine

Function Description:

Administrators can allocate and deallocate VMs to and from tenants.

Precautions:

A VM that has been allocated to a tenant cannot be allocated to another tenant.

Prerequisite:

A VM has been created.

Steps:

Step 1. Go to the **Alibaba Cloud** page.

Step 2. Click **More** of the VM then **Allocate**, select a tenant or tenant user, and click **OK**.

Step 3. Click **More** of the VM then **Deallocate** to deallocate the VM allocated to a tenant to the platform or the VM allocated to a tenant user to the platform or a tenant.

4.2.5.3.3 Delete Virtual Machine

Function Description:

Administrators can delete VMs.

Precautions:

After a VM is deleted, all its resources and information will be cleared, without affecting resources on the third-party cloud platform.

Prerequisite:

A VM has been created.

Steps:

Step 1. Go to the **Alibaba Cloud** page.

Step 2. Click **More** of the VM then **Delete**, and click **OK**.

4.3 Compute

4.3.1 Virtual Machine Management

As one of the basic units of Sangfor's SCP platform to carry services, the virtual machine can manage the entire life cycle of the virtual machine: creation, startup, shut down, import, export, deletion, allocation, revoke, etc.

4.3.1.1 Create a Virtual Machine.

Function Description:

The SCP platform supports ISO and built-in (HCI images) to create a new virtual machine and import existing virtual machines from the local node.

Prerequisite

When using an image to create a virtual machine, the required ISO image has been uploaded, or the HCI built-in image has been created.

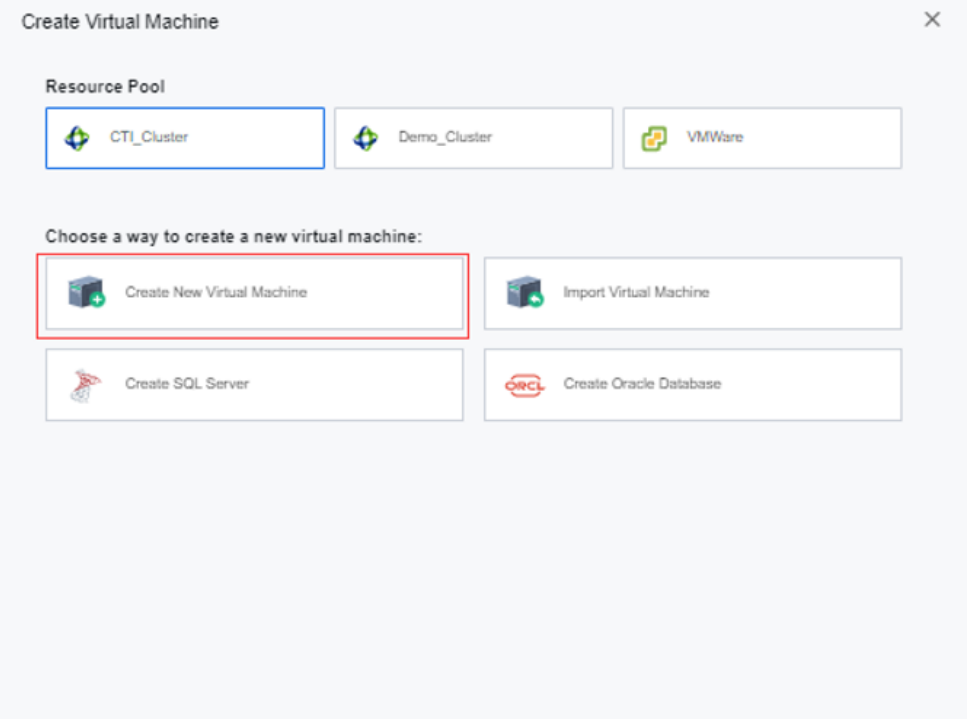
Precautions:

1. You need to enter the console to manually install the operating system for the virtual machine created through ISO.
2. The virtual machine created by the built-in image can be used directly after creation without installing the operating system manually.

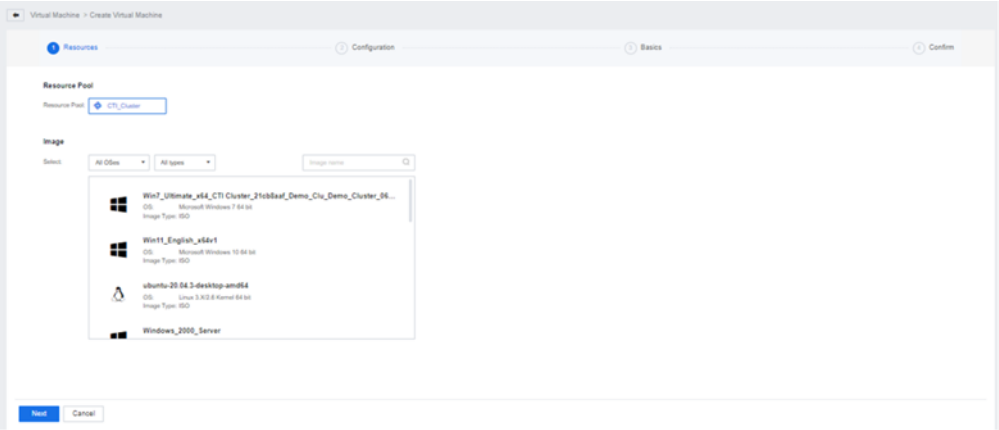
Steps:

1. New virtual machine creation

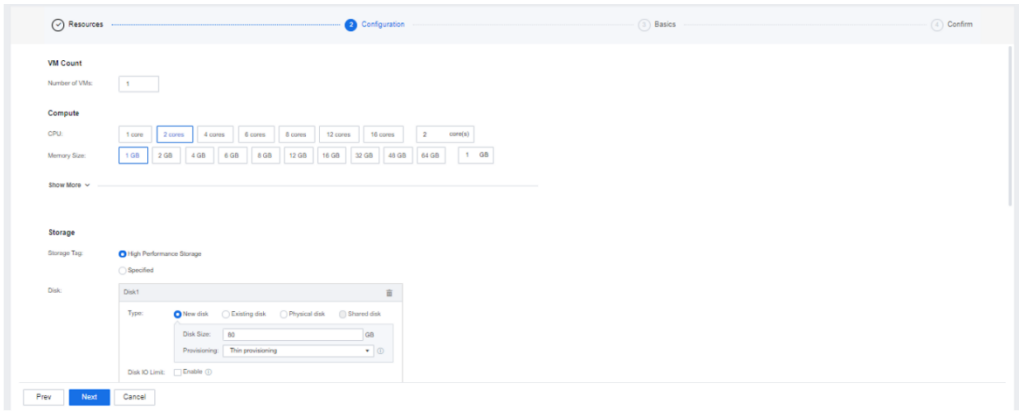
Step 1. Login to the SCP platform, select **Compute** > **Virtual Machine**, click the **New** button, and select **Create New Virtual Machine.**

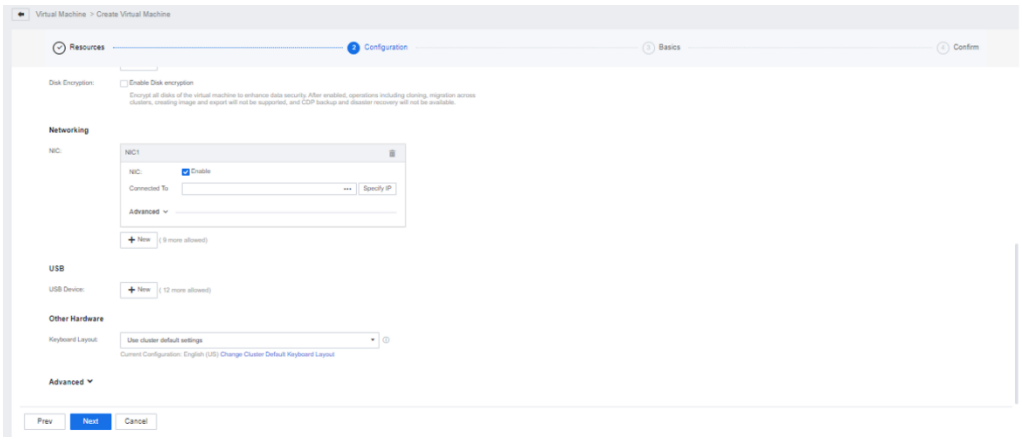


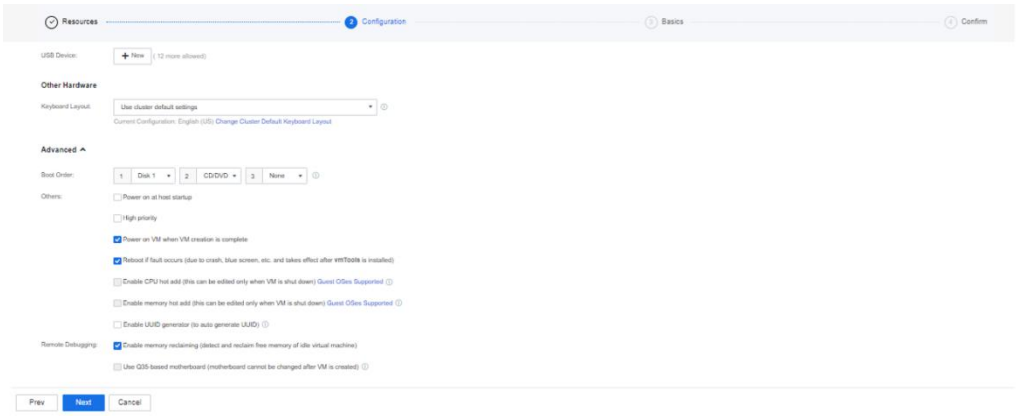
Step 2. Select the resource pool where the new virtual machine is located, select the required image, and click the **Next** button.



Step 3. Enter the Configuration interface.







A. Compute

CPU: The number of vCPU cores allocated to the virtual machine does not exceed the running node's total number of physical CPU threads.

Memory size: The virtual machine's memory allocation does not exceed a single node's memory.

Total number of cores: The number of virtual sockets * number of cores per socket.

CPU Clock Speed Limit: If you check the **Enable** checkbox, you can configure the highest total clock speed of a node in the cluster.

NOTE

1. SCP needs to manage HCI version 6.7.0 and above.
2. If the disk IO limit is too low, the virtual machine may not start and run normally. Please set it carefully. Please set it carefully.
3. CPU Clock Speed limit value range: 100MHz-1000GHz.
4. After the virtual machine runs for a week, the system will take the average clock speed (0 will not be calculated) for a recent period (maximum one month) as the recommended clock speed limit value. The value will be displayed in the input box after checking the **Enable** checkbox.

Huge page memory: Enabling huge page memory for a specific application can improve the virtual machine's performance, but disks will be pre-allocated. After the Huge page memory is enabled, the virtual machine's memory reclamation mechanism will be disabled. Prioritize memory usage and improve business performance.

Run Location: The run location specifies which node's CPU and memory resources are used when the virtual machine is running, and you can select and specify a node automatically. When the **Storage location** is selected as a stretched volume, you can also specify the run location of the virtual machine as a fault domain. When specified as a fault domain, you can set priority to run at the selected location or must run at the selected location.

B. Storage

Storage Tag: You can select **High Performance Storage** or **Specified.** You may choose the preferred datastore if Specified is selected.**Storage Policy**: The default policy stores two replicas, while the HA policy stores three replicas.

Disk: Virtual machine disk allocation, including the following four allocation methods.

New disk

Dynamic provisioning: According to the data occupancy, the storage space is dynamically allocated. While improving the performance, the storage space

utilization rate can also be increased. The maximum capacity is 8T.

Thin Provisioning: According to the actual data occupancy, the storage space is allocated on demand, saving storage space. The maximum capacity is 63T.

Pre-allocating: Pre-allocate a fixed storage space, which can improve disk performance but will take up more storage space. The maximum capacity is 4T.

NOTE

1. The disks with the built-in images are configured as thin provisioning by default, and the disk allocation method is not supported to be modified.
2. Two-node VS storage does not support the dynamic provisioning of disks.
3. When tenants create a virtual machine and add disks, they prioritize storage that supports dynamic provisioning by default.
4. The conversion of the disk allocation mode only supports one-way operation, **thin provisioning > dynamic provisioning > pre-allocating**. It can only be modified from low-performance mode to high-performance mode and cannot be changed from high-performance mode to low-performance mode.
5. The disk allocation methods are simplified for operations involving the virtual machine's rapid pull-up (backup recovery, cloning, disaster recovery, etc.).

Existing disk

Use the disk image file of the virtual machine created earlier, such as a qcow2 format file.

Physical disk

Mount the physical storage directly to the virtual machine for use.

Shared disk

Choose an existing shared virtual disk, generally used to deploy Oracle RAC and other applications requiring shared disks.

- **Disk IO limit**

  You can configure the IO limit of each disk of the virtual machine CPU.

NOTE

1. Need to manage HCI version 6.7.0 and above.
2. If the disk IO limit is too low, the virtual machine may not start and run normally. Please set it carefully. Please set it carefully.
3. After the virtual machine runs for a week, the system will take the average value of a recent period (maximum one month) as the recommended disk IO limit value. It will be displayed in the input box after checking the **Enable** checkbox.
4. Supported IO limit range:

1. **Max Read Speed** and **Max Write Speed**: 128KB/s to 102400MB/s.
2. Max Read IOPS and Max Write IOPS: 16 to 2147483647.

Disk encryption: All virtual machine disks will be encrypted if you check the **Enable disk encryption** checkbox. Once enabled, the virtual machine will not support cloning, cross-cluster migration, mirroring and export operations, and CDP backup and disaster recovery functions.

C. Networking

Networking: Specify the connection location of the virtual machine's NIC. You can also set the IP address of the network card. You can specify the adapter model and MAC address in the advanced options.

- **Adapter Model**: The default is Virtio.
- **MAC address**: Set the MAC address of the network card and keep it automatically obtained, or you can click **Specify IP** to specify it manually.
- **Jumbo frame receiving function**: If the jumbo frame receiving function is not enabled, TCP jumbo frame messages will be processed by TCP fragmentation, and non-TCP jumbo frame messages will be processed by IP fragmentation before entering the virtual network card. IPsec equipment may not support Network devices that receive jumbo frames and need to turn off this option.

USB: Map the USB device on the physical server to the virtual machine, or the virtual machine deployed on the virtualization platform needs to use the USB device. The USB device plugged into the virtualization platform needs to be

mapped to the virtual machine.

Other hardware: Configure the keyboard layout of the virtual machine. Here you can inherit the cluster default keyboard layout, or you can configure the keyboard layout for the virtual machine separately. For cluster keyboard layout settings, please refer to the **Edit Cluster** chapter.

NOTE

1. Only the shutdown virtual machine supports modifying the keyboard layout.
2. Need to manage HCI version 6.7.0 and above.

D. Advanced Options

Boot order: The boot sequence of the virtual machine system. This option can be edited when shutting down or creating a virtual machine.

Power on at host startup: The server starts the virtual machine automatically when it is turned on.

High priority: Pre-allocate resources according to the memory specifications of the user's virtual machine. This resource is exclusively used by the virtual machine and will not be preempted by other virtual machines, and memory will not be reclaimed.

Reboot if fault occurs: When the virtual machine does not respond (such as stuck, blue screen), it will automatically restart, and the virtual machine will take effect after restarting. This option is selected by default.

Enable CPU hot add/Enable memory hot add: The booted virtual machine can manually add CPU and memory. Note that the support levels of different operating systems are different. When operating, check the system support list first, and this feature requires the virtual machine to install vmtools support. This option can be edited when shutting down or creating a virtual machine. After this configuration takes effect, the memory and CPU can be hot-added when the virtual machine is powered on. When the virtual machine is edited in the power-on state, the number of CPU and memory can be changed. The size can be modified to be higher than the originally allocated CPU and memory size.

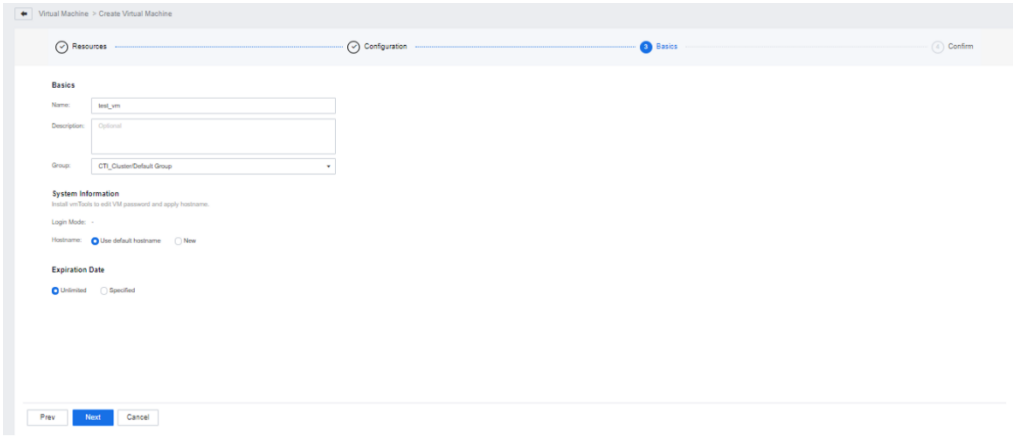
Enable UUID generator: The unique identifier of the virtual machine, some

software needs to obtain the virtual machine UUID to use it. After disabling the UUID, when re-enabled, the user can choose to use the new UUID or continue to use the original UUID. Please decide whether to regenerate the UUID according to the actual needs of cloned and template-deployed virtual machines.

NOTE

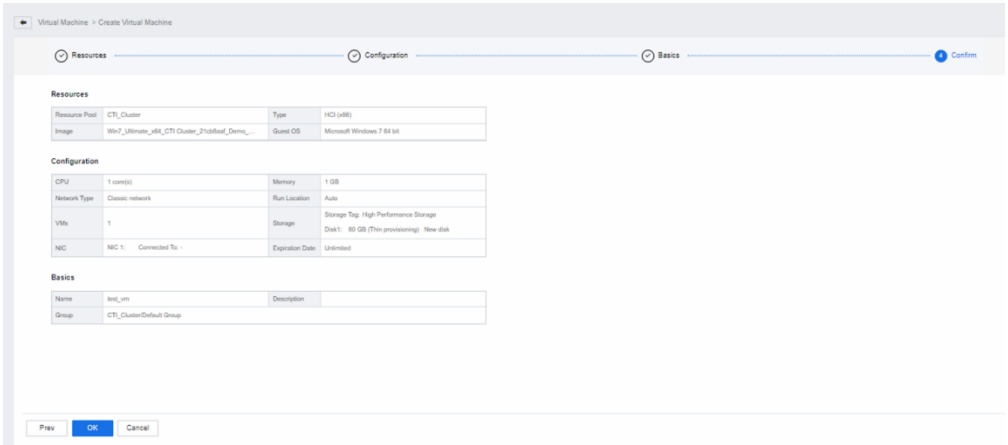
For version 6.X and above, it will only take effect when Linux is checked, and the previous version will not take effect. The UUID is not used when joining the AD windows SID. Generally, some special software authorization will use UUID.

Step 4. Enter the virtual machine name, description, belonging group, administrator's password, hostname, and expiration date according to actual needs.



System Information: Users are not recommended to modify by themselves.

Step 5. Finally, confirm the information. After confirming it is correct, click **OK** to create the virtual machine.



2. Import Virtual Machine

Step 1. Log in to the SCP platform, select **Compute** > **Virtual machine**, and click the **Create** button.

Step 2. Select the resource pool where the new virtual machine is located and select **Import Virtual Machine** as the creation method.

Step 3. Select the OVA or VMA format file to be uploaded, select the group, running location, and storage of the upload virtual machine, and click **Import** to upload.

Step 4. After importing the virtual machine, its network card is not connected to any device. You can edit the virtual machine for configuration.

4.3.1.2 Edit Virtual Machine

Function Description:

The related configuration of the virtual machine can be adjusted by editing the virtual machine.

Precautions:

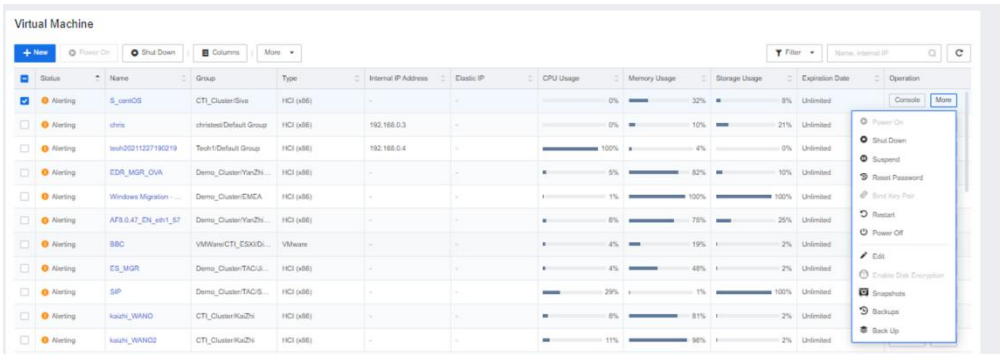
1. Some operations need to be performed with the virtual machine powered off.
2. Do not hot-plug the mapped disks when the virtual machine has made a raw disk mapping for more than two disks.
3. You can view the information on PCIe devices (NIC and cryptographic module) of your VM. You can add a cryptographic module to your VM in the HCI console but not the SCP console.

Prerequisite

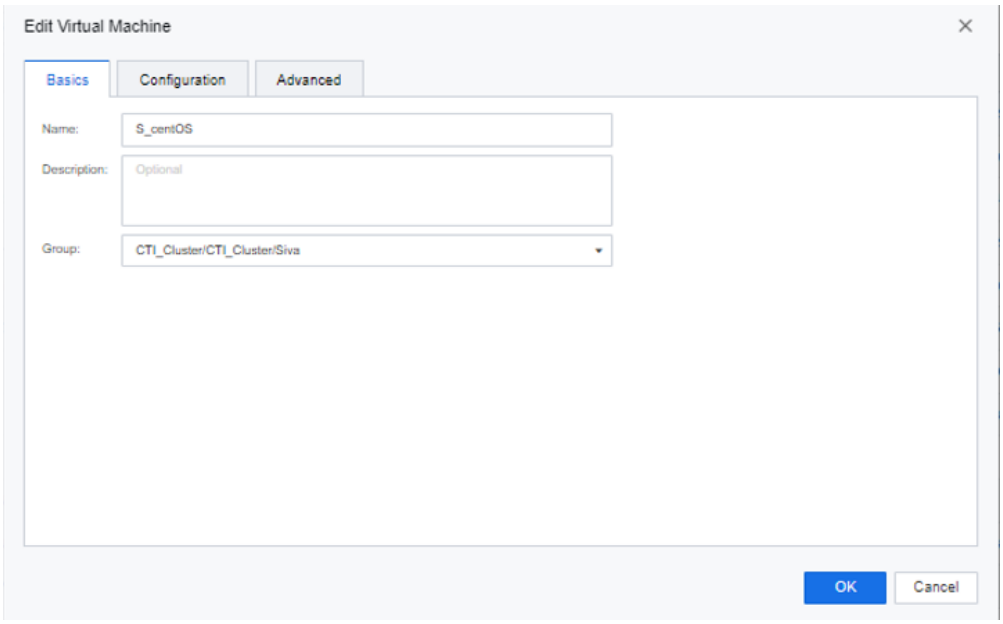
None.

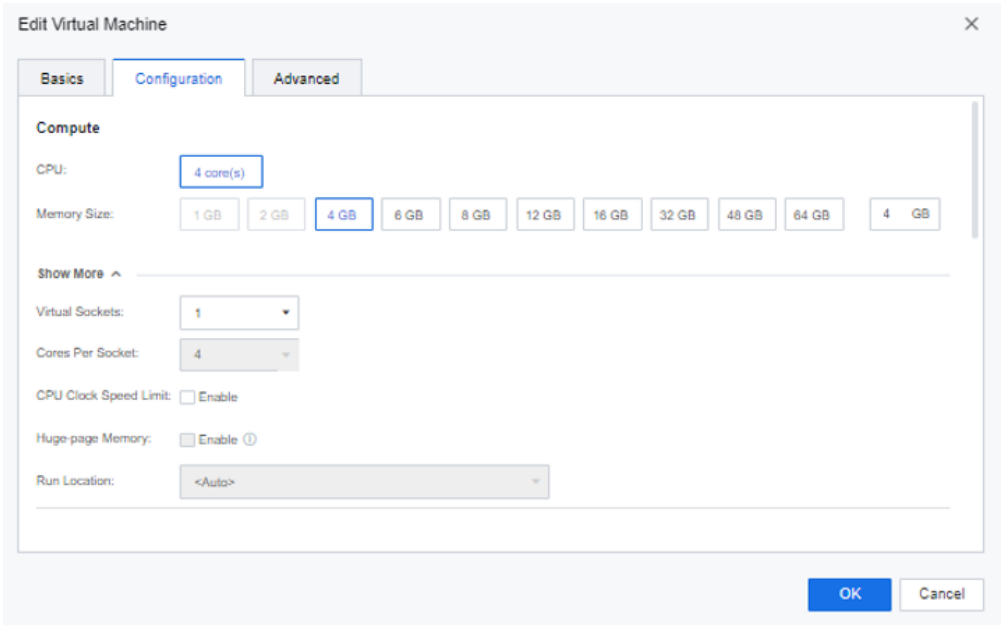
Steps:

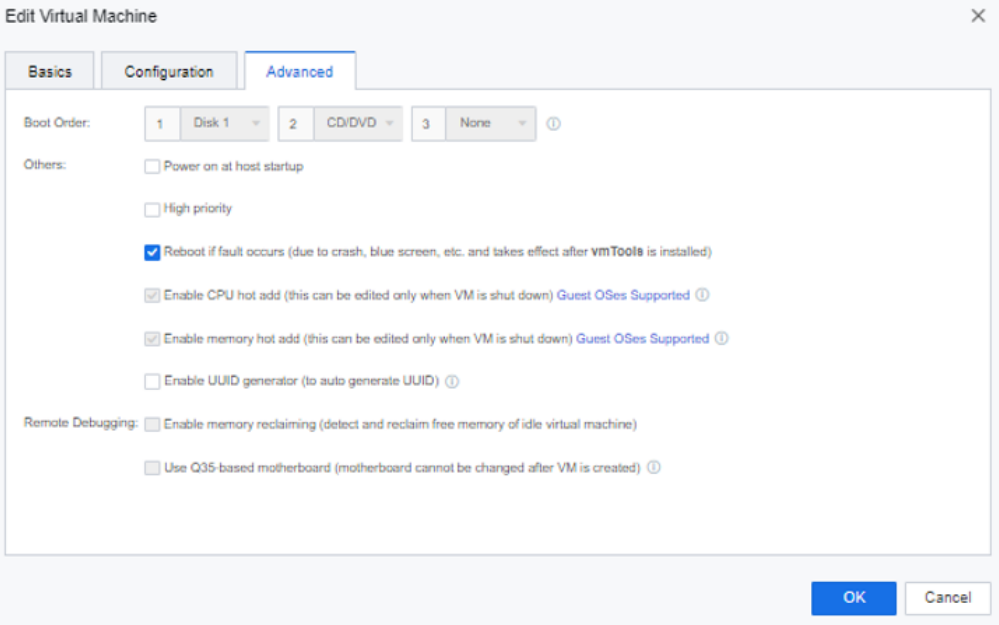
Step 1. Place the mouse cursor on the virtual machine that needs to be edited, and then click **More** > **Edit**.



Step 2. You can edit **Basic, Configuration**, and **Advanced** on the virtual machine edit page. Please refer to **Chapter 4.2.1.1 Create Virtual Machine** in this manual for more information.







4.3.1.3 Virtual Machine Details

Function Description:

The SCP platform supports viewing virtual machine details, including operating status, hardware configuration, backup data, operation audit, alarm logs, and VM scheduling records, and supports viewing and exporting monitoring trend charts for a customized period, and viewing various VM detail fields, such as **hostname**, **DUID**, **IAID**, **CBT Status**, and **Time Sync**.

Precautions:

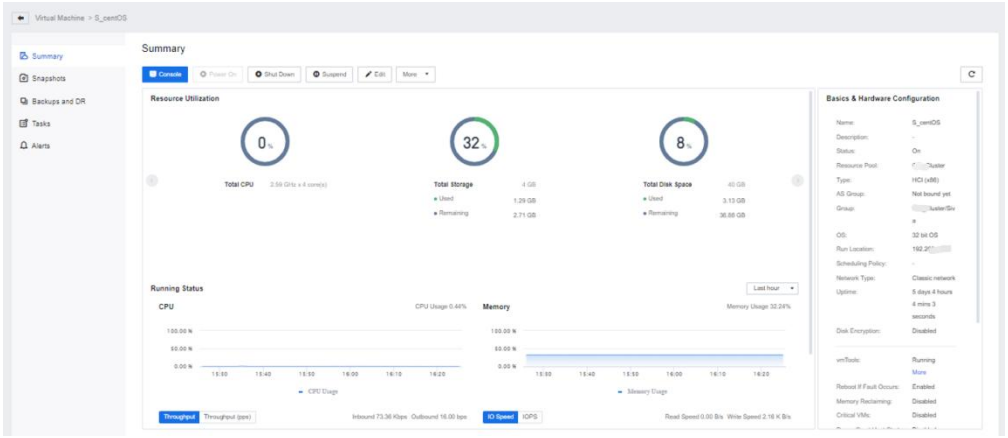
None.

Prerequisite

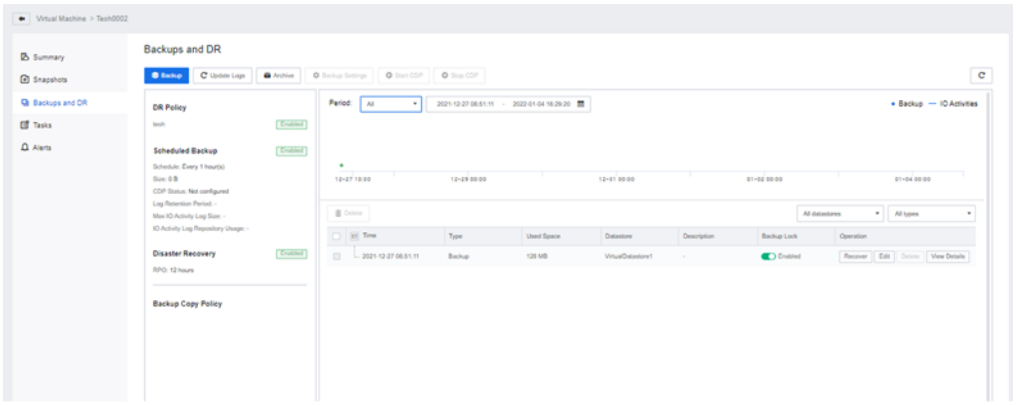
None.

Steps:

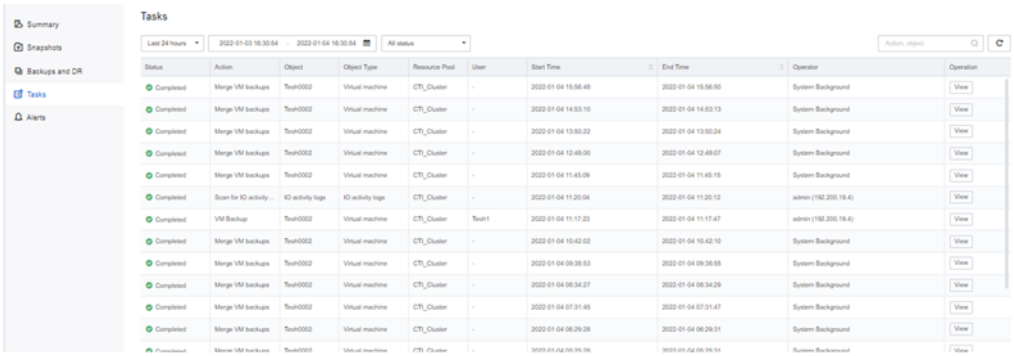
Step 1. Log in to the SCP platform, select **Compute** > **Virtual Machine** to enter the virtual machine list, find the target virtual machine, and click the virtual machine name to re-direct.



Step 2. Go to the **Backup and DR** page to view the backup data information.



Step 3. Go to the **Tasks** page to view virtual machine operation records.



Step 4. Enter the **Alerts** page to view historical alarm records.

4.3.1.4 Virtual Machine List

Function Description:

SCP displays all VMs in the VM list and supports displaying their tenants, **Guest OS**, **resource usage**, **Run Location**, **hostname**, **Scheduling Policy**, **Tags**, **CPU Clock Speed**, **Datastore**, **Storage Policy**, **Logical Space Used**, **Used Memory**, **Uptime**, and **Scheduled Backup**.

Precautions:

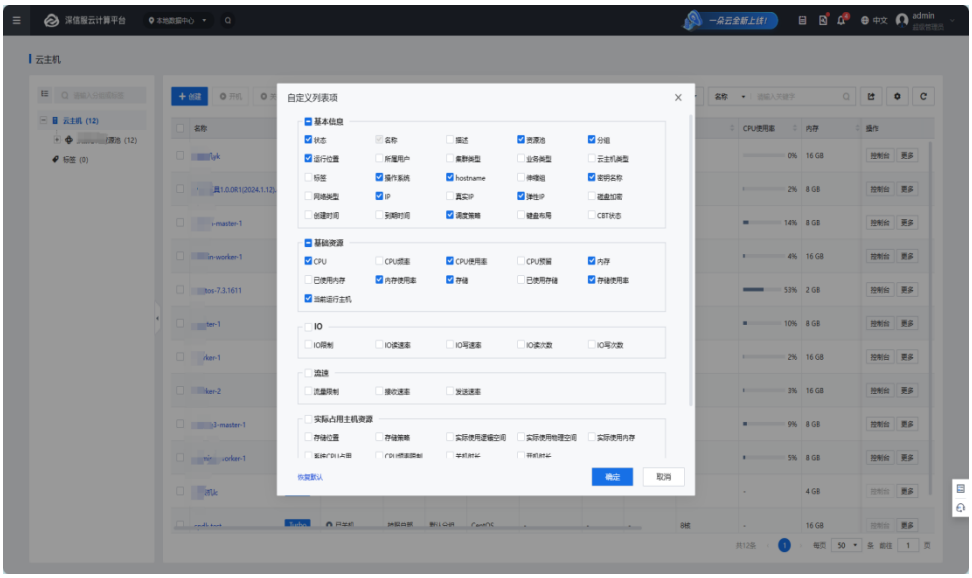
None.

Prerequisite:

None.

Steps:

Step 1. Log in to SCP, and then go to **Compute** > **Virtual Machines** to go to the VM list.



4.3.1.5 Set Validity

Function Description:

SCP platform supports setting a validity for the virtual machine, and the virtual machine that exceeds the validity will generate alarm messages.

Precautions:

1. The validity of the virtual machine is based on days, and the minimum granularity of the service life is set to days.
2. Clone a virtual machine with a lifespan, and the cloned virtual machine has an unlimited lifespan.
3. Only support the setting of the use period for the HCI virtual machine and not support the setting of the use period for the VMware virtual machine.
4. The virtual machine is about to expire or has expired. It will not affect any operation of the virtual machine. Only one new alarm log about expiring will

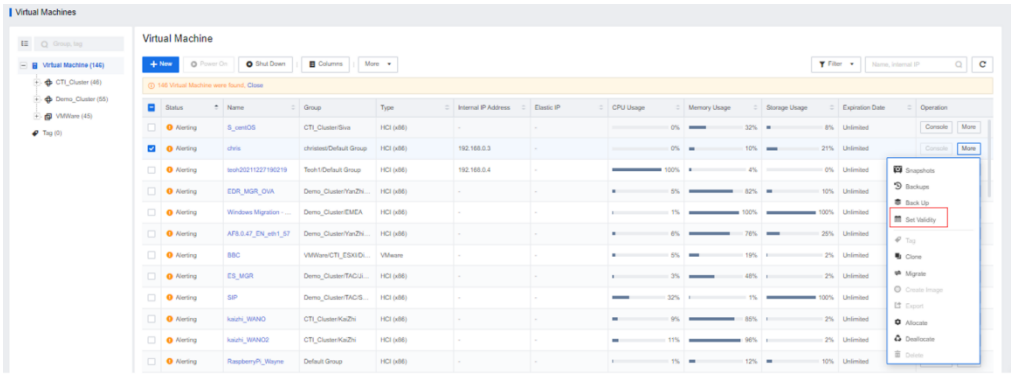
be added, and the virtual machine's status will be changed to an alarm.

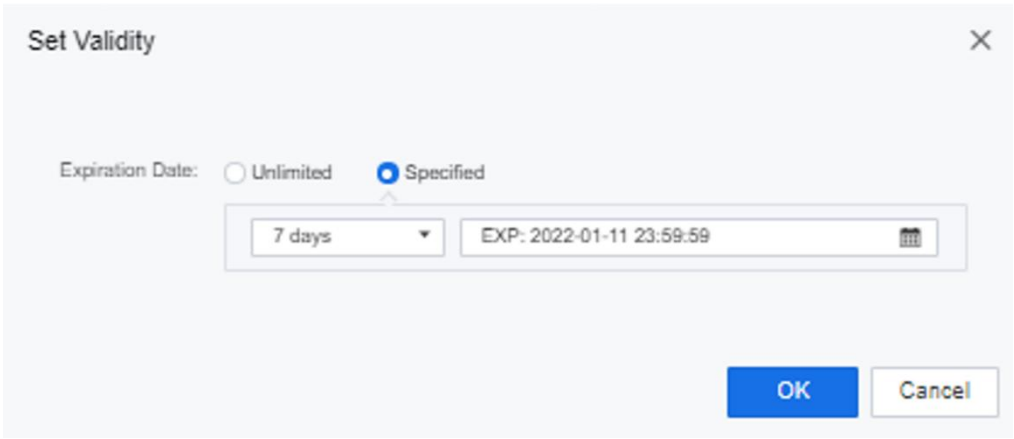
Prerequisite

None.

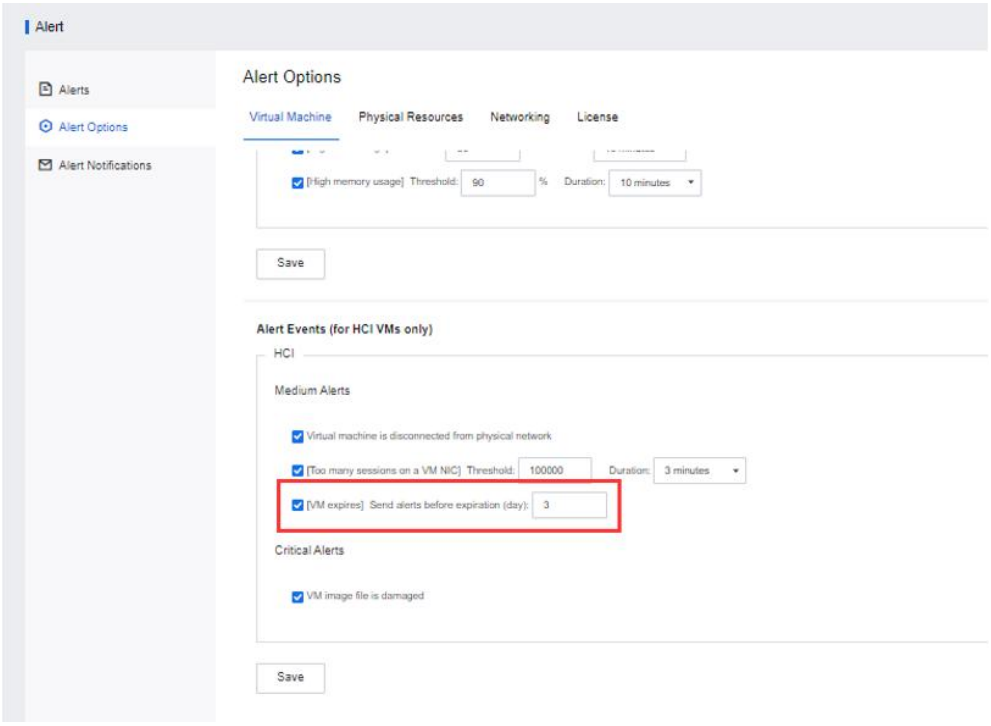
Steps:

Step 1. Log in to the SCP platform, select **Compute** > **Virtual Machine** to enter the virtual machine list, find the target virtual machine, and click the virtual machine name to **re-direct.**





Step 2. The admin can set the number of days of early warning of the virtual machine. The default is 3 days. Suppose you need to customize the number of days of early warning. In that case, you can remind xx days before the virtual machine life cycle expires in **Monitoring Center** > **Alerts** > **Alert Options**.



4.3.1.6 Export Virtual Machine

Function Description:

This function supports exporting virtual machines in VMA or OVA format. When exporting the list, you can choose to include **Run Location**, **hostname**, **Scheduling Policy**, **Tags**, **CPU Clock Speed**, **Datastore**, **Storage Policy**, **Logical Space Used**, **Used Memory**, **Uptime**, **Scheduled Policy**, etc.

Precautions:

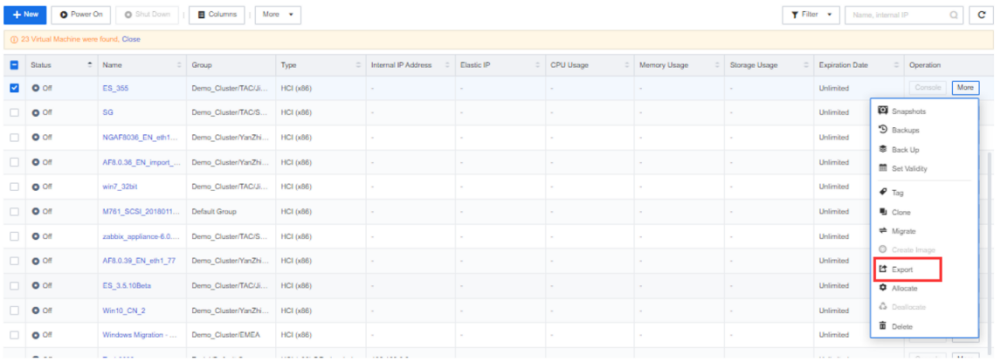
Only the shutdown virtual machine can perform the export operation.

Prerequisite

Virtual Machine already shut down.

Steps:

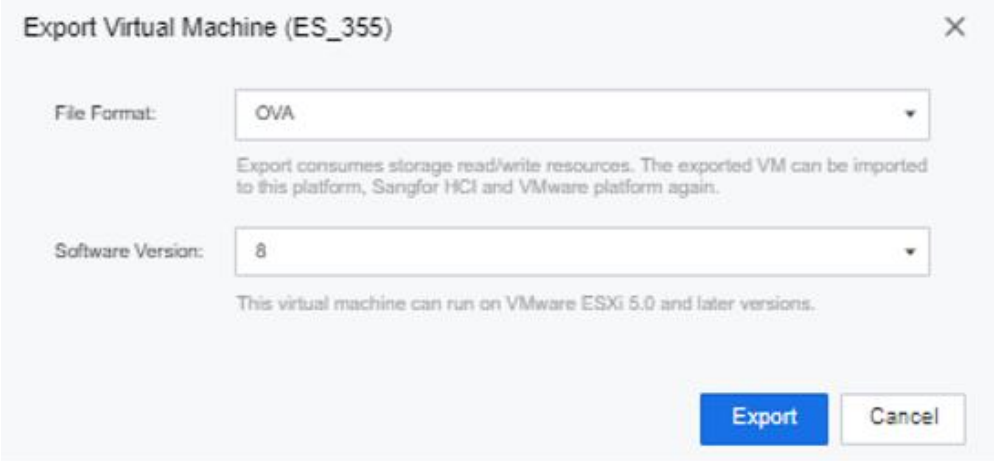
Step 1. Log in to the SCP platform, select **Compute** > **Virtual Machine**, select the virtual machine that needs to be exported, click the **More** button on the right, and click the **Export** option.



Step 2. Select the format that needs to be exported. OVA and VMA formats are available, and click the **Export** button.

NOTE

There are two formats, **VMA** and **OVA**, with different export options. To export in VMA format, you can directly click to start exporting. But to export to OVA format, you must select the **software version. T**he software version is the version number of VMware Station.



Step 3. Please wait for the virtual machine to produce and download the export file.

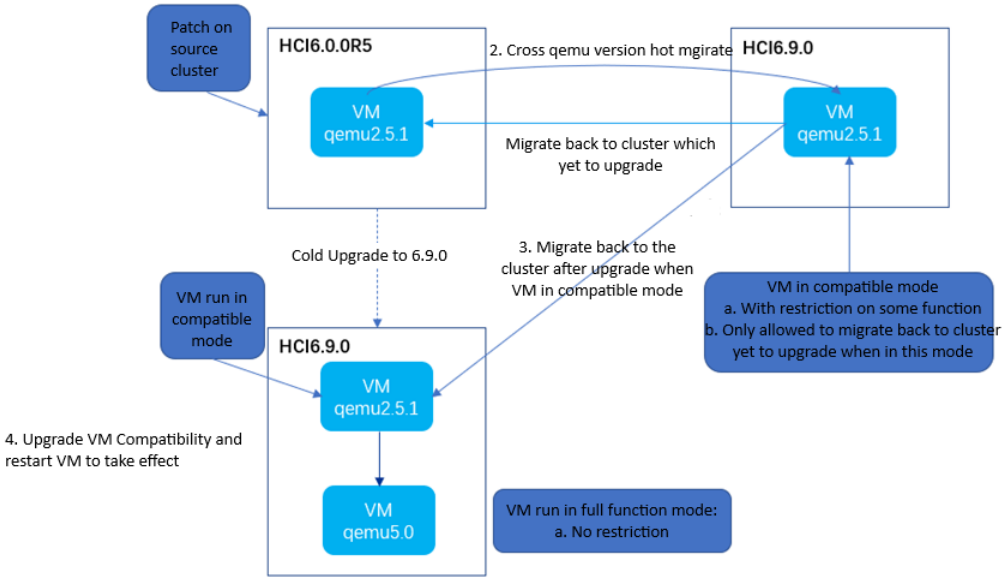
4.3.1.7 Migrate Virtual Machine

Function Description:

This function supports the migration of the virtual machine's running location and storage location and the migration of the virtual machine across resource pools.

Precautions:

3. The migration can be performed even for shut down VMs.
4. We recommend that you perform cross-cluster migration during off-peak hours, because data needs to be transmitted over the management network.
5. After cross-cluster migration is completed, the source VM will be shut down and moved to the recycle bin.
6. You can migrate multiple VMs across clusters simultaneously.
7. Supports setting **CPU Throttling** for the VMs to be migrated.
8. Supports setting **Concurrent Migration Tasks per Datastore** of a cluster. Range: 1-50, default: 1.
9. Supports setting **Concurrent Migration Tasks per Node** of a cluster. Range: 1-50, default: 2.
10. Bulk migration tasks must be executed one by one.
11. During bulk migration, the VMs must have the same destination datastore.
12. During cross-cluster migration, SCP may report an image damage error for the destination side. This is because SCP detects images every 30 minutes and will report this error if the detected image is being migrated. Of course, the image is not damaged.
13. Hot migration is not supported for VMs on which graphic card allocation and RDM have been performed in the HCI console.
14. HCI 6.9.0 and later support cross-cluster cross-version hot migration. (After patching, the VM will undergo an in-place active upgrade, with up to 1 second of business jitter.) After the migration, you need to upgrade the VM compatibility for the features of the new version to take effect. This process will restart the VM.



1. Currently, the versions in the following table support cross-version hot migration.

Type	Source Version	Destination Version
x86	6.0.0 R5	6.8.0/6.9.0
	6.2.0	
	6.3.0	
	6.3.0 R1	
	6.3.0 R2	
	6.3.0 R3	
	6.3.0 R1 (EN)	6.9.0 (EN)
	6.3.0 R2 (EN)	
ARM	6.2.0 ARM	6.9.0 ARM
	6.2.0 R1 ARM	
	6.2.0 R2 ARM	

Some kernel features take effect only after a restart.

Version	Feature Restriction
6.0.0 R5	The maximum memory is 960 GB. You cannot change the operating system of VMs. L3 cache is not supported. Disk space deallocation is not supported.

	Anti-escape is not supported for VMs. You cannot use a VirtIO NIC for a VM if vmTools is not installed on the VM.
6.2.0, 6.3.0 R1, and 6.3.0 R2	You cannot change the operating system of VMs. L3 cache is not supported. Disk space deallocation is not supported. Anti-escape is not supported for VMs. You cannot use a VirtIO NIC for a VM if vmTools is not installed on the VM.
6.2.0 ARM, 6.2.0 R1 ARM, and 6.2.0 R2 ARM	VM guest OS cannot be modified by editing the VM. L3 cache is not supported. Disk space cannot be deallocated. Graphic cards cannot be added. High Performance Mode cannot be enabled. Disks cannot be pre-allocated. Serial ports cannot be added. E1000 NICs are not supported.

2. After the cross-cluster cross-version hot migration, if you restart the VM without clicking **Upgrade VM Compatibility**, the VM is still a compatible VM.
3. The following are restrictions on some of the features of a compatible VM after the cross-cluster cross-version hot migration:

- If you export a compatible VM and then import it, the imported VM will not be a compatible one but a full-featured VM.
- If you back up a compatible VM and then recover it, the recovered VM will not be a compatible one but a full-featured VM.
- If you snapshot a compatible VM and then recover or clone it based on the snapshot, the new VM will not be a compatible one but a full-featured VM.
- If you clone a compatible VM, the new VM will not be a compatible one but a full-featured VM.

4. If you enable migration optimization, the VM will undergo an in-place active upgrade with up to 1 second of business jitter.
5. The following are further scenario-specific restrictions of cross-version hot migration:

- You can perform migration among clusters on the classic network but not VPC.
- Migration optimization is not supported for a VM if you have configured its memory hot add settings when it is powered on or if you have not restarted it after installing or uninstalling vmTools.
- Cross-QEMU cluster migration is not supported if the underlying system of the host is UOS.

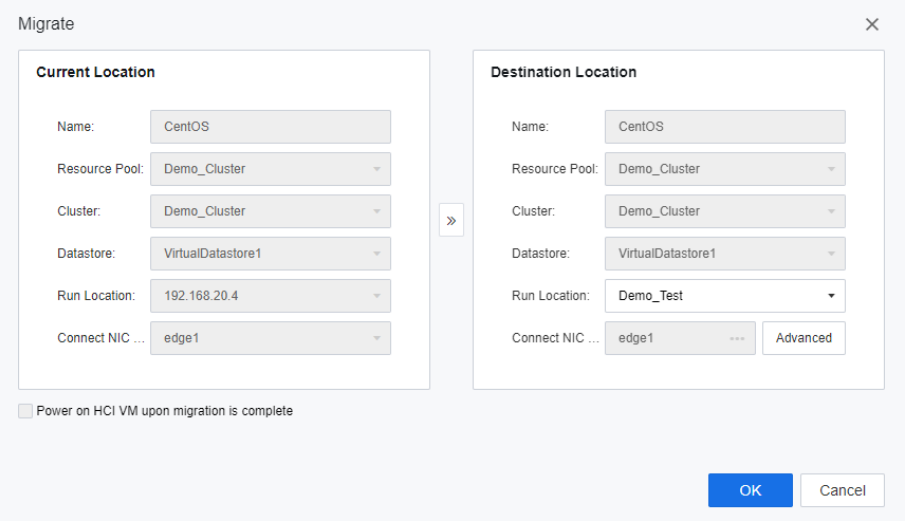
Prerequisites

The source VM can properly access the interface used for migration to the destination host, and the VM migration service has been enabled on the **Port Management** page of HCI.

Steps:

Step 1. Log in to the SCP platform, select **Compute** > **Virtual Machines**, select the virtual machine that needs to be migrated, and click **More** > **Migrate**.

Step 2. Select the information of the migration destination: **Resource Pool, Datastore**, **Run Location**, and **Connect NIC** and click **OK** to start the migration.

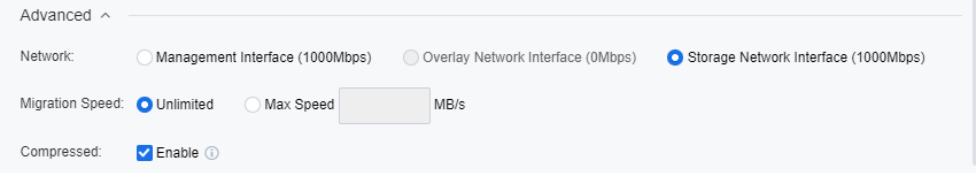


Step 3. You can set the Network and Migration Speed for migration within the cluster and enable **Compressed** under the **Advanced** setting.

- **Network**: The bandwidth of the network port will be automatically identified here. When the bandwidth of the management interface, overlay network interface, and storage network interface is inconsistent, the network port with the highest bandwidth will be recommended. The priority of the interface is shown below when all interfaces have the same bandwidth.

  Overlay Network Interface > Storage Network Interface > Management Interface

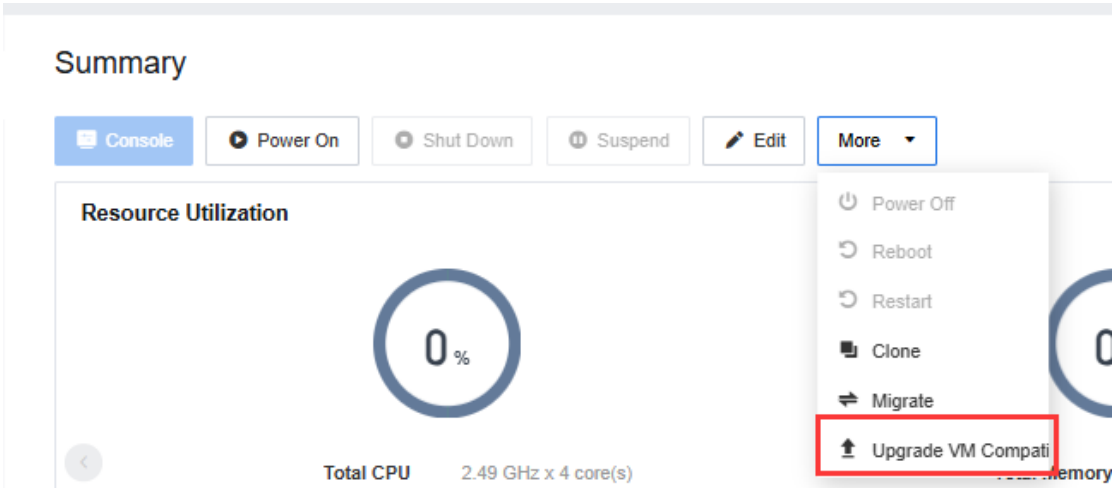
- **Migration Speed**: The default is unlimited, and the maximum migration speed can be set before or during live migration. The minimum value of the migration speed limit is 50MB/s, and the maximum value cannot exceed the bandwidth value of the physical network port of the current network.
- **Compressed**: After enabling it, the hot migration speed can be improved, but it will consume certain CPU resources (up to 4 threads).



NOTICE

1. When migrating a VM, the target location can be the resource pool where the VM is located or migrate to another resource pool.
2. If it is a live migration, the migration to the HCI cluster will remain powered on, and the migration to the VMware cluster will be in the shutdown state. You can check **Power on HCI/VMware VM upon migration is complete**, and you need to check **Auto power off HCI VM to complete migration** checkboxes. Otherwise, you need to shut down to complete the migration manually.
3. If the migration is cold migration, it will be in the shutdown state after the migration. You can check the **Power on HCI/VMware VM upon migration is complete** checkbox.
4. During the migration, view the migration progress in the **Status** column and suspend the VMs as required. Upon VM suspension, businesses will be stopped for a period of time to prevent the VMs from generating new memory data before migration is completed. We recommend that you suspend VMs during off-peak hours.

5. In cross-cluster cross-version hot migration scenarios, the VMs will be in compatible mode after being migrated to the destination cluster, and some of their features will be restricted. Therefore, you need to go to the VM details page and go to **More** > **Upgrade VM Compatibility** to restart the VM for the features to become available.



Note:

- After the cross-cluster cross-version hot migration, we recommend that you upgrade the VM compatibility during off-peak hours.
- After the cross-version hot migration and before the VM compatibility upgrade, if you find that the VM businesses are abnormal, you can migrate them back to the source cluster. If you have upgraded the VM compatibility, this operation is not allowed.

4.3.1.8 Virtual Machine Allocation

Function Description:

This function supports assigning virtual machines to tenants or tenant user accounts.

Precautions:

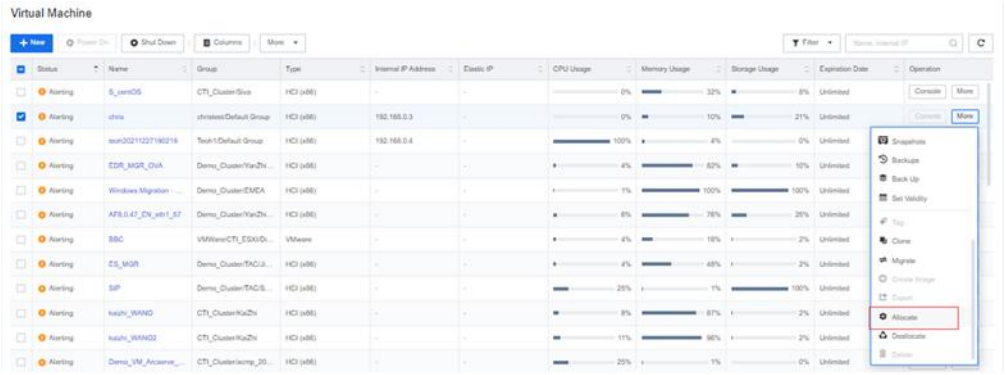
After deallocation, the HCI-type virtual machine will be disconnected from the network. You can go to the default grouped virtual machine list to configure the network for the virtual machine.

Prerequisite

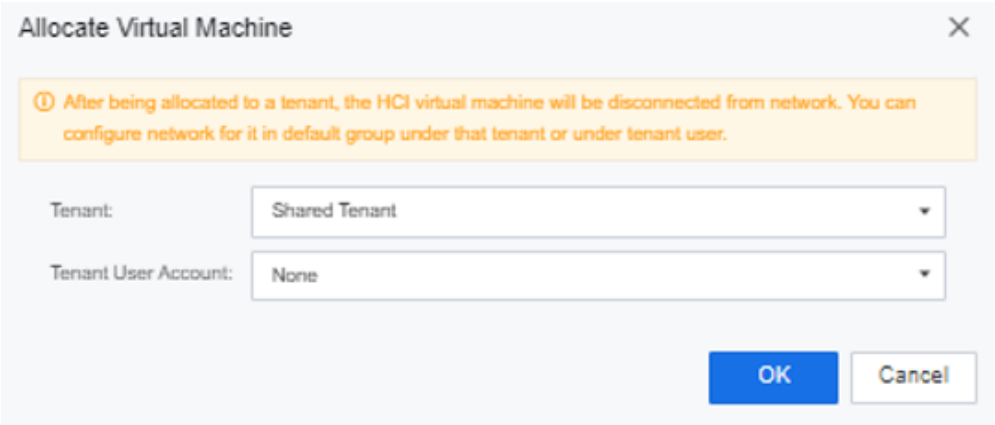
The assigned tenant or tenant user account has a sufficient quota.

Steps:

Step 1. Log in to the SCP platform, select **Compute** > **Virtual Machine**, select the virtual machine that needs to be allocated, and click **More** > **Allocate**.



Step 2. Select the **Tenant** and **Tenant User Account** (it can be empty) and click the **OK** button.



4.3.1.9 Virtual Machine Deallocation

Function Description:

This function supports the virtual machines' deallocation to the SCP platform.

Precautions:

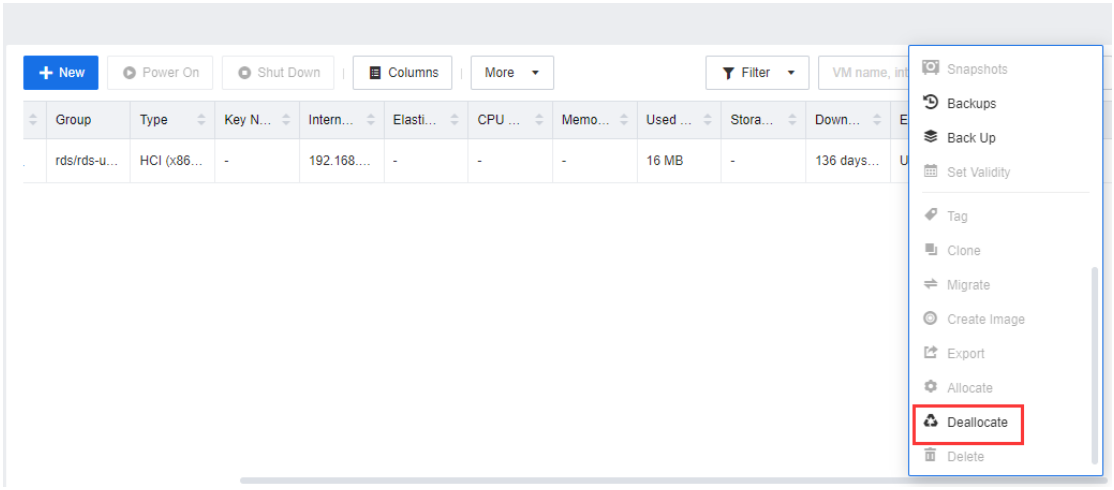
1. After deallocation, the HCI-type virtual machine will be disconnected from the network. You can go to the default grouped virtual machine list to configure the network for the virtual machine.
2. Only the shut down virtual machines can be deallocated.

Prerequisite

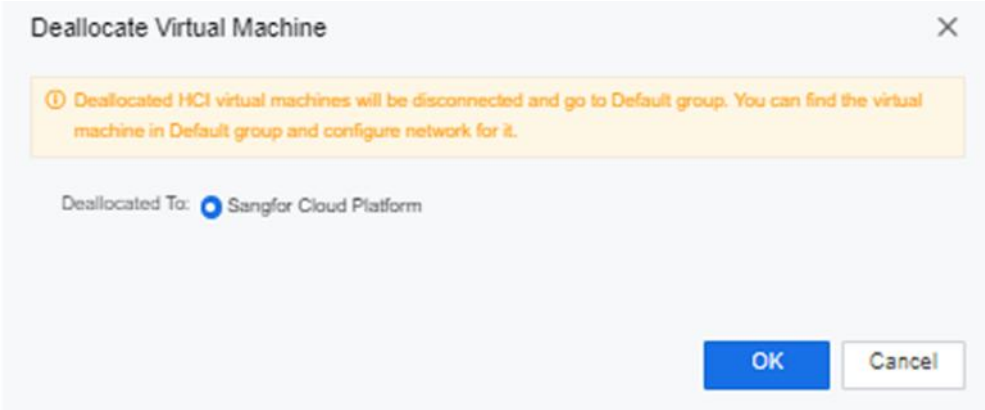
The virtual machine that needs to be deallocated has been shut down.

Steps:

Step 1. Log in to the SCP platform, select **Compute** > **Virtual Machine**, select the virtual machine that needs to be deallocated, and click **More** > **Deallocate**.



Step 2. You can see the deallocate progress on the taskbar.



4.3.1.10 Create SQL Server

Function Description:

The SCP platform supports creating a **Standalone SQL Server** and **SQL Server AlwaysOn Cluster**.

Precautions:

None.

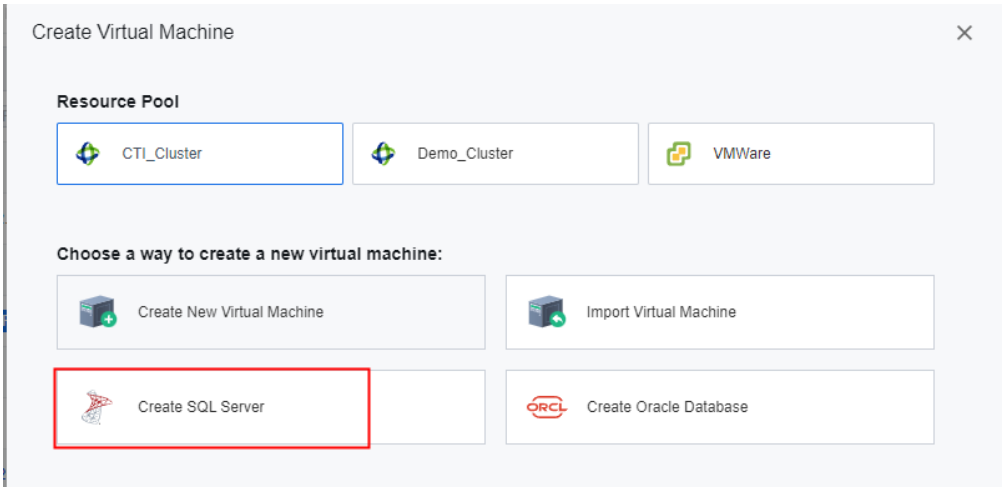
Prerequisite

None.

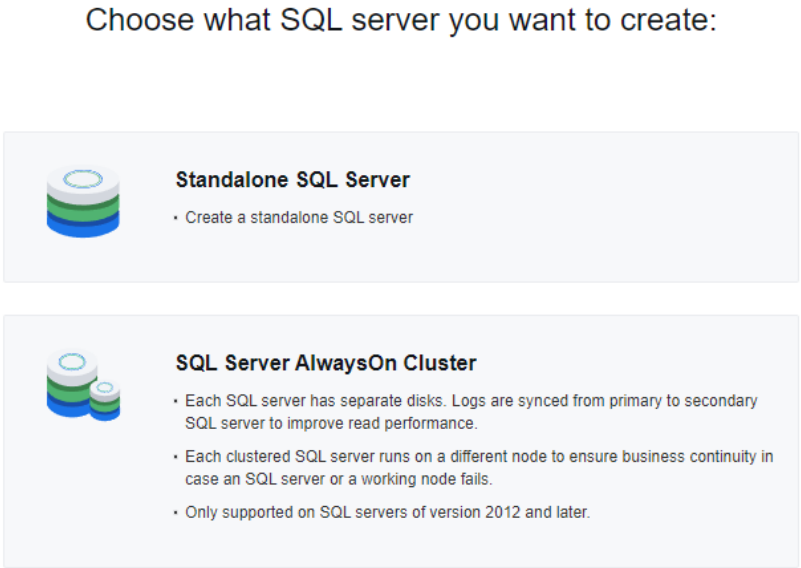
Steps:

Step 4. Navigate to **Resources**, and select **Virtual Machines** under **Compute**.

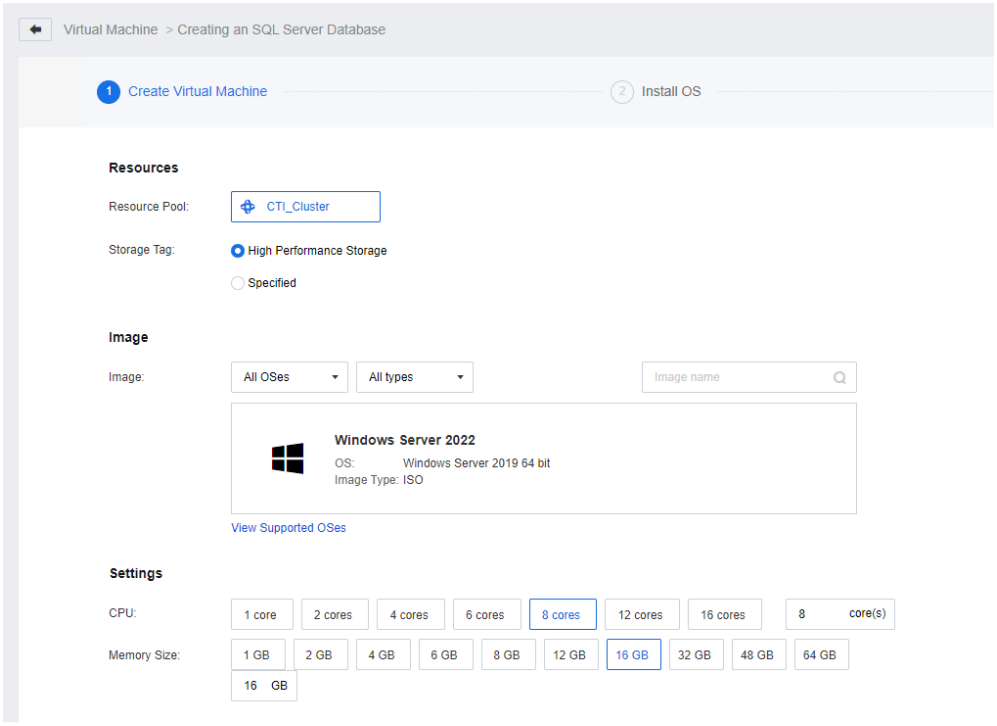
Step 5. Click **New**, select **Resource Pool** for where the SQL server will be located, and click **Create SQL Server** to create a new SQL Server.



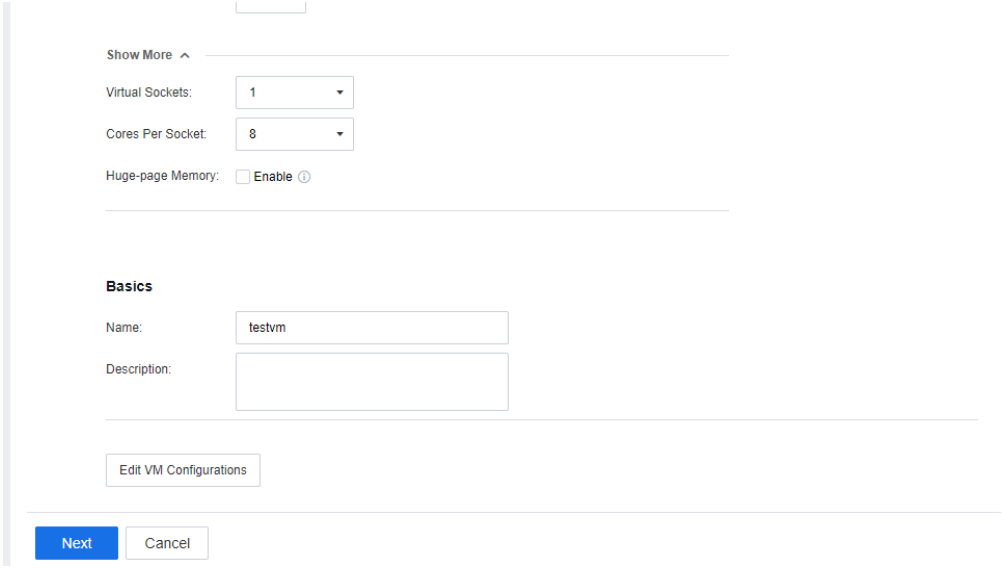
Step 6. Choose the type of SQL server you want to create.



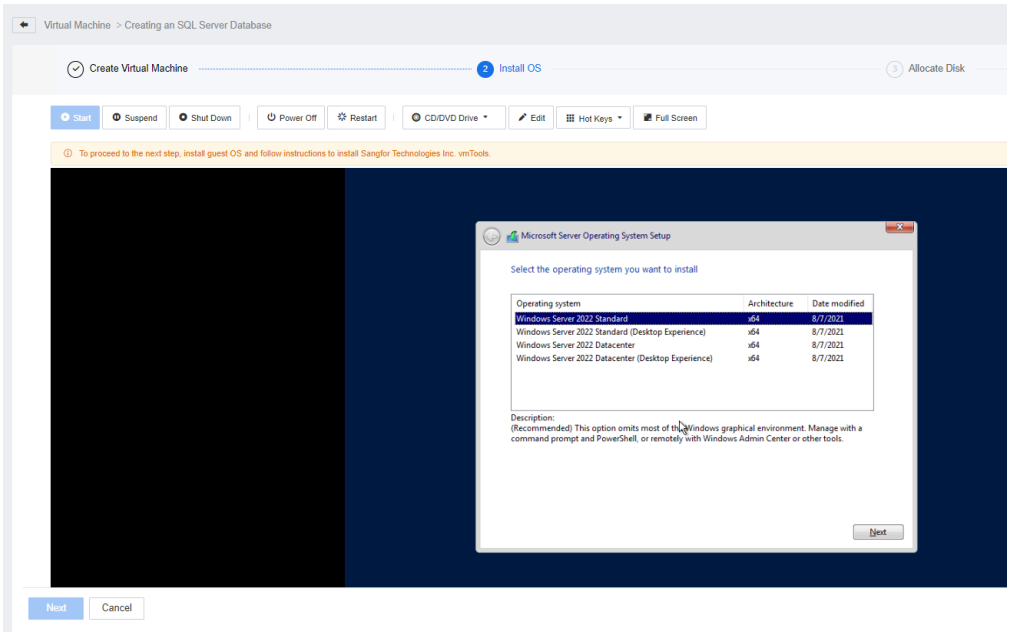
Step 7. Enter the SQL Server Database creation page, pick the appropriate **Storage Tag**, select **Image** and configure the **Settings** for **CPU** and **Memory Size**.



Step 8. Click **Show More** to configure the **Virtual Socket**, **Cores Per Socket,** and **Huge-page Memory**. Lastly, configure the **Basics**, then click **Next** to install OS.



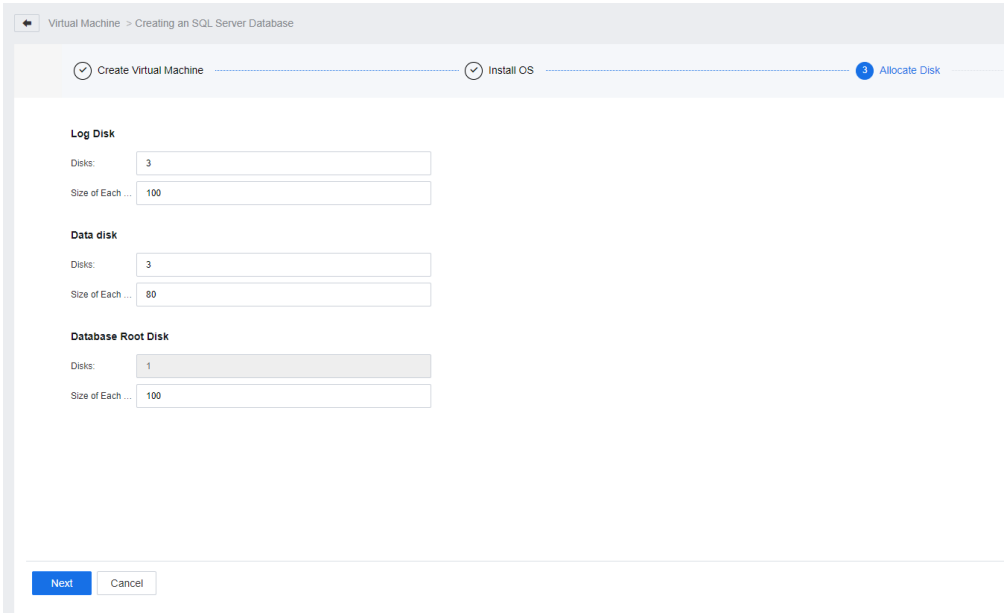
Step 9. Install the SQL Server.

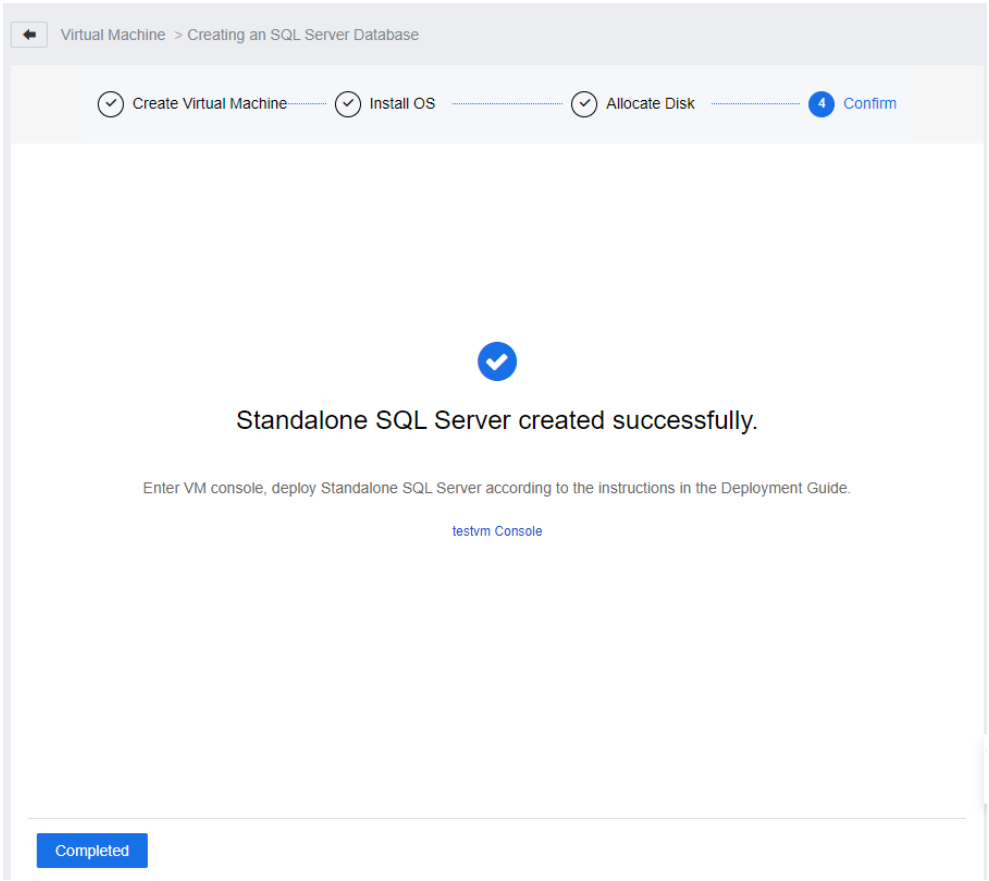


NOTE

To proceed to the next step **Allocate Disk**, install vmTools, and restart this VM first.

Step 10. Configure the **Log Disk**, **Data Disk**, **Database Root Disks,** and click **Next** to complete the SQL Server creation.





4.3.2 Image Management

Function Description

SCP supports public, private, and network function virtualization (NFV) images. Public images are uploaded by platform administrators and used by platform administrators, tenants, and tenant users. Private images are uploaded by tenants and used by tenants and tenant users. Platform administrators can delete private images. NFV images are uploaded by administrators and used by administrators and tenants.

Public and private images are ISO or built-in images (HCI images). ISO images indicate that the image files are in the .iso format, and built-in images are converted from VMs.

Precautions

1. Cross-version image distribution is supported for SCP 6.9.0 and later versions. With the service pack for cross-image distribution installed, you can distribute public, private, network device, and advanced service images

to resource pools of different cluster versions. The supported versions are as follows.

Source HCI Cluster Version	Destination HCI Cluster Version
6.0.0 R5	6.0.0 R5, 6.3.0 (R1 and R2), and 6.9.0
6.2.0	6.2.0, 6.3.0 (R1 and R2), and 6.9.0
6.3.0 (R1 and R2)	6.0.0 R5, 6.2.0, 6.3.0 (R1 and R2), 6.7.0 (R1, R2, and R3), 6.8.0, and 6.9.0
6.7.0 (R1, R2, and R3)	6.3.0 (R1 and R2), 6.7.0 (R1, R2, and R3), and 6.9.0
6.8.0	6.3.0 (R1 and R2), 6.8.0, and 6.9.0
6.9.0	6.0.0 R5, 6.2.0, 6.3.0 (R1 and R2), 6.7.0 (R1, R2, and R3), 6.8.0, and 6.9.0

2. Cross-version image distribution has the following restrictions:

(1) Distribution to HCI 6.9.0 or earlier versions is not supported for VMs with 4K or 8K resolution enabled.

(2) Distribution to HCI 6.8.0 or earlier versions is not supported for multi-disk VM templates.

(3) Distribution to HCI 6.8.0 or earlier versions is not supported for VMs with more than one graphics card.

(4) Distribution to HCI 6.8.0 or earlier versions is not supported for VMs whose OS is Linux Kernel 4.X, Linux Kernel 4.X 64-bit, Linux Kernel 5.X 64-bit, Windows 11 64-bit, or Windows 2022 64-bit.

(5) Distribution to HCI 6.8.0 or earlier versions is not supported for VMs whose description has more than 100 characters.

(6) Distribution to HCI 6.8.0 or earlier versions is not supported for VDI VMs.

(7) Distribution to HCI 6.8.0 or earlier versions is not supported for VMs that use the Q35-based motherboard.

(8) Distribution to HCI 6.0.0 R5 or 6.0.0 R5 (EN) is not supported for HCI VMs that use the AMD or Hygon CPU.

(9) Distribution to HCI 6.8.0 or earlier versions is not supported for VMs that use the VirtIO NIC without vmTools installed.

4.3.2.1 Public VM Image Management

Function Description:

The public VM image is uploaded or produced by the admin administrator and can be used by the admin administrator, tenants, and tenant users.

Precautions:

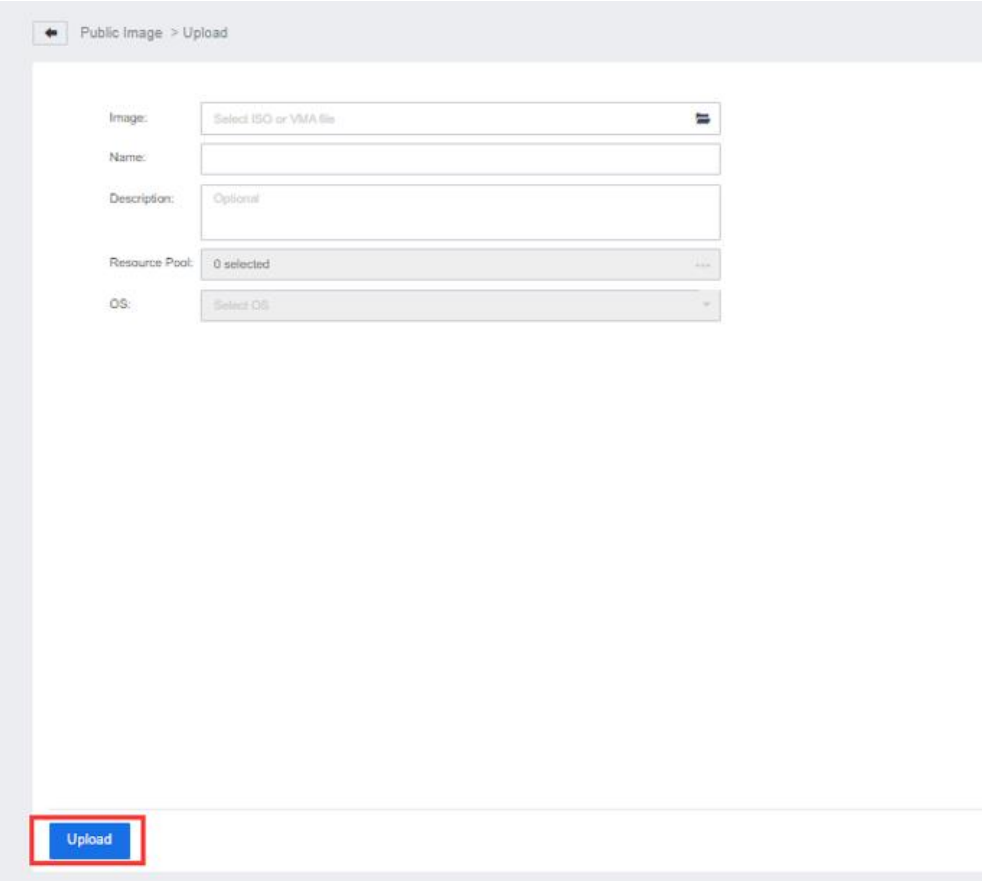
1. ISO-type public VM images can be directly uploaded and allocated to resource pools of different versions.
2. Public VM images of the built-in image type can only be allocated to resource pools of the same version and cannot be allocated to different versions.
3. When the HCI virtual machine makes the image, the image is made from the virtual machine's system disk. Therefore, please migrate important data from other disks to the system disk before making the image.

Prerequisite

1. Sangfor HCI platform has enough image storage space.
2. Please prepare the ISO image file to be uploaded.
3. If the HCI virtual machine makes the image, please install the VM optimization tool first and make it after shutting down.
4. Steps:

Upload ISO image

Step 1. Log in to the SCP platform, select **Compute** > **Images**, click the **Upload** button, and select the ISO file to be uploaded. Then, add a description according to the actual situation, select the corresponding operating system, select the resource pool to which the mirror is uploaded, and click the **Upload** button.

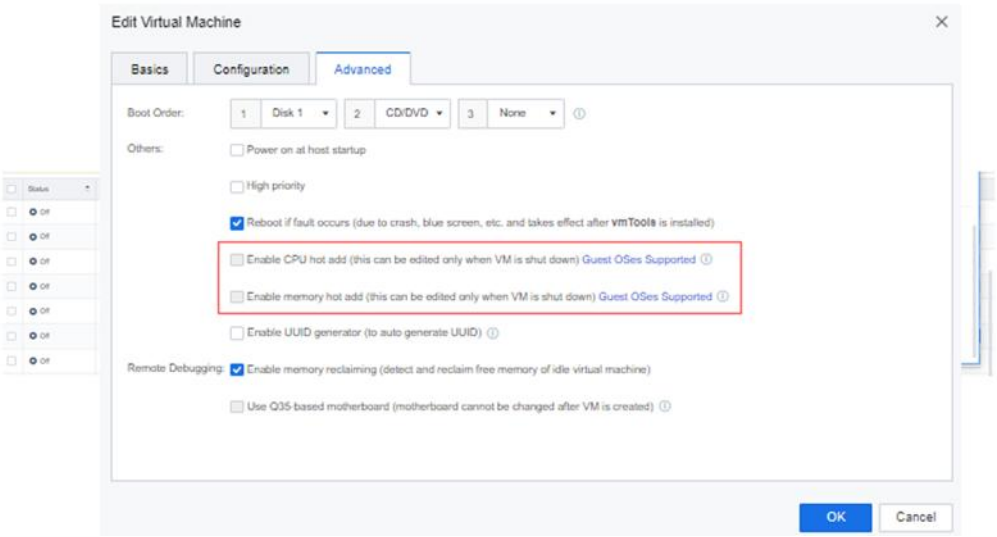


Step 2. After the upload is complete, click the **Finish** button to continue uploading or click the **Close page** button.

Make built-in image

Step 1. Log in to the SCP platform, select **Compute** > **Virtual Machines**, select the virtual machine that needs to be used to make the image, click **More**, enter the console, install the vmTools, and **shut down** the virtual machine.

Step 2. Click **More** and select **Edit, then click Advanced.** It is recommended to check the **Enable CPU hot add** and **Enable memory hot add** checkboxes.

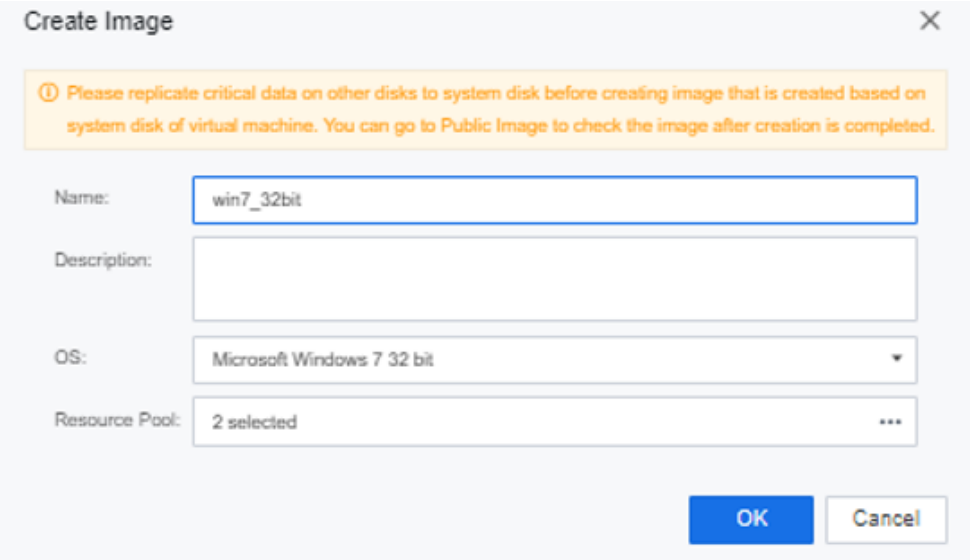


Step 3. Click **More**, select **Create Image**, enter the name and description of the mirror, select the type of operating system, select the resource pool to be distributed by the mirror, and click **OK** to start creating an image.

4.3.2.2 Private image management

Function Description:

1. The admin can upload private VM images for tenants, and the tenants can only use private VM images. At this time, the private VM images will occupy the tenant's private VM image space.



2. The admin can upload the image to the SCP and share the image with tenants without occupying the private image space of other tenants.
3. The admin can convert a tenant's private VM image into a public VM image

for other tenants to use.

Precautions:

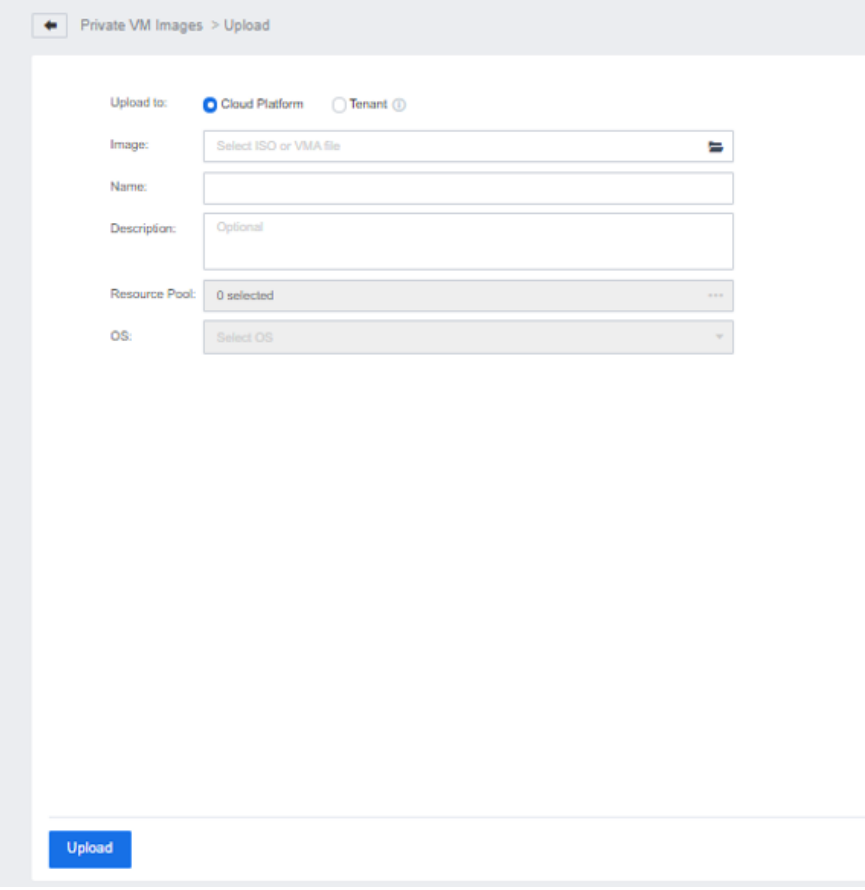
When a private VM image is a built-in image type, it cannot be allocated to resource pools of different versions.

Prerequisite

1. The tenant has enough private image quota space.
2. Prepare the ISO file to be uploaded.
3. If the HCI virtual machine makes the image, please install the VM optimization tool first and make it after shutting down.

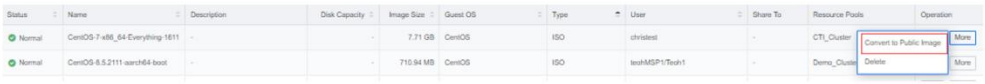
Steps:

Step 1. Log in to the SCP platform, select **Compute** > **Images** > **Network Device Images**, and click the **Upload** button. Then, select the platform or the specified tenant, upload the ISO file, add the description according to the actual situation, select the corresponding operating system, select the image to upload to the Resource pool, and click the **Upload** button.



Step 2. After successfully uploading the image to the cloud platform, the

admin can delete and convert the tenant's private VM image to a public VM image. All tenants can use the image after the image is converted to a public VM image.



4.3.2.3 Network Device Image Management

Function Description:

1. The administrator must upload the image to create the corresponding network device instance when the virtual network device is in use.
2. NFV equipment mainly includes NGAF (Next-Generation Firewall), ADC (Application Delivery Controller), SSL VPN, and IAM (Internet Access Management).

Precautions:

In the SCP 6.7.30 version, the classic and VPC use the same image templates. The specific NFV versions are as follows: vAF8.0.17, vAD7.0.9R1, vSSL 7.6.8R2.

NOTE

The classic network also supports vIAG12.0.14.

Prerequisite

1. Sangfor HCI has enough image storage space.
2. Prepare Network Device Images.

Steps:

Step 1. Log in to the SCP platform, select **Compute** > **Images** > **Network Device Images**, and click the **Upload** button.

Step 2. Select the local network device image file (vma format) to be uploaded, select the resource pool to be allocated, and click the **Upload** button.

Step 3. After the upload is complete, click the **Finish** button to continue uploading or click the **Close** button.

4.3.2.4 Advanced Service Images

Function Description:

When using the aSecurity service platform and database services, the admin administrator needs to upload the advanced service image to deploy the corresponding aSecurity service platform components or database platform components.

Prerequisite:

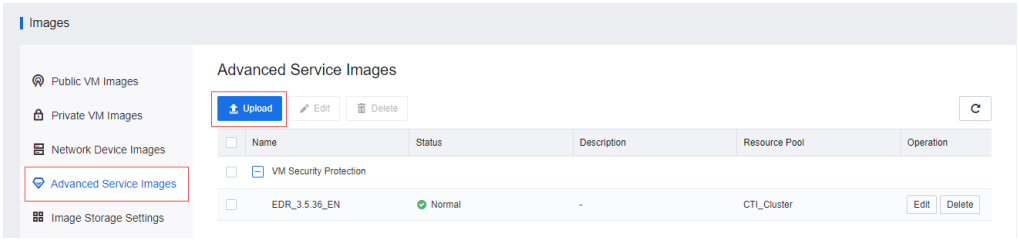
aSecurity service platform image version: EDR_3.5.36EN_for_HCI.vma

Precautions:

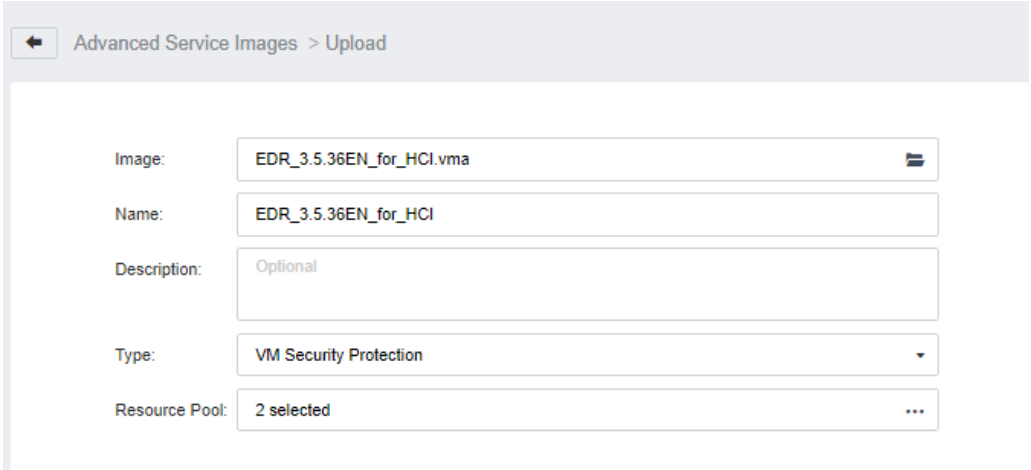
1. The resource pool has enough image storage space.
2. The advanced service image file has been prepared.

Steps:

Step 1. Log in to the SCP platform, select **Compute > Images > Advanced Service Image**, and click the **Upload** button (you can download the image file from Sangfor Community).



Step 2. Select the local advanced service image file (vma format) to be uploaded, select the service type, resource pool, and click the **Upload** button, as shown below.



Step 3. After the upload is complete, click the **View Image** button to return to the **Advanced Service Image** page, or click the **Close** button.

4.3.2.5 Image Storage Settings

Function Description:

After uploading or creating an image, the system will allocate the image to the designated datastore of each resource pool according to the configuration.

Prerequisite

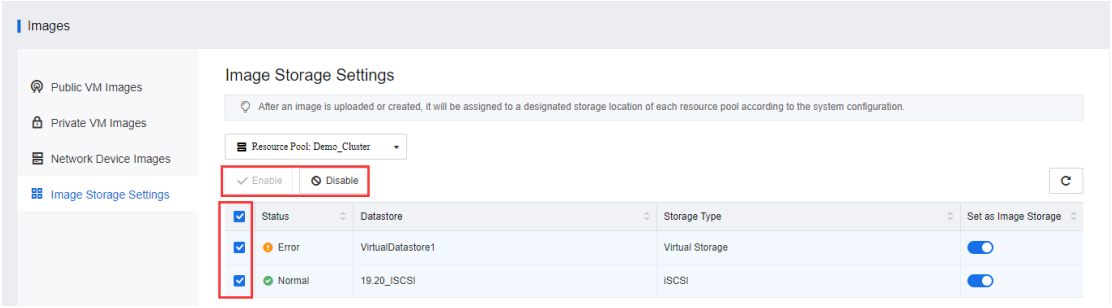
None.

Precautions:

None.

Steps:

Log in to the SCP as admin, select **Compute > Images > Image Storage Settings,** select the corresponding resource pool and click **Enable** or **Disable** to set the datastore of the image.



4.3.3 aDesk VDI

Function Description:

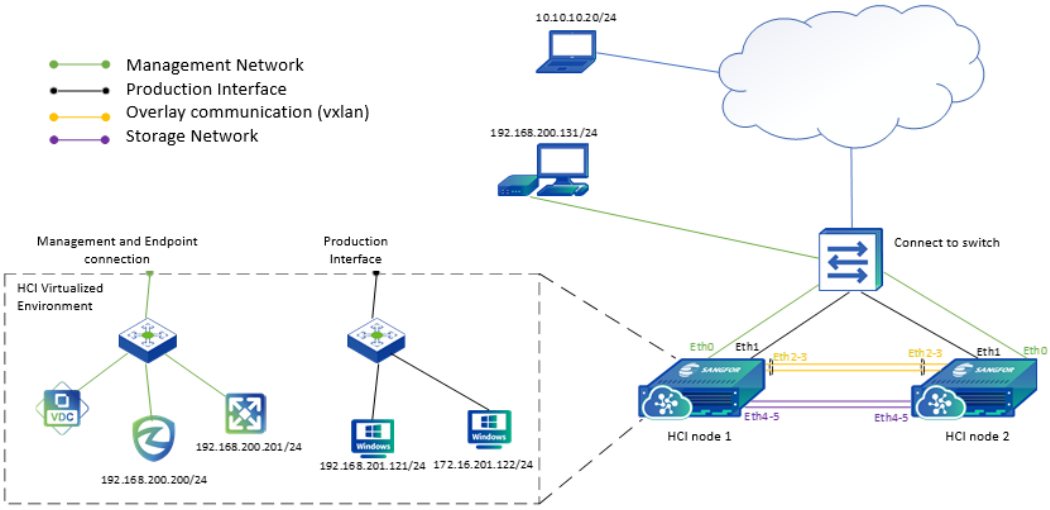
By combining virtualization technology, Sangfor VDI migrates all desktops, applications, and data originally running and stored locally on traditional PCs to the data center for unified hosting and management. The data center deploys HCI in aServer, and the storage resources are virtualized into desktop virtual machines according to the needs of different users. They are transmitted to the user's access device in the form of images through the desktop delivery protocol operating system interface, forming a desktop environment that is the

same as the PC.

Prerequisite

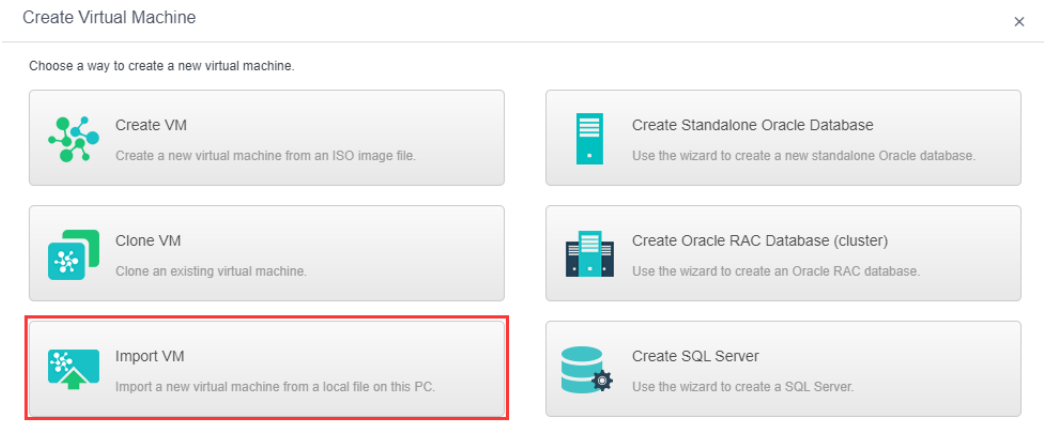
1. Sangfor HCI 6.8.0 and SCP 6.8.0 have been correctly deployed or upgraded.
2. Prepare an IP address for the VDI on the same network segment (or network) as the HCI and SCP management interfaces.
3. The virtual machine or resource package quota has been allocated to the tenant.
4. The template VM has been deployed on the VDC platform.
5. The aSV or aSV for aDesk license has been imported into the SCP. One of the licenses can exist at the same time.

Topology Planning:

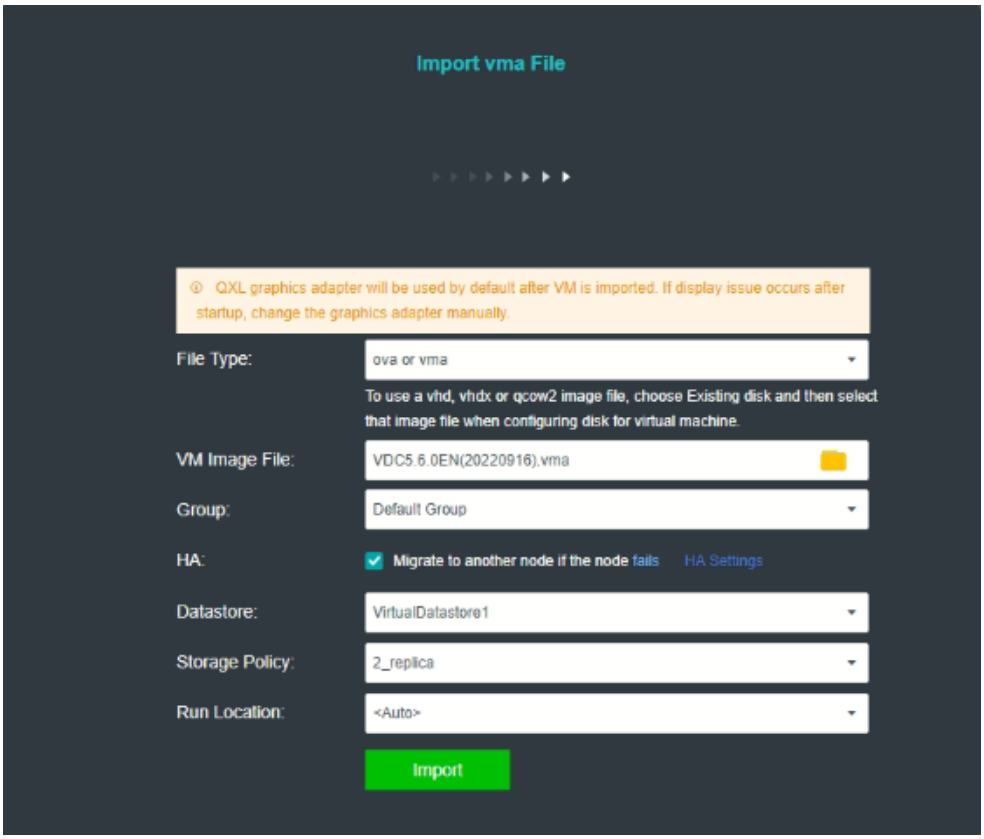


Steps:

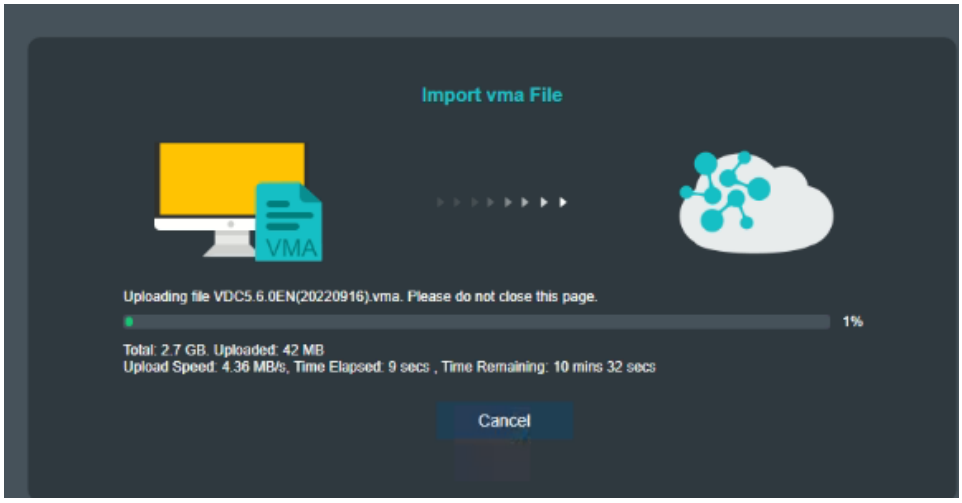
1. Log in to the HCI platform as the admin, enter the **Compute** interface, and click **New > Import VM.**

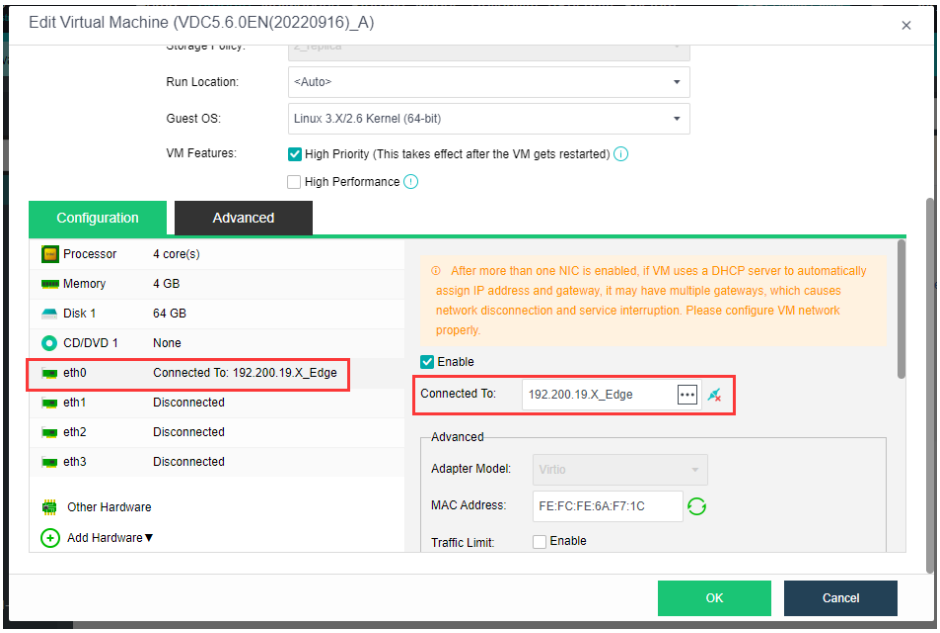


2. Set the group, datastore, storage tag, and running location of the virtual machine, and click **Import**.



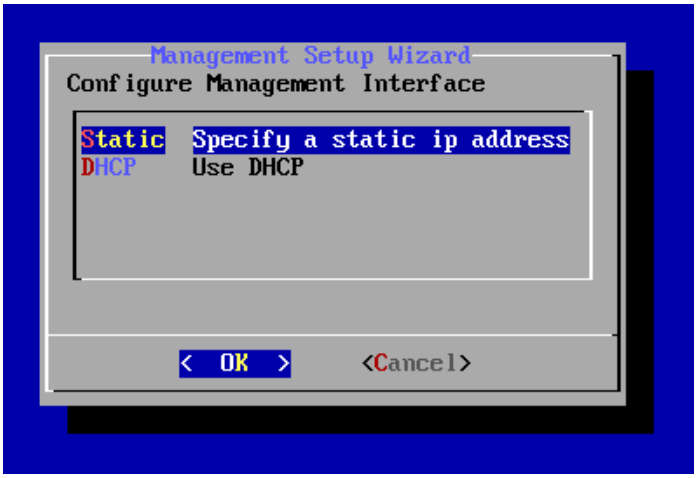
3. After the import is successful, edit the virtual machine and connect the eth0 network card of the virtual machine to a physical edge that can communicate with the HCI management network.

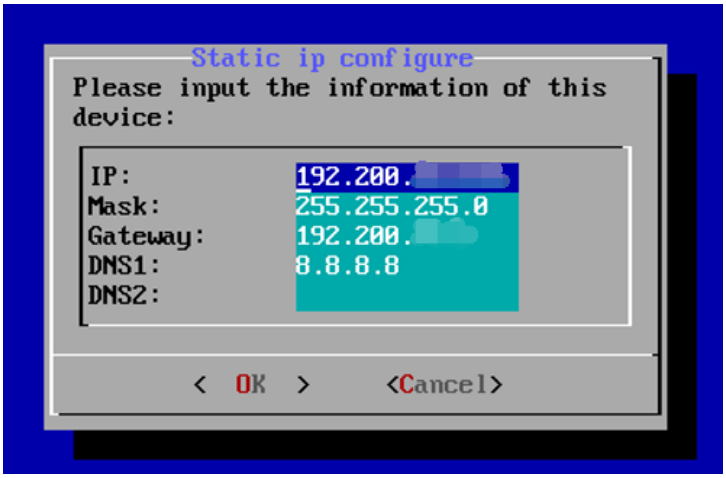




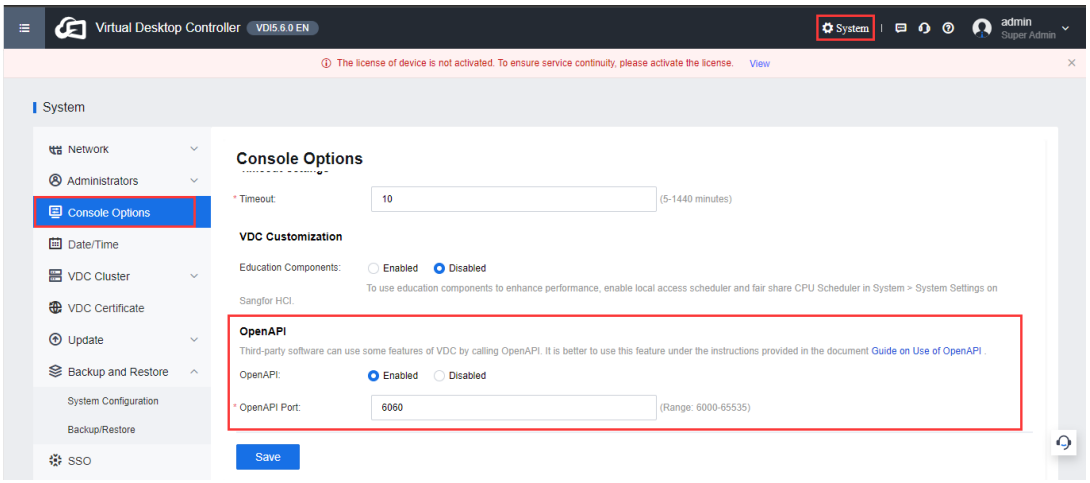
4. Enter into the virtual machine console, and configure an IP for the VDC platform.


Sangfor VDC
Application Manager is at
https://200.201.202.34:4430
1 Network Setup Wizard
2 Show Current Network Settings
3 Enter Maintain Shell
4 Login
5 Reboot
< OK >
<Cancel>

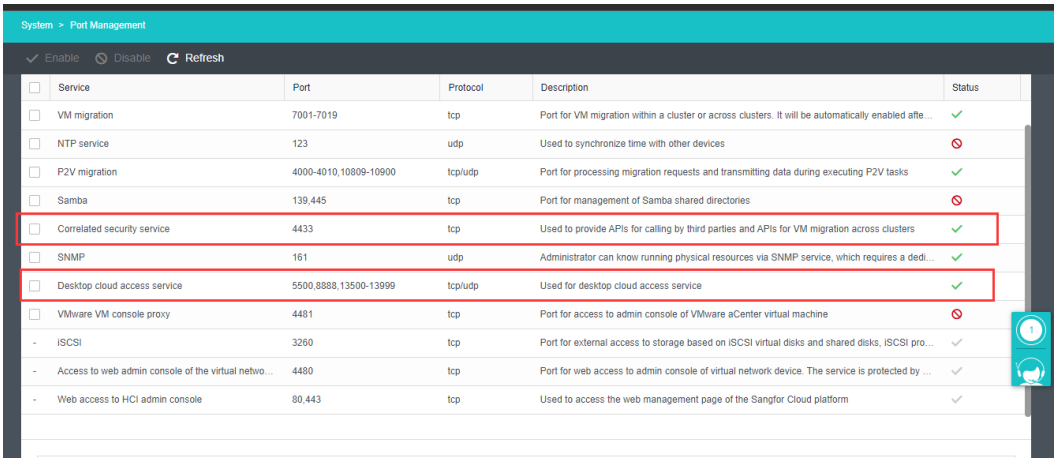

Management Setup Wizard
Configure Management Interface
Static Specify a static ip address
DHCP Use DHCP
< OK >
<Cancel>


Static ip configure
Please input the information of this device:
IP: 192.200.
Mask: 255.255.255.0
Gateway: 192.200.
DNS1: 8.8.8.8
DNS2:
< OK >
<Cancel>

5. Use the admin user to log in to the VDC platform (https://VDC IP:4430), enter the **System > Console Options > OpenAPI** interface, enable the OpenAPI interface, set the OpenAPI port, and click **Save**.



6. Log in to the HCI cluster hosting the VDI virtual machine, and enable the **Correlated security service** and **Desktop cloud access service** ports to allow the related services. Otherwise, the VDI function will not be available.



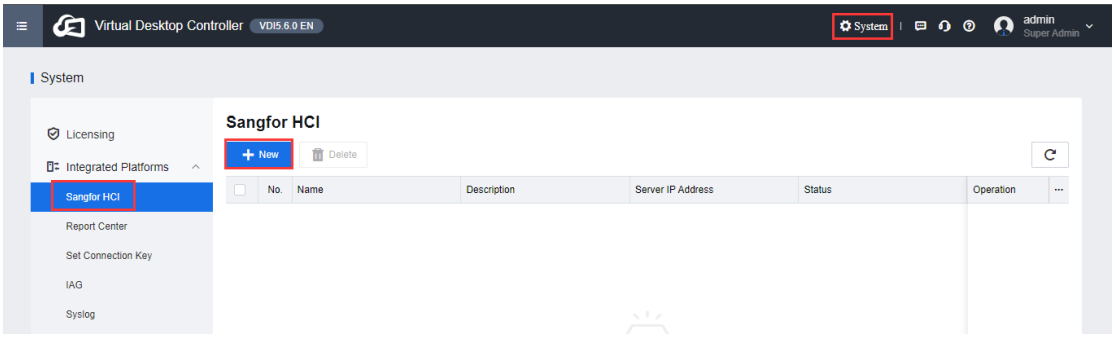
7. Use the admin user to log in to the VDC platform, enter the **System > Integrated Platforms > Sangfor HCI** interface, click **New**, and configure the following parameters:

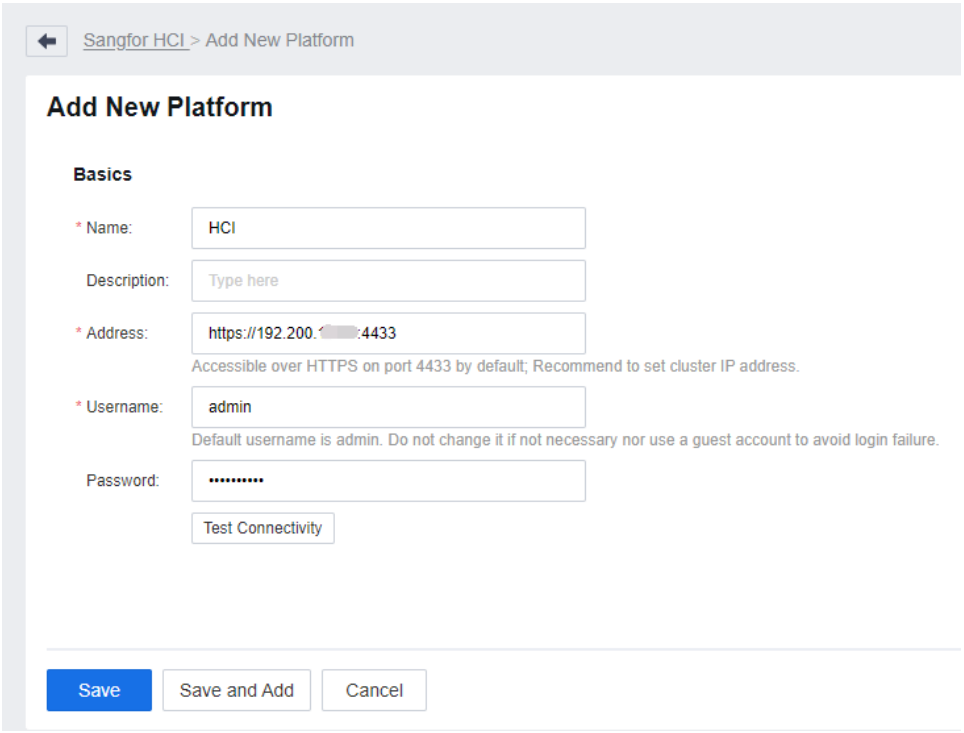
   Name: Self-Defined

   Controller address: https://HCI cluster address: 4433

   Connection account: admin

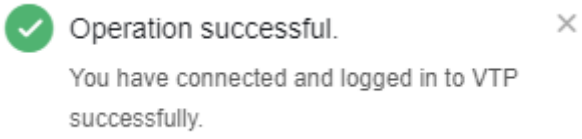
Password: admin account password



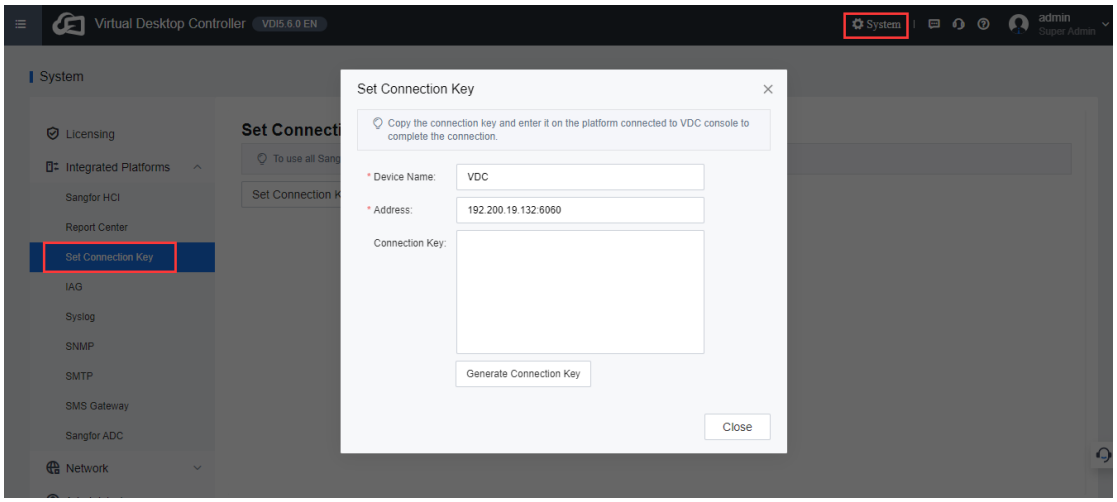


8. Click **Test Connectivity** to verify connectivity to the HCI platform.
9. Enter the **System > Integrated Platforms > Set Connection Key** interface, click **Set Connection Key**, configure the **Device Name** and **Device Address**, and click **Generate Connection Key**.

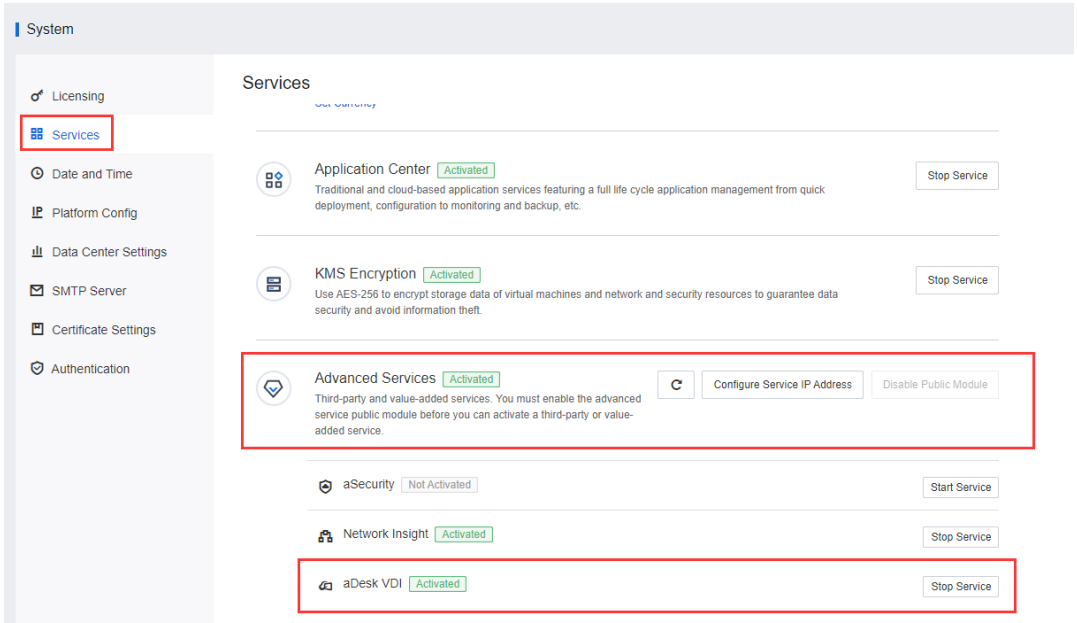
   Device name: Self-defined



Device address: VDC Platform address: OpenAPI port

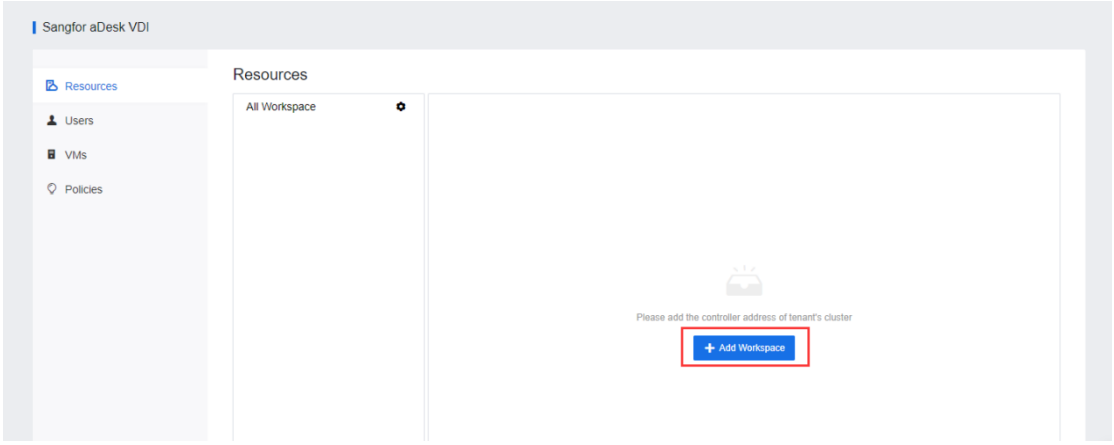


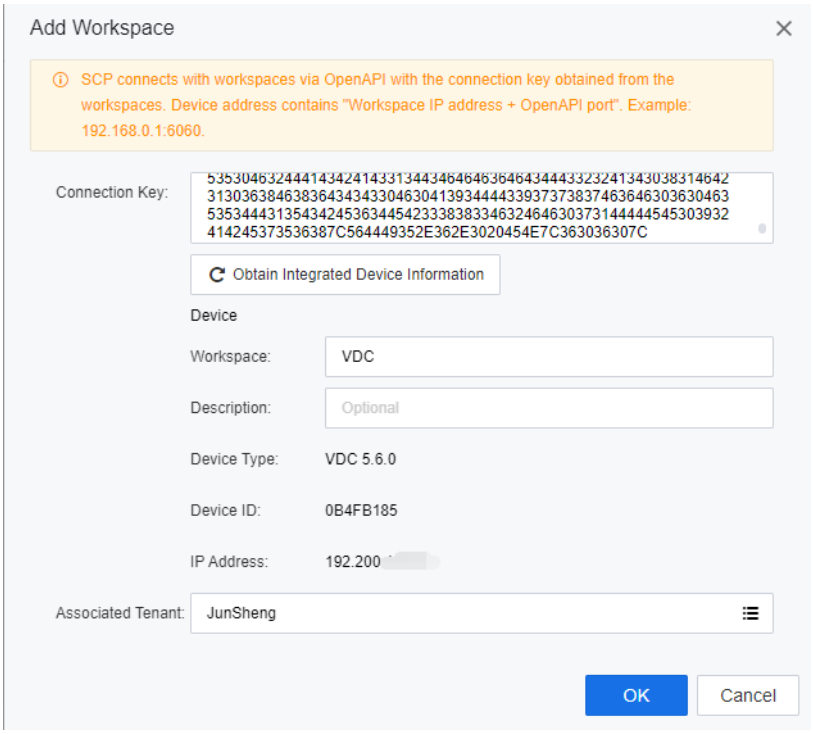
10. Use the admin user to log in to the SCP platform.
11. Proceed to **System > Services > Advanced Service > aDesk VDI** interface, and activate the **aDesk VDI** service.



12. After entering the aDesk VDI redirection page, click **Activate Now**.

13. Enter the **Compute > aDesk VDI > Resources** interface, click **Add Workspace**, fill in the **Connection Key**, click **Obtain Integrated Device Information** to obtain Integrated Device Information, select the tenant to be associated, and click **OK**.





4.3.4 aDesk VDI Configuration Guide

Sangfor SCP supports docking with the Sangfor aDesk, manages aDesk resources in a unified way, realizes the DAAS of the aDesk platform, and provides aDesk services for multiple tenants.

4.3.4.1 Workspace Management

The SCP regards VDC as a workspace. A workspace on the SCP corresponds to a set of VDC clusters managed by the SCP. The SCP administrator can manage the corresponding VDC cluster in the workspace.

4.3.4.1.1 Add a new workspace

Function Description:

Sangfor SCP cloud management platform realizes the connection and management of SCP and the corresponding VDC cluster by adding a new workspace.

Precautions:

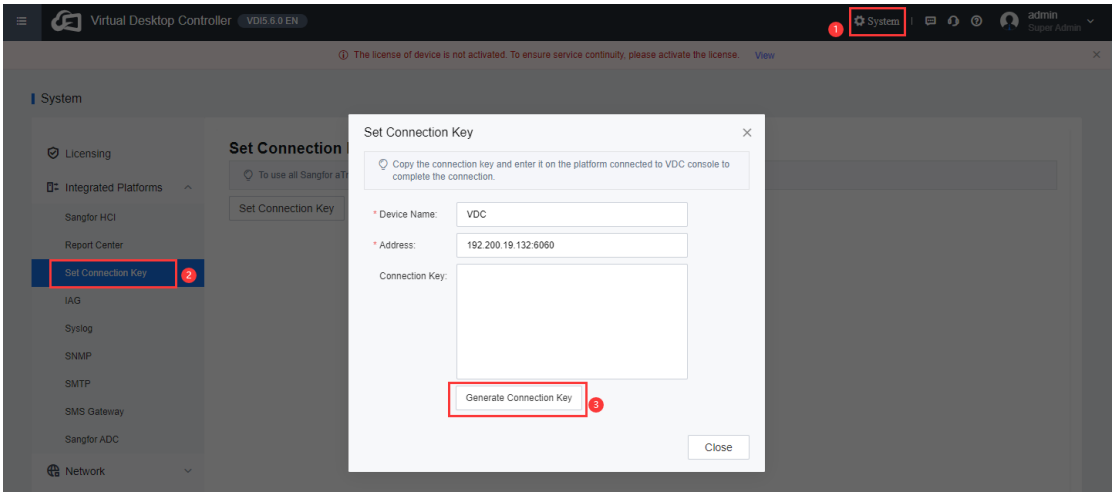
None.

Prerequisite

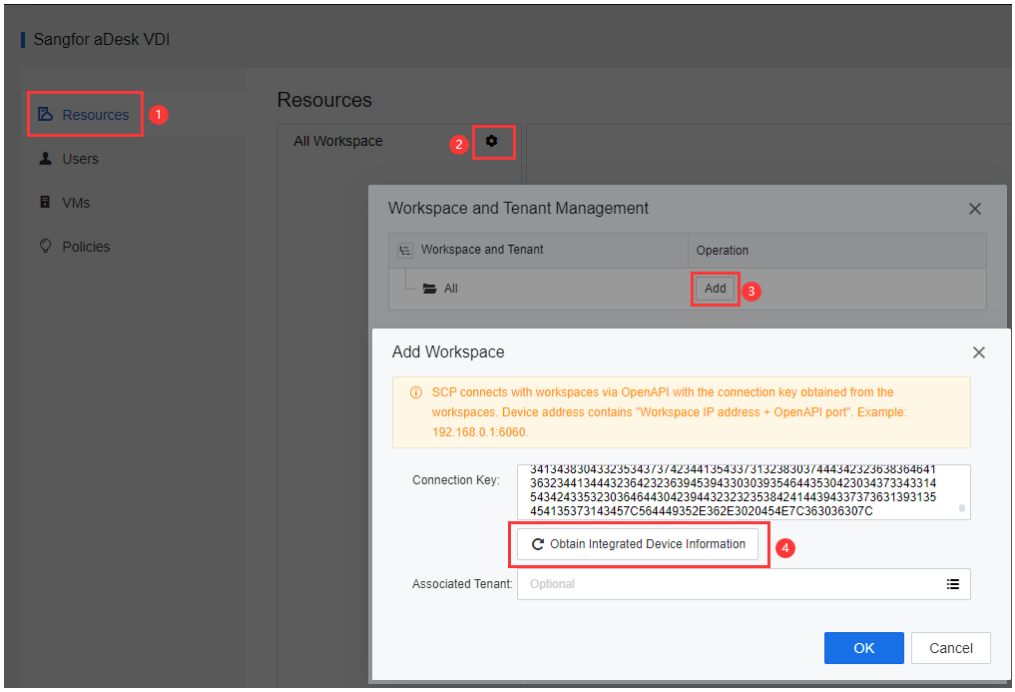
SCP has activated the **aDesk VDI** service.

Steps

1. Log in to the VDC platform as admin, **select System > Console Options > OpenAPI,** select **Enable,** and save the configuration.
2. Select **System > Integrated Platforms > Set Connection Key** in the VDC console, and click **Set Connection Key**. In the pop-up Set Connection Key window, after confirming that the VDC address and port are correctly connected, click **Generate Connection Key** to copy and save the Connection Key information.



3. Log in to the SCP platform as admin, select **Compute > aDesk VDI**, and click the ⚙ icon. Then, in the **Workspace and Tenant Management** window, click **Add**, and in the pop-up **Add Workspace** window, fill in the connection key you obtained in the previous step. After confirming that the information is correct, click **OK** to complete the connection between the SCP and the VDC.



4.3.4.1.2 Delete workspace

Function Description:

Sangfor SCP platform removes the association with the VDC cluster that is no longer used by deleting the workspace.

Precautions:

This operation will delete related data and cannot be recovered. Please operate with caution.

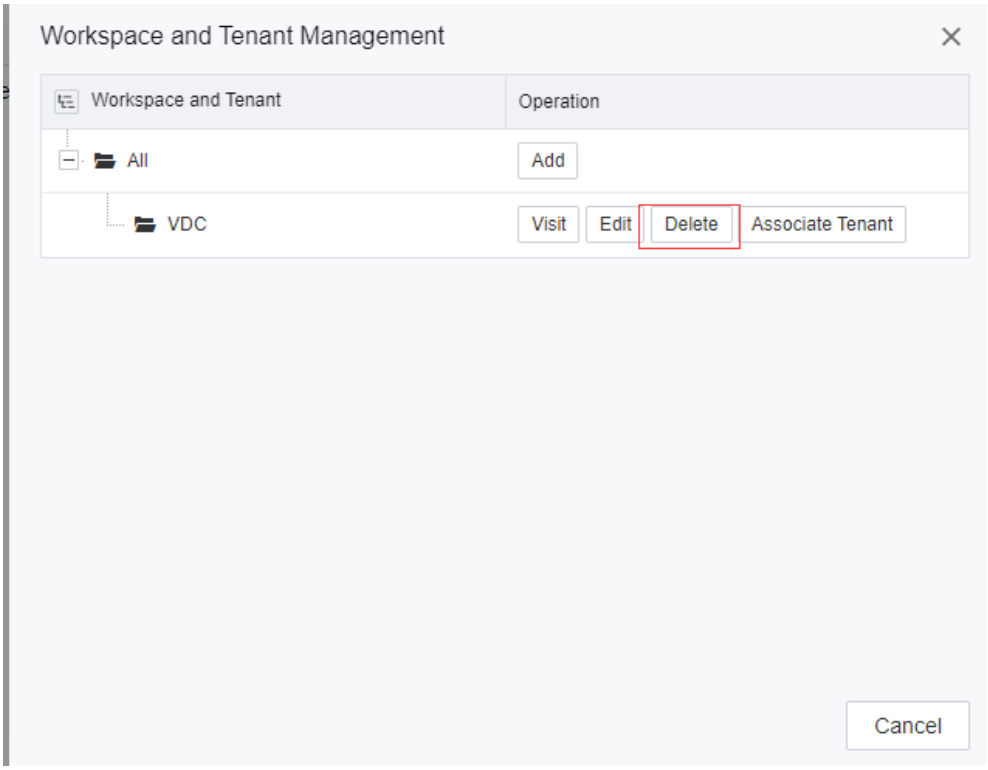
Prerequisite

None.

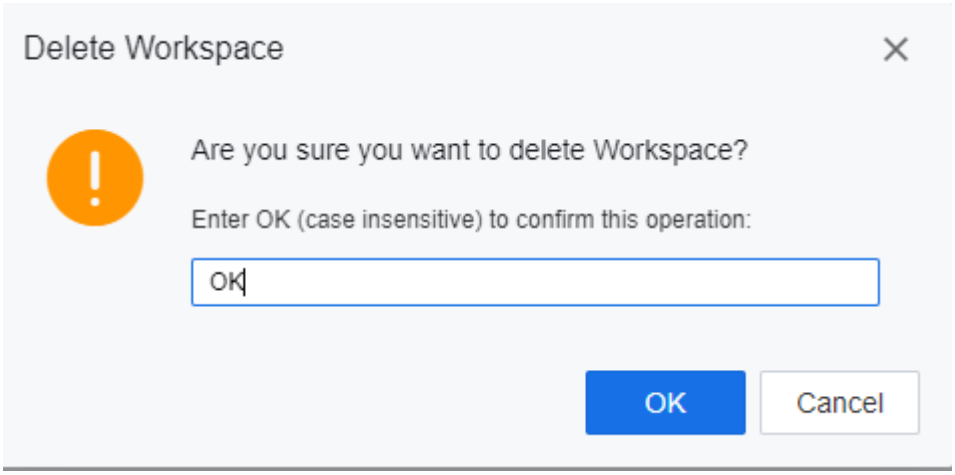
Steps:

1. Log in to the SCP platform as admin, select **Compute > Sangfor aDesk VDI**,

click the ⚙ icon, and in the Workspaces and Tenant Management window, click **Delete** corresponding to the workspace entry to be deleted.



2. In the pop-up Delete Workspace window, enter **OK** and click **OK** to complete the deletion.



4.3.4.1.3 Associate tenant

Function Description:

The Sangfor SCP platform authorizes tenants to use the corresponding VDC by associating tenants for the workspace.

Precautions

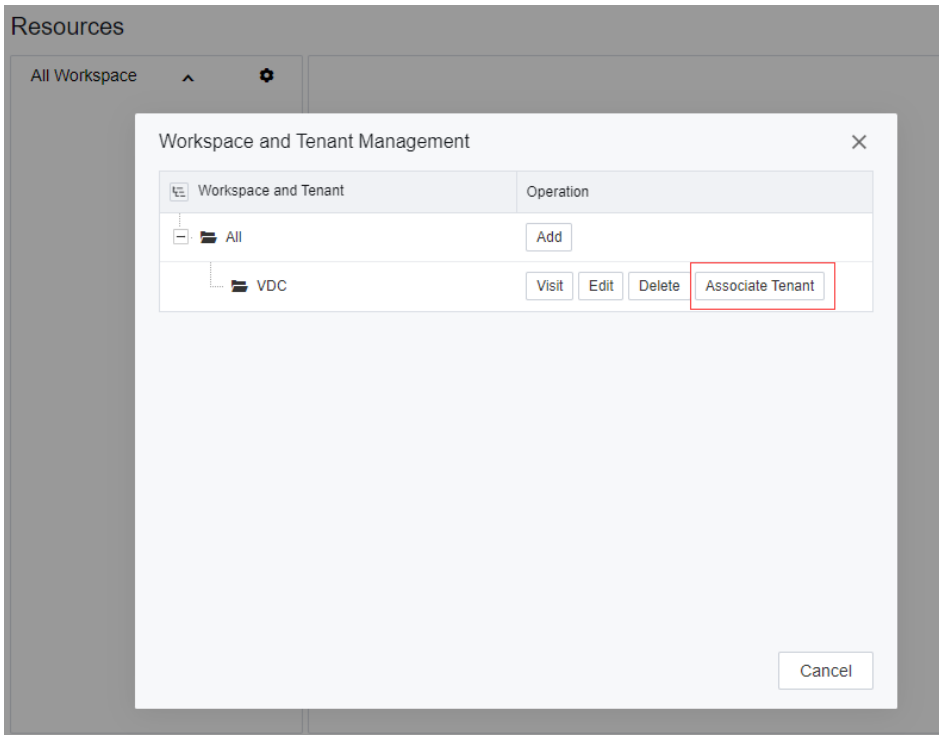
None.

Prerequisite

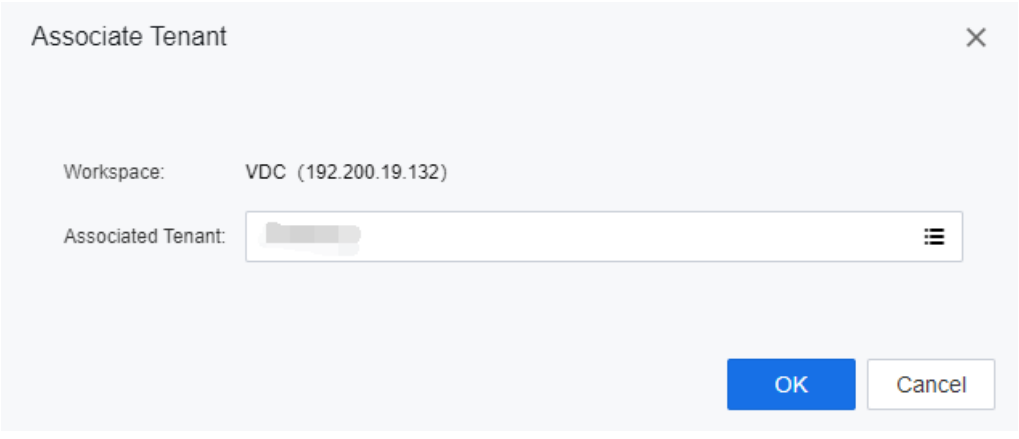
A workspace has been built in SCP.

Steps:

1. Log in to the SCP platform as admin, select **Compute > aDesk VDI**, click the ⚙ icon, and in the Workspaces and Tenants Management window, click **Associated Tenant** corresponding to the workspace entry to which the tenant needs to be associated.



2. In the pop-up Associate Tenant window, select the tenant information to be associated, and click **OK**.



4.3.4.1.4 De-associate Workspace

Function Description:

Sangfor SCP reclaims the tenant's permission to use VDI resources by disassociating related tenants under the workspace.

Precautions

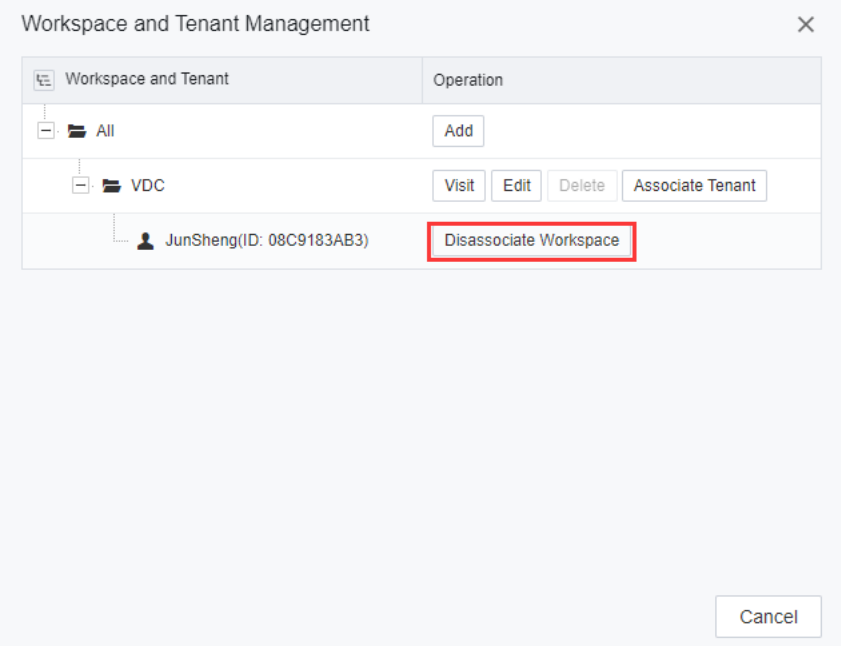
This operation will delete related data and cannot be recovered. Please operate with caution.

Prerequisite

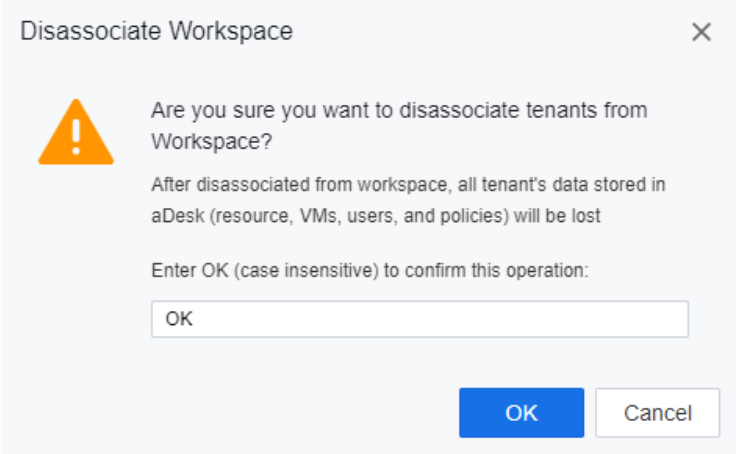
To disassociate a tenant, you must delete all tenant resources in the corresponding workspace.

Steps:

1. Log in to the SCP platform as admin, select **Compute > Sangfor aDesk VDI**, click the ⚙ icon, and in the Workspace and Tenant Management window, click **Disassociate Workspace** corresponding to the tenant entry to be disassociated.



2. In the pop-up Disassociate Workspace window, enter **OK** and click **OK** to complete the disassociation operation.



4.3.4.1.5 Switch workspace tenant management

Function Description:

Sangfor SCP platform realizes the management of tenants' VDI resources under the workspace by selecting different tenants associated with the workspace.

Prerequisite

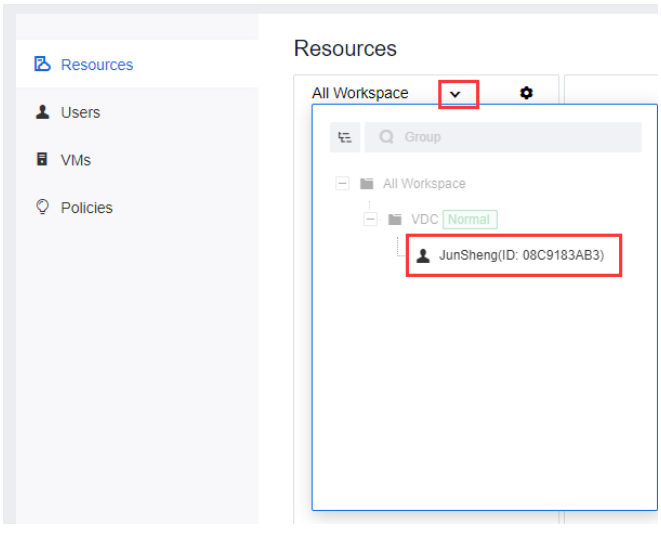
None.

Precautions:

None.

Steps:

1. Log in to the SCP platform as admin, select **Compute > Sangfor aDesk VDI**, click the drop-down arrow, and select the tenant under the workspace to be managed from the drop-down menu that appears.



4.3.4.2 Resources

4.3.4.2.1 Create VDI resources

Function Description:

Sangfor SCP cloud management platform supports the creation of **Persistent, Nonpersistent,** and **Floating Pool** VM for tenants in the corresponding workspace.

Prerequisite

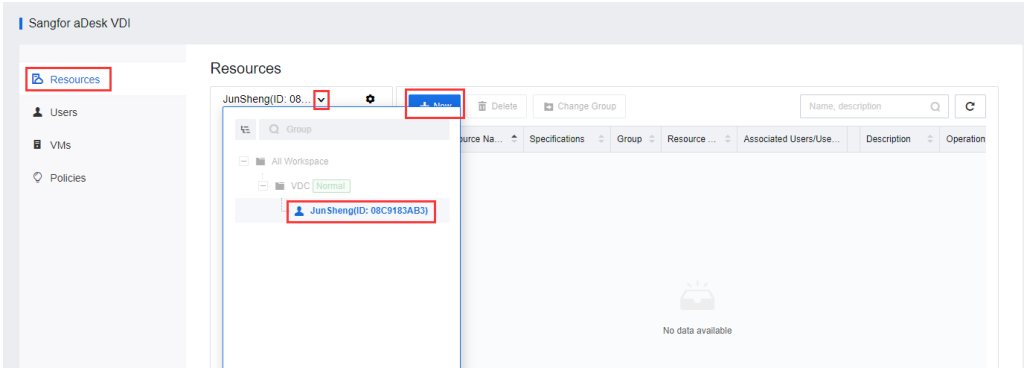
1. The SCP and the VDC of the corresponding workspace must be associated with the same HCI cluster at the same time.
2. The tenant has associated the resource pool corresponding to the HCI cluster on the SCP and has allocated the quota and VPC.
3. A desktop template must be created on the VDC of the corresponding workspace.

Precautions:

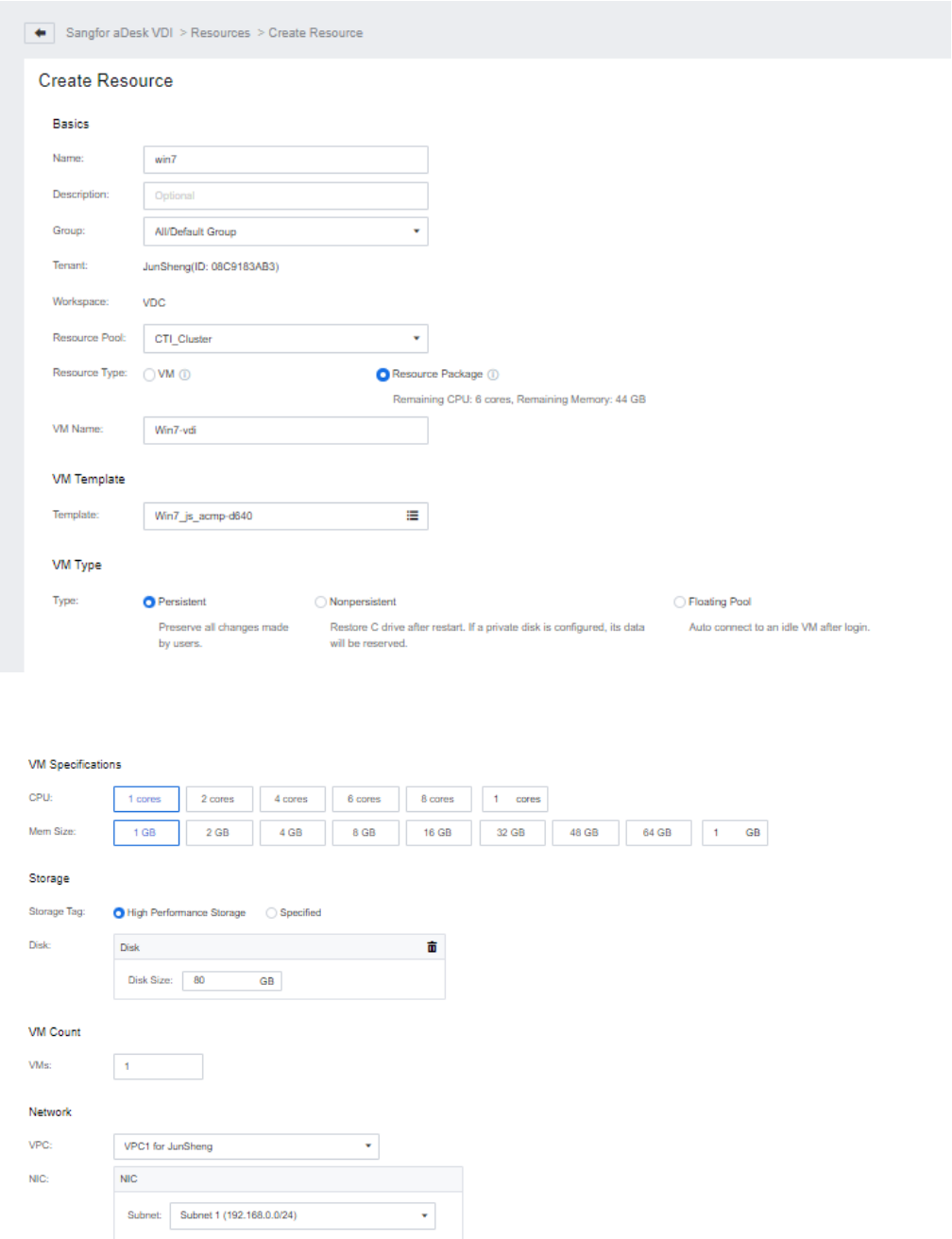
None.

Steps:

1. Log in to the SCP platform as admin, select **Compute > Sangfor aDesk VDI > Resources**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and click **New**.



2. On the **Create Resource** interface, configure various parameters of the desktop resource according to actual needs.



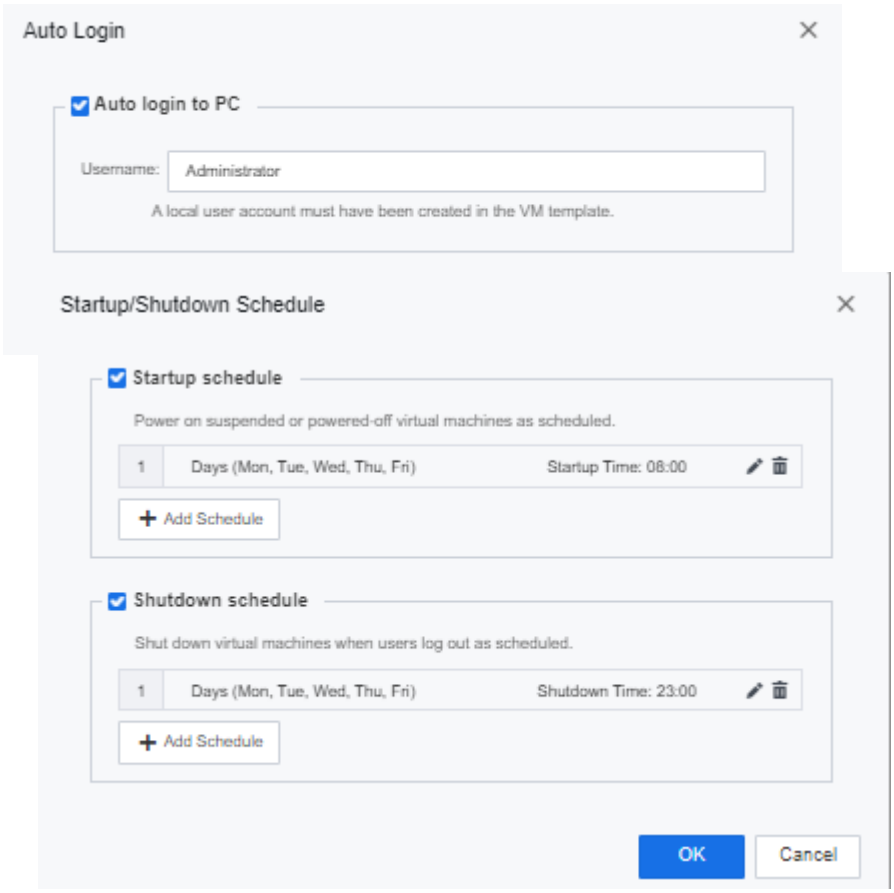
Parameters	Description	Remark
Name	Used to name the desktop resource, the filled-in text will be displayed in the resource list after the user successfully logs in.	Compulsory
Description	To note resource usage, type, etc.	Optional

Group	The resource can be assigned to the corresponding **resource group** and can be created manually.	Default belongs to the **default group.**
Tenant	Shows which tenant the current resource belongs to.	Cannot be changed
Workspace	Displays which workspace (VDC cluster) the current resource belongs to.	Cannot be changed
Resource Pool	Select which HCI cluster to create the desktop resource in the background.	A resource can only select one HCI cluster.
Resource type	Sets the type of tenant quota that this resource consumes when creating virtual desktops. **Virtual Machine**: Select the SCP built-in fixed virtual machine specifications (CPU, memory) configuration to create a virtual machine, and consume the quota of the number of virtual machines corresponding to the specification of the VDI allocated by SCP to the tenant. **Resource package**: Administrators can customize virtual machine specifications to create virtual machines and consume the virtual machine resource package quota allocated by SCP to tenants.	
VM Name	Specify the computer name prefix of the virtual desktop. The platform will automatically add the corresponding four-digit number after the name prefix according to the number of derived virtual desktops. It is recommended to add **-**, such as "**demo-**" to the first derived virtual desktop. The computer's name is "**demo-0001**".	-
Template	Select the template on the HCI as the derived virtual desktop. When the virtual desktop is derived, the	-

	template must be disabled. VMs with Turbo mode enabled cannot be templates for quick deployment.	
VM work mode	**Persistent:** After the desktop restarts, all user data is preserved. **Non-Persistent:** Restore the C drive after a restart. If a private disk is configured, its data will be reserved. **Floating Pool:** Auto connect to an idle VM after login.	Adjust according to needs.
VM Specifications	To configure the CPU and memory hardware configuration of the derived virtual desktop.	
Storage Tag	To set the storage type of virtual desktop storage. The selectable items are related to the storage authorization obtained by the tenant.	
Disk	Set the capacity of the virtual desktop personal disk.	
VM Count	Set the number of virtual desktops that need to be derived.	
VPC	Set which VPC the resource virtual desktop belongs to.	
NIC	Set which virtual switch in the tenant VPC the resource virtual desktop is connected to.	

3. **Snapshot Policy:** Configure the snapshot strategy according to actual needs.
4. **Security Policy:** The security policy is used to optimize the use and management of desktop resources, mainly including three functional modules: **Auto Login, Startup/Shutdown Schedule,** and **Idle VM Management**.

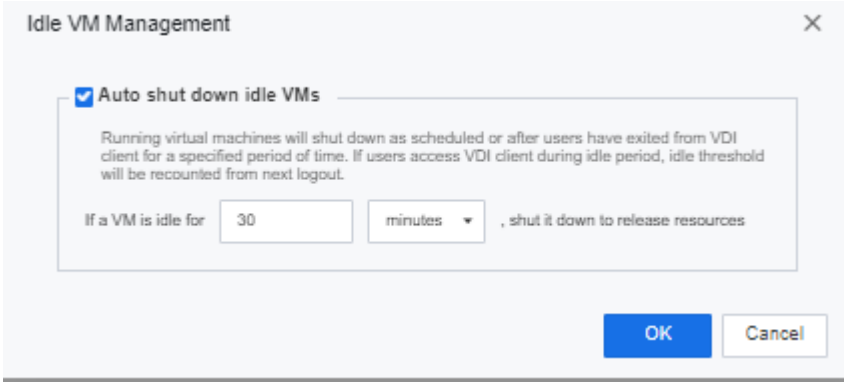
5. **Auto login:** It is not enabled by default. If users need to log in to the aDesk with a single sign-on after logging in to VDI, they need to configure auto login.



6. **Startup/Shutdown Schedule:** It is not enabled by default, and the administrator can configure the startup and shutdown schedule of the virtual desktops in the resource pool according to the actual needs so that the virtual desktops in the resource pool can be powered on and off according to the plan.

7. Suppose the desktop pool has a large number of desktop resources. In that case, it is recommended to configure a startup plan to avoid the cloud platform caused by a startup storm caused by a short period and a large batch of startups during working hours.

8. **Idle VM management:** It is not enabled by default. To fully use cloud platform resources, administrators can configure the idle VM management policy to automatically shut down virtual desktops that users have not accessed for a long time to release resources and improve performance. Resource utilization and avoid resource waste.



4.3.4.2.2 Adding VDI resources

Function Description:

Sangfor SCP cloud management platform's existing VDI (desktop) resources can add new virtual desktops when tenants have a remaining quota.

Prerequisite

None.

Precautions:

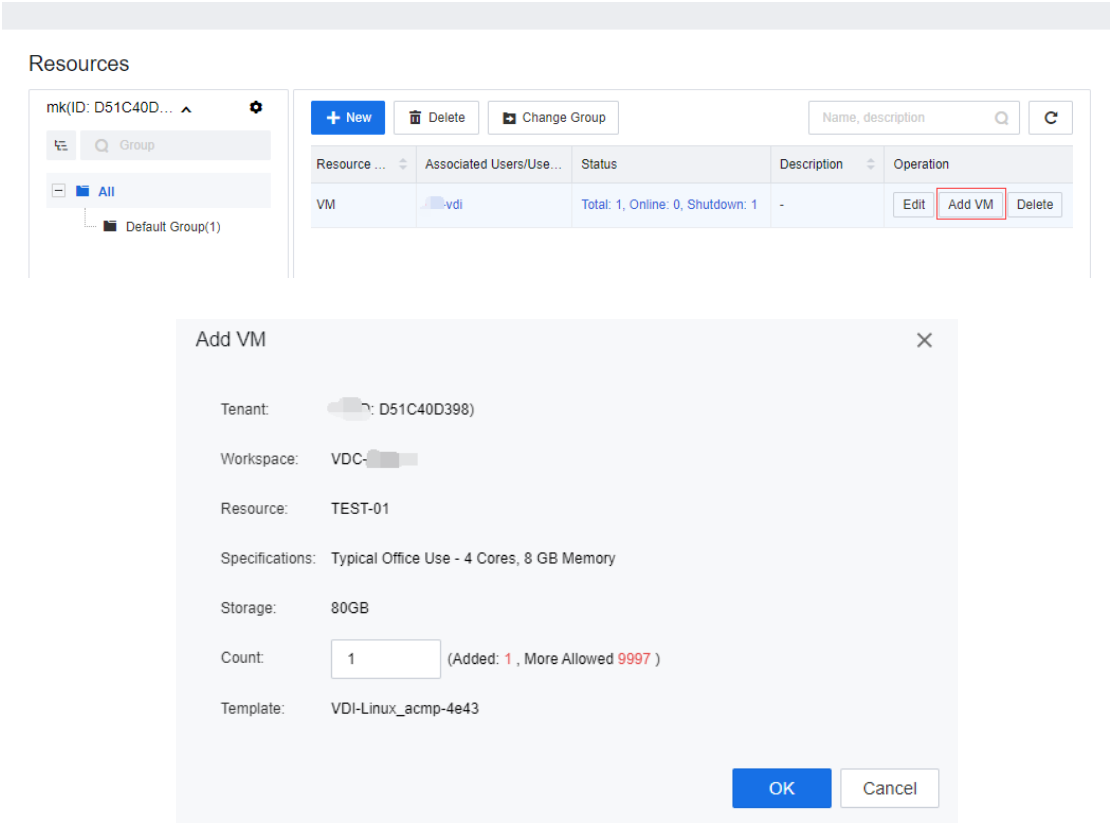
1. The tenant has created virtual machine resources on the SCP.
2. The SCP and the VDC in the corresponding workspace need to be associated with the same HCI cluster at the same time.
3. The tenant has associated the resource pool corresponding to the HCI cluster on the SCP and has allocated quota and VPC.
4. The template associated with the virtual machine resource must be in the shutdown state.

Steps:

Step 1. Log in to the SCP platform as admin, **select Compute > aDesk VDI > Resource**, click the drop-down arrow, select the tenant under the workspace to be managed in the drop-down menu that appears, and enter the

corresponding tenant resource management page.

Step 2. Click **Add** corresponding to the virtual machine resource that needs to add virtual desktops, enter the number to be added in the pop-up **Add VM** window, and click **OK**.



4.3.4.2.3 Delete VDI resources

Function Description:

When the existing VDI resources of the Sangfor SCP cloud management platform are no longer in use, the relevant resources can be deleted to release the resource quota of the corresponding tenant.

Prerequisite

This operation will delete relevant data and cannot be restored. Please proceed with caution.

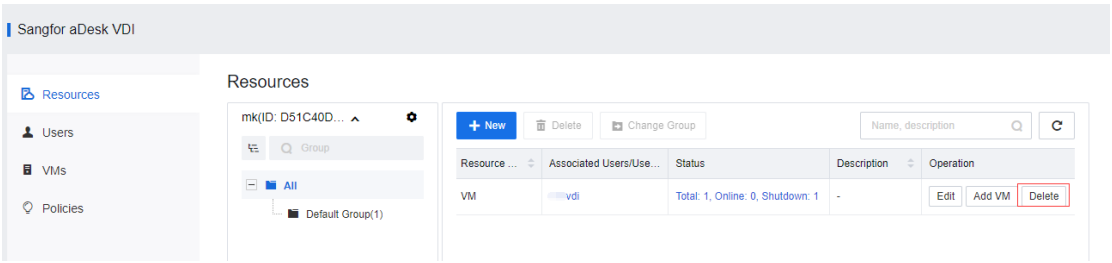
Precautions:

The tenant has created virtual machine resources on the SCP.

Steps:

Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > Resource**, click the drop-down arrow, select the tenant under the workspace to be managed in the drop-down menu that appears, and enter the corresponding tenant resource management page.

Step 2. Click **Delete** corresponding to the virtual machine resource to be deleted, enter **OK** in the pop-up **Delete Resource** window, and click **OK**.



4.3.4.3 Users

4.3.4.3.1 Create and manage user groups

1. Create New user group

Function Description:

Group users during initial deployment or add user groups later.

Prerequisites:

None.

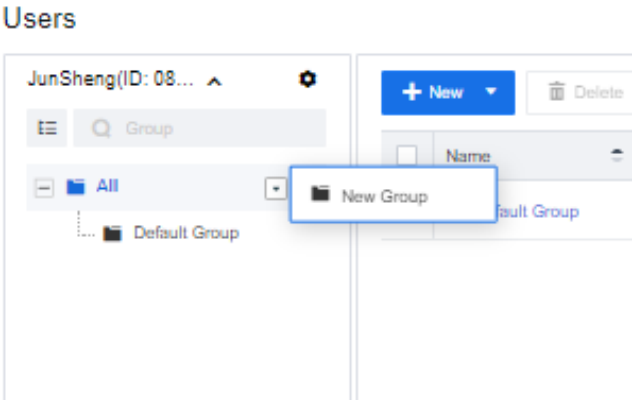
Precautions:

None.

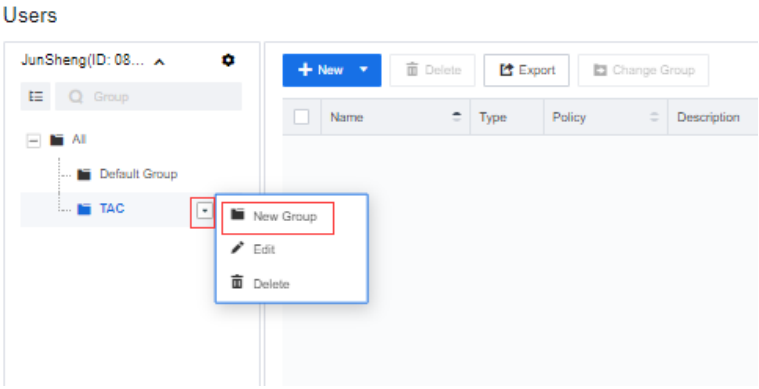
Steps:

Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > Users**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the user management page of the corresponding tenant.

Step 2. Click the drop-down arrow corresponding to the location where the user group needs to be created in the user group list on the left side of the user management page, and click **New Group** in the drop-down menu.



First-level user group creation



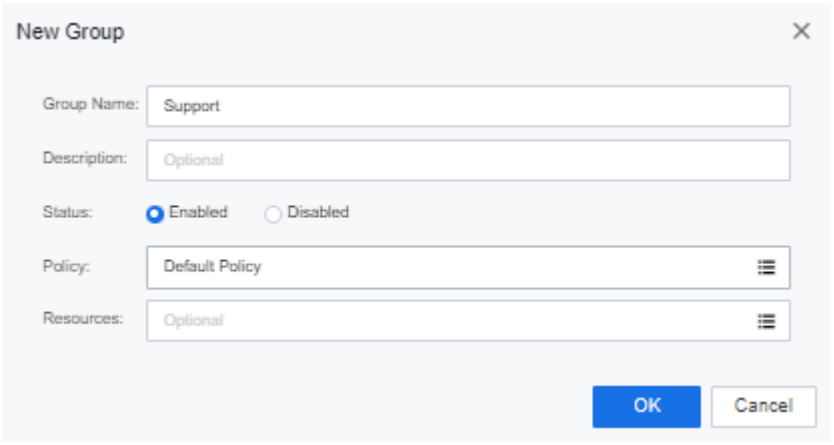
Subordinate user group creation

NOTE

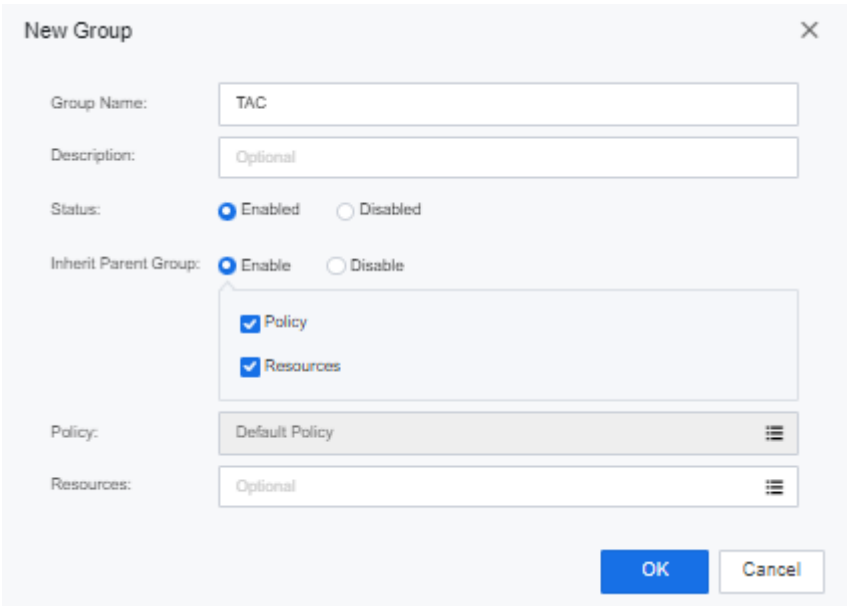
User groups are divided into first-level user groups and lower-level user groups. The user groups created under the **All** item are first-level user groups, and those created under the first-level user groups are lower-level user groups.

Step 3. On the **New Group** page, as shown in the figure below, fill in the corresponding information as required.

The first-level user group creation window:



Subordinate user group creation window:



Parameters	Description
Group Name	Name that identifies the VDI user group and must be filled in.
Description	You can optionally fill in the relevant description information of the user group.
Status	Check **Enable** to activate this user group; check **Disable** to disable this user group. The platform is enabled by default.
Inherit Parent Group	Only lower-level user groups can set whether to inherit policies and resources associated with upper-level user groups. **Policy:** Checked by default. After checking, this user group inherits the policy associated with the upper-level user group. It can no longer configure the policy independently (the associated policy

	option below is grayed out). After unchecking, it can be associated with the different upper-level user groups. **Resources:** Checked by default. After checking, the users in this user group automatically have the virtual desktop resource of the upper-level user group. After unchecking, the users in this user group only have the virtual desktop resource associated with this user group.
Policy	A user group can be bound to the corresponding policy group so that users in the user group can use the corresponding policy, and a policy group must be associated with it.
Resources	The optional configuration specifies the virtual desktop resources the user group can use.

2. Edit User Group

Function Description:

Modify the policies and resources associated with existing user groups.

Prerequisites:

None.

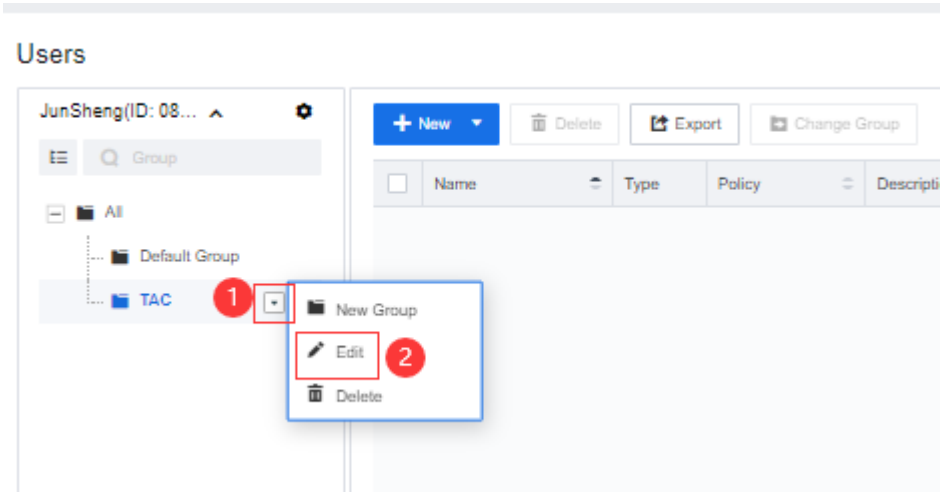
Precautions:

None.

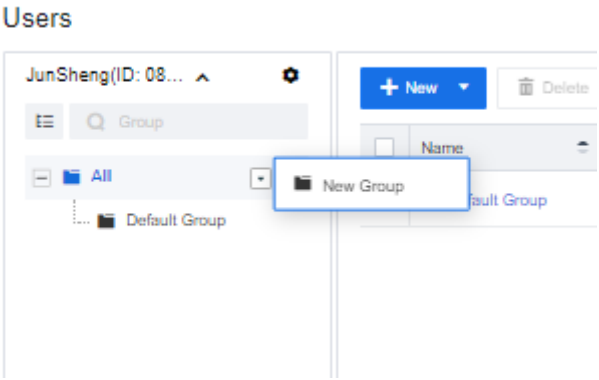
Steps:

Step 1. Log in to the SCP platform as admin, select **Compute> aDesk VDI > Users**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the user management page of the corresponding tenant.

Step 2. Click the drop-down arrow corresponding to the user group to be edited in the user group list on the left side of the user management page, and click **Edit** in the drop-down menu.



Step 3. The **Edit Group** window is shown in the figure below, and its content is the same as the newly added user group. You can modify the corresponding information as required. For specific item descriptions, please refer to the newly created user group.



3. Delete User Group

Function Description:

Delete unused user groups.

Prerequisite

None.

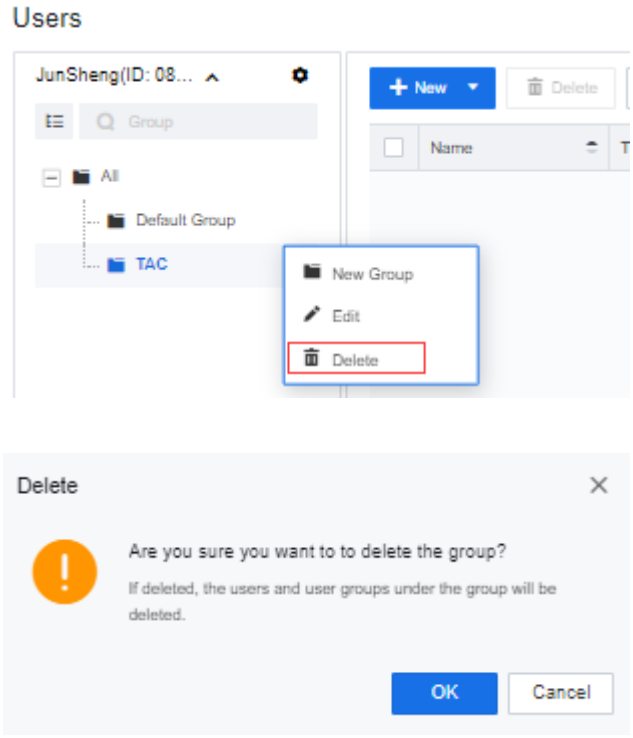
Precautions:

Deleting a user group will delete all users and subgroups under this group and cannot be restored. You need to confirm that there is no need to retain users or subgroups.

Steps:

Step 1. Log in to the SCP platform as admin, select **Compute> aDesk VDI > Users**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the user management page of the corresponding tenant.

Step 2. Click the drop-down arrow corresponding to the user group to be deleted in the user group list on the left side of the user management page, click **Delete** in the drop-down menu, and click **OK** in the pop-up Delete window.



4.3.4.3.2 User creation and management

1. Create New User

Function Description:

Create local users during the initial deployment or add new users later.

Prerequisite

None.

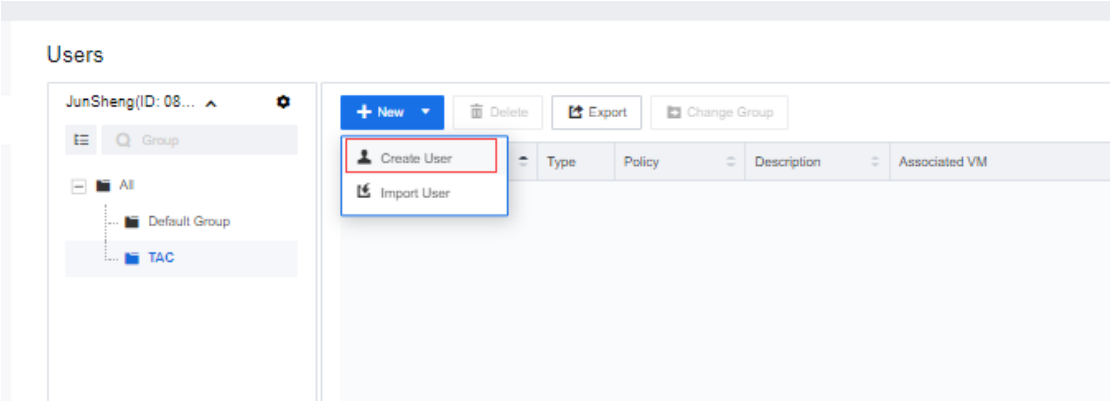
Precautions:

None.

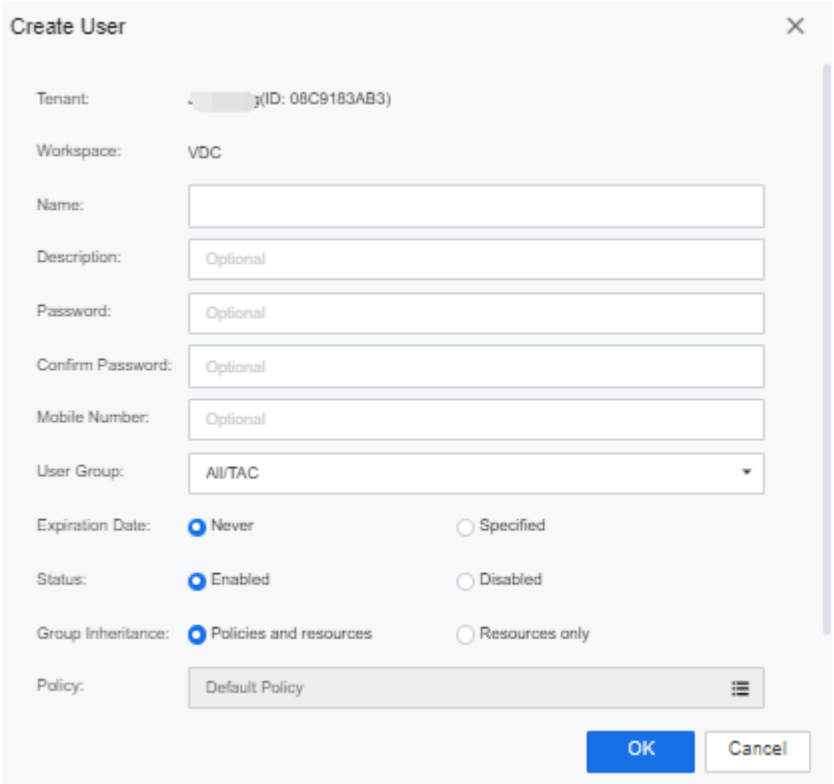
Steps:

Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > Users**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the user management page of the corresponding tenant.

Step 2. Select the user group to be created in the user group list on the left side of the user management page, click **New,** and select **Create User.**



Step 3. In the pop-up **Create User** window, fill in the relevant information of the user account and click **OK**.



Parameters	Description
Tenant	Unmodifiable, automatically displayed by the system to indicate which tenant the currently created account belongs to.
Workspace	Unmodifiable, the system automatically displays it to indicate which workspace (VDC) the currently created account belongs to
Name	The account used by the VDI user to log in to the cloud desktop.
Description	You can optionally fill in the relevant description information of the user.
Password.	It is used to set the password of the VDI login account.
Confirm Password	Password for reconfirming the VDI login account.
Mobile Number	Fill in the user's mobile phone number.
User Group	Set which user group the user belongs to.
Expiration Date	Including **Never Expires** and **Specified.** 1. If **Never expires** is selected, the user can always use it. 2. If **Specified** is selected, then select the date in the following box. If this time is reached, the user will be disabled.
Status	Can choose **Enabled** or **Disabled**. 1. If **Enable** is selected, the account can be used normally; 2. If **Disable** is selected, the account is disabled and cannot be used.
Group Inheritance	Set the user group association policy and resource mode the user inherits. **Policies and Resources**: This option is selected by default. The user inherits the policies and resources associated with the user group to which he belongs and can no longer configure the policies individually (the associated policy option below is grayed out) but can associate with other virtual desktops resource. **Resources only**: After selecting this option, this user will only inherit the resources associated with the user group to which he belongs, and the associated policy needs to be set in the associated policy.
Policy	Users can be bound to corresponding policy groups so that users in the user group can use corresponding policies.
Resources	Optional configuration to specify the virtual desktop resources available to this user.

2. Import User

Function Description:

For scenarios where users need to be created in batches, SCP supports batch creation of users by importing from a CSV file.

Prerequisite

None.

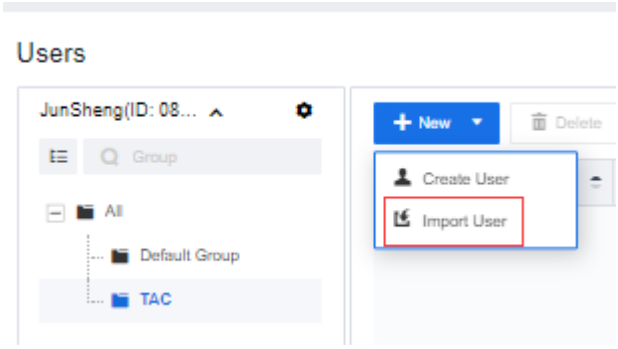
Precautions:

None.

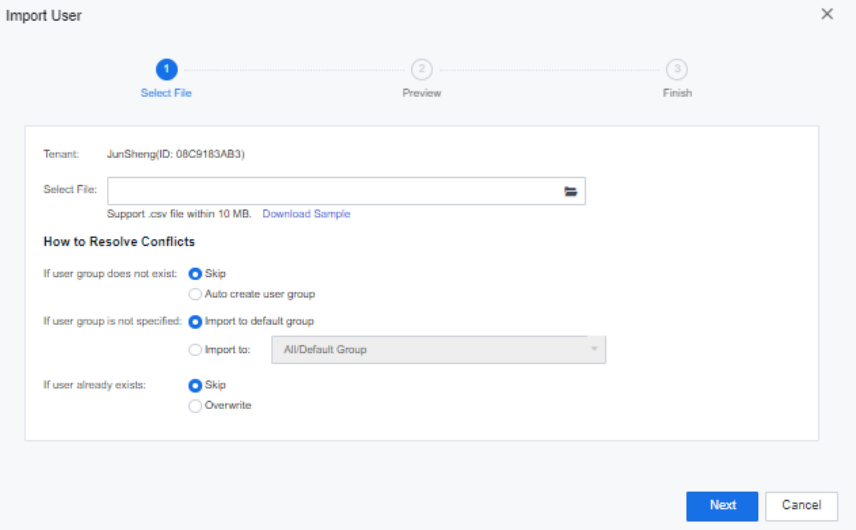
Steps:

Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > Users**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the user management page of the corresponding tenant.

Step 2. Select the user group to be created in the user group list on the left side of the user management page, click **New,** and select **Import User**.



Step 3. In the pop-up **Import User** window, select the CSV file where the user account information is configured. After setting the conflict handling rules, follow the guidance and click **Next** until it is complete.



The description of each function of conflict handling rules is shown in the following table:

Conflict Scenario	Description
If the user group does not exist.	Set the processing rules for the user group to which the user set in the CSV file belongs when the workspace corresponding to the SCP tenant does not exist. You can choose one of the following two processing methods. **Skip:** The default option. SCP will skip this user and not import it. **Auto create user group:** SCP will automatically create a new user group with the same name in the workspace of the corresponding tenant for related users to import.
If user group is not specified	To set the processing rules of SCP for the user accounts of the specified user group in the CSV file, you can choose one of the following two processing methods: **Import to default group:** the default option. SCP will import all user accounts in the CSV file that does not specify the user group to which they belong to the default user group. **Import to:** The administrator needs to specify the target user group to be imported into. SCP will import all user accounts in the CSV file that does not specify the user group to which they belong to the specified user group.

If user already exist	To set the processing rules for the user account with the CSV file that already exists in the tenant's workspace on the SCP. You can choose one of the following two processing methods: **Skip:** The default option. SCP will skip this user and not import it. **Overwrite:** SCP will overwrite the existing account with the same name in SCP with the user information recorded in the CSV file.



You can import user accounts in batches through CSV files and support the import of **Username, Added to Group, Password, Mobile Number,** and **Description**, where **Username** is a required item, others are optional. Click the **Download Sample** to download the sample CSV file format.

3. Edit User

Function Description:

Modify the attributes of existing users.

Prerequisite

None.

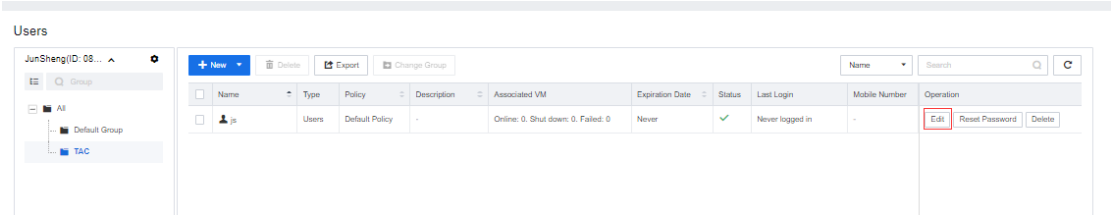
Precautions:

None.

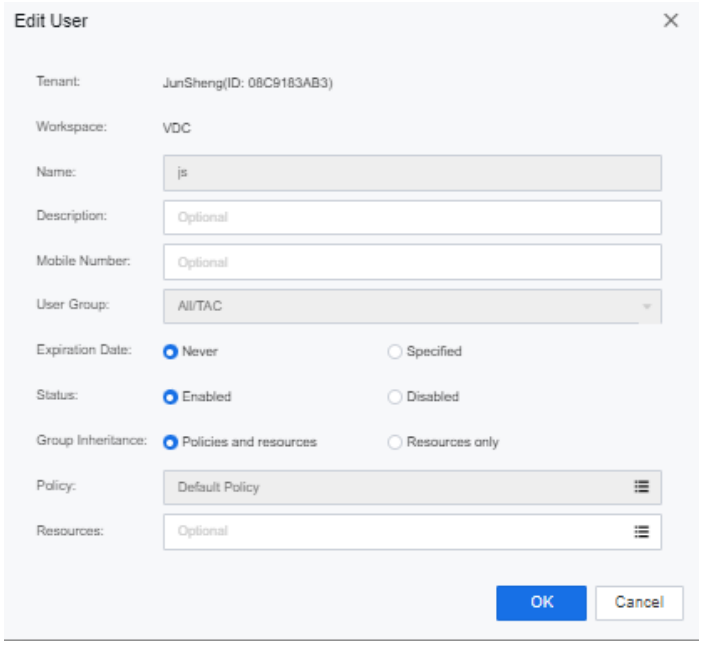
Steps:

Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > Users**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the user management page of the corresponding tenant.

Step 2. Select the user account to be edited and click **Edit**.



Step 3. The **Edit User** window is shown in the figure below, and its content is the same as that of the newly added user (excluding setting passwords). You can modify the corresponding information according to your needs. For specific item descriptions, please refer to **Create New User**.



4. Reset User Password

Function Description:

When a VDI user forgets his password, the administrator can reset it on the SCP.

Prerequisite

None.

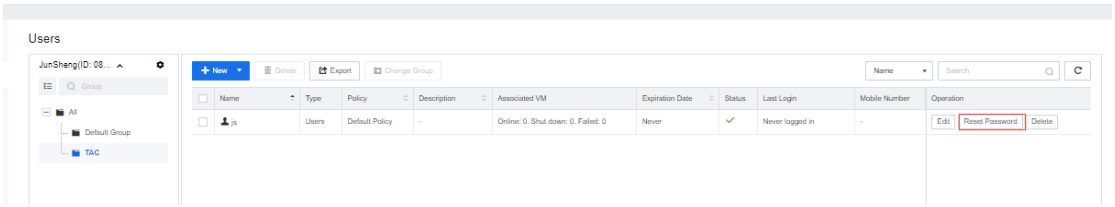
Precautions:

None.

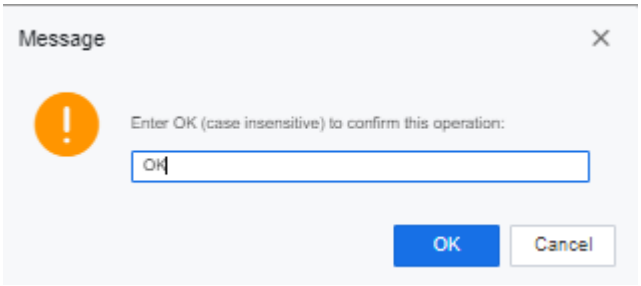
Steps:

Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > Users**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the user management page of the corresponding tenant.

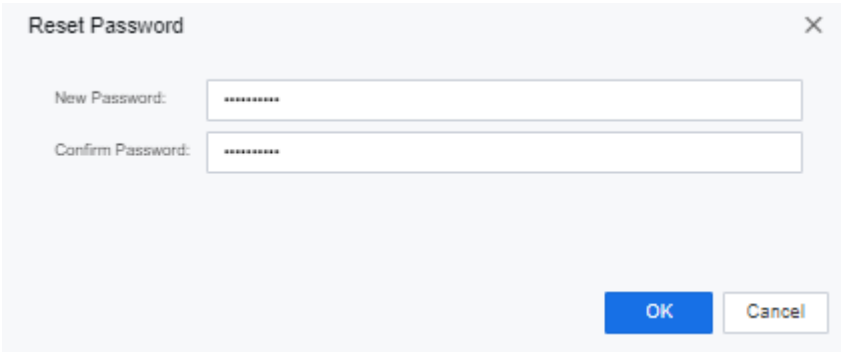
Step 2. Select the user account to be edited and click **Reset Password**.



Step 3. Enter **OK** in the pop-up window and click **OK** to confirm the password that needs reset.



Step 4. In the **Reset Password** window, enter the user's new password after resetting and click **OK**.



5. Export User

Function Description:

Export the user information of the tenant in the corresponding workspace on the SCP for the administrator's statistical use.

Prerequisite

None.

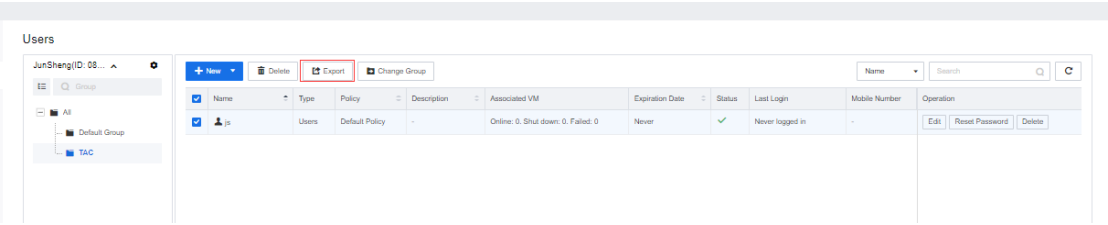
Precautions:

None.

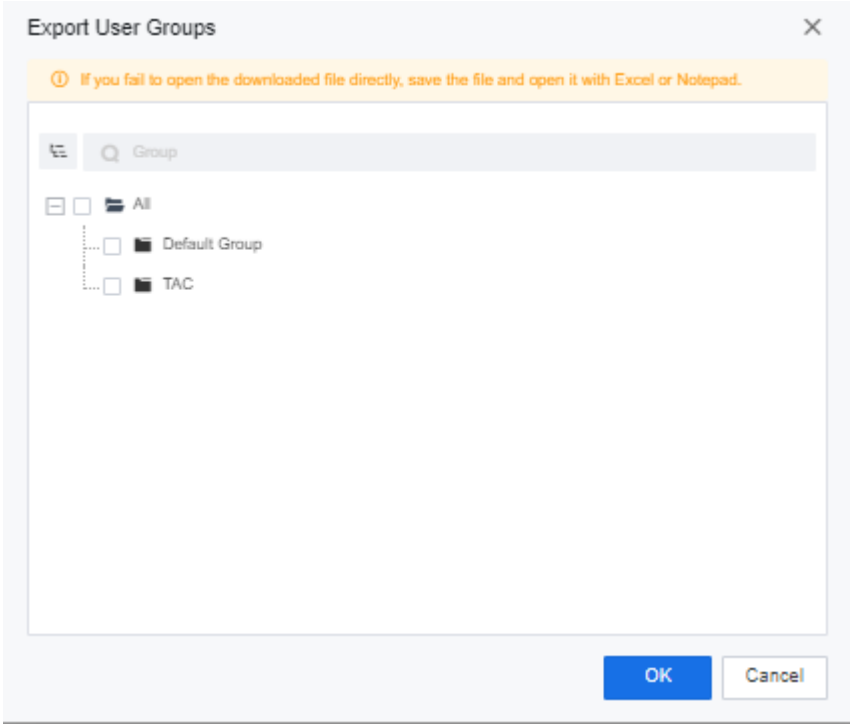
Steps:

Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > Users**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the user management page of the corresponding tenant.

Step 2. Click **Export**, select the range of user groups to be exported in the pop-up Export Users window, and click **OK** to export and download the user information under the corresponding user group as a CSV file to the local.



Step 3. The **Export User Groups** window is shown below.



6. Delete User

Function Description:

Delete users that are no longer in use.

Prerequisite

None.

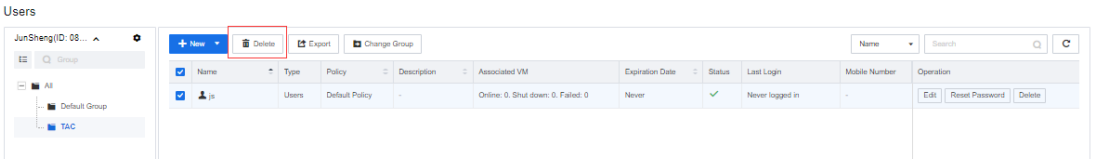
Precautions:

None.

Steps:

Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > Users**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the user management page of the corresponding tenant.

Step 2. Select the user accounts to be deleted, click **Delete**, and click **OK** in the pop-up **Delete User/User Group** window.



4.3.4.4 VMs

4.3.4.4.1 VM password recovery

Function Description:

Applicable to scenarios where virtual machine passwords need to be recovered.

Prerequisite

None.

Precautions:

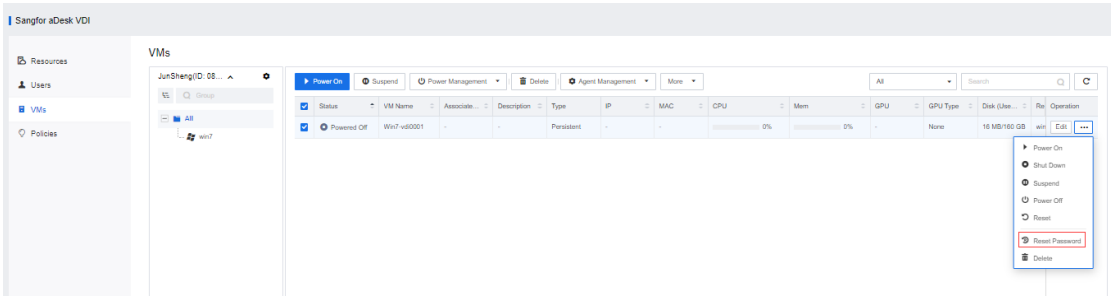
User credentials related to passwords may be lost. For example, NTFS encrypted files will be lost.

Steps:

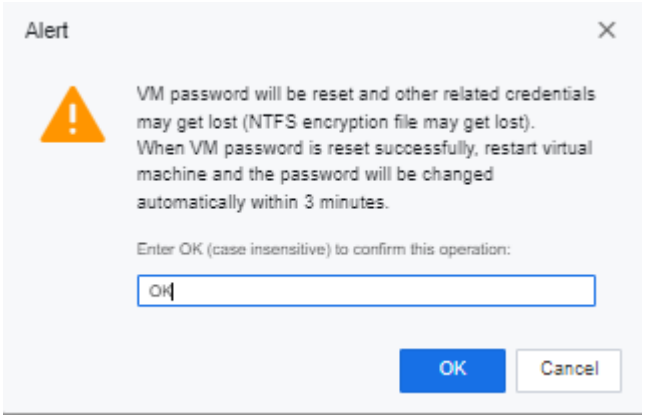
Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > VMs**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the VMs

management page of the corresponding tenant.

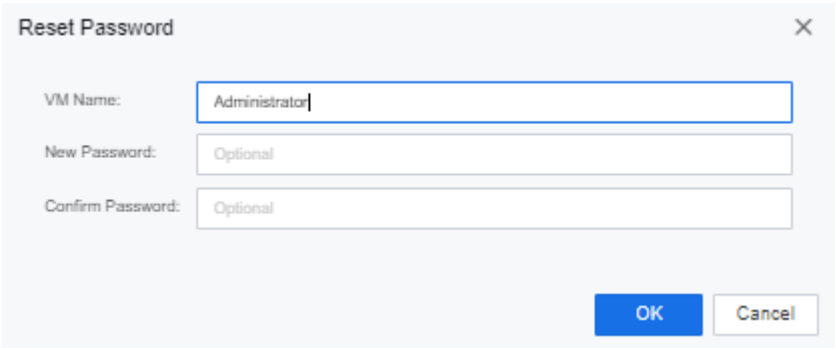
Step 2. Find the virtual machine whose password needs reset, click the corresponding ... button in the virtual machine entry, and select **Reset Password**.



Step 3. At this point, the system will display the following alarm. After understanding the risks in detail, enter **OK**, and then click **OK**.



Step 4. The system will pop up a reset password input box. After the administrator enters the Windows login user name and password corresponding to the reset virtual machine, the user restarts the virtual machine to take effect.



4.3.4.4.2 Modify VM computer name

Function Description:

It is suitable for scenarios where the computer name of the virtual machine needs to be modified or user-defined.

Prerequisite

None.

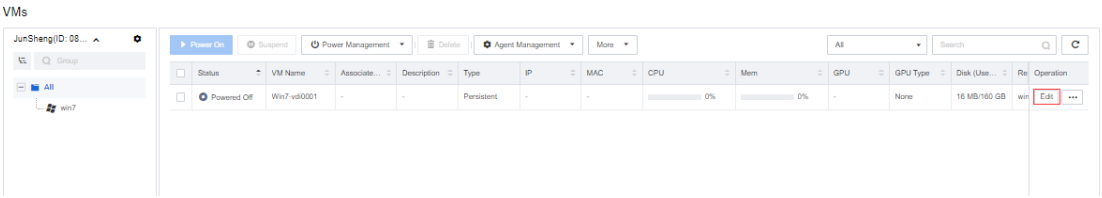
Precautions:

The credential information related to the password may be lost, such as NTFS encrypted files will be lost.

Steps:

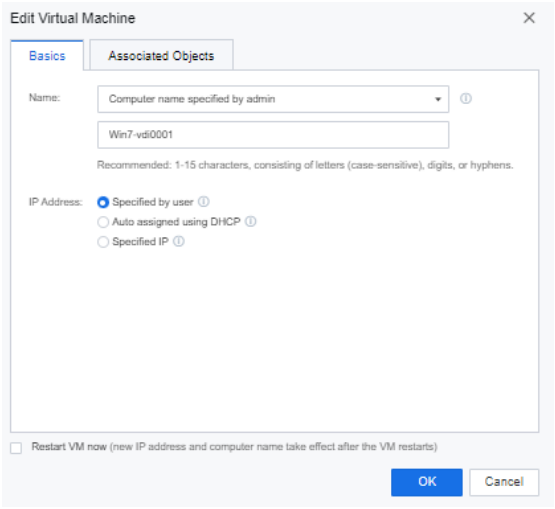
Step 1. Log in to the SCP platform as admin, **select Compute > aDesk VDI > VMs**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the VM management page of the corresponding tenant.

Step 2. Find the virtual machine whose computer name needs to be modified, and click the **Edit** button in the corresponding virtual machine entry.



Step 3. In the pop-up **Edit Virtual Machine** window, under the **Basic** tab, select one of the following three methods to modify:

- **Computer name specified by admin:** Fill in the new name.
- **Specified by user**: The user can modify it in the virtual machine.
- **Same as username**: After the virtual machine is associated with the user, it will be automatically changed to the user account name



Step 4. Check **Restart VM now (new IP address and computer name take effect after the VM restarts) checkbox,** and click **OK** to restart the virtual machine immediately to take effect of the modified configuration.

4.3.4.4.3 Virtual machine binding user

Function Description:

It is suitable for scenarios where virtual machines and users need to be manually bound.

Prerequisite

None.

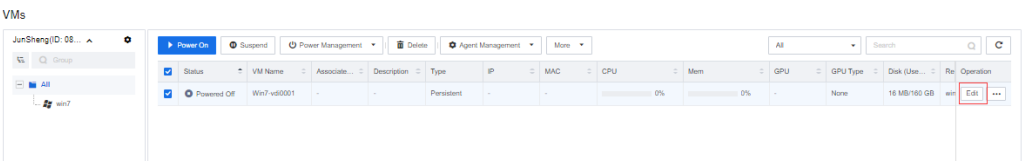
Precautions:

After the bound user of the virtual machine is changed, the original bound user cannot log in to the virtual machine.

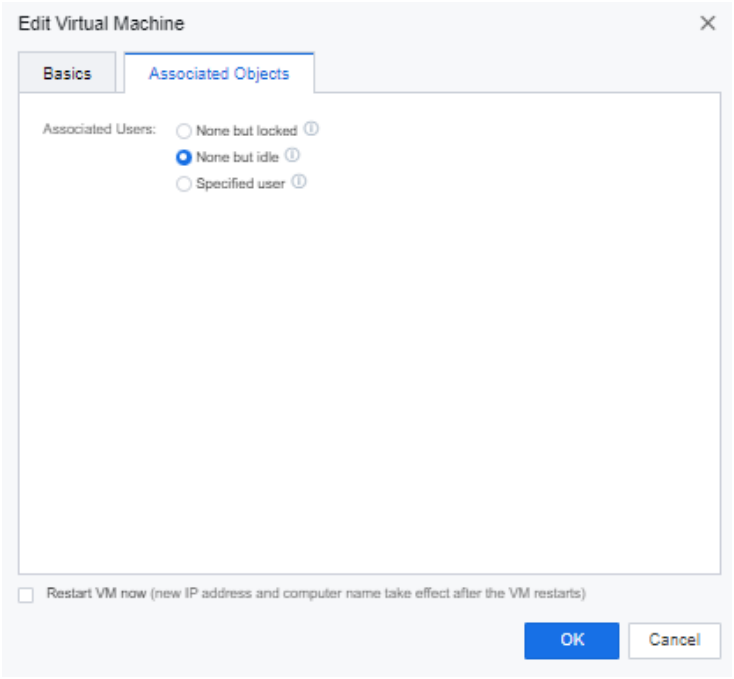
Steps:

Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > VMs**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the VM management page of the corresponding tenant.

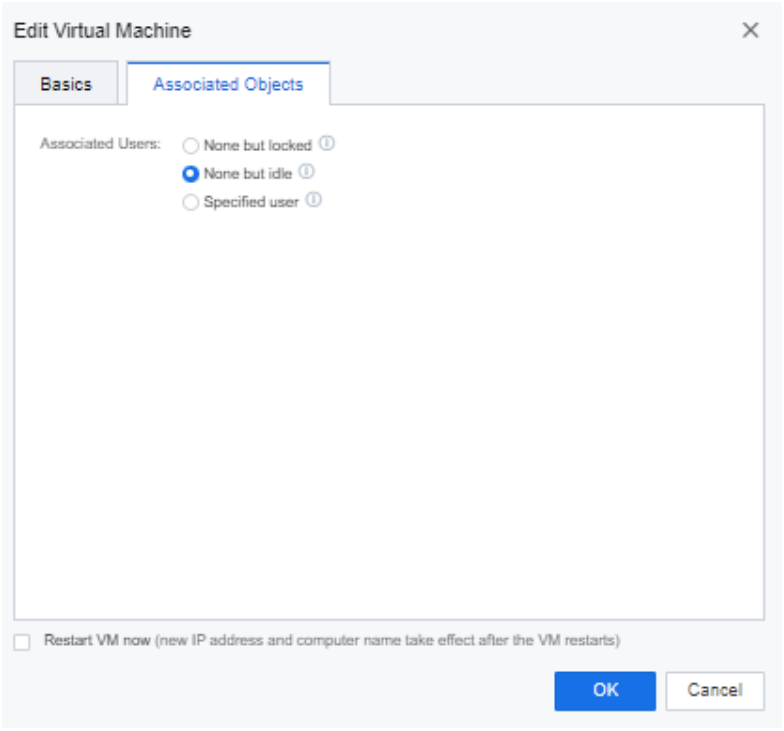
Step 2. Find the virtual machine whose computer name needs to be modified, and click the **Edit** button in the corresponding virtual machine entry.



Step 3. In the pop-up **Edit Virtual Machine** window, under the **Associated Objects** tab, under **Associated User**, select **Associated User** and select the user to be bound.



Step 4. Check **Restart VM now (new IP address and computer name take effect after the VM restarts)** checkbox and click **OK** to restart the virtual machine immediately to take effect of the modified configuration.



4.3.4.4.4 Specify the IP address of the virtual machine

Function Description:

It applies to scenarios where a single IP address of a virtual machine needs to be specified or modified.

Prerequisite

None.

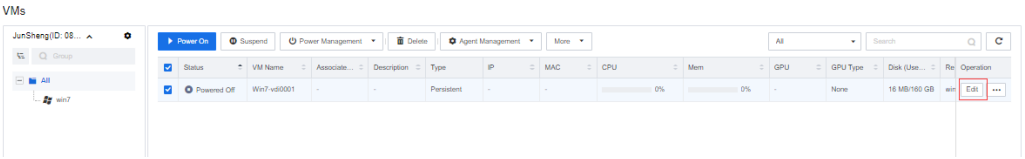
Precautions:

None.

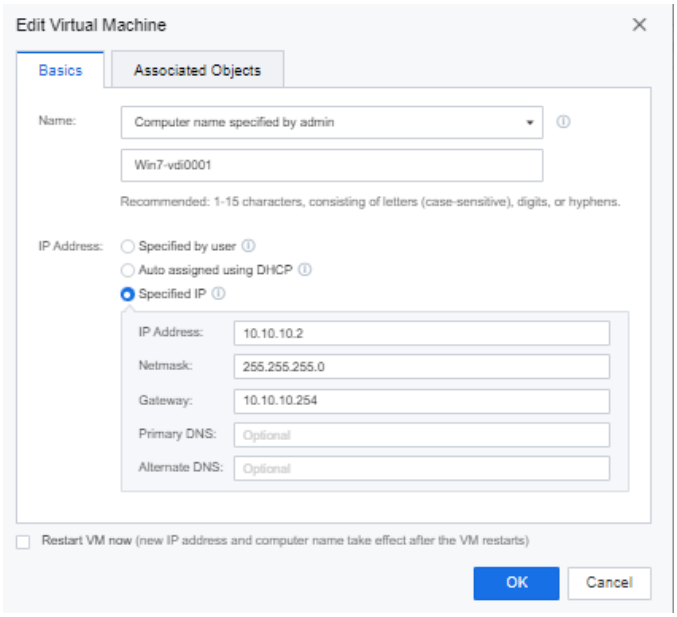
Steps:

Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > VMs**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the virtual machine management page of the corresponding tenant;

Step 2. Find the virtual machine whose computer name needs to be modified, and click the **Edit** button in the corresponding virtual machine entry.



Step 3. In the pop-up **Edit Virtual machine** window, under the **Basic tab > IP Address**, select **Specify IP**, and modify the IP address, subnet mask, and other information.



Step 4. Check **Restart VM now (new IP address and computer name take effect after the VM restarts)** and click **OK** to restart the virtual machine immediately to take effect of the modified configuration.

4.3.4.5 Policies

4.3.4.5.1 Create Policies

Function Description:

Sangfor SCP cloud management platform requires administrators to manage the platform, and the platform has a built-in super administrator admin. Super administrators can create three administrator roles: system administrator, security administrator, and audit administrator, assign different permissions to manage the cluster, and assist super administrators in managing the SCP platform.

Prerequisite

1. Only one policy group can be associated with the same user/user group;

2. The associated policy group must be configured on the user management and user/user group property pages.

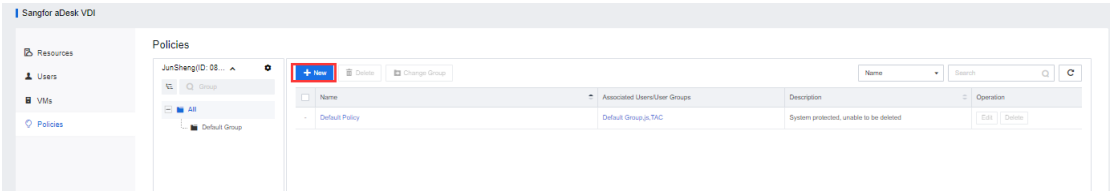
Precautions:

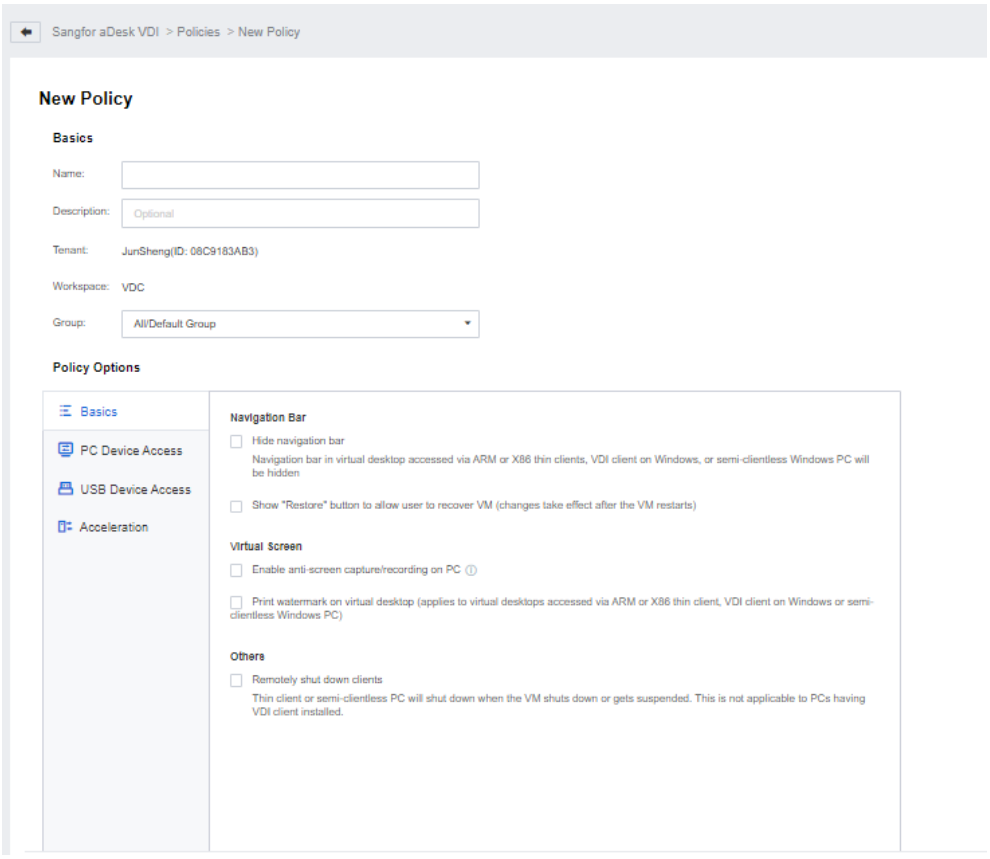
None.

Steps:

Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > Policies**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the policy management page of the corresponding tenant.

Step 2. 2. Click **New**, fill in the policy-related information as needed on the pop-up **New Policy** page, and configure each policy.





4.3.4.5.2 Basic Configuration

1. Navigation bar

Function Description:

In the case of using a thin terminal or a PC all-in-one terminal, if you want to operate in the same way as the local PC and do not need additional control functions, you can enable the hidden navigation bar so that the top of the desktop does not display the navigation bar after accessing the virtual desktop.

Prerequisite

None.

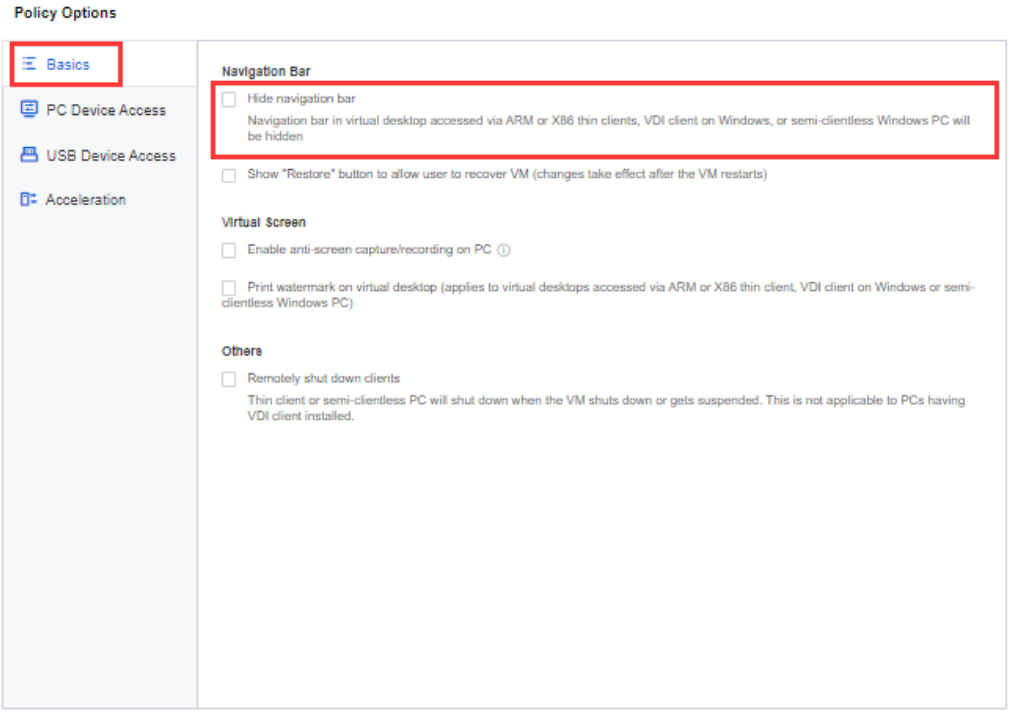
Precautions:

Suppose the integration of shutdown is selected, and the Hide navigation bar is not selected. In that case, the navigation bar on the user's desktop does not provide the functions of windowing, minimizing, and closing windows. Other functions, such as restarting, restoring, and locking the navigation bar are provided.

Steps:

Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > Policies**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the policy management page of the corresponding tenant.

Step 2. To create or edit an existing policy, select **Hide Navigation Bar** in **Navigation Bar** on the **Basics** tab of the policy option.



2. User Self-Recovery Snapshot

Function Description:

When an administrator configures an automatic snapshot policy for a virtual machine, before enabling the self-recovery snapshot function of users, the user can select a snapshot to perform a restore operation in the virtual machine navigation bar to quickly restore the desktop working state and solve the problem that cannot be solved by restarting.

Prerequisite

At least one snapshot of the user virtual machine already exists.

Precautions:

1. Restoring the system disk is risky. Please back up important data on the system disk in advance.

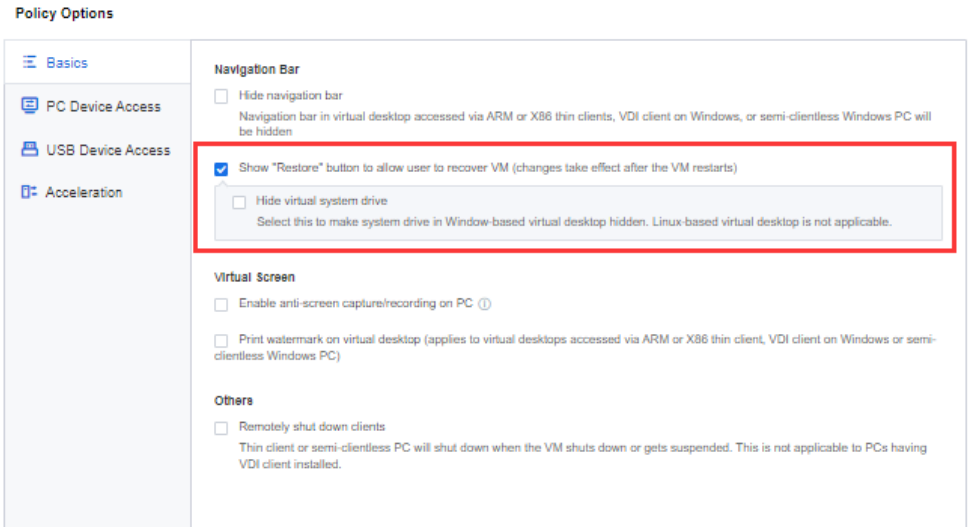
2. This snapshot restore is only for the user's system disk and does not support restoring the data disk. The data disk restoration needs to be operated by the administrator in the background, and the system disk needs to be restored synchronously.

Steps:

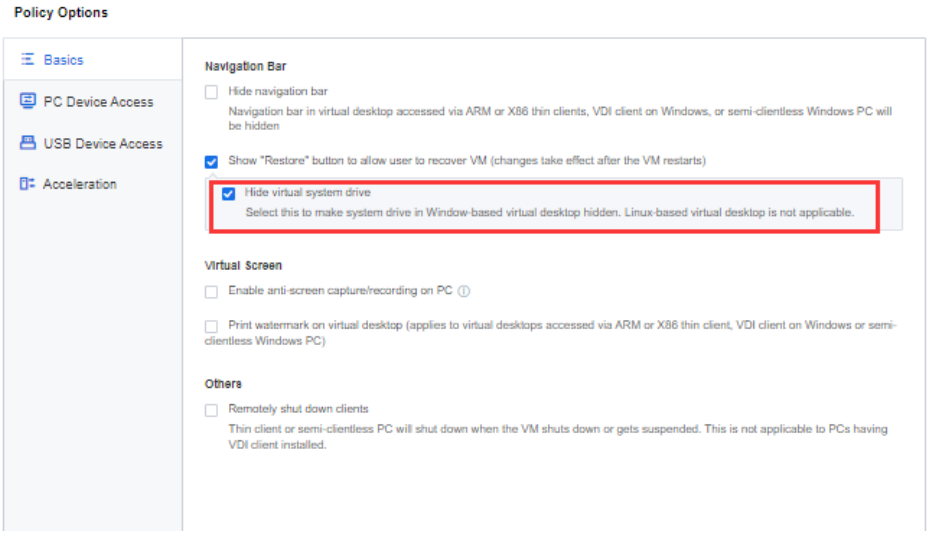
Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > Policies**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the policy management page of the corresponding tenant.

Step 2. To create or edit an existing policy, **select Show "Restore" button to allow user to recover VM** under the **Basic > Navigation Bar.**

Step 3. After selecting **Show "Restore" button to allow user to recover VM**,



you can further configure **Hide virtual system drive** to hide the system C drive to prevent users from actively writing personal data to the C drive-related directories to avoid this part of personal data from being lost when restoring snapshots.



3. PC anti-screenshot / anti-screen recording

Function Description:

For enterprise customers with high data security requirements, the **PC anti-screenshot/anti-screen recording** function can enable users to access virtual machines through VDI clients, preventing users from capturing virtual desktop images through PC local screen capture/screen recording software. Thereby obtaining confidential data on the virtual desktop.

Prerequisite

Only applicable on Windows endpoints.

Precautions:

1. Anti-screen recording only supports Win10 and Win11 PC terminals, other terminals are not supported.

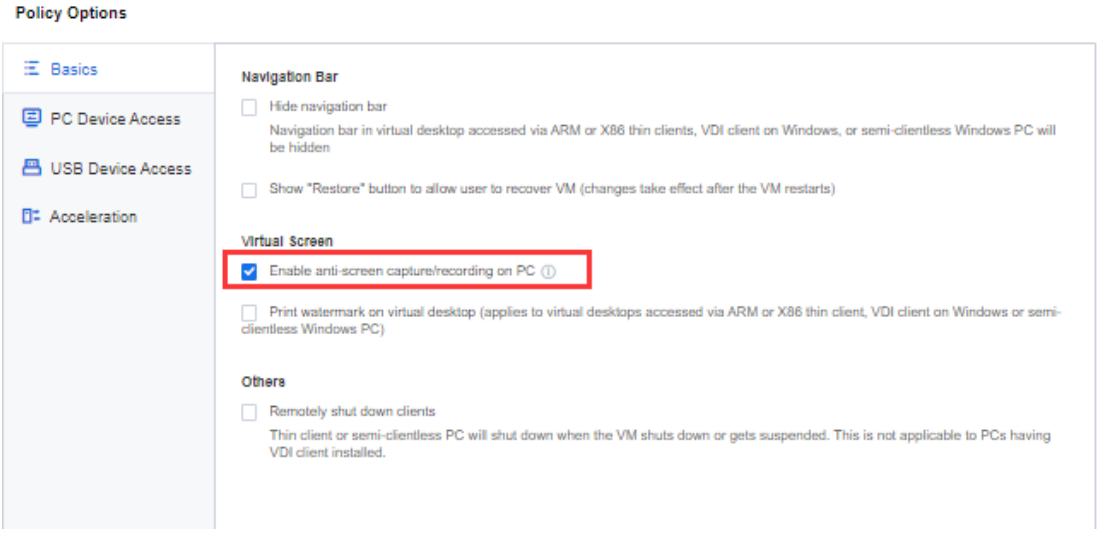
2. After enabling the **PC anti-screenshot/anti-screen recording** function, non-win10/11 Windows PC client virtual desktops cannot be windowed and self-service functions cannot be used.

Steps:

Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > Policies**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the policy management page of the corresponding tenant;

Step 2. To create a new or edit an existing policy, in the **Virtual Screen**

Configuration on the **Basics** tab, select **Enable anti-screen capture/recording on PC.**



4. Screen Watermark

Function Description:

For some enterprises or institutions, internal data leakage may bring huge losses. Enable a screen watermark to display information such as user name and IP address on the user's virtual machine. When the user uses the VDI desktop, the screen capture/photograph will be accompanied by a watermark, thereby preventing users from taking screenshots/photographs of intranet data, reducing the risk of data leakage, ensure data security.

Prerequisite

None.

Precautions:

1. The screen watermark supports PC clients, ARM thin terminals, X86 thin terminals, and Windows PC-integrated client access but does not support mobile terminals.

2. The custom location of the screen watermark is not supported at the moment. Therefore, the screenshot and screen recording tools used locally in the virtual machine do not include the watermark.

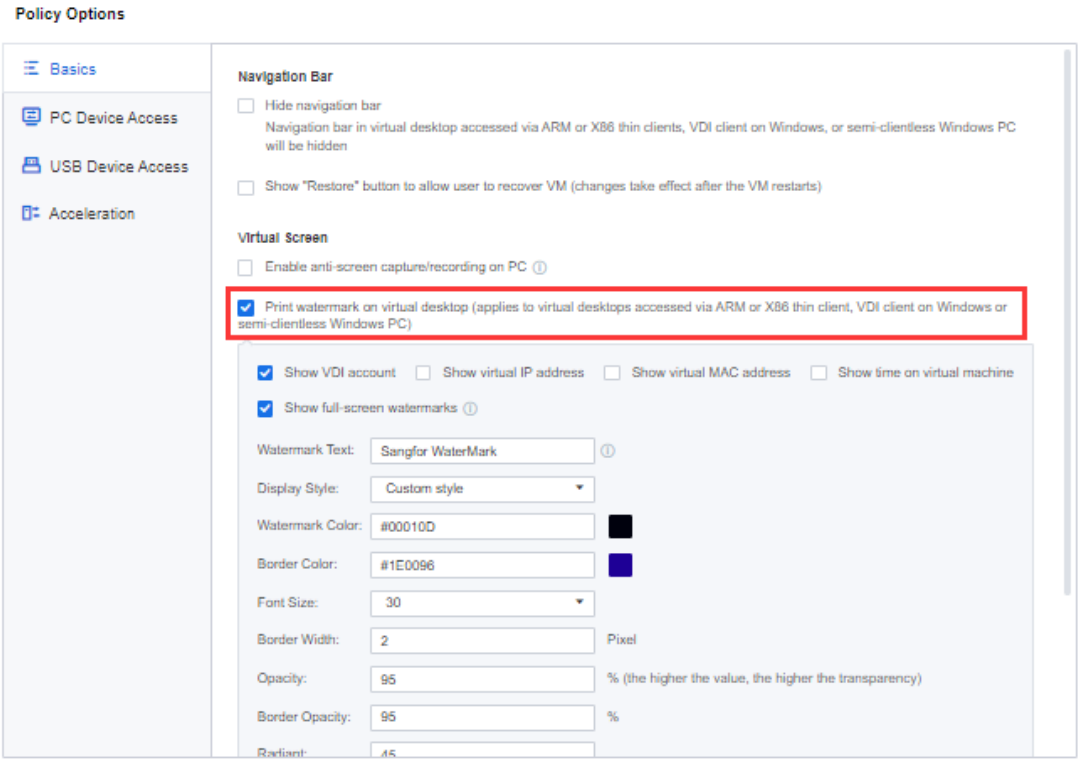
3. Modifying the configuration related to the screen watermark on the VDC requires the client user to log out and log in again to take effect (there is no need to restart the VM).

4. If **Show virtual machine IP address** and **Show time on virtual machine** are configured, the watermark content will be refreshed once a minute without flickering.

Steps:

1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > Policies**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the policy management page of the corresponding tenant.

2. Under the virtual screen section of the **Basic** Configuration tab of the **Policy Options**, select the **Print watermark on virtual desktop** and set relevant parameters for the watermark display.



- **Optional watermark content: D**isplay VDI account, display virtual machine IP address, display virtual machine MAC address, display virtual machine time, and display full-screen watermark.
- **Custom watermark content: Text is supported only and cannot exceed 46 characters (a Chinese or English character occupies width of one character, and so is a space).**

- **Display style:** You can choose one of the four styles that come with the system or a custom style. Only after you choose a custom style can you modify the watermark content color, font size, border color, etc.
- **Opacity:** The higher the opacity value, the more transparent it is. The same is true for the transparency of the watermark border.

4.3.4.5.3 Shutdown integration

Function Description:

To shut down the thin client and the PC VDI client that accesses the cloud desktop. After the shutdown integration is enabled, the terminal can be shut down synchronously while the dedicated desktop is shut down. To achieve an experience similar to a physical PC, there is no need to shut down twice (one for the dedicated and one for the terminal), improving the product's usability.

Prerequisite

None.

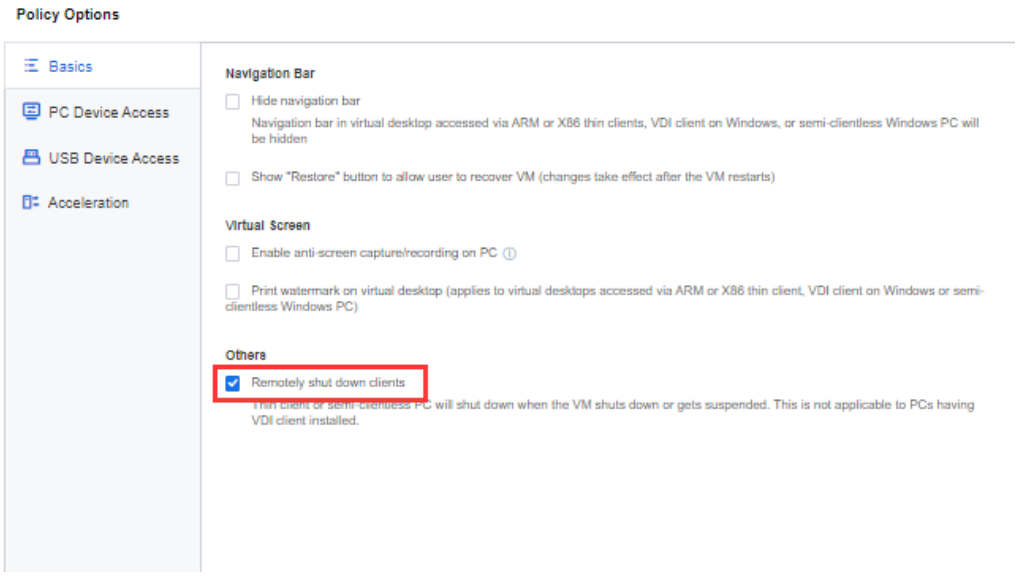
Precautions:

This function only takes effect on dedicated desktop resources and does not take effect on remote applications, remote desktops, and shared desktop resources. PC client scenarios are not supported.

Steps:

Step 1. Log in to the SCP platform as admin, select **Compute> aDesk VDI > Policies**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the policy management page of the corresponding tenant.

Step 2. To create a new or edit an existing policy, on the **Basic** tab of the policy option, select **Remotely shut down clients under Others.**



4.3.4.5.4 PC Device Access

Function Description:

Users can use this configuration to set whether to allow the PC clipboard, PC hard drive, PC CD/DVD drive, serial port redirection, and parallel port redirection.

Prerequisite

None.

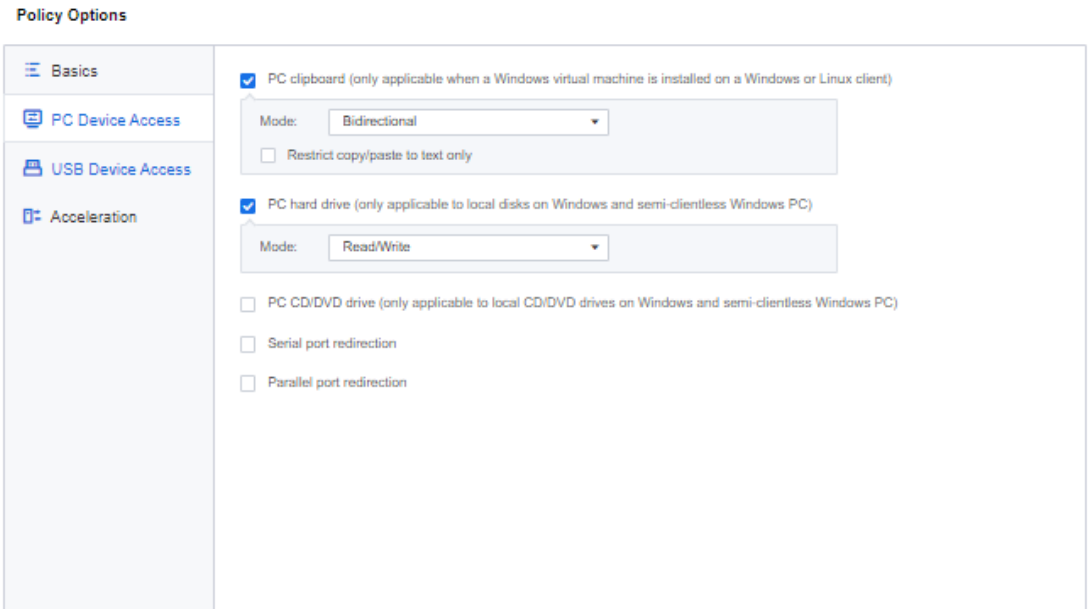
Precautions:

The PC clipboard currently only supports using Windows and Linux clients to access Windows virtual desktops but not Linux clients or Windows clients to access Linux virtual machines.

Steps:

Step 1. Log in to the SCP platform as admin, select **Compute> aDesk VDI > Policies**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the policy management page of the corresponding tenant.

Step 2. Create or edit an existing policy. On the **PC Device Access** tab of the policy option, configure Allow **PC Clipboard, PC Hard Drive, PC CD/DVD drive, Serial port redirection**, and **Parallel Port Redirection** as required.



- **PC clipboard:** Enabling the client clipboard function, and you can choose from **Bidirectional, Guest to host, Host to guest** three options. If the **PC clipboard** is not selected, the client clipboard function is not enabled. At this time, users corresponding to the group policy will not be able to use this function.
- **Restrict copy/paste to text only:** Only text can be copied between the client and the virtual desktop through the clipboard, not files.
- **PC hard drive:** The client's local disk is mapped to the virtual machine if selected. There are two options: **Read/Write** and **Read-Only**. If the PC hard drive is not selected, the client's local disk cannot be mapped to the virtual machine.
- **PC CD/DVD drive**: The client's local CD-ROM is mapped to the virtual machine if selected. There are two options: **Read/Write** Mode and **Read-Only** Mode. Unchecking the **PC CD/DVD drive** means that the client's local CD-ROM drive cannot map to the virtual machine.
- **Serial port redirection, Parallel port redirection:** It refers to redirecting the serial port and parallel port of the PC to the virtual machine so that the user can use the serial port and parallel port devices (such as printers, plotters, scanners, other serial port, and parallel port interface devices)

plugged into the PC on the virtual machine. Like using on PC. The virtual machine can use serial and parallel devices if selected. It is not allowed to use if not selected.

A. When creating a new policy group, the serial port number and parallel port number mapped to the virtual machine are bound to the PC serial port number and parallel port number, which is the same as those of the PC, for example:

- The local serial port number of the PC is COM3, and the serial port number of the virtual machine is also COM3.
- The parallel slogan of the PC is LPT3, and the virtual machine's parallel slogan is LPT3.

B. When using the default policy group:

- The local serial port of the PC is COM3, and the serial port of the virtual machine is COM2;
- The local parallel port of the PC is LPT3, and the parallel port of the virtual machine is LPT3.

C. Instructions for use and precautions:

- The local PC and virtual machine must install the same corresponding driver. The virtual machine's serial/parallel port settings need to be consistent with the local PC, and the peripherals can be used(the picture shows the printer).
- In the device manager of the PC, check whether the PC's local serial/parallel device state is normal.
- Check the serial port/parallel port device redirection is successful in the device manager of the virtual machine.
- The third-party software has exclusive access to the COM port and does not support multiple software using one COM port simultaneously.
- Repeated printer driver installation will cause driver confusion, so you need to uninstall and reinstall the driver.

4.3.4.5.5 USB Device Access

Function Description:

Set whether the virtual machine can use a certain type of USB device and

perform special processing on a certain USB device in the exception list during the mapping process. The device permission control in the exception list has a higher priority than the permission control configured on the upper-layer page.

Prerequisite

None.

Precautions:

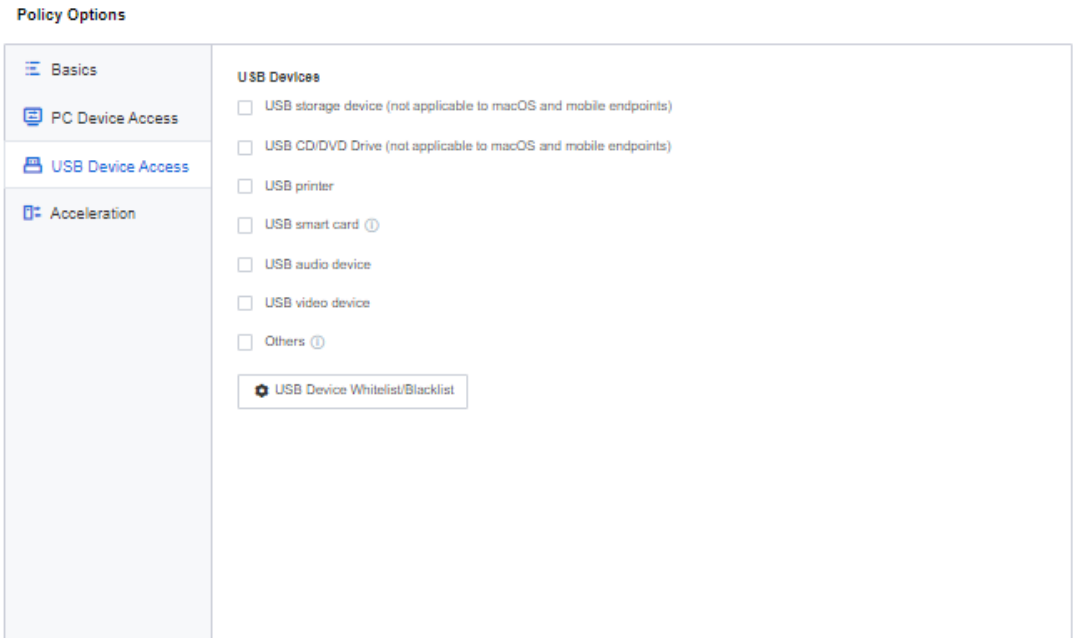
None.

Steps:

Step 1. Log in to the SCP platform as admin, select **Compute> aDesk VDI > Policies,** click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the policy management page of the corresponding tenant;

Step 2. Create or edit an existing policy. Under the **USB Device Access** tab of the policy option, set allow **USB Storage device, USB CD/DVD Drive, USB Printer, USB smart card, USB audio device, USB video device**, and **Others**.

- **USB storage device:** Check to enable the USB storage mapping function.



There are two options: **Read-Write Mode** and **Read-Only Mode**. Checking **Map USB storage device to hard drive** means that the USB storage connected to the PC client will execute the disk mapping mode first. Unchecking the **USB storage device** means that the USB storage function

is not enabled, and users corresponding to the group policy will not be able to use this function.

- **Speed up USB storage devices**: The USB storage device will not go through the USB channel mapping but will be mapped through the disk channel, equivalent to recognizing the USB device as a disk. In this case, the file reading and writing are faster, but the traffic consumption is higher.
- **USB CD/DVD Drive**: Check to enable USB CD/DVD drive function, only **Read/Write mode**. Checking **Map USB CD/DVD drive to hard drive** means that the USB CD/DVD connected to the PC client is given priority to execute the disk mapping mode. If **USB CD/DVD Drive** is not selected, the USB optical drive function is not enabled. At this time, users corresponding to the group policy will not be able to use this function.
- **USB printer** and **USB smart card**: If selected, it means that printer devices and smart cards using a USB interface are supported. If it is not selected, they are not allowed to be used.
- **USB audio device and USB video devices**: If selected, the audio and video devices using the USB interface are supported. If not selected, it is not allowed to use.
- **Others:** If selected, the devices using USB ports other than those listed above are supported. If not selected, it is not allowed to use.
- **USB Device Whitelist/Blacklist**: The system will perform special processing on the USB devices that meet the VID:PID in the exception list during the mapping process. The device permission control behavior in the whitelist (Reset, MpQuirks, Acc, Camera, Audio, UsbBan, drive mapping blacklist, Usb interrupt non-cached mode) takes precedence over the permission control configured on the upper page. For specific functions of the list, please refer to the configuration interface illustrate.

4.3.4.5.6 Acceleration

1. WAN transport protocol optimization settings

Function Description:

For users who access through IPSEC VPN (wide area network private line), pure wide area network, and independent private line, the configuration of this function can improve the user's exclusive desktop experience.

Prerequisite

None.

Precautions:

1. The name of the WAN transmission optimization protocol is HEDC. The name of the LAN protocol is SRAP.

2. The maximum resolution in the virtual machine supports 2560*1600.

3. Win10 supports versions 1709, 1809, 1903, 1909, 2004, 21H1, and 21H2, and there may be software compatibility problems in lower versions. Ensure that the operating system patch package is the latest.

4. The installation of Agent has requirements for the operating system. The following operating systems support Agent installation (there is no limit to AGNET upgrade).

5. WIN7: SP1 and above (including SP1).

6. WIN10: 1709 and above (including 1709).

7. The PC client hardware does not support device configurations lower than intel Celeron G550@2.6Ghz and integrated graphics.

Steps:

Step 1. Log in to the SCP platform as admin, select **Compute> aDesk VDI > Policies**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the policy management page of the corresponding tenant.

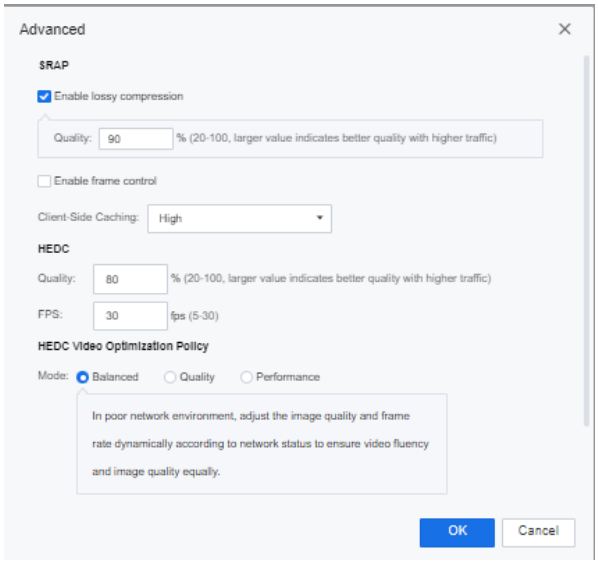
Step 2. Create a new or edit an existing policy, and select the corresponding transmission protocol according to the actual environment at **2D-Supported Desktop** on the **Transfer Protocol** tab of the policy option.

- **SRAP (applicable to LAN access environment):** If the user client associated with this policy uses LAN access, it is recommended to select this option. Compared with the HEDC protocol, the SRAP protocol consumes

less CPU and memory on the server but requires higher network quality and bandwidth.

- **HEDC (applicable to non-LAN access environment):** If the user client associated with this policy uses non-LAN access, it is recommended to select this option. When the network quality of the user client is poor, or the network bandwidth is limited, using the HEDC protocol can reduce the client's network requirements and improve the user's exclusive desktop experience, such as smoother desktop-related operations and smoother video playback, etc. However, the HEDC protocol consumes a lot of server CPU and memory. Compared with the SRAP protocol access, the number of concurrent virtual machines on the server is reduced by about 25%.
- **Automatically use HEDC protocol when VDC proxy:** If the user client associated with this policy has both LAN and non-LAN access scenarios, and the use of non-LAN access is the VDC proxy scenario, it is recommended to select this option, and select the transfer protocol **SRAP (for access over LAN)** at the same time, HEDC only supports 2D desktop.

Step 3. Click **Advanced to set** the compression quality and frame rate of the SRAP and HEDC protocols. It is recommended to keep the default values.



2. 3D-Supported Desktop

Function Description:

aDesk VDI supports transfer settings for 3D desktop images. You can set the image compression mode, frame rate, and average code stream. In **Lossless**

mode, the picture quality experience is higher, but the data consumption is higher; in **Lossy** mode, the picture quality experience is slightly worse, but the data consumption is lower.

Prerequisite

None.

Precautions:

3D dual-screen extended scene:

1. STD-500 thin client does not support lossless compression mode. Only lossy compression can be used.

2. STD-600 thin client support both lossy and lossless compression mode.

Use the 2D-supported desktop for 3D-supported desktop scenario:

1. Only supports Win10 virtual desktop.

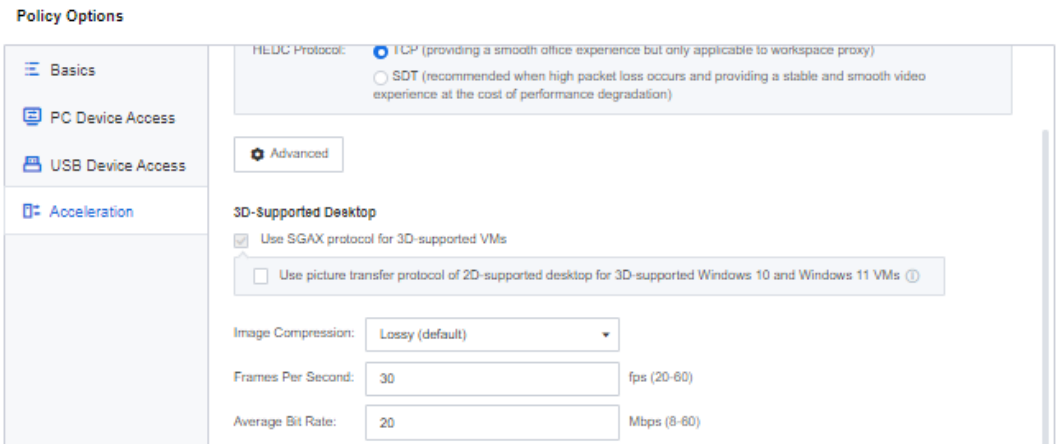
2. Only ARM, X86, PC client is supported;

3. Supports up to 2K resolution.

Steps:

Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > Policies**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the policy management page of the corresponding tenant.

Step 2. Create a new or edit an existing policy, and set the image compression mode according to the actual environment in 3D-Supported Desktop on the Acceleration tab of the policy option. The default is lossy compression.

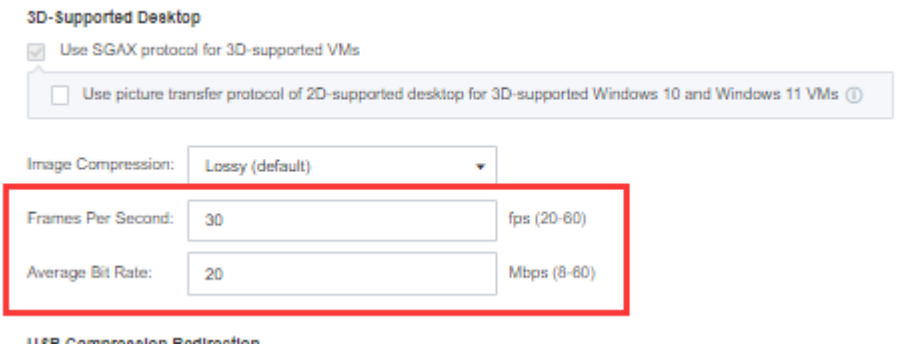


NOTE

1. **Lossy compression**: The source data is encoded in YUV420 format, converted into an H264 stream for decoding at the terminal, and supports Android client, X86 client, and PC client.

2. **Lossless compression**: The source data is encoded in YUV444 format and converted into an H264 stream for decoding at the terminal, which only supports the X86 client and PC client. Lossless compression picture quality is higher than lossy compression.

- Set the frame rate and average bit rate of 3D images.



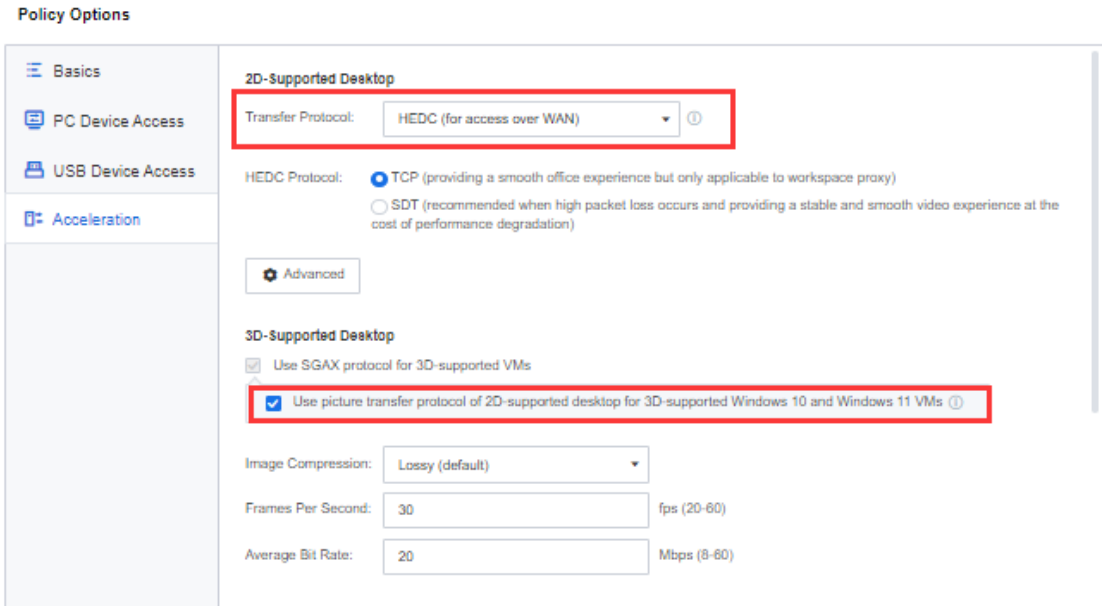
NOTE

1. Frame Per Second: The graphics acceleration frame rate is used to control the number of encodings per second of the graphics card (that is, the number of screenshots sent to the box per second. If the **Frames Per Second** is set to 30, 30 screenshots will be sent to the box per second), and increase appropriately. The frame rate will make the 3D picture smoother, but it will increase the load on the graphics card and the client.

2. **Average Bit Rate**: The average code stream controls the average traffic per second encoded. Properly increasing the code stream will improve the picture quality and increase the traffic from the server to the terminal.

- 3D Win10 virtual machine enables 2D desktop image protocol transmission.

When there is a need to access 3D desktops through the WAN, 2D desktop protocol access can be enabled to reduce the bandwidth requirements for accessing cloud desktops and improve the WAN experience. Select the HEDC protocol as the transfer protocol at 2D-Supported Desktop, and check the **Use picture transfer protocol of 2D-supported desktop for 3D-supported Windows 10 and Windows 11 VM** as the HEDC protocol.



3. USB Compression Redirection

Function Description:

It is suitable for scenarios like WAN access with limited bandwidth and using USB mobile storage devices. By compressing the data traffic when using USB devices, the bandwidth occupancy is reduced, and the bandwidth is avoided when using USB storage devices, improving the desktop operation experience.

Prerequisite

None.

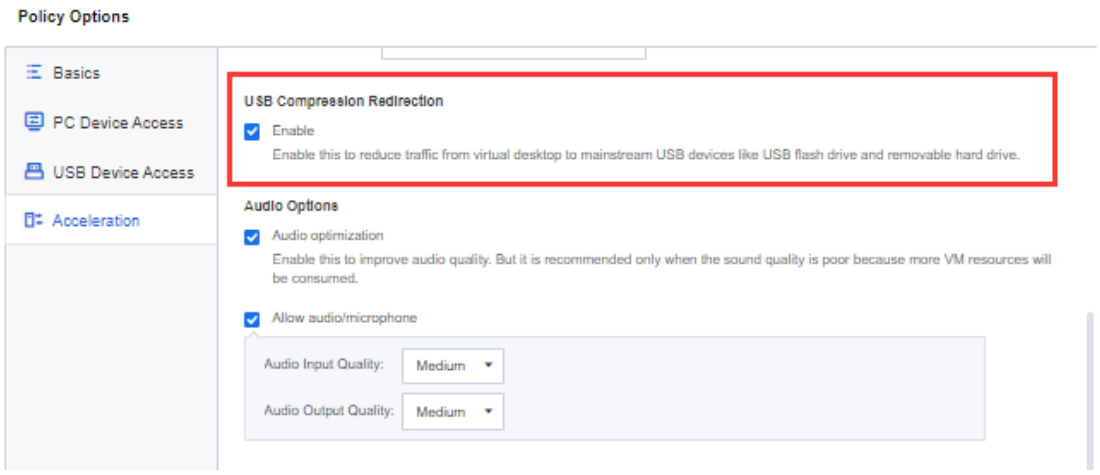
Precautions:

None.

Steps:

Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > Policies**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the policy management page of the corresponding tenant.

Step 2. To create or edit an existing policy, **select USB Compression Redirection** in the **Acceleration** tab of policy options.



4. Audio Options

Function Description:

Turn it on when there is noise in the audio to optimize the cloud desktop audio effect.

Prerequisite

None.

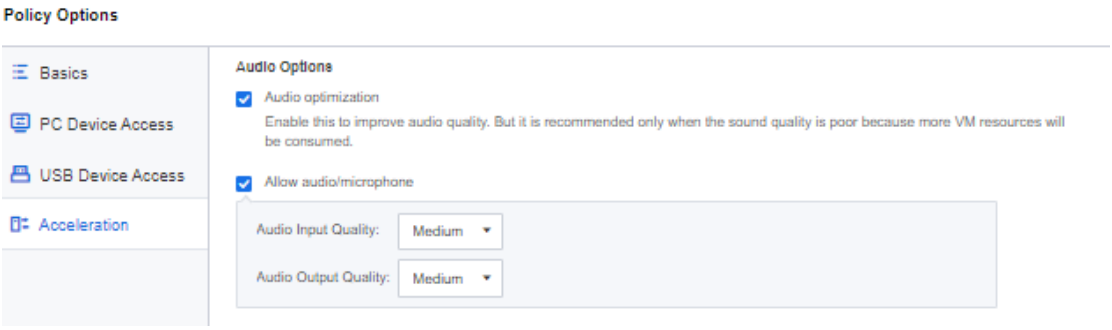
Precautions:

Enabling audio optimization will increase virtual machine performance consumption.

Steps:

Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > Policies**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the policy management page of the corresponding tenant.

Step 2. Create a new or edit an existing policy, and configure the relevant parameters in **Audio Options** on the **Acceleration** tab of the policy option.



5. Webcam Traffic Optimization

Function Description:

In the case of ordinary private line or wide area network access to the VDI, configuring the traffic optimization mode can ensure the normal and smooth use of camera peripherals / high-speed cameras without increasing the cost of bandwidth; and the need to set high-speed camera frame rate and definition level parameters Scenes.

Prerequisite

None.

Precautions:

1. The resolution range supported by the ARM-based terminal box traffic optimization mode high-speed meter is the width and height must exceed 32 and less than 4 * 1920 * 1080.

2. If the resolution of the high-speed camera is higher than 4 * 1920 * 1080, the encoding mode will automatically switch to the dynamic optimization mode.

3. The ARM box high camera cannot be used in the OTG port. Due to the limited bandwidth of the OTG port, there may be a phenomenon that the screen is blurred or the camera cannot be turned on.

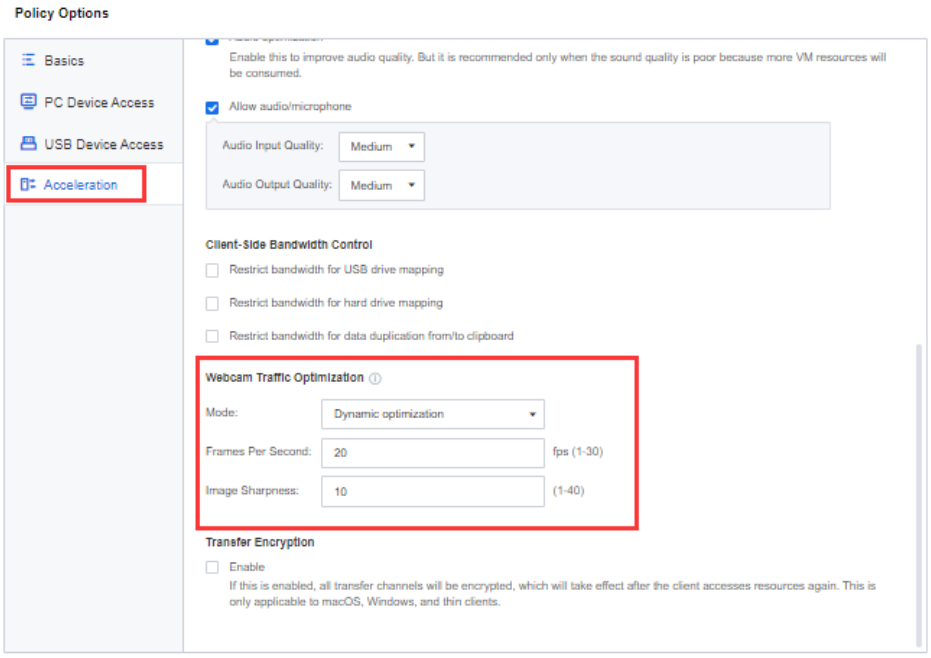
4. The traffic optimization mode is not recommended for dual-core ARM boxes. Using dual-core may cause insufficient CPU performance and abnormal phenomena such as freezing.

Steps:

Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI >**

Policies, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the policy management page of the corresponding tenant.

Step 2. To create a new or edit an existing policy, go to **Webcam Traffic Optimization** on the **Acceleration** tab of the policy options and configure the relevant parameters as needed.



- **Traffic optimization mode:** Consume less traffic under the same conditions.
- **Dynamic optimization mode:** Encode the whole picture, and the picture has the advantage of being lossless.
- **Image Sharpness:** The higher the definition level, the clearer the picture and the more data consumption.

6. Client-Side Bandwidth Control

Function Description:

After the disk mapping and clipboard are released, when copying files between the PC client's local disk and the exclusive desktop's local disk, flow control needs to be performed to avoid the situation where copying large files will occupy the bandwidth of the entire host.

Prerequisite

None.

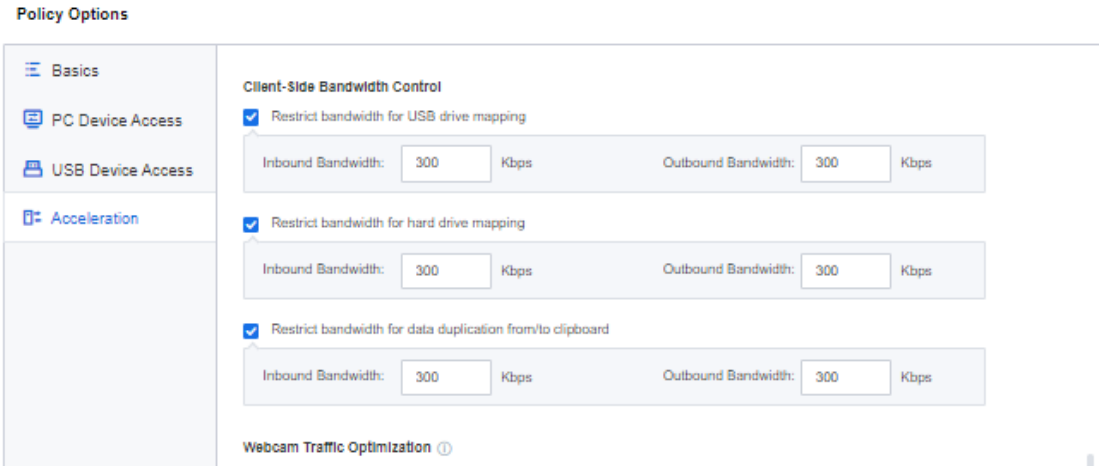
Precautions:

It only supports PC client access.

Steps:

Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI > Policies**, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the policy management page of the corresponding tenant.

Step 2. To create a new or edit an existing policy, select the corresponding control channel as needed in **Client-Side Bandwidth Control** on the **Acceleration** tab of the policy option and limit the flow rate according to the actual situation in the network.



7. Transfer Encryption

Function Description:

For WAN access or scenarios with high access security requirements, protocol encryption can be enabled to encrypt and transmit VDI access traffic to improve security.

Prerequisite

None.

Precautions:

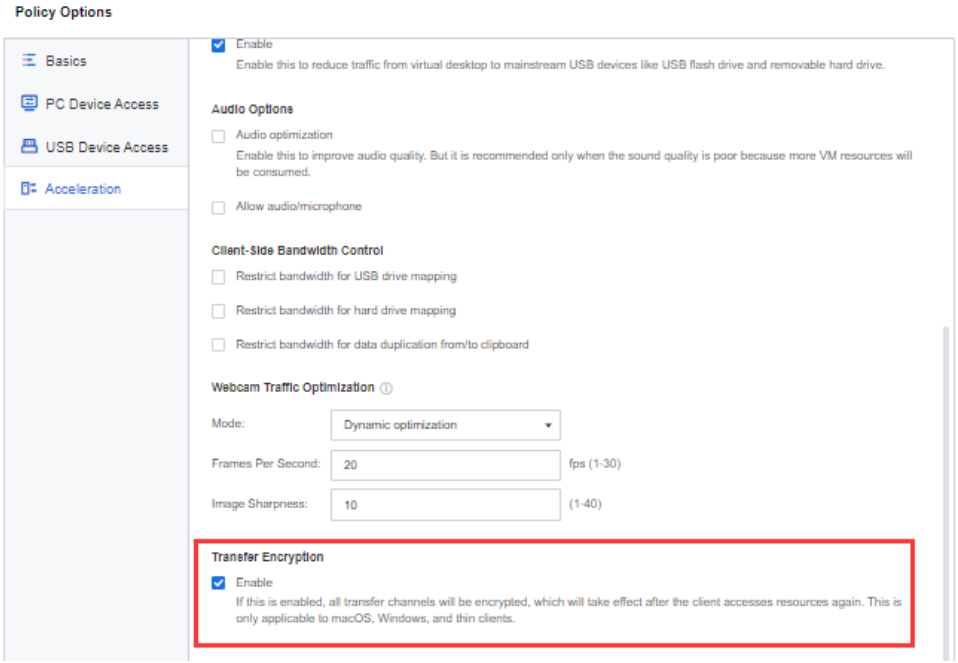
It only supports thin clients, Windows PC clients, and MAC OS terminals.

Steps:

Step 1. Log in to the SCP platform as admin, select **Compute > aDesk VDI >**

Policies, click the drop-down arrow, select the tenant under the workspace to be managed from the drop-down menu that appears, and enter the policy management page of the corresponding tenant.

Step 2. To create or edit an existing policy, select **Transfer Encryption** in the **Acceleration** tab of the policy option.



4.3.5 vGPU Management

Function Description:

- The user used the traditional physical architecture but wants to virtualize the business now. On HCI, a few businesses, such as GIS, required graphics card support. Now they need to be virtualized together. Therefore, the virtualization platform needs to support the configuration of graphics cards.
- Users have large-scale applications that require graphics card support, and the use of GPU resources will encounter idle waste and inflexible allocation. It would be better to use the GPU flexibly, allocate on demand and share the resources.
- When the graphics card resources of the platform are allocated, used, and adjusted, they need to be visualized so that the administrator can better manage the graphics card resources.

Prerequisite:

1. The use of vGPU requires authorization from NVIDIA.
2. The virtual machine using vGPU must install the NVIDIA graphics driver corresponding to the HCI platform. To obtain the graphics driver, you can go to **Sangfor Community > Self-Service > Download > aCloud(HCI)**.
3. There are two types of vGPU authorizations for HCI: **vWS** and **vCS**. vWS is for professional graphics and computing scenarios. vCS is for optimization for everyday computing, such as artificial intelligence, deep learning, and scientific research scenarios.
4. vCS does not support Windows virtual machines, the minimum cutting granularity is 4GB, and the maximum is 32GB.
5. Not all graphics cards support vGPU. Only graphics cards that support vGPU can use vGPU, and those not supported graphic cards can use Passthrough mode.
6. It supports directing two graphics cards to a virtual machine. T4 and 2080Ti can support up to 8 cards.
7. In the vGPU scenario, the graphics card compatibility can refer to the SCP **Compatibility List** in the Sangfor community or obtain it from the Sangfor Technical Support team.
8. You need to use the NVIDIA public version driver in the Passthrough scenario. For the graphics card version and driver download, please refer to the following link: https://www.nvidia.cn/Download/index.aspx?lang=en.

Precautions:

1. Two graphic card servers form a cluster, or one graphic card server and one ordinary server form a cluster. Therefore, at least one graphics card is required. You can use the graphics card purchased by Sangfor or the user's original graphics card.
2. The server is divided into 2D and 3D servers. You cannot insert a graphic card into the original all-in-one machine, and a dedicated graphics card server is required to insert a graphics card.

Steps:

HCI environment deployment:

In terms of hardware, plug in the graphics card on the server, and pay attention to the power supply line of the graphics card so that the graphics card will work (the power of the graphics card is high, and there is a special power supply line).

In terms of software, the platform detects whether the hardware has a graphics card during the installation of HCI on the server or whether a cluster is plugged in with a graphics card. The interface will automatically display whether to enable IOMMU, and you may select **Enable** (the host needs to restart to take effect after it is enabled).

4.3.5.1 Nvidia licensing server deployment

Function Description:

Deploy the NVIDIA vGPU license server to provide licenses for 3D vGPU virtual machines. To use vGPU, you need to grant NVIDIA's license key. Otherwise, the performance of vGPU will not be able to play out. The licensing server is a virtual machine template installed on the HCI platform and used as a virtual machine. Fill in the applied vGPU test license key on the licensing server, and then fill in the IP of the licensing server on the graphics card driver of the virtual machine that needs to use vGPU. Then, the virtual machine can use the vGPU.

Prerequisite

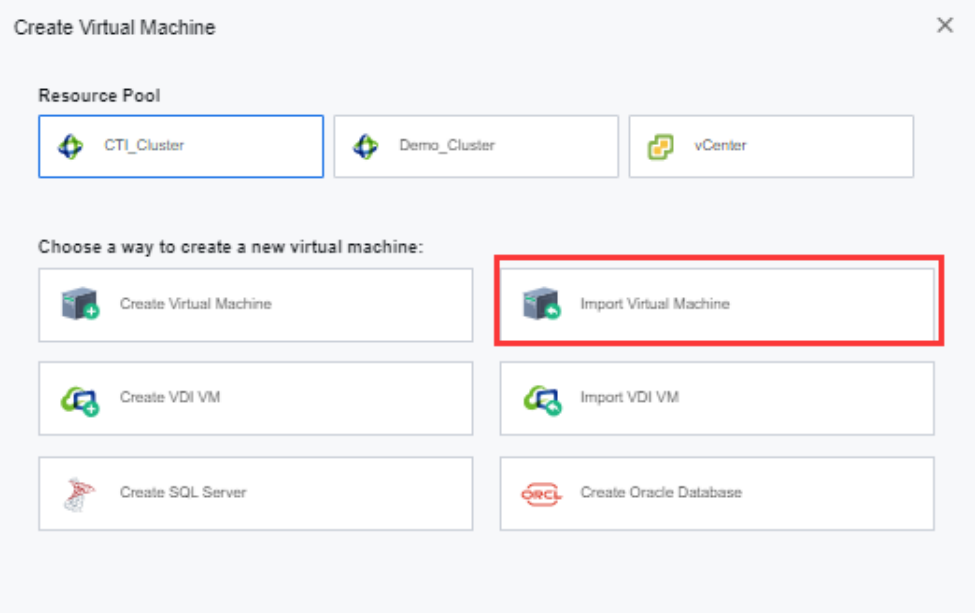
None.

Precautions:

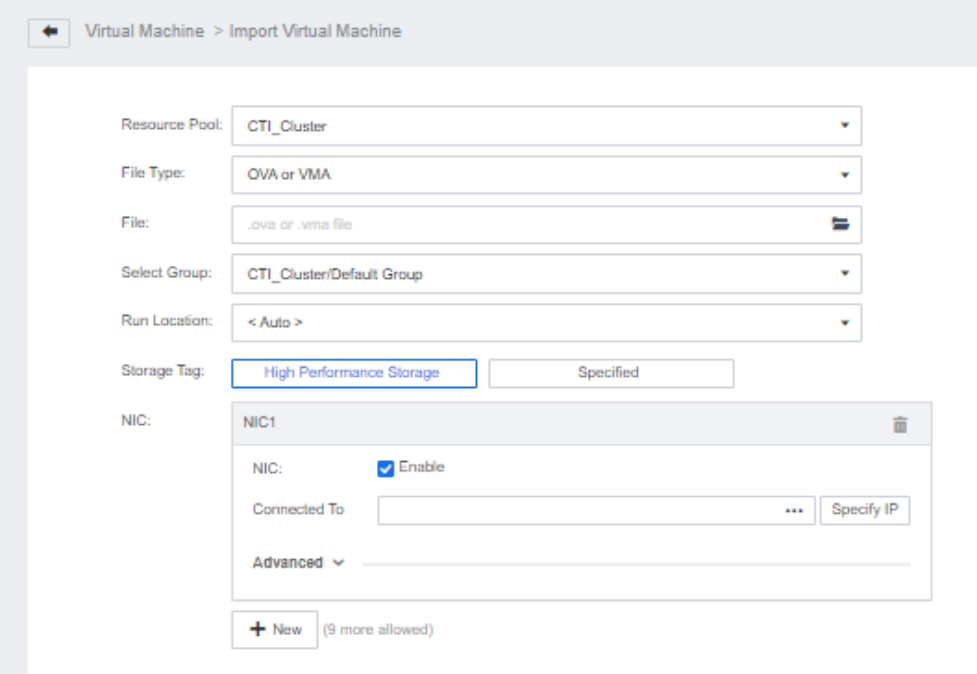
Download the license server image.

Steps:

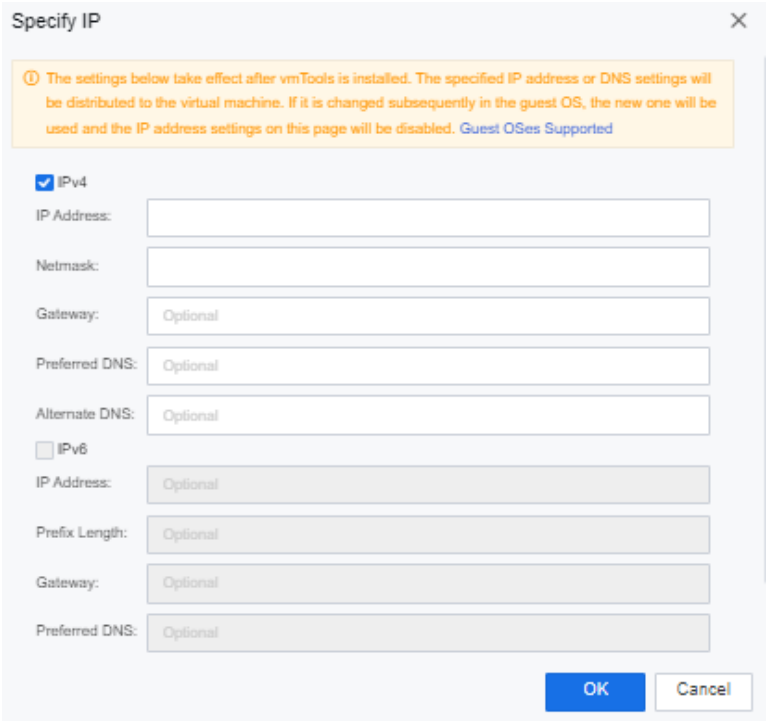
Step 1. Log in to the SCP platform, click **Compute > Virtual Machines > New > Import Virtual Machine**, and select the NVIDIA licensing server vma image to import.



Step 2. Enter the page for importing virtual machine, and a page for importing virtual machine files from local will pop up. Configure the following parameters: **Resource Pool, File Type, File, Select Group, Run Location, Storage Tag, and NIC**.

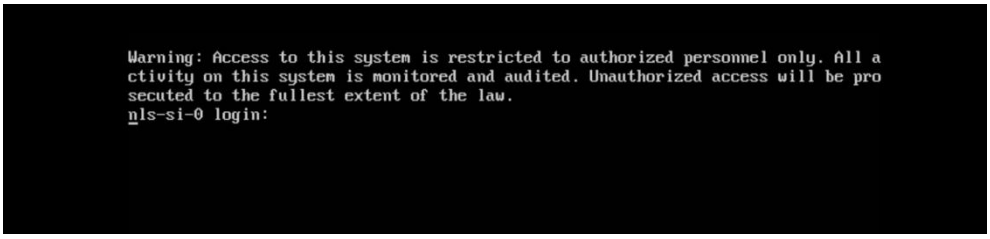


Step 3. Click **Specify IP** to configure the IP address of the licensing server, and click **OK**.

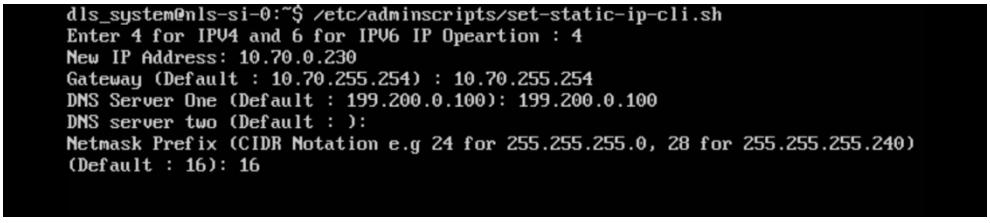


Step 4. After clicking **Import**, it will start the import process.

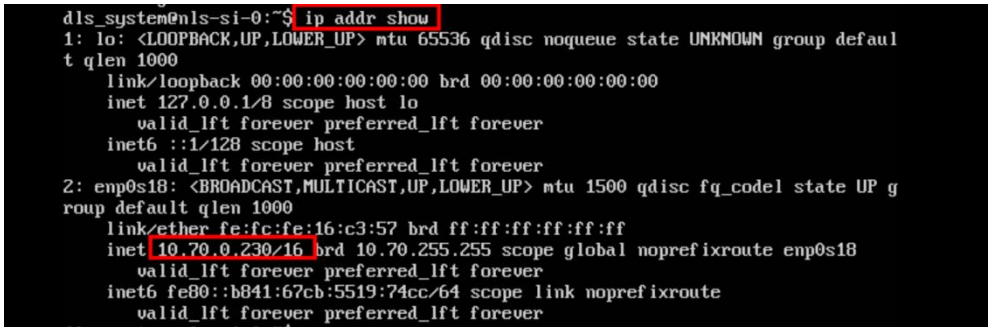
Step 5. After the import is complete, enter the virtual machine console interface and log in. Enter **dls_system** in the following interface and press **Enter**.



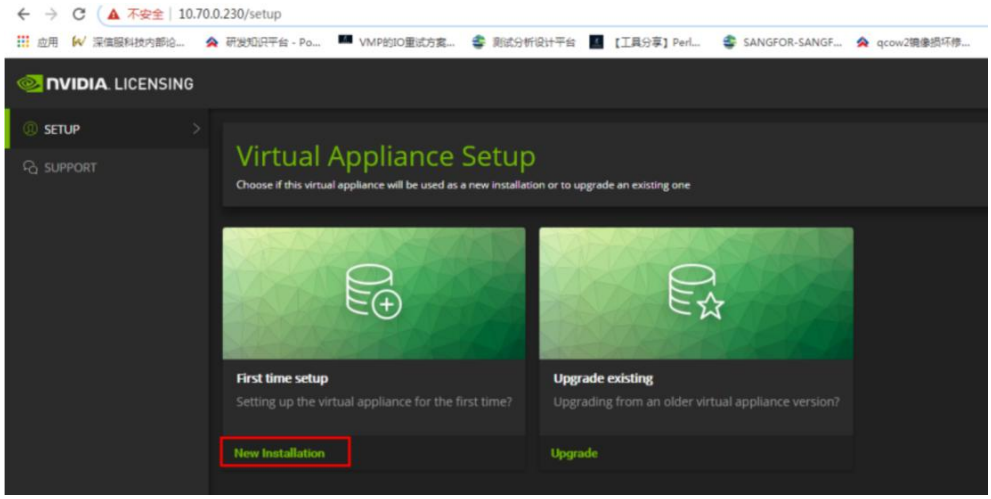
Step 6. Execute **/etc/adminscripts/set-static-ip-cli.sh** to set a static IP, as shown in the following figure.



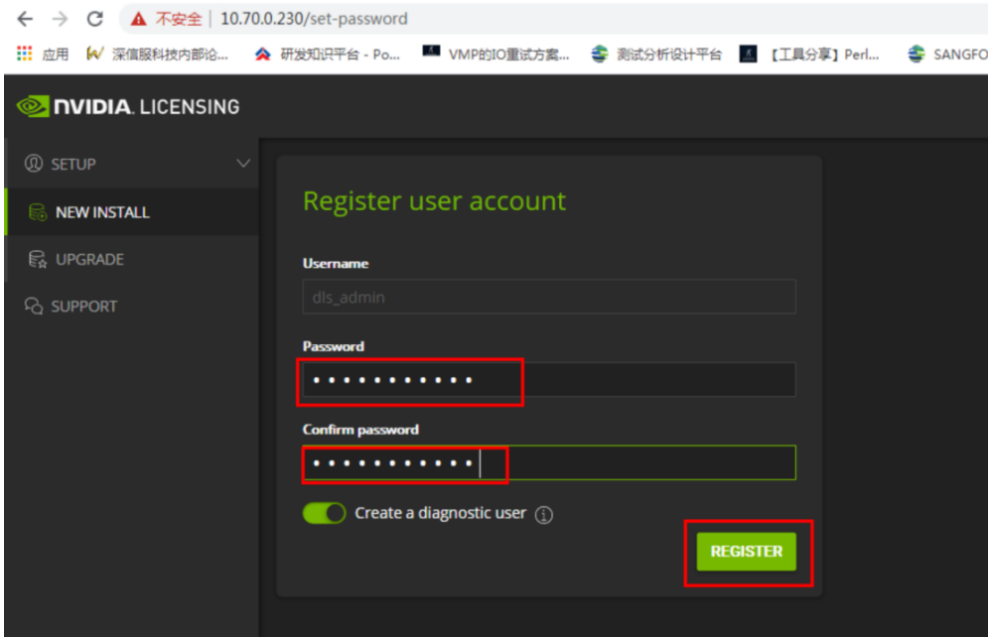
Step 7. Execute **ip addr show** to confirm that the IP takes effect.



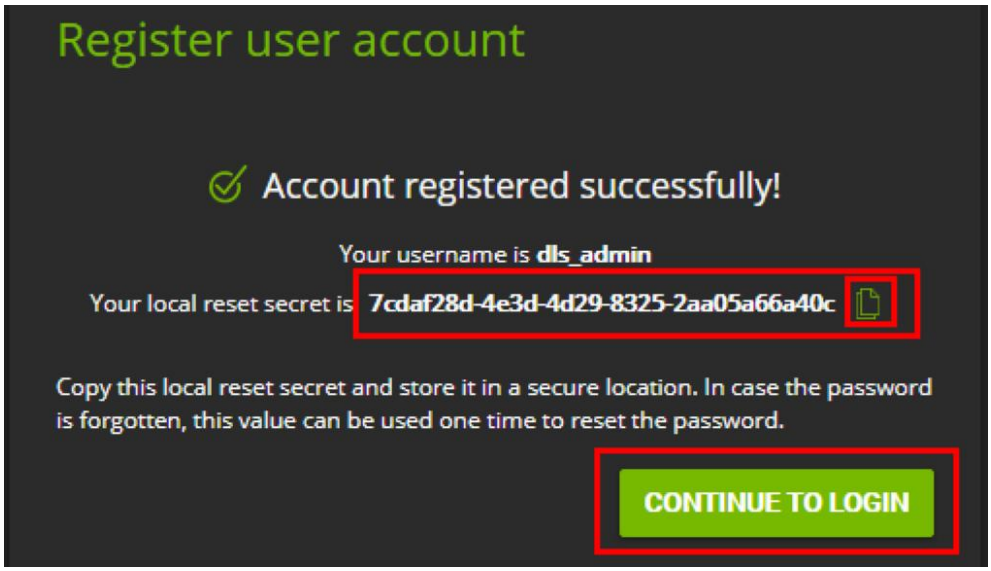
Step 8. Enter the fixed IP in the browser (as above, directly enter 10.70.0.230) to access the licensing server web page, and select **New Installation**.



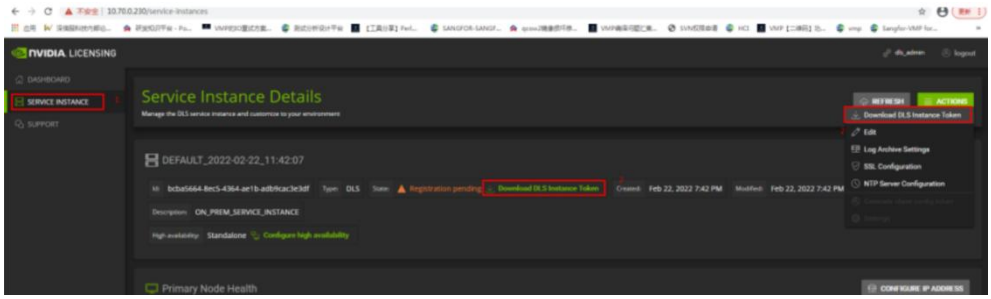
Step 9. Enter the password to be set and click **REGISTER** to register an account.



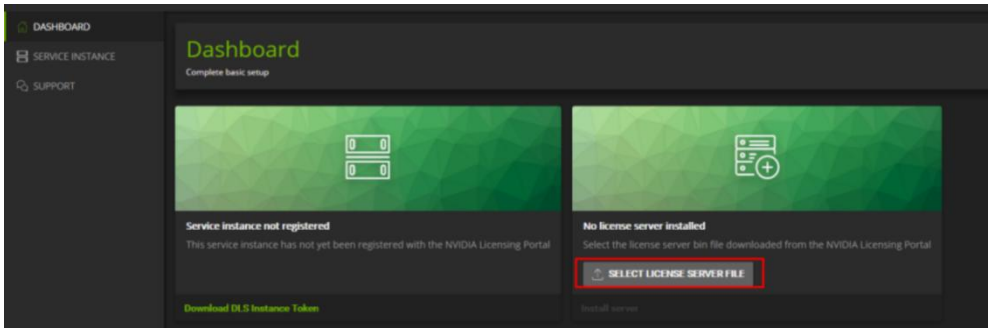
Step 10. Save the string in the figure to a local file. This string can reset the password. Click **CONTINUE TO LOGIN**.



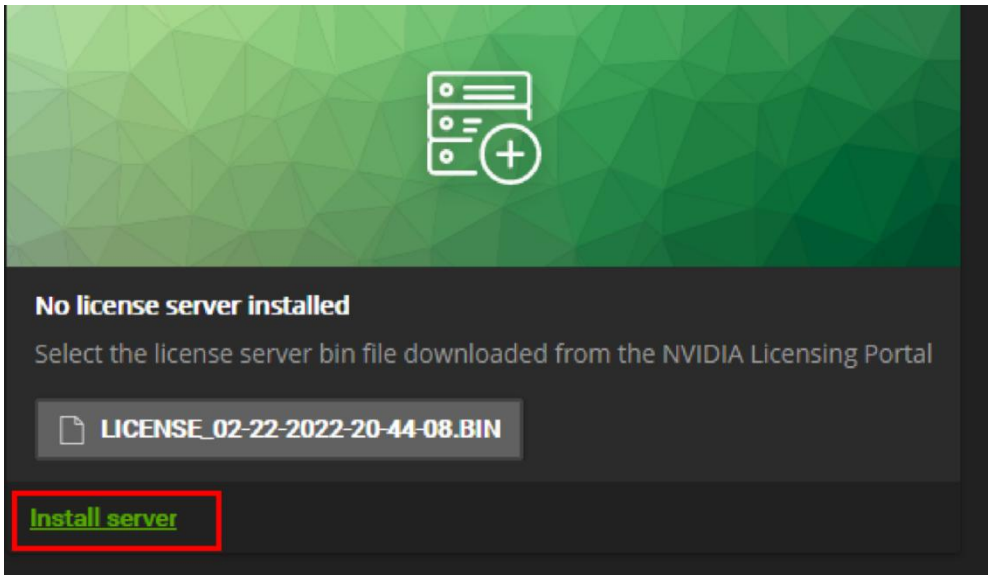
Step 11. Select **SERVICE INSTANCE**, click **Download DLS Instance Token**, and download the DLS instance Token file. If you need to test authorization, pass the file to Sangfor technical service to obtain the authorization file.

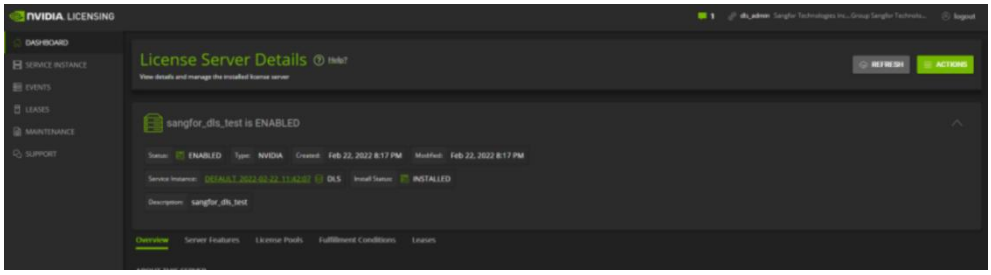


Step 12. After obtaining the licensing file, click **SELECT LICENSE SERVER FILE** to upload the file.

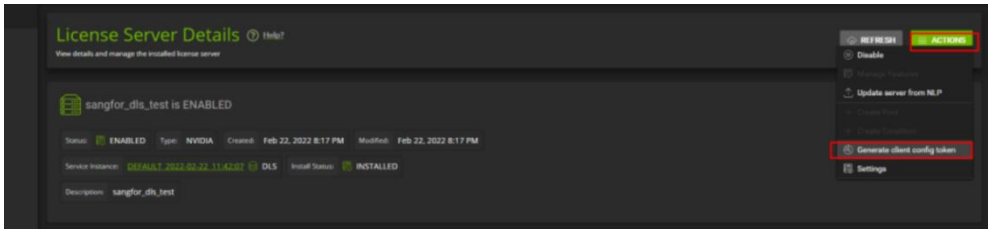


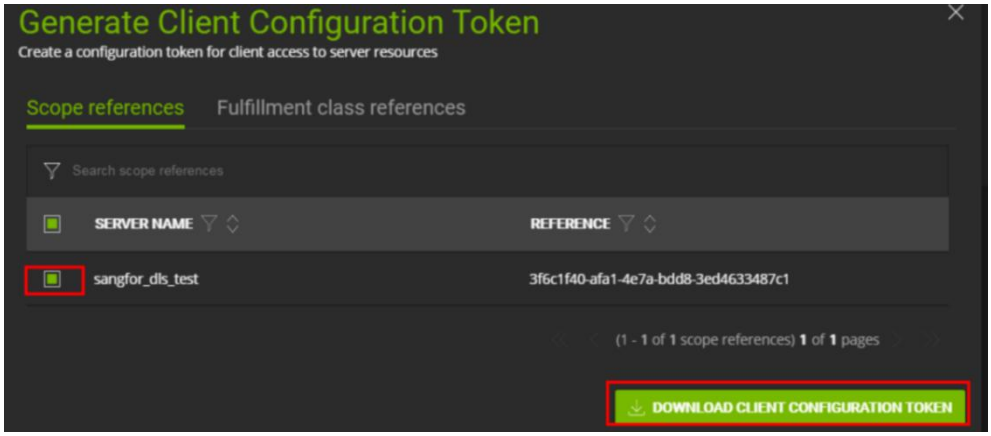
Step 13. Click **Install server** to configure the authorization service.





Step 14. Download the client config token to authorize the GPU virtual machine.





4.3.5.2 Graphics Card Management

Function Description:

The graphics card core of the server can be configured to passthrough mode or to specify the segmentation type automatically or manually. By default, the system automatically configures the segmentation type. Supports splitting graphics cards into Q-series or C-series vGPUs.

The Q-Series is a virtual workstation for creative and technical professionals who need the performance and functionality of Quadro technology.

The C-Series is suitable for compute-intensive server jobs such as artificial intelligence (AI), deep learning, or high-performance computing (HPC).

Prerequisite

1. For passthrough graphics cards, it will default to passthrough mode. For graphics cards that support vGPU, it will default to automatic mode. You can adjust the split mode according to the test needs.

2. It supports the direct connection of 2 graphics cards to one virtual machine, of which T4 and 2080Ti can support up to 8 graphics cards, and does not support assigning multiple vGPUs to one virtual machine.

3. The vGPU versions 10.2 and 13.2 are supported. The compatibility list of related software can be found on the NVIDIA official website. For fresh installation or upgrade to HCI6.8.0, you need to re-import the GRID driver and restart the node to take effect.

4. Virtual machines on HCI that have graphics cards assigned do not support live migration.

5. In the vGPU scenario, the video memory resources of the graphics card are allocated and exclusive. The computing resources of the graphics card will be scheduled according to the scheduler. This version supports three schedulers: Best Effort (preemption), Equal Share (equal share), and Fixed Share (fixed ratio).

Best Effort: When a multiple VM runs on the graphics card, it will preempt computing resources according to the workload.

Equal Share: When multiple VM runs on the graphics card, the computing resources will be equally divided.

Fixed Share (fixed ratio): When a multi-virtual machine runs on the graphics card, computing resources will be allocated according to the proportion of video memory configured by the virtual machine.

6. A single server is prohibited from using two different types of graphics cards. Different nodes in the same cluster can support different types of GPUs.

7. When two graphics cards, A and B, are inserted into the two adjacent PCI slots, and the core of graphics card B is damaged, graphics card B will be recognized as that of graphics card A. Therefore, please replace the damaged graphics card in time.

Precautions:

When adjusting the graphics card split mode, the virtual machine that occupies the graphics card resources needs to be shut down.

Steps:

Step 1. Click **Compute > GPU. In** the GPU window, you can view the overview of graphics card usage, resource pool overview, and tenant overview.

Step 2. Click the number of graphics cards corresponding to the number of Graphics Cards to view the graphics card information on each node in the resource pool.

Step 3. Click the **Edit** button on the right side of the target graphics card to edit the graphics card:

- The name of the graphics card to be edited.
- How to use the graphics card: You can choose straight-through or split. When the use mode is "Segmented", if the graphics card has multiple cores, it supports splitting the video memory size according to different cores.
- Choose whether to enable video memory ECC: Turning on can improve the running stability of the GPU
- Select the split method, which can be split into Q series or C series vGPU
- Select GPU computing scheduler

Step 4. Click **OK**, you can see the configuration information of the graphics card on the interface.

4.3.5.3 Virtual Machine add graphics card

Function Description:

Add graphics card hardware to the virtual machine to transform it into a 3D virtual machine, improving the support for scenes with high image processing requirements.

Prerequisite

1. After the graphics card is added to the virtual machine that is powered on, it will take effect after restarting.

2. Only Windows 10 and Windows 2016 can view the 3D virtual machine desktop through the virtual machine console. Other Windows operating system versions do not currently support viewing in the virtual machine console. Therefore, when installing the graphics card driver, you need to access the virtual machine through the client or remote desktop. system. The 3D virtual machine desktop of the Linux system supports console viewing.

Precautions:

Pass-through graphics cards require the platform to have a graphics core locked in pass-through mode in order to be used.

Steps:

Step 1. Select the virtual machine to be configured, enter the edit virtual machine page, select Configuration and Network, and click **Add Graphics Card**.

Step 2. Select the model of the graphics card to be configured, and then click **OK**.

- Add a graphics card to the virtual machine.
- Select the direct or split mode for the graphics card.
- When there are multiple graphics cards on the host, select the graphics card model.
- Select the segmentation method that has been set for the graphics card.
- Display the video memory capacity in this split mode.
- Select the scheduler. When multiple graphics cards of the same model have different scheduler policies, the virtual machine will select the graphics card according to the scheduler policy.

4.3.5.4 Windows Virtual Machine add graphics card

Function Description:

After configuring a vGPU for a virtual machine, you need to install a graphics card driver on the virtual machine before the virtual machine can be used normally.

Prerequisite

None.

Precautions:

If the GPU graphics card hardware is compatible, the Windows system compatibility is subject to the NVIDIA official website.

Steps:

Step 1. Configure the corresponding IP address, subnet mask, gateway and other information for the Windows virtual machine.

Step 2. Install the corresponding version of the graphics card driver for the template virtual machine, run the installer, and select the default installation all the way. After installation, restart the virtual machine.

Step 3. In the device manager, you can check whether the driver is installed successfully, as shown in the figure below.

Step 4. Right-click on the desktop and select NVIDIA Control Panel. Configure the licensing server IP and port in the NVIDIA control panel.



After the configuration, confirm that the virtual machine can successfully obtain the authorization. Otherwise, it means that there is a problem with the deployment and needs to be checked, and the screen will not be black because the authorization is not obtained.

4.3.5.5 Linux Virtual Machine add graphics card

Function Description:

After configuring a vGPU for a virtual machine, you need to install a graphics card driver on the virtual machine before the virtual machine can be used normally.

Prerequisite

None.

Precautions:

If the GPU graphics card hardware is compatible, the Linux system compatibility is subject to the NVIDIA official website.

Steps:

Step 1. Configure the corresponding IP address, subnet mask, gateway and other information for the Linux virtual machine.

Step 2. Disable the nouveau driver. nouveau is an open source NVIDIA driver that may interfere with subsequent driver installations. The method of disabling is as follows.

- CentOS_7 or RedHat7 environment. Add in /usr/lib/modprobe.d/dist-blacklist.conf or /lib/modprobe.d/dist-blacklist.conf.

  blacklist nouveau

  options nouveau modeset=0

- Ubuntu16.04 environment. Create the file /etc/modprobe.d/blacklist.conf with the following content.

  blacklist nouveau

  options nouveau modeset=0

  Execute the command: $ sudo update-initramfs –u

- Execute dracut --force. After the execution is complete, restart the virtual machine.

  dracut --force

  reboot

- Use the command lsmod | grep nouveau. If there is no output, the disable is successful.

Step 3. Close the X window. This can be done with the command: "init 3". (Not the only way)

Step 4. Install the driver.

- Copy the correct version of the vGPU driver runfile to the system. For example: the corresponding driver file in centOS is: NVIDIA-Linux-x86_64-390.75-grid.run In the following, this file is used as an example to explain.
- Modify the file permissions as super user and execute it. Note that the following parameters need to be added during execution.

  sudo chmod +x NVIDIA-Linux-x86_64-390.75-grid.run

  ./NVIDIA-Linux-x86_64-390.75-grid.run -Z --no-opengl-files

- When the installation starts, a blue dialog box will be displayed. Follow the prompts to install, all options are selected by default. The specific process is shown in the figure below.



- Whether to install: Yes.



- Whether to automatically upgrade the X configuration file, NO.



- The installation is complete.

Step 5. Obtain authorization. Ubuntu recommends authorizing directly through the configuration file /etc/nvidia/gridd.conf (this file may not be available when you use it for the first time, but there will be a gridd.conf.template file in this directory, and you can copy a copy from this file directly.). Here, fill in the ServerAddress item (you can also ignore ServerPort if it is not necessary).

```
# Description: Set License Server Address
# Data type: string
# Format:  "<address>"
ServerAddress=200.201.0.60

# Description: Set License Server port number
# Data type: integer
# Format:  <port>, default is 7070
ServerPort=
```

NOTE

After modification, restart the service: systemctl restart nvidia-gridd.

Step 6. During the testing, enter the command: **init 5** to enter the graphical interface, and the display is normal. Open the command line and enter the command **nvidia-smi** to view the graphics card usage. It will display the graphics card model, driver model, resource usage, etc.

```
[roo@localhost ~]$ nvidia-smi
Mon Aug 20 11:17:04 2018
+-----------------------------------------------------------------------------+
| NVIDIA-SMI 390.75                 Driver Version: 390.75                    |
|-------------------------------+----------------------+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|===============================+======================+======================|
|   0  GRID P40-8Q         On   | 00000000:00:03.0 Off |                  N/A |
| N/A   N/A    P0    N/A /  N/A |    528MiB /  8192MiB |      0%      Default |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                       GPU Memory |
|  GPU       PID   Type   Process name                             Usage      |
|=============================================================================|
|  No running processes found                                                 |
+-----------------------------------------------------------------------------+
```

4.3.5.6 Edit Graphics Card

Function Description:

Modify the graphics card hardware for the virtual machine to flexibly adjust the use of the graphics card.

Prerequisite

After the graphics card type is changed in the power-on state, the virtual machine restarts to take effect.

Precautions:

None.

Steps:

Step 1. Enter the virtual machine interface, find the virtual machine whose graphics card type needs to be modified, and click **More > Edit**.

Step 2. Click the original graphics card, modify the graphics card model to the desired model, and then confirm.

4.4 Networking

4.4.1 Network Topology

Function Description:

SCP platform administrators can view classic networks and tenant networks in the network topology and achieve efficient and clear network management through **what you draw is what you get**.

Prerequisite

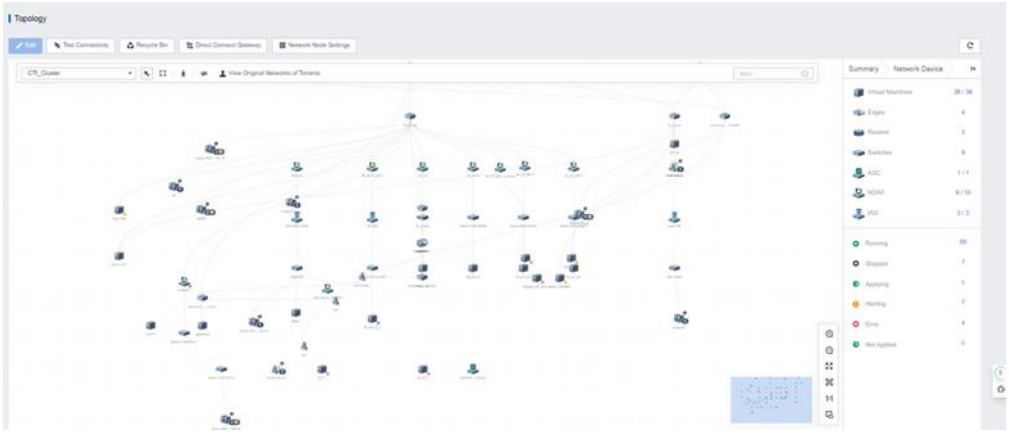
None.

Precautions:

None.

Steps:

Step 1. Login to the SCP platform and select **Networking** > **Topology** to enter the network topology interface.



Step 2. Select the appropriate Resource Pool. You can view, edit the classic network topology and manage the network topology.

Step 3. Select a tenant under the resource pool to view and edit the tenant's VPC to manage the VPC.

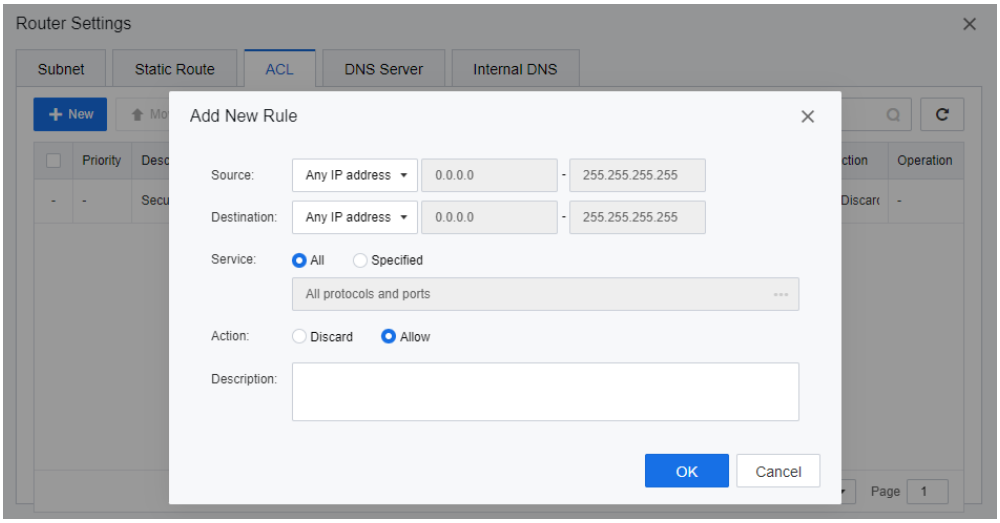
- Select the router and click the **Settings** button to enter the ACL page.

NOTE

1. For SCP6.7.30 and above, a security baseline policy will be configured by default to deny access to public network traffic.

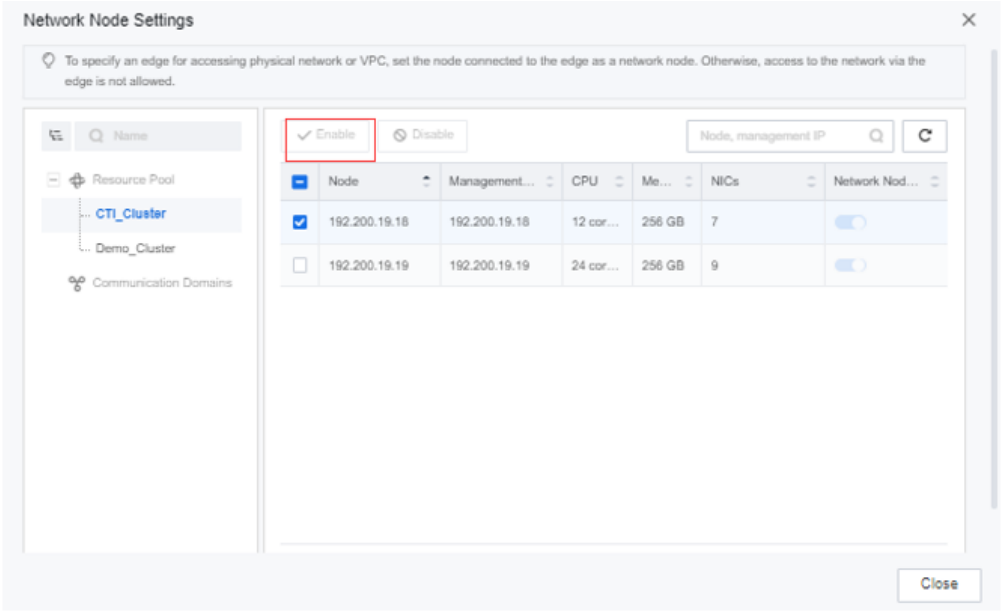
2. You need to manually create an access control policy if it is an upgraded version.

3. When there is a public network inbound traffic blocking policy under the subnet, if there is a need for external network traffic access, you need to create a regular ACL to release traffic. In addition, the blocking policy of high-risk ports can only be edited and released by administrators, not tenants.



Step 4. Network node settings: used to deploy and run network resources. In the communication domain scenario, physical egress and virtual routers in the communication domain are only allowed to be bound to network nodes, and only network nodes are allowed to provide physical egress for the VPC.

- On the **Topology** page, click the **Network Node Settings** button, select the corresponding resource pool host, click **Enable**, and mark it as a network node.

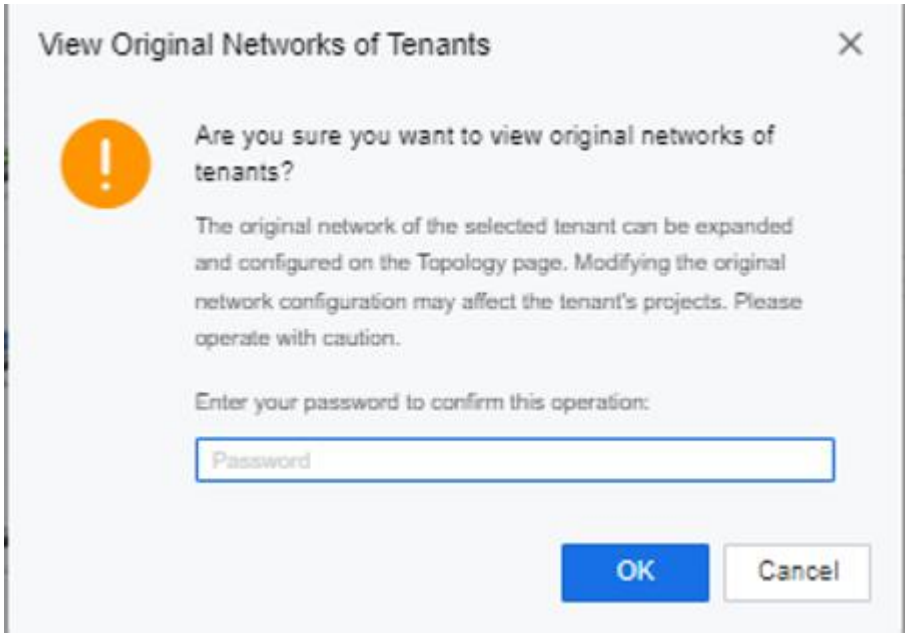


NOTE

By default, all nodes are marked as network nodes. Nodes not marked as network nodes are not allowed to run virtual routers.

Step 5. View the original network of the tenant: The tenant network can be disassembled to support viewing and quick configuration of the tenant network.

- On the **Topology** page, click the **View Original Network of Tenants** button, enter the admin password, select the tenant to be viewed, and click **OK** to view and edit the original network of the tenant.



4.4.1.1 Test Connectivity

Function Description:

This task guides administrators to check virtual machine connectivity and troubleshooting network communication failures. Both IPv4 and IPv6 protocols are supported.

Precautions:

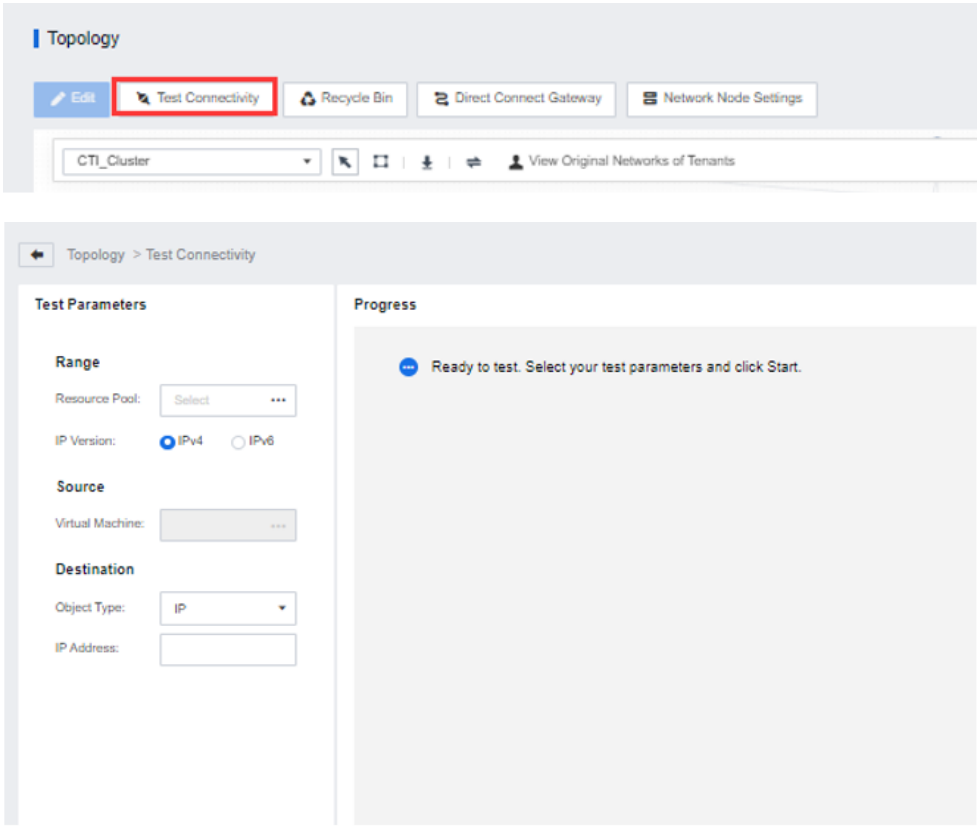
Connectivity detection does not support mutual access between IPv6 and IPv4.

Prerequisite

1. The virtual machine has installed VM performance optimization tools.
2. Linux requires perl to be installed.

Steps:

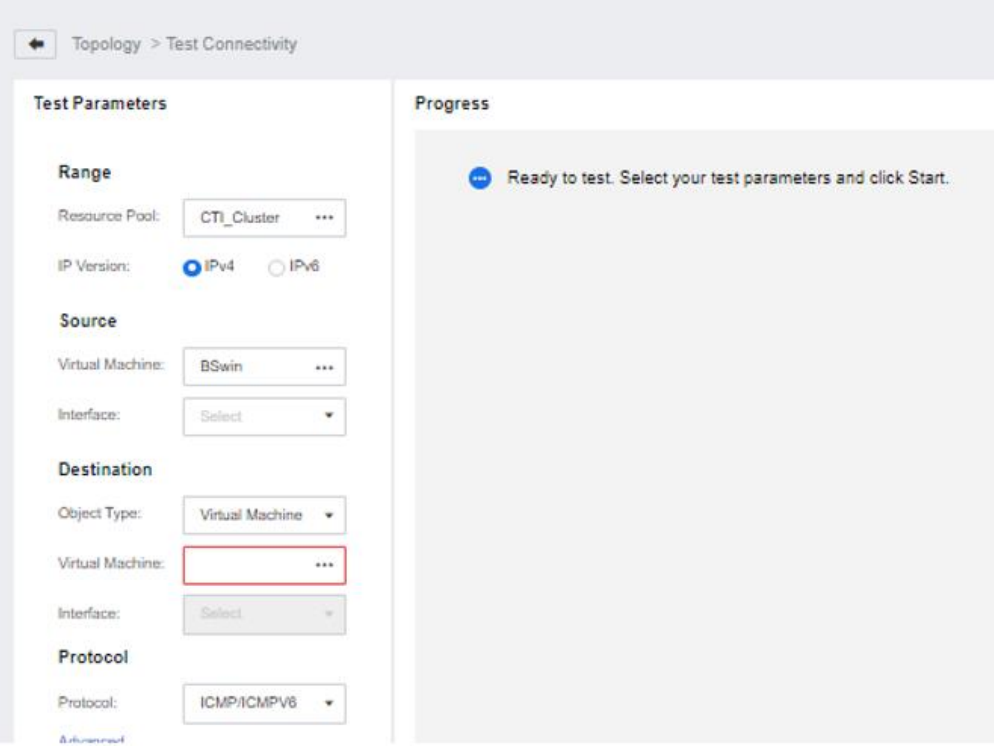
Step 1. On the **Topology** page, click **Test Connectivity** to enter the **Connectivity Detection** page.



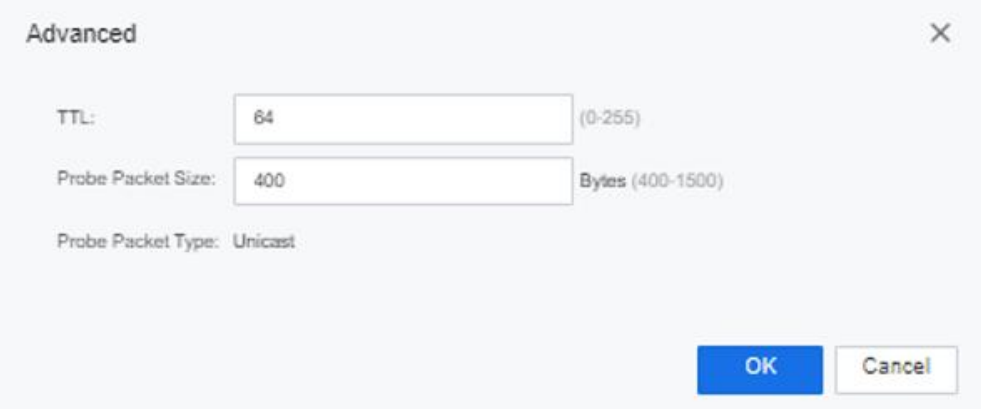
Step 2. Select the resource pool and IP Version and select IPv4 or IPv6 protocol.

Step 3. Select the source virtual machine and the corresponding network

port. When the destination object type selects the virtual machine, you need to select the destination virtual machine and the corresponding interface. When the destination object type selects IP, enter the destination IP.

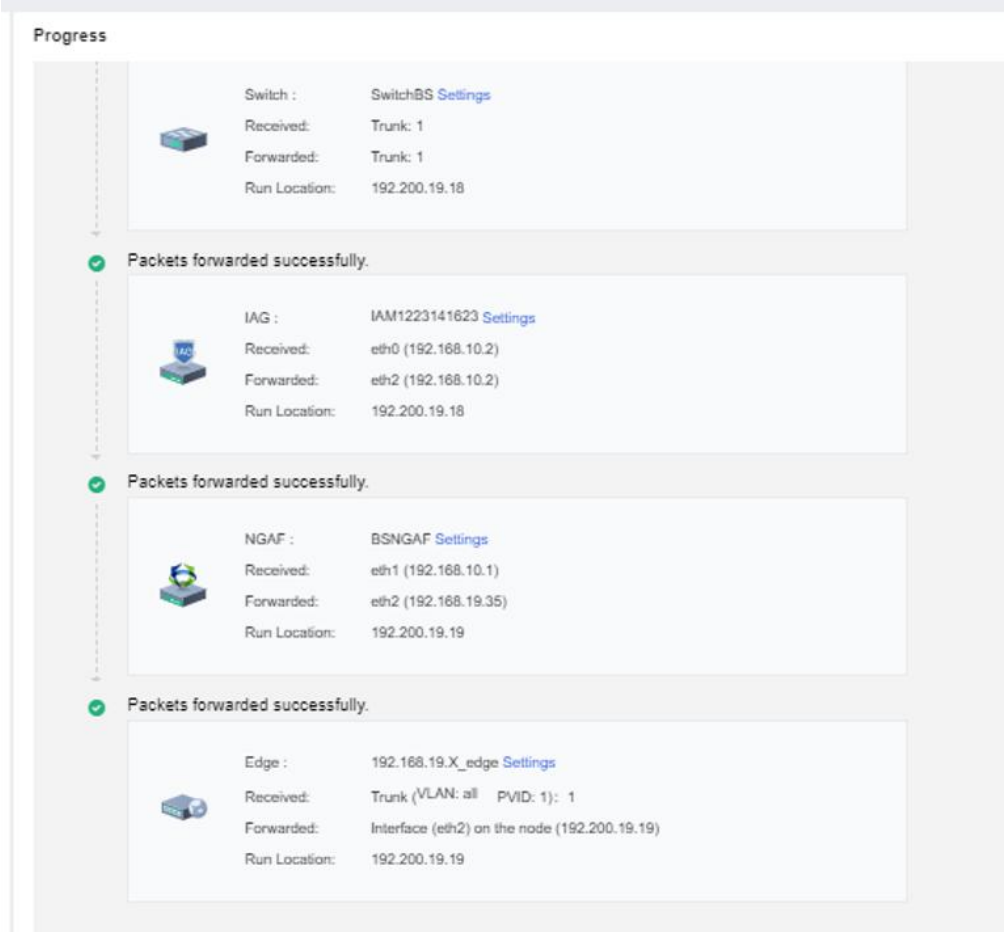


Step 4. Select the protocol and click **Advanced** Settings to set the TTL and probe packet size.



Step 5. Click **Start** to test the network.

Step 6. Example of successful network test.

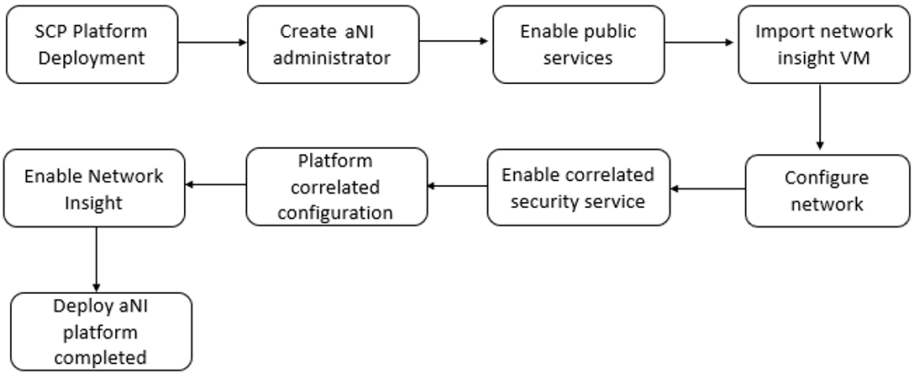


4.4.2 Advanced Network Insight(aNI)

Advanced Network insight (aNI) realizes automatic collection and sorting of virtual machine access relationships, automatic addition and display of new assets, and timely synchronization of asset status. From a business perspective, it provides an intuitive and clear access relationship topology diagram and access details between virtual machines. It is convenient for optimizing policy configuration, discovering business access risks, and reducing risk port exposure. SCP supports the deployment of network visualization by importing virtual machines. This chapter mainly introduces the installation and deployment of aNI, including installing the aNI virtual machines.

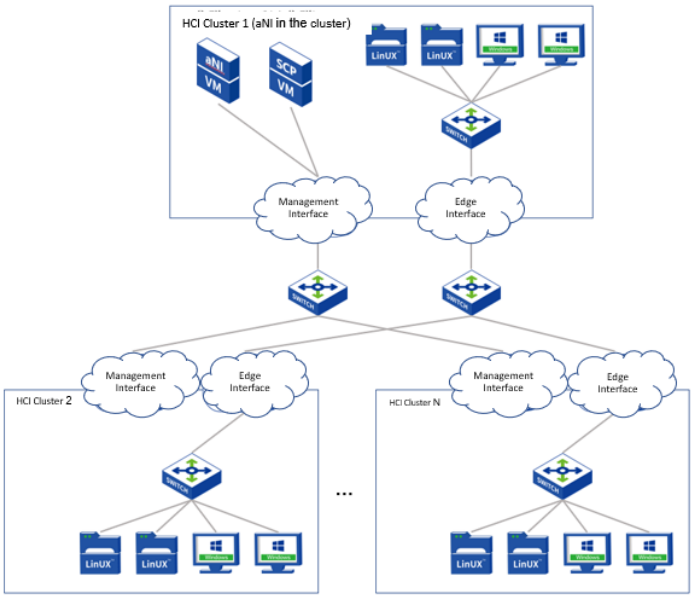
4.4.2.1 Installation and Deployment

- The flow chart of aNI installation and deployment is shown in the following figure.



- The network topology planning for aNI is shown in the following figure. The aNI platform needs to communicate with the management network of HCI and SCP (recommended to be on the same network segment as the management network). It is mainly for the aNI platform to call the API interface of HCI and SCP to collect virtual machine data.

- The overloaded virtual machine will randomly lose packets and access



data if the number of access relationship records for a single host exceeds the specified limit. Specifications are as follows.

Type	Cores	Memory	Storage	Total of applicable VM
Small	8	16GB	500GB	100
Medium	32	64GB	1T	1000

Large	64	128GB	1.5T	3000

Precautions:

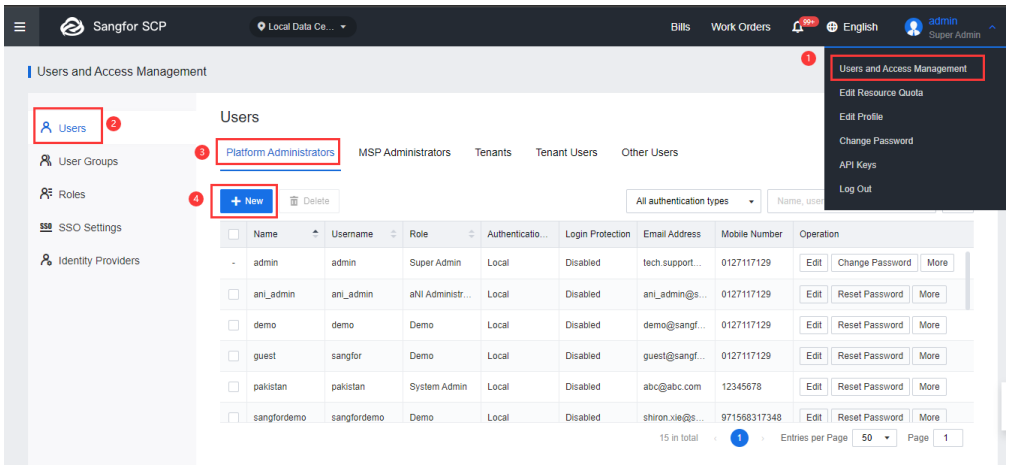
1. It only supports the deployment of aNI on SCP6.8.0 currently.
2. Currently, the collection of traffic between virtual routers/virtual switches and NFV traffic is not supported.
3. Currently, IPv6 traffic information collection is not supported.
4. When HCI changes the virtual machine's IP address, the traffic visualization service update will be delayed, and the latest update time of a stream is 5 minutes.
5. The aNI authorization is integrated into aNET, and there is no need to activate the license separately.
6. The aNI password must change every three months.
7. When the aNI virtual machine is deployed, the console language does not change with the SCP platform language.
8. When the aNI has been deployed on the SCP platform, the aNI cannot be deployed on other platforms.
9. When directly modifying the aNI virtual machine configuration, the configuration needs to restart to take effect.
10. After the aNI virtual machine expands the disk capacity, the aNI virtual machine needs to restart for the expansion to take effect.
11. When the virtual machine is deleted on HCI, the data information of the virtual machine may still exist on the aNI.
12. The interface does not currently support expanding groups of more than 100 virtual machines.
13. Only the traffic passing through the DWF is collected (the DWF of the 670 is enabled by default), and the traffic that does not pass through the DWF cannot be collected and reported. (The traffic between virtual routers, virtual switches, and NFV are not collected).

Prerequisite

None.

Steps:

Step 1. Log in to the SCP platform as admin, select **User and Access Management > Users > Platform Administrators**, and click the **New** button to create a platform administrator.



Step 2. Configure the following information to complete the creation of the platform administrator.

Name: ani_admin

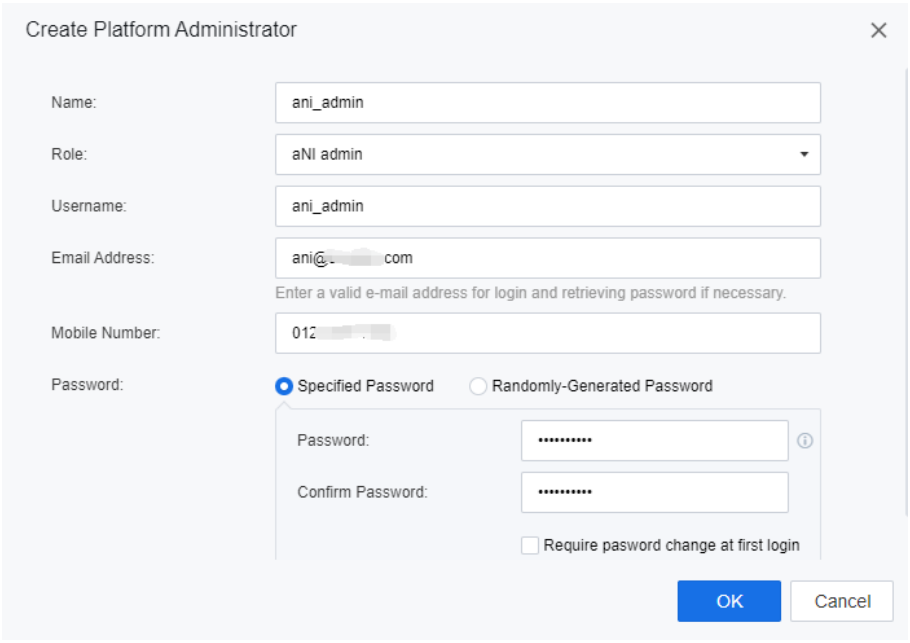
Role: aNI administrator

Login username: ani_admin

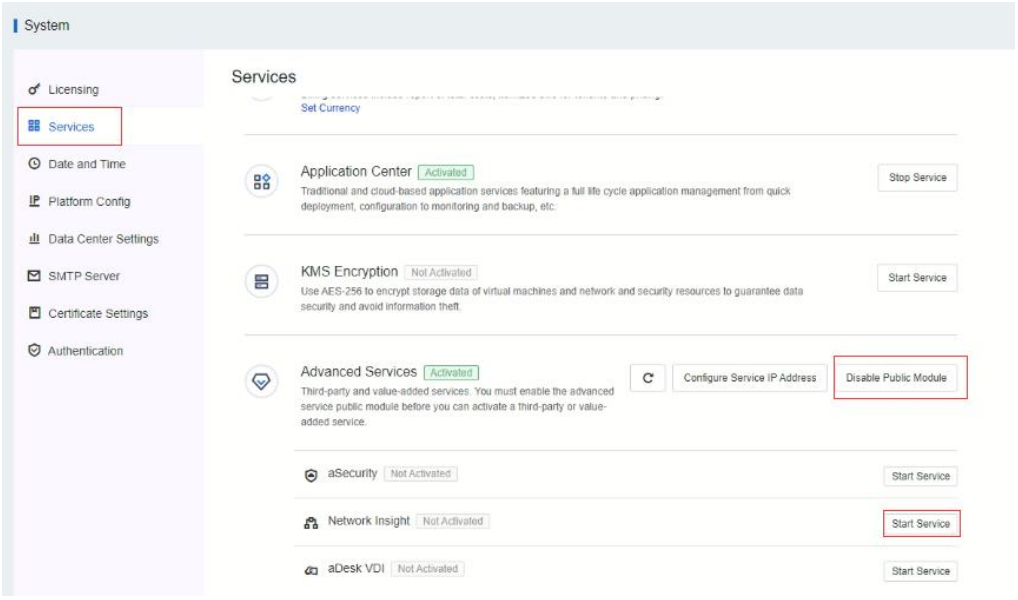
Email: custom

Mobile: Custom

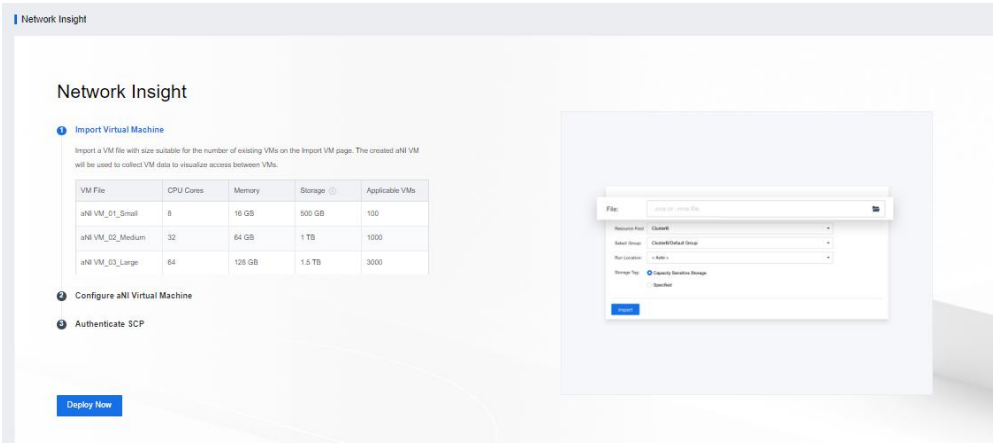
Password: custom



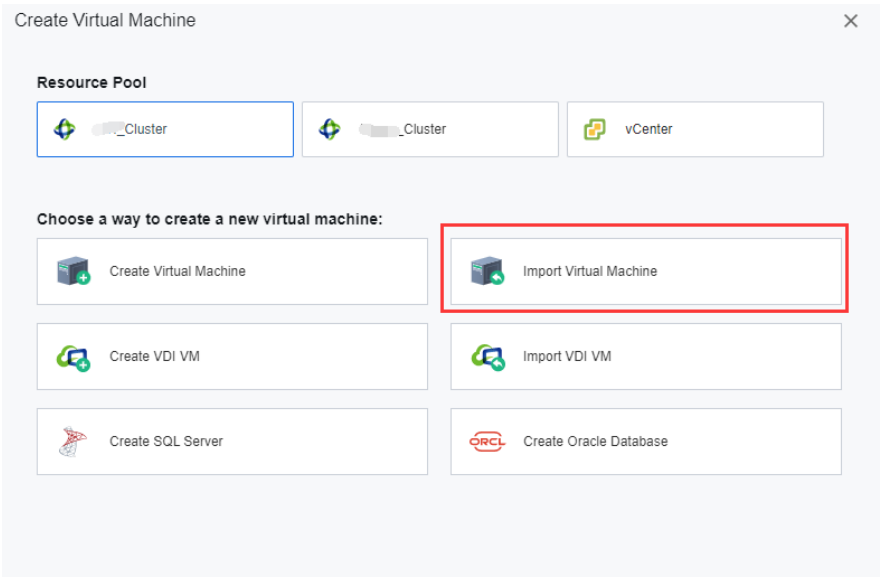
Step 3. Enter the **System > Services** interface, select **Advanced Services**, and click **Enable Public Module,** Start **Network Insight** services.

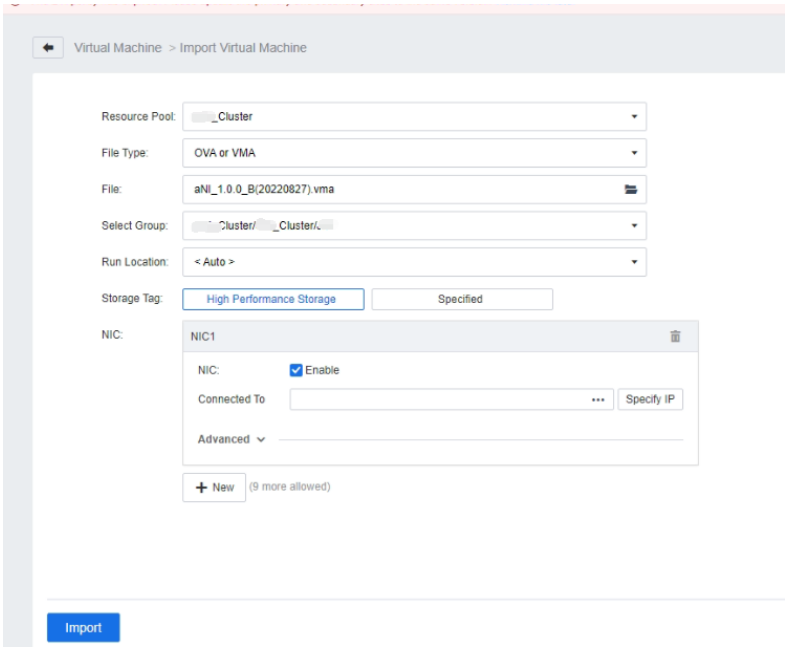


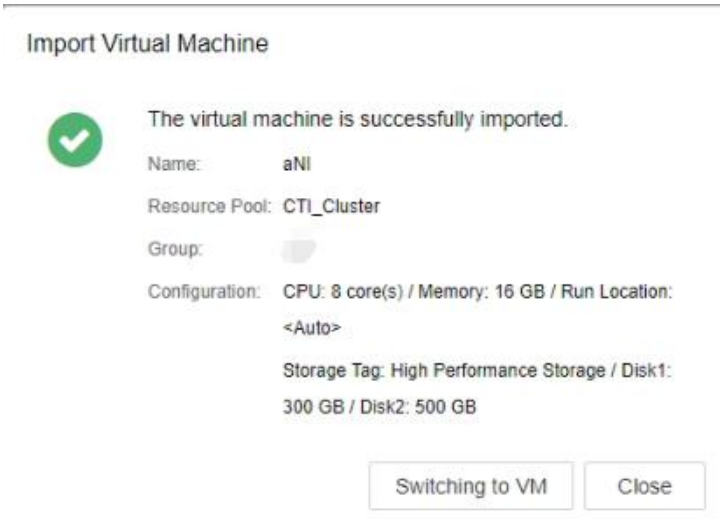
Step 4. Go to the **Compute > Virtual Machines** page, click **New**, select **Import Virtual Machine**, or enter the **Network Insight** interface and click the **Deploy Now** button.



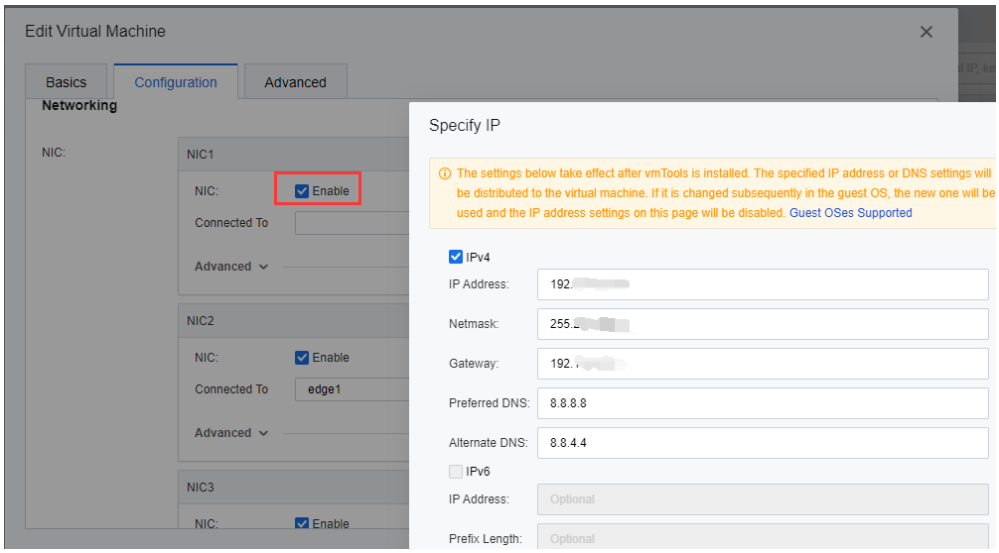
Step 5. Import the vma file, and select the resource pool, Virtual machine group, running location, storage performance, and network card.



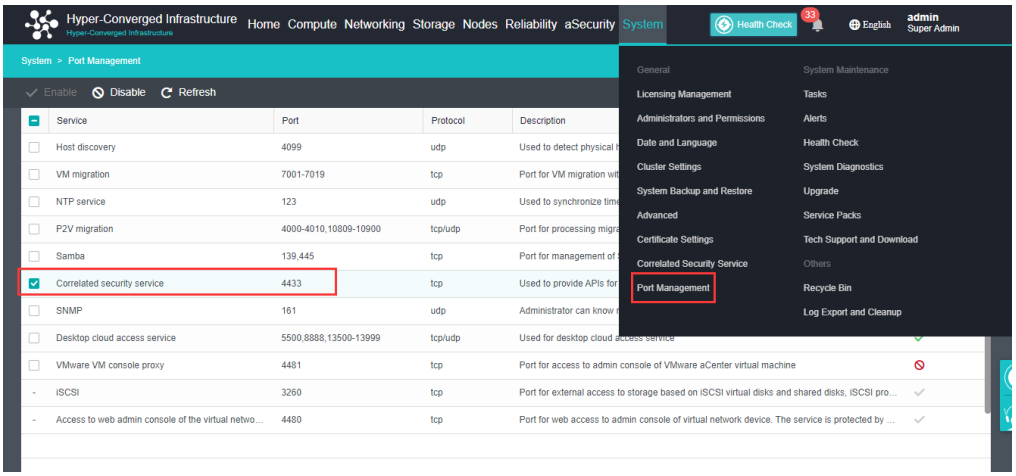




Step 6. After the import is successful, enter the **Edit virtual machine** interface to configure the network card. Check **Enable**, connect to the physical edge, click the **Specify** IP button, select IPV4, and configure the IP address of the aNI virtual machine as the aNI management network (it is necessary to plan to be able to communicate with the SCP management network segment, It is recommended to be on the same network segment as the SCP management network).



Step 7. Log in to the HCI cluster where the aNI is located, enable the correlated service port, and enable the **Correlated security service**. Otherwise, the network insight service will not be accessible.

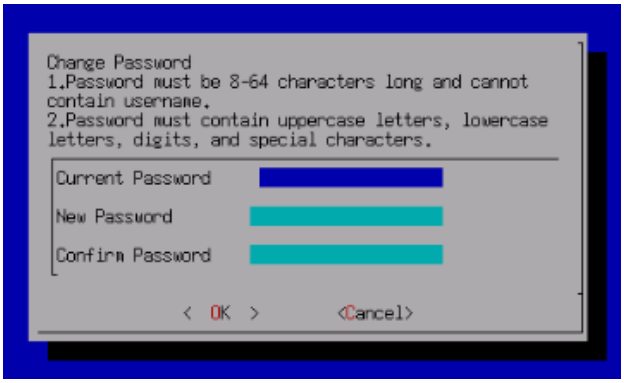


Step 8. Power on the virtual machine, enter the VM console and configure the platform security linkage.

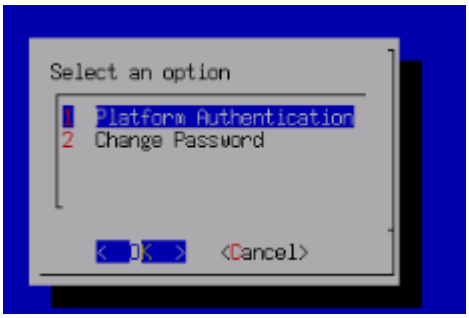
I. Enter the password of the cloud security center to log in. You need to change the password for the first login. There are only five chances to try to enter the password. If you enter the wrong password five times, the account will be locked for 5 minutes, and you can enter it again after 5 minutes. The default password is **Sfcsec@123**, and the password modification policy is as follows:

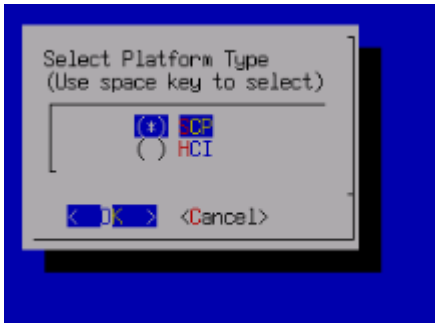
- The length is 8~64 characters.
- Must contain 4 items of uppercase letters, lowercase letters, numbers, and special characters, special characters support ~`@#%&<>'",;_-^$.*+?=!:|{}()[]/.





II. After successful login, click **Platform Authentication** and select SCP for platform type configuration.

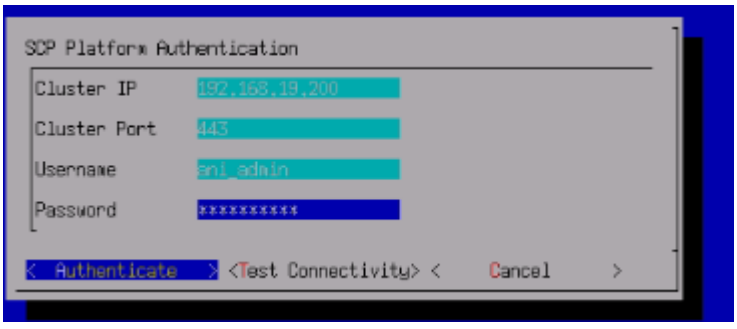




III. Enter the platform authentication page:

- Cluster IP: IP of the SCP management port.
- Username/Password: ani_admin/password.

IV. Click **Authenticate** to complete the aNI deployment.

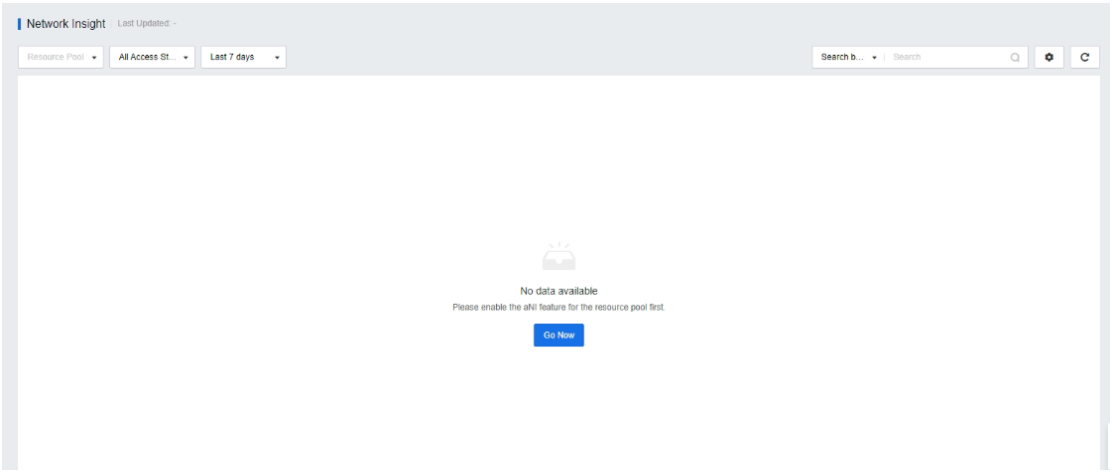


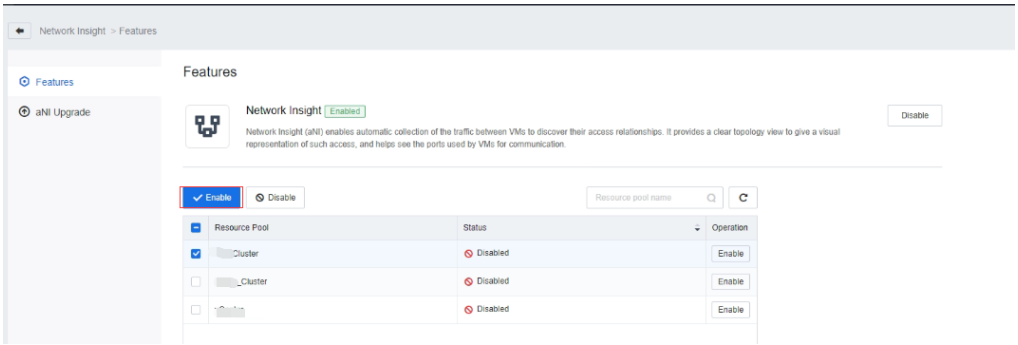


4.4.2.2 Configuration Steps

Step 1. After completing the aNI installation, enter the Network Insight page and click **Go Now.**

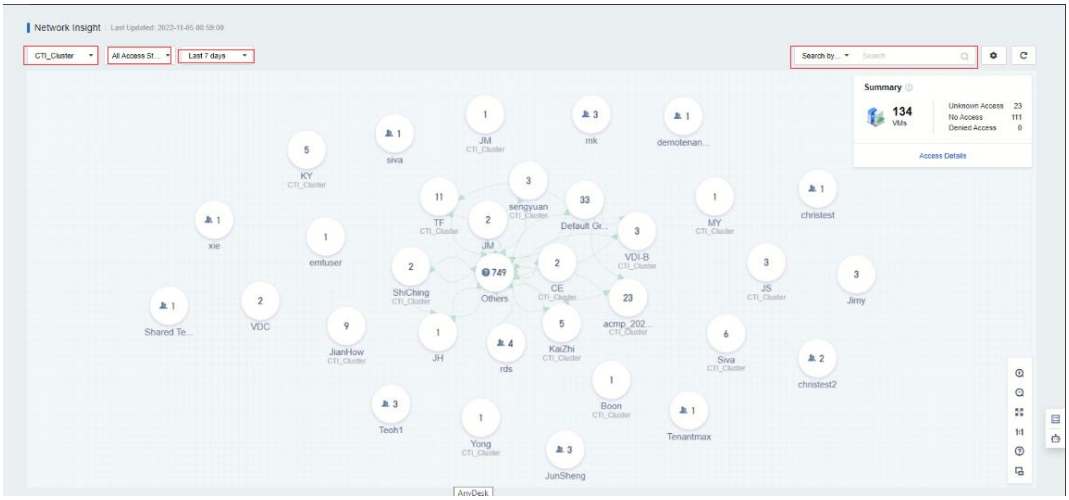
Step 2. Proceed to the **Networking > Network Insight** page, select the resource pool for which network visualization needs to be enabled, and click **Enable** to enable the resource pool network visualization function.



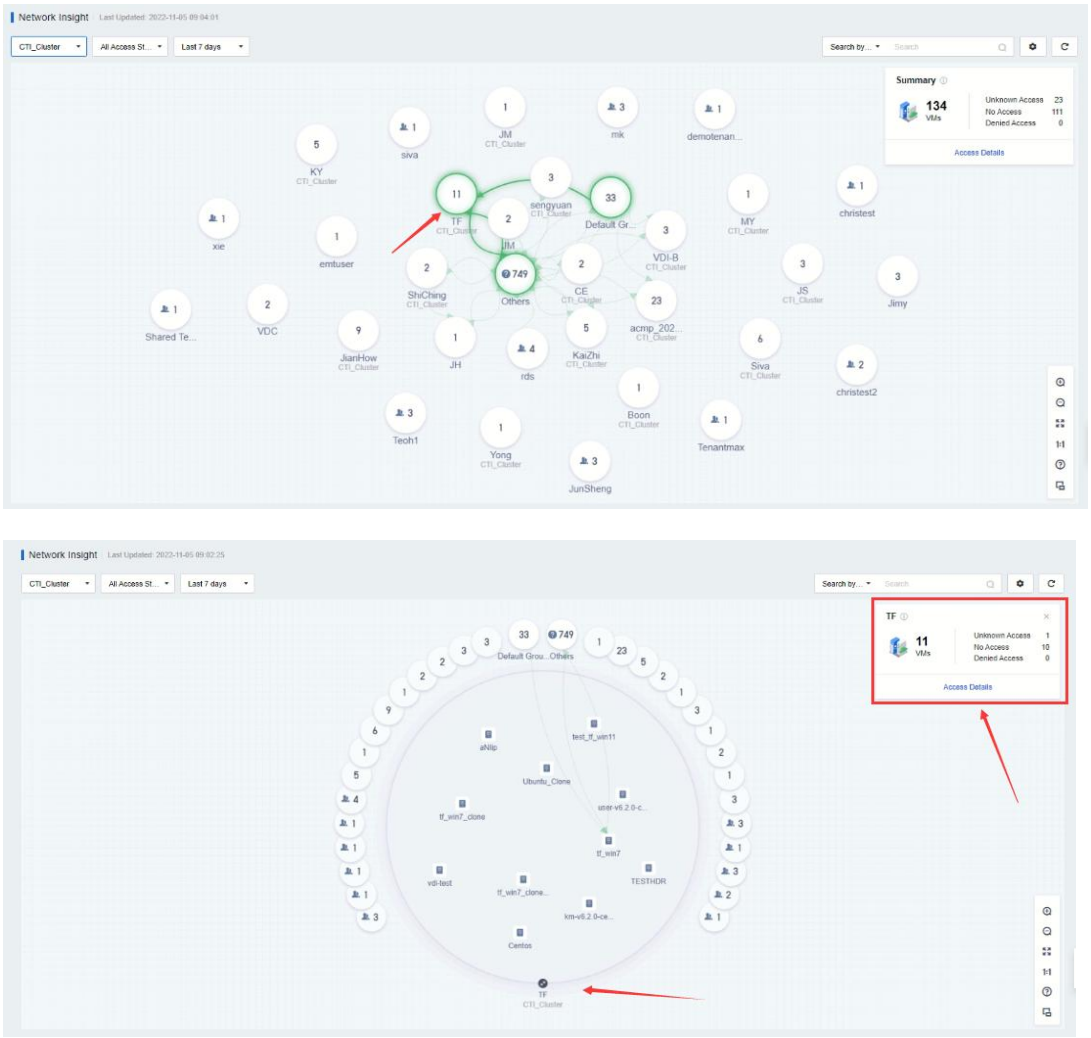


3. On the **Network Insight** page, view the access records of all VMs on the platform. You can filter the records by using the filter in the upper-left corner. You can also filter the records by VM or VM group.

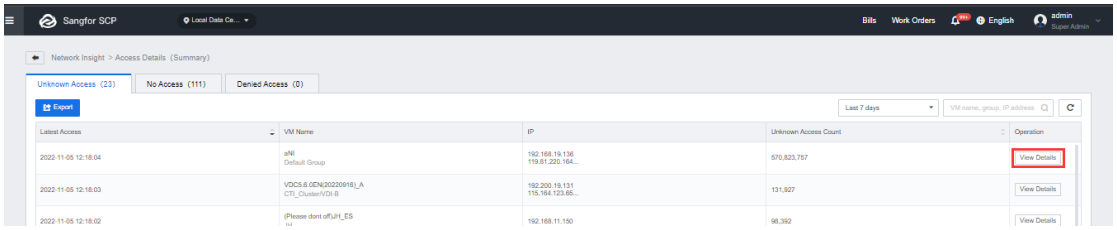
- Filter by access status: You can select **All**, **Allowed**, **Denied**, or **No Policy Matched**.
- Filter by time: You can select **Last 30 days**, **Last 7 days**, **Last 3 days**, or **Today**.
- Access details: Click the card in the upper-right corner of the page to enter the **Access Details** page, where you can quickly export an access list.
- **Time screening**: last 30 days, last 7 days, last 3 days, today.



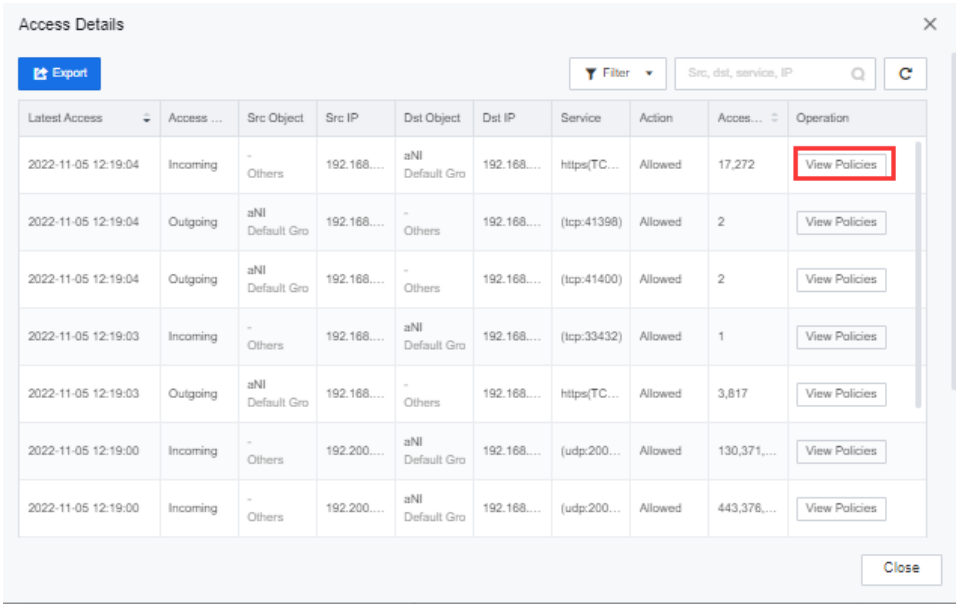
Step 3. Select a group to enter the virtual machine group display page. The card in the upper right corner displays the access relationship information of the virtual machines in the current group, including the total number of virtual machines, location communication, no access, and intercepted access. Click the zoom out button to collapse back to the initial interface.



Step 4. Click the **Access Details** button to enter the details page, and click the operation bar **View Details** to obtain the detailed information of each record, including the firewall policy quintuple information: **Src Object, Src IP, Dst Object, Dst IP**, and **Service**.



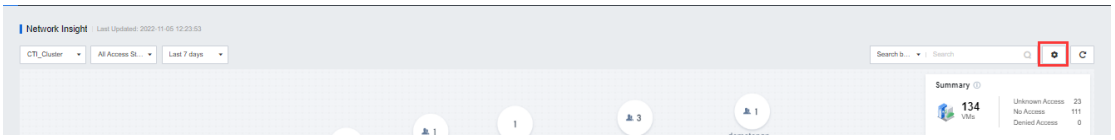
Step 5. Click the **View Policies** button to jump to the **Distributed Firewall** page, where you can add, delete, modify, and check access policies.

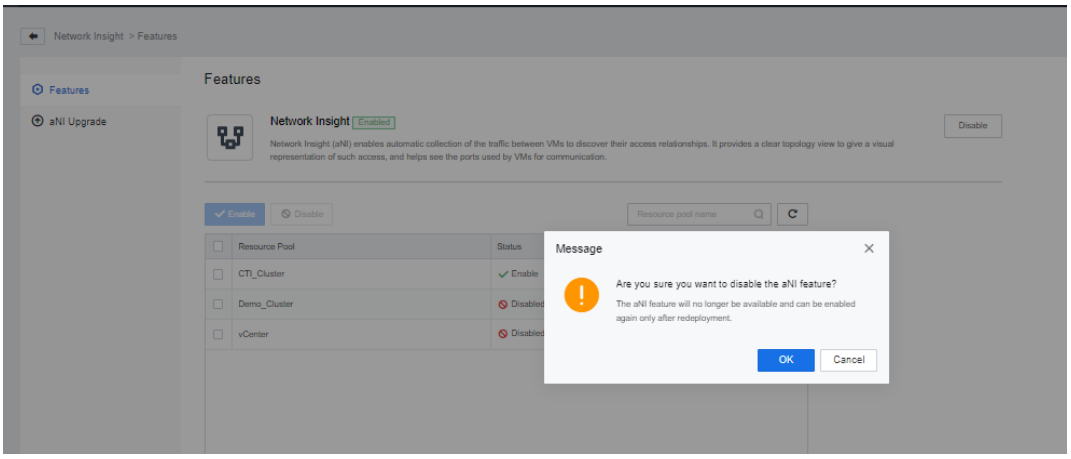


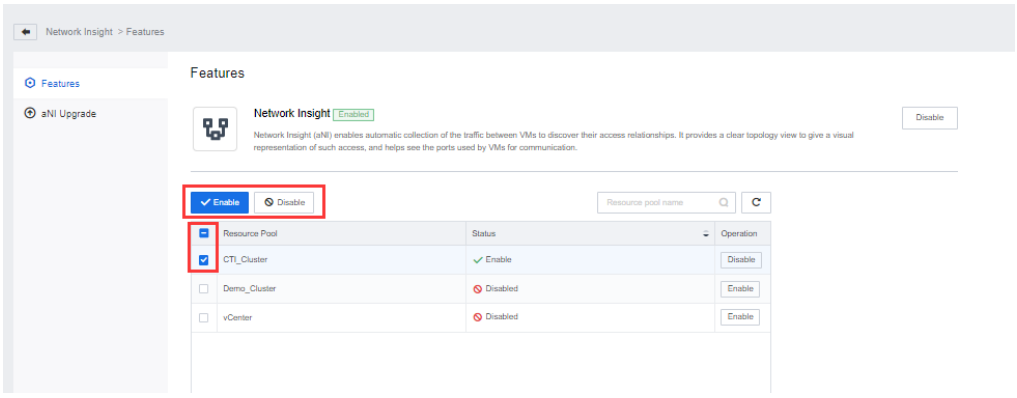
Step 6. The platform also supports setting operations for network insight services. Click the **Settings** button to enable, disable, upgrade and other settings for the service.

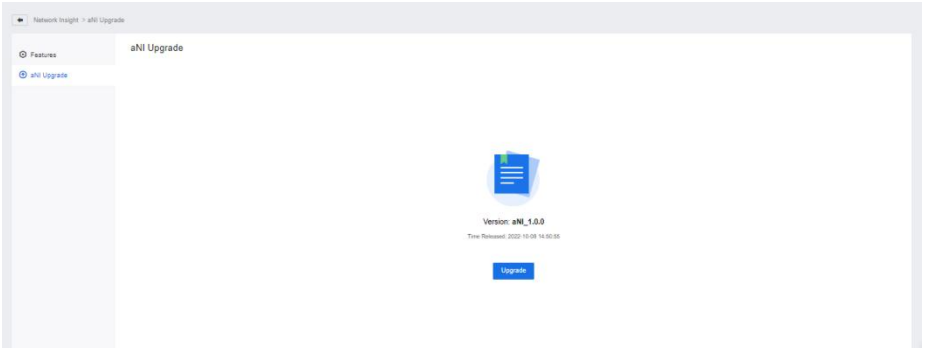
NOTE

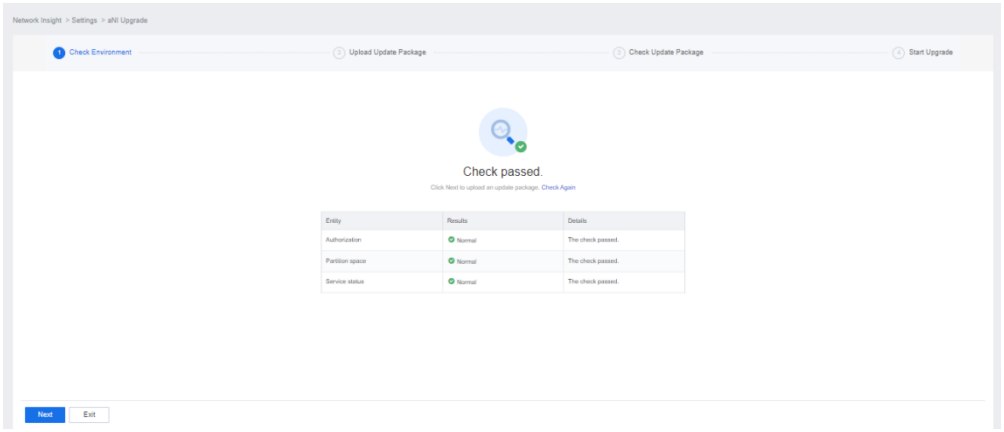
After the network insight service is closed, the function can no longer be used. If the function needs to be enabled, it must redeploy.











4.4.3 Traffic mirroring

Function Description

In the operation and maintenance scenario, the network traffic of the production virtual machine needs to be mirrored to the security review device to realize traffic filtering and monitoring. Sangfor SCP supports copying and forwarding the NIC traffic of the virtual machine/network device to the SCP egress. You need to configure traffic mirroring on the intermediate switch to mirror it to an external device.

Precautions

1. A mirror rule source object can select up to 1024 interfaces.
2. The target object can only select one virtual machine interface or network device interface.
3. If a Virtual machine/network device interface or physical host service port is used as a source object, it can only belong to one traffic mirroring policy. It can belong to multiple traffic mirroring policies if it is used as a destination object.
4. The mirroring function of the physical network to the virtual network is not supported.
5. As the number of rules increases, the delay of service traffic increases, and the throughput decrease. It is recommended to configure less than 100 rules.
6. The virtual machine referenced by the traffic mirror supports migration within the same resource pool, and the traffic mirror still takes effect after the migration.
7. Support separate physical egress configuration for traffic mirroring. In the scenario where virtual network traffic is mirrored to an external device, the mirrored traffic occupies the service communication interface. When mirroring across nodes in a cluster, the mirrored traffic occupies the data communication interface. To prevent the mirrored traffic from occupying bandwidth with the service interface or data communication interface in a high-load scenario, it is recommended to plan a separate physical NIC for traffic mirroring and forwarding.
8. When mirroring to a physical service port, a VLAN must be configured, and the VLAN must be consistent with the VLAN allowed on the physical switch (truck port) connected to the physical port. Therefore, the mirrored traffic cannot include the traffic of this VLAN.
9. When the service port connected to the physical egress is modified, the corresponding physical service port in the traffic mirroring rule also changes accordingly.
10. Mirroring across resource pools is supported only in connected areas.
11. The traffic captured by DFW and the traffic restricted by QoS will be captured

and forwarded by traffic mirroring.

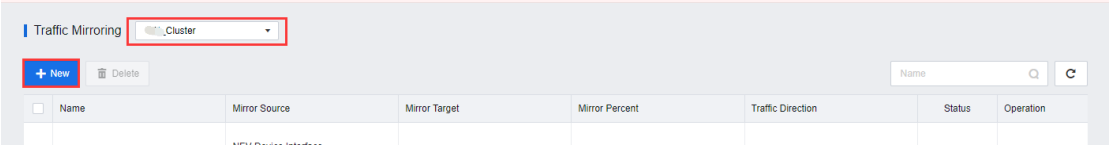
12. Only business traffic is captured when the multi-network integration network port is the mirroring source.

Prerequisite

None.

Steps:

1. Go to the **Networking > Traffic Mirroring** page, select the resource pool for traffic mirroring, and click the **New** button to configure the traffic mirroring policy.



2. The platform supports the configuration of 3 traffic mirroring: traffic mirroring within the virtual network, traffic mirroring from the virtual network to the physical network, and traffic mirroring between physical network ports.

- **Specify the mirror source:**

  Internal traffic mirroring of virtual network: specify the interface of the virtual machine/network device.

  Mirror virtual network traffic to physical network: specify the interface of the virtual machine/network device.

  Traffic mirroring between physical network ports: Specify the service port of the physical node.

- **Specify the mirroring target:**

  Internal traffic mirroring of virtual network: specify the interface of the virtual machine/network device.

  Mirror virtual network traffic to the physical network: specify the service port of the physical node.

  Traffic mirroring between physical network ports: Specify the service port of the physical node.

- **VLAN ID:**

Internal Traffic Mirroring of Virtual Network: No need to fill in.

Mirror virtual network traffic to physical network: Specify the VLAN ID carried in mirrored packets.

Traffic mirroring between physical network ports: Specify the VLAN ID carried by mirrored packets.

- **Mirror Percent:**

  The ratio of the source object traffic to be mirrored, the default is 100%, which means that the traffic is completely mirrored.

- **Traffic direction:**

  The traffic direction of the source object is to be mirrored.

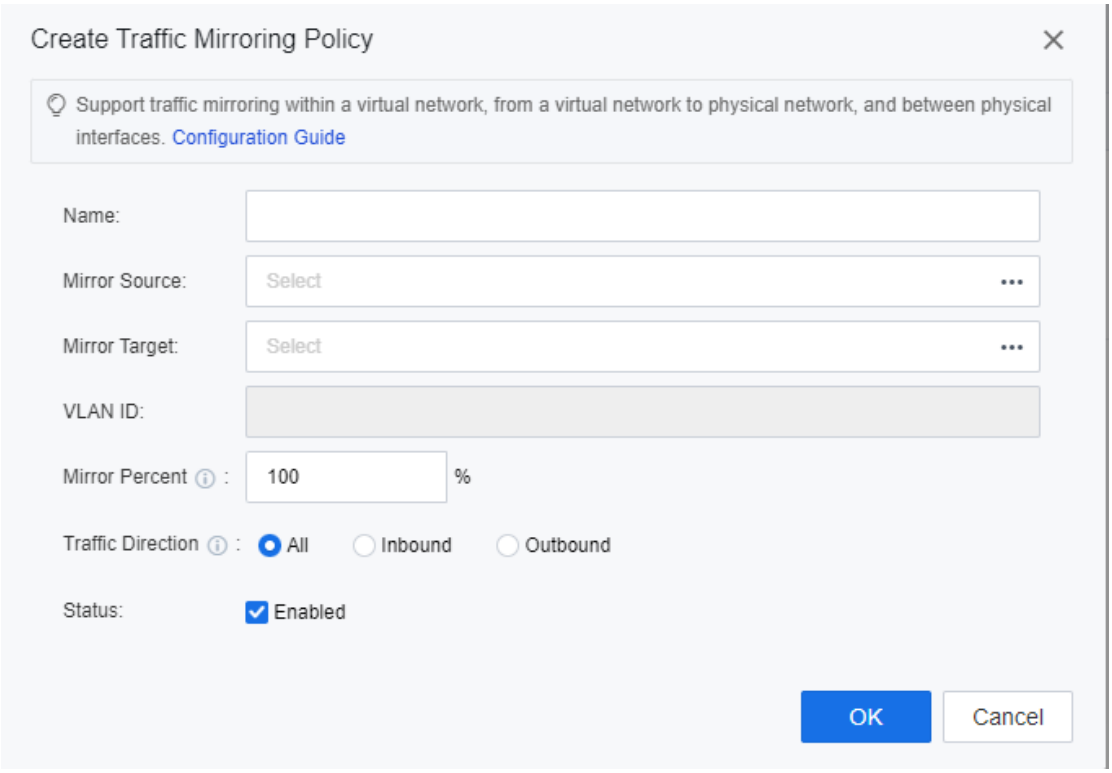
  All means the traffic received and sent by the mirror source object at the same time.

  Inbound means only mirroring the traffic received by the source object.

  Outbound means only mirroring the traffic sent by the source object.

- **Status:**

  Check **Enable** checkbox to make the policy take effect.



3. After the policy configuration is complete, the network traffic to the source

can be monitored on the destination device.

4.4.4 Network Deployment

Function Description:

1. The administrator can manage the tenant's network in the network deployment module and create a VPC and a classic network for the tenant.
2. The VPC is suitable for scenarios that require high network security isolation. Tenants can freely use subnets within the VPC without worrying about network conflicts.
3. The classic network is suitable for direct communication scenarios between tenants and other tenants or physical environments. When a classic network is created, an egress switch will be created by default, which can be connected to uplink physical egress, routers, NFV, and other devices.

Precautions:

1. In versions before SCP 6.7.0, only one VPC can be created in a resource pool associated with a tenant, while for SCP 6.7.0 and later versions, a tenant can create up to 10 VPCs in the same network domain.
2. SCP 6.7.0 and later versions support creating multiple VPCs exist for a resource pool.
3. A physical egress can only be associated with one VPC egress, and multiple VPC egresses cannot be associated with one physical egress.

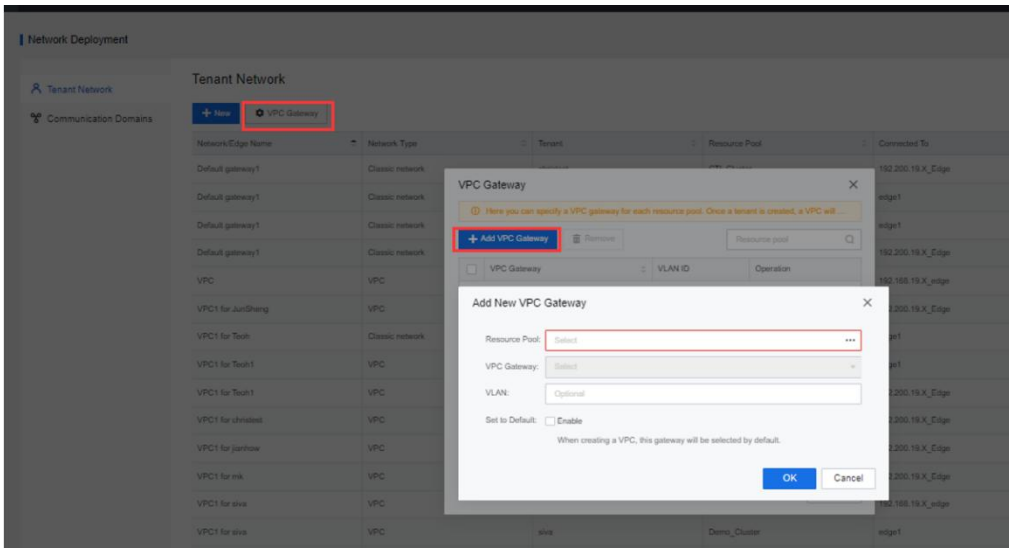
Prerequisite

The platform administrator has successfully created the tenant.

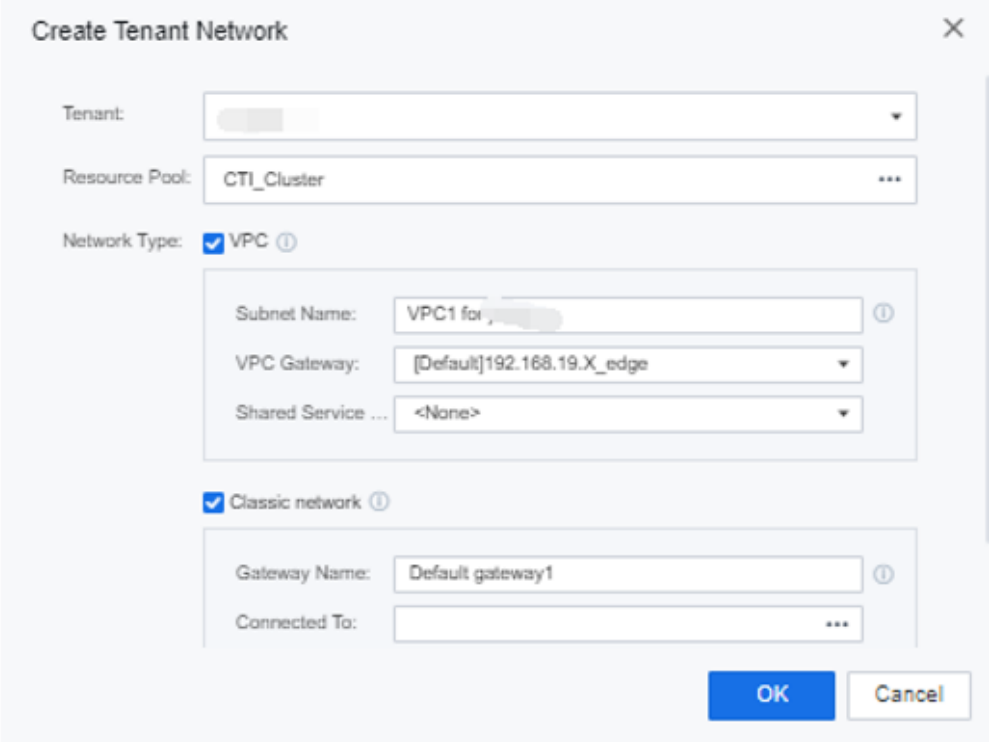
Steps:

VPC subnet

Step 1. Create a VPC gateway by clicking **VPC Gateway**, click the **Add VPC Gateway** button on the pop-up page, select a resource pool or VPC gateway, and check the **Enable** checkbox to set the default VPC gateway.



Step 2. Click **New** to create a tenant VPC.

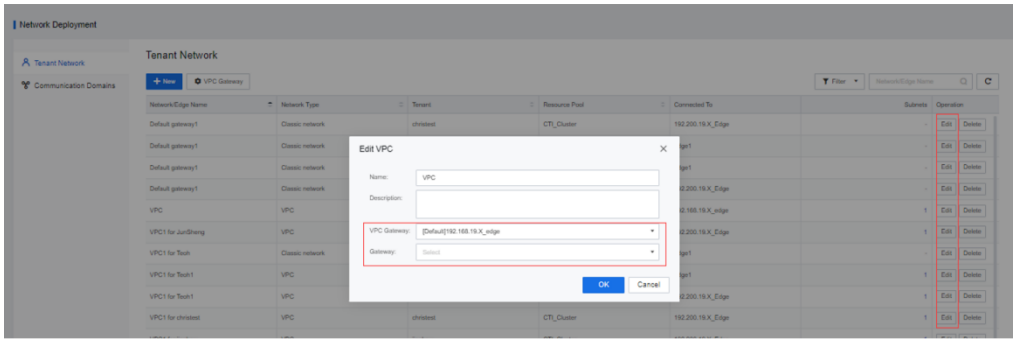


Step 3. Click **OK** to complete the creation.

Step 4. Once created, you can view all network types in the list.

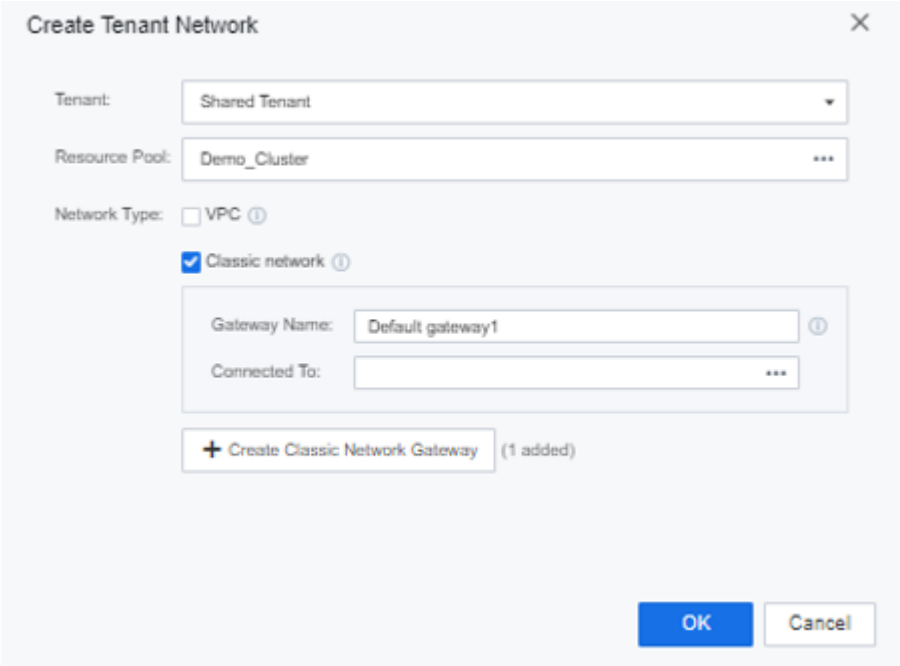
Network/Edge Name	Network Type
Default gateway1	Classic network
Default gateway1	Classic network
Default gateway1	Classic network
Default gateway1	Classic network
VPC	VPC
VPC1 for .	VPC
VPC1 for	Classic network
VPC1 for	VPC

Step 5. Click the **Edit** button to edit the VPC gateway and public service gateway of the VPC subnet.



Classic Network

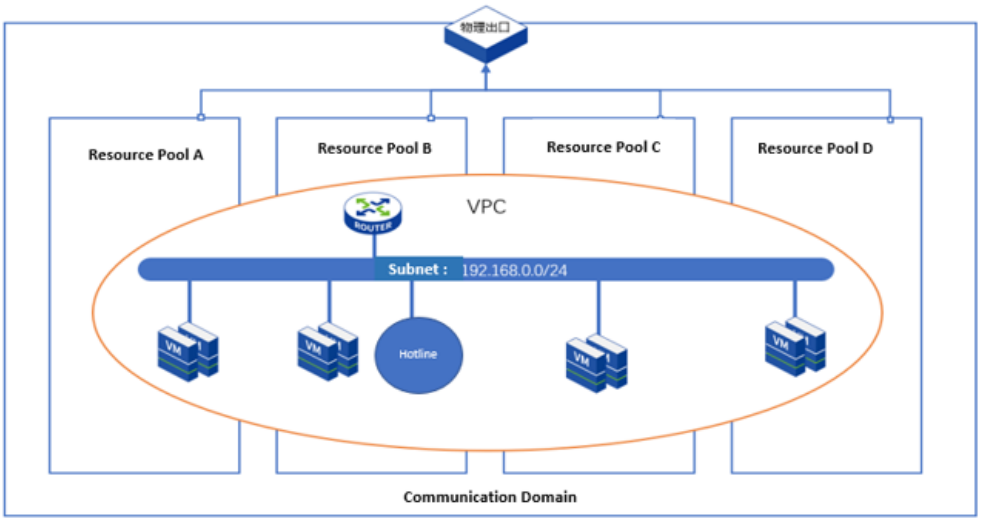
Click **New** to start creating the tenant classic network. Select the connected device as **Physical egress**. If the tenant's classic network requires VLAN isolation, you can select different port groups in the physical egress.



4.4.4.1 Communication Domains

Function Description:

By forming a communication domain, the resource pool network within a communication domain can be connected at Layer 2, enabling the cross-cluster deployment of large-scale services and cross-regional multi-cluster management. It supports multi-cluster and multi-data center networks to form a network connectivity domain to achieve unified network orchestration. Ensure that a single cluster's physical network level isolation between clusters and network failures (such as broadcast storms and loops) will not extend to other sites.



A complete communication domain consists of the primary controller, backup locations, and several common resource pools:

- **Main controller:** The main controller manages network resources in the connected domain.
- **Backup location:** The backup location backs up the network resource configuration information on the main controller to realize the disaster recovery function for the main controller.

Precautions:

1. SCP6.7.0 and above can support the formation of communication domains, and the HCI version corresponding to the resource pool in the communication domain also needs to be 6.7.0 and above.
2. At least three nodes are required to form a resource pool of a communication domain.
3. Only after the NICs of all virtual machines and NFV devices in the resource pool are disconnected can they be removed from the communication domain.
4. NAT deployment is not supported between HCI clusters forming connected domains.
5. After a communication domain is formed, it is necessary to ensure that the VXLANs of different resource pools in the connectivity zone can communicate. Changing the VXLAN IP pool will temporarily interrupt services.
6. The network topology of the cluster where the resource pools that make up

the connected domain are located will not be displayed in the HCI. You need to view and edit the network topology in the SCP.

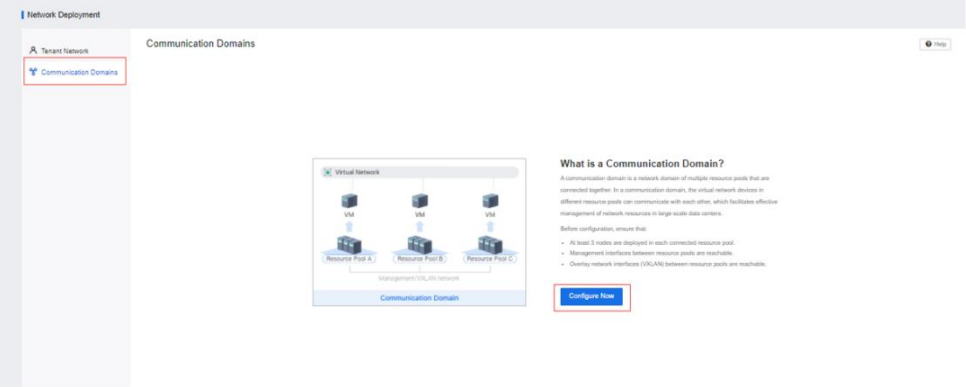
7. Stretched clusters are not currently supported as the primary controller or backup location in a Communication Domain and can only be added to Connectivity Domains as a common resource pool.
8. After the resource pool on the SCP is added to the communication domain, the distributed firewall policy of HCI cannot be viewed, and the use of firewalls is not supported.

Prerequisite

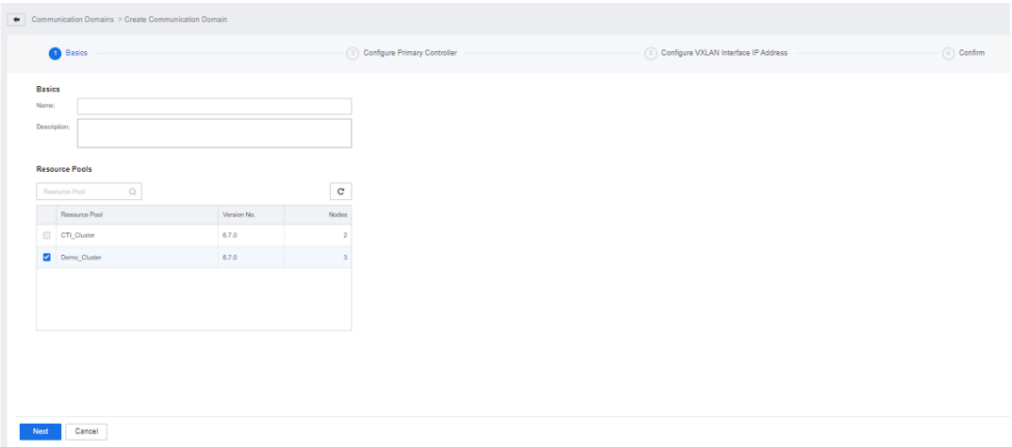
The cluster to be added to the communication domain has been added as a resource pool.

Steps:

Step 1. Log in to the SCP platform, select **Networking** > **Network Deployment** > **Communication Domains**, and click **Configure Now**.

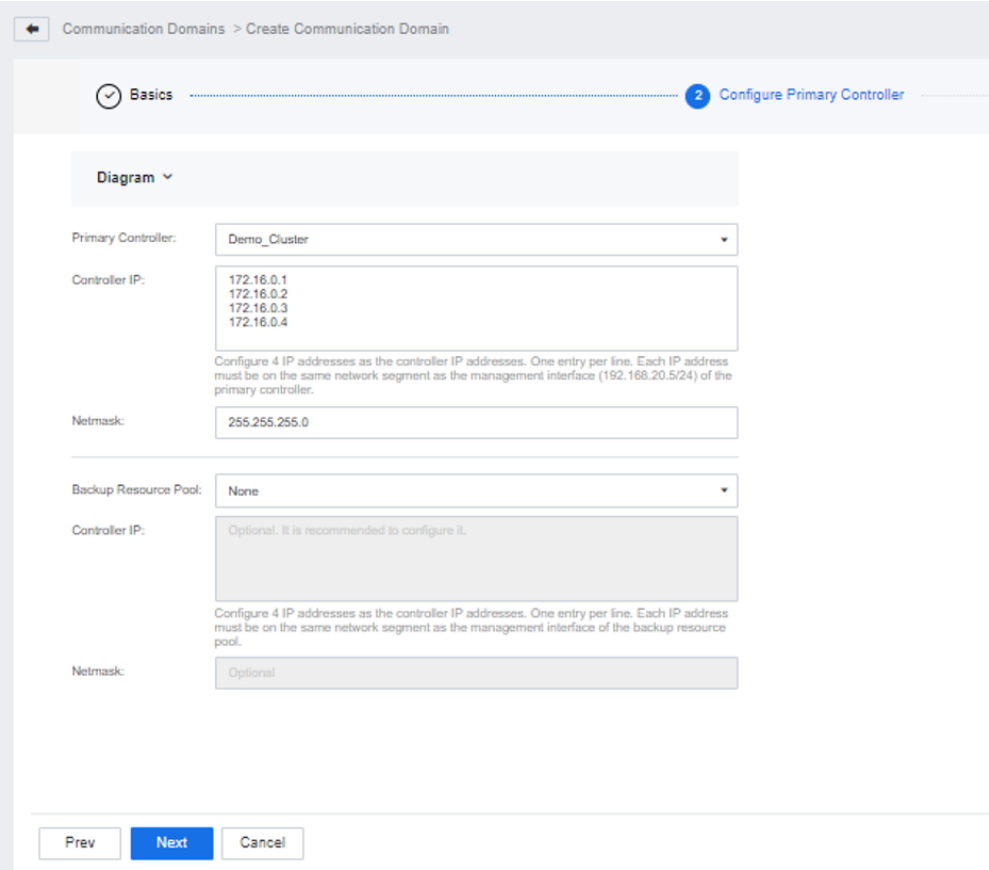


Step 2. Fill in the basic information of the communication domain, select the resource pool to be added to the connected domain, and click **Next**.



Step 3. For the resource pool to be added to the Communication Domain,

you need to designate one as the primary controller and the other as the backup repository and set the controller IP. Here, 4 IPs need to be configured as controller IPs, the first 3 are the IPs of the 3 network control nodes of the controller, and the last one is a virtual IP. It is necessary to ensure that the controller IP and the management interface of the main controller/backup repository are in the same network segment.

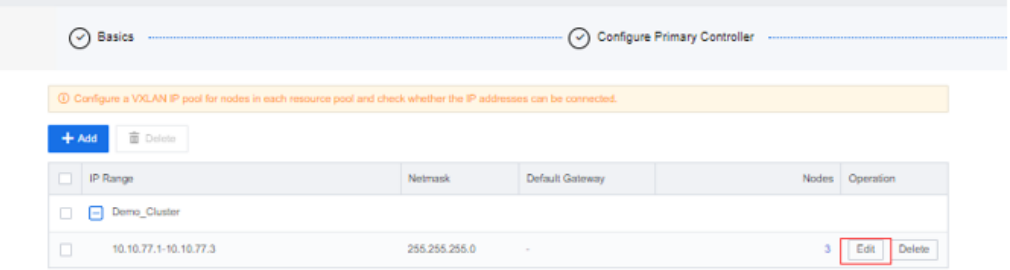


Step 4. Click **Next** to see the current resource pool's existing data communication IP pools. Currently, it is not supported to form a communication domain by combining two data communication IP pools as resource pools on the same network segment:

- If the data communication IP pools of the two resource pools are in different network segments, click **Next** directly.
- If the data communication IP pools of the two resource pools are the same network segment, click the **Edit** button, and after modifying one of the resource pools to be a different network segment, click **Next**.

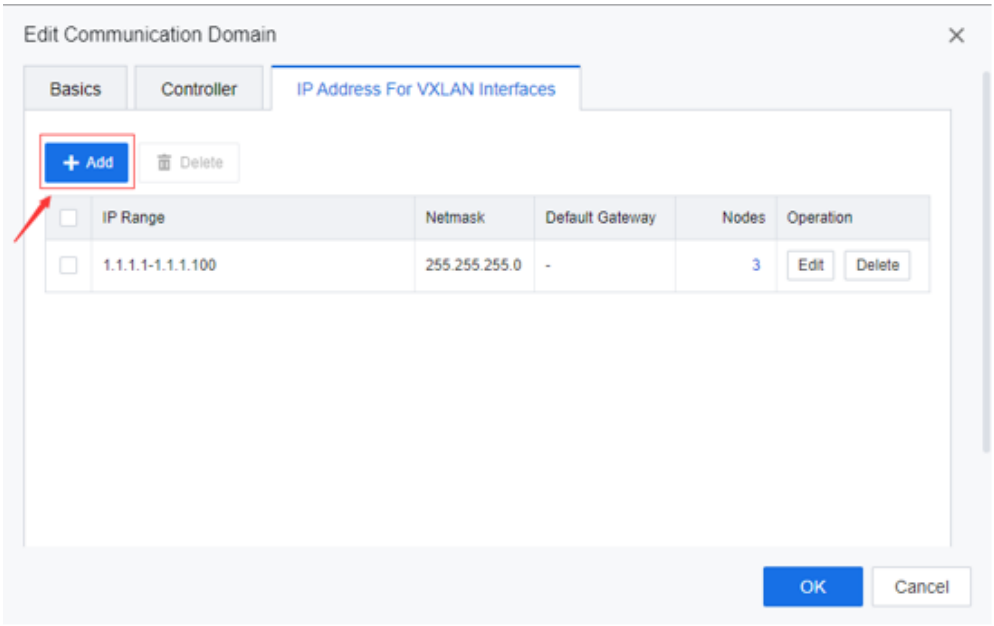
NOTE

Modifying the data communication IP here will affect the east-west traffic of the platform virtual machine.



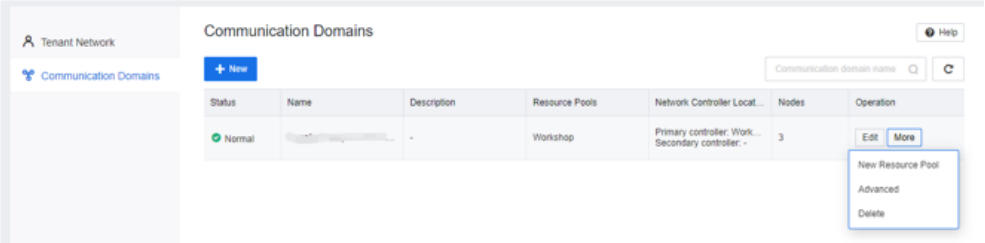
Step 5. Click **OK** after the connected domain configuration is completed, enter the communication domain list, and click **Edit** to configure the data communication IP pool of the communication domain. The following two methods are available:

- If the data communication IP pool is the same network segment: Click the **Delete** button. After deleting all the original configurations, click **Add IP Pool** to reconfigure the IP pool for the connected domain.
- If the data communication IP pools are in different network segments: delete one of the IP pools, select another IP pool, and click the **Edit** button to expand the IP pool to ensure that all physical nodes in the connected domain can communicate.

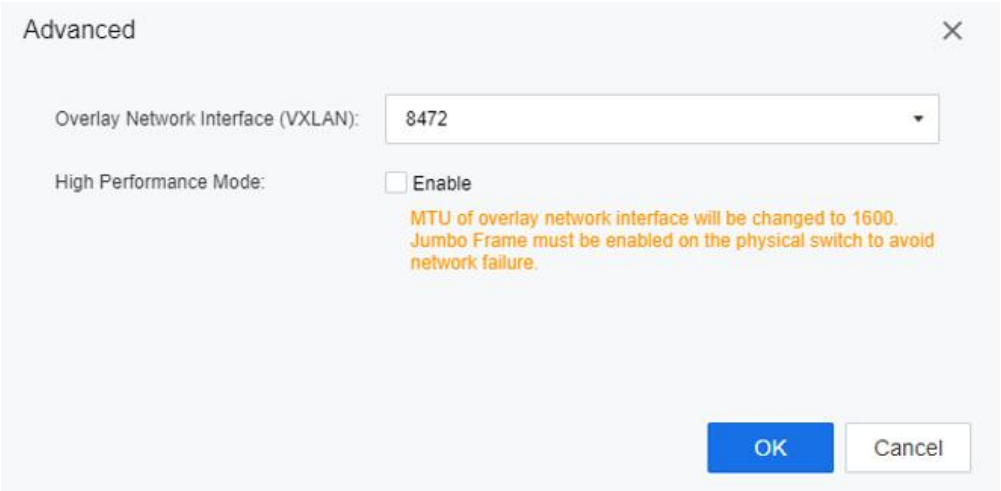


Step 6. After completing the communication domain configuration, go back to

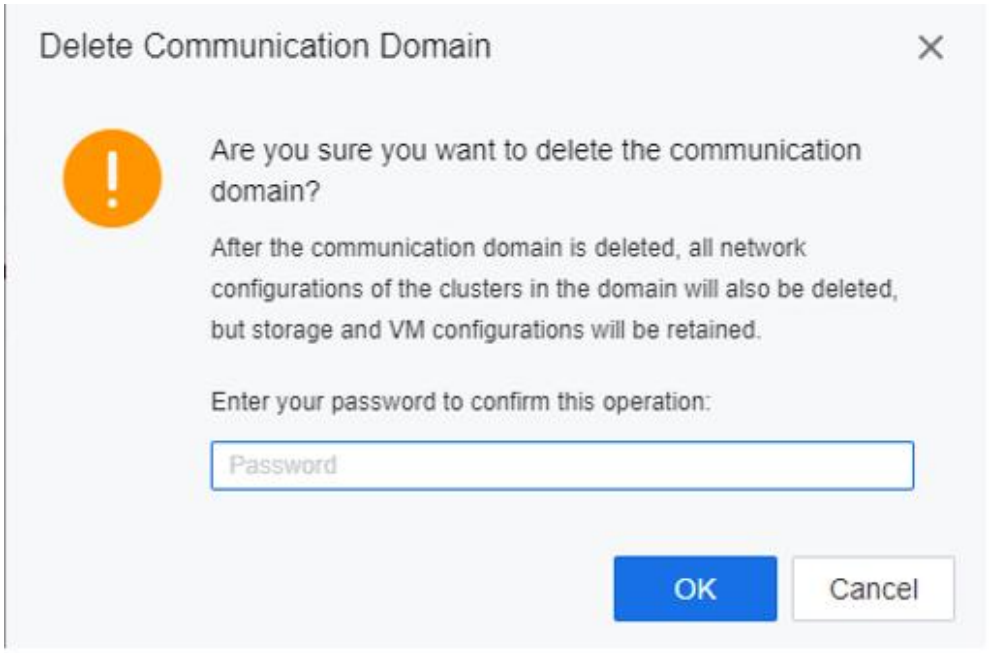
the communication domain list and click **More** to perform operations such as **New Resource Pool**, **Advanced**, and **Delete**.



- **New Resource Pool**: You can add an independent resource pool to the communication domain.
- **Advanced**: support to modify the data communication port of the communication domain and support to enable the high-performance mode of the network port.



- **Delete**: When only the main controller is left in the communication domain, the user can delete the communication domain. After the communication domain is deleted, the main controller will continue to be used as an independent resource pool.

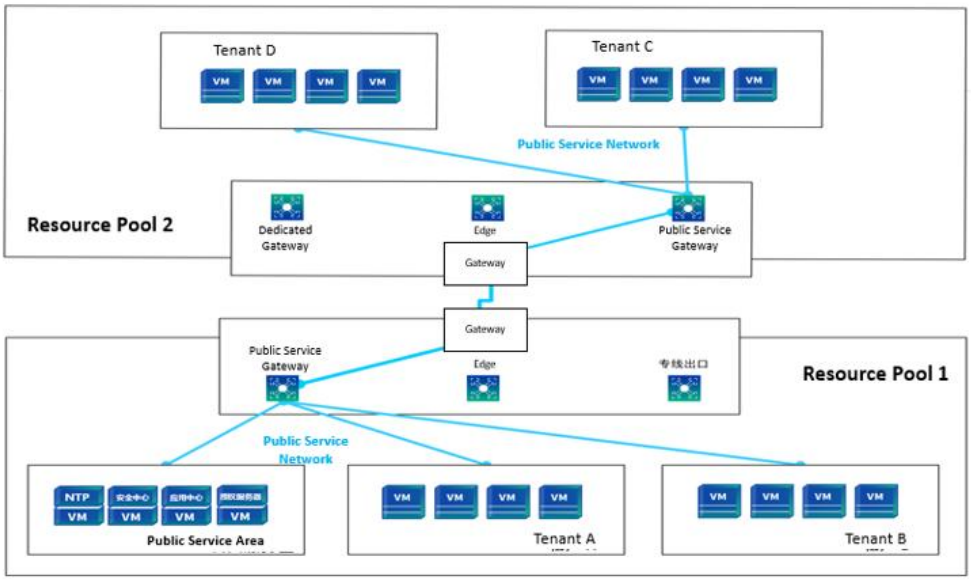


Step 7. When an exception occurs in the resource pool in the communication domain, place the mouse on the exception symbol to see the exception prompt, click **Repair Now**, and the system will retry and continue execution from the point of the last failure. The repaired scenarios include failure to switch between active and standby, failure to modify controller IP, and failure to add resource pool.

4.4.5 Shared Service Network

Function Description:

Sangfor SCP joins the shared service network for public service scenarios on the cloud and builds the shared service network as a dedicated channel between the public service area and resource pool tenants. NTP servers, licensing servers, NAS, security centers, and application centers can be deployed in shared service areas to meet tenants' access to public services.



Precautions:

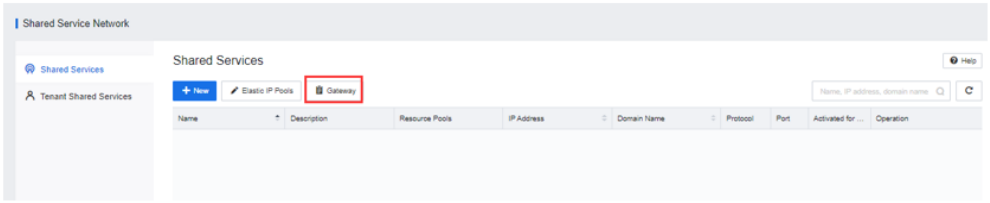
1. The tenant classic network cannot access shared services through domain names, and a DNS server needs to be deployed separately.
2. The shared service IP must be in the same segment as the shared service network elastic IP and be excluded from the elastic IP pool.
3. The shared service network gateway cannot be modified in the presence of shared services.
4. The admin can only access the management interface of the shared service network, and the tenant has no management interface.
5. The configuration of the shared service network will only take effect under the VPC network. The classic network needs to be manually configured by the administrator, which requires a DNS server to be able to resolve the shared service domain name, and the network of the user virtual machine needs to be reachable to the public service area.
6. Shared services only support one-way access. Tenants can access public services, while shared service areas cannot access the tenant's VPC intranet.
7. For versions earlier than SCP 6.7.0, only one shared service gateway is allowed to be planned for each resource pool. For SCP6.7.0 and above, the resource pool supports the planning of multiple shared service gateway.
8. A physical edge can only be associated with one shared service gateway, and multiple public service gateways cannot be associated with one physical gateway.

Prerequisite

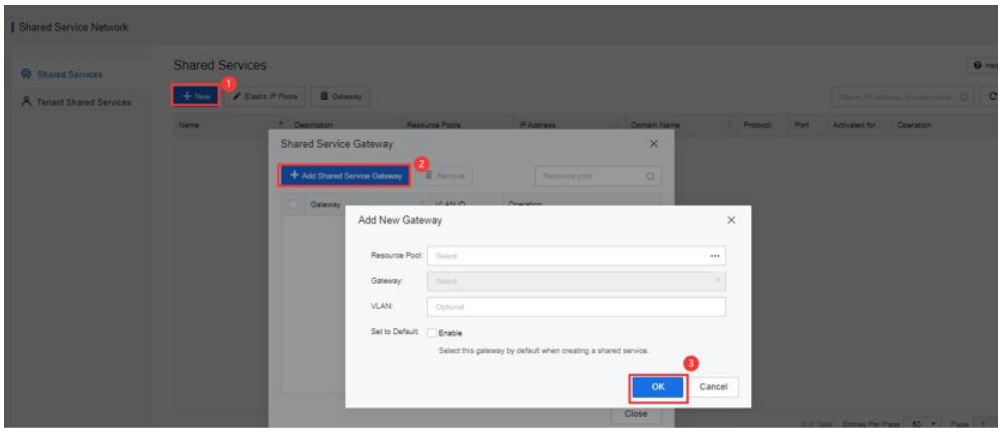
1. The SCP has planned shared service IP and domain name.
2. The SCP has completed the planning of **Chapter 3.7 Configure Shared Services Gateway**.

Steps:

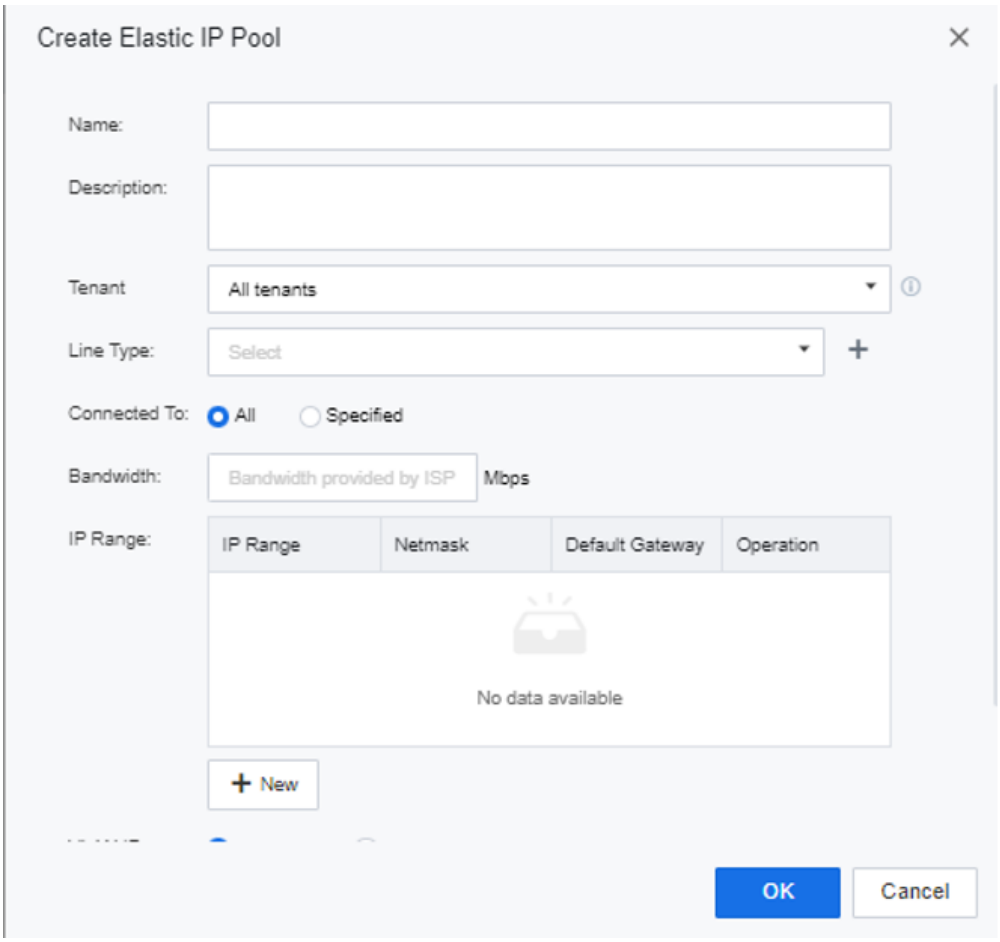
Step 1. Enter the **Networking** > **Shared Service Network** interface and click **Gateway** to plan the shared service network gateway for the resource pool.



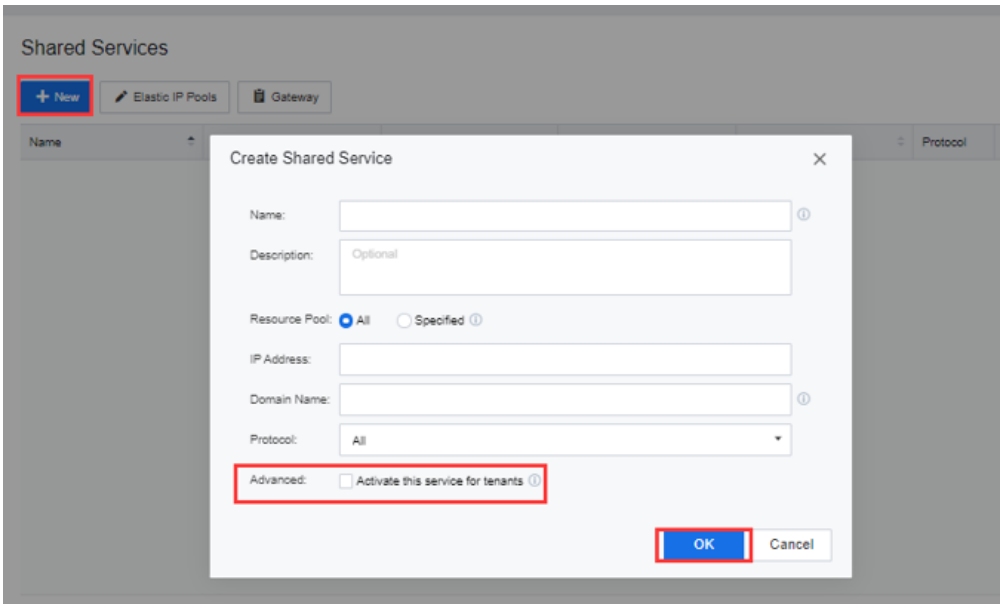
Step 2. Confirm that the shared service gateway planning has been completed, select the resource pool and public service gateway, and check **Enable** to set the default public service gateway.



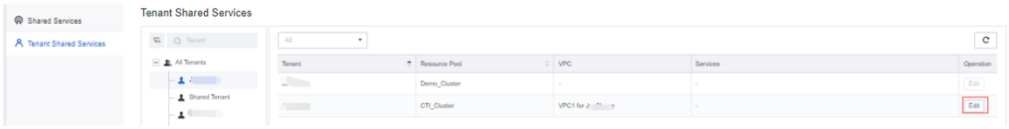
Step 3. Once set up the shared services gateway, enter the elastic IP management interface, and click **Elastic IP Pools** for the shared service network. The public service, security center, and other IPs that need to communicate with the VPC through the public service network are excluded from the elastic IP pool.

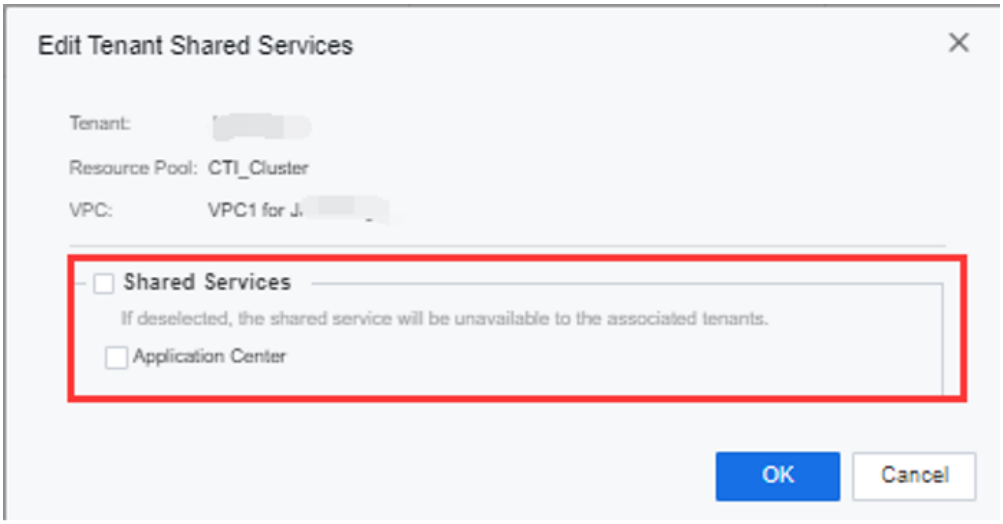


Step 4. Click **New** to add a shared service, which can connect this shared service network to all resource pools or specified resource pools. Shared services rely on IP addresses and domain names to work, and IP and domain names need to be configured for the public service network. The supported protocol can be selected from TCP and UDP ports. After selecting **Activate this service for tenants**, all new tenants can use this shared service by default.



Step 5. If you don't wish to select **Activate this service for tenants**, enter the **Tenant Shared Service** interface to find the target tenant. Click **Edit** to configure the required public services for the target tenant, provided that the tenant has used the VPC.





Step 6. After service is activated for a tenant, you can use the virtual machine in the tenant's VPC to access it through IP or domain name.

4.4.6 IP And Bandwidth

4.4.6.1 Elastic IP Pool

Function Description:

Elastic IPs are independent **public IP** resources bound to devices such as virtual machines, routers, ADC (application delivery controller), and SSL VPNs in the VPC. They can be dynamically unbound to realize the decoupling of public IPs and these devices. Meet the requirements of flexible management and dynamic allocation.

Precautions:

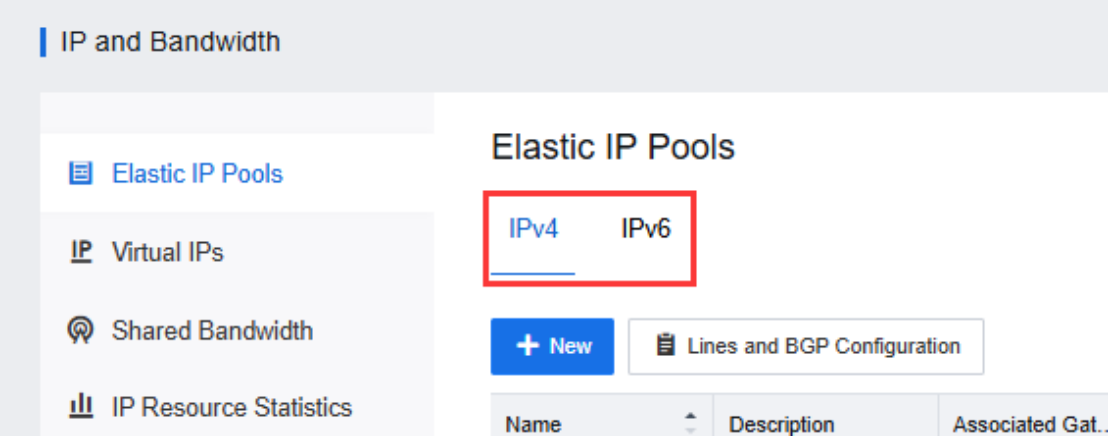
1. An elastic IP pool needs to be created before tenants can use the IP pool.
2. Support binding multiple elastic IP pools for tenants.
3. Supports specifying different exits for elastic IP pools of different lines.
4. The line type can be customized, but the built-in line type of the system does not support editing.
5. The elastic IP quota supports setting quotas for tenants by line type.
6. The elastic IP pool that has allocated quotas does not support modifying the elastic IP line type or deleting the elastic IP.

Prerequisite

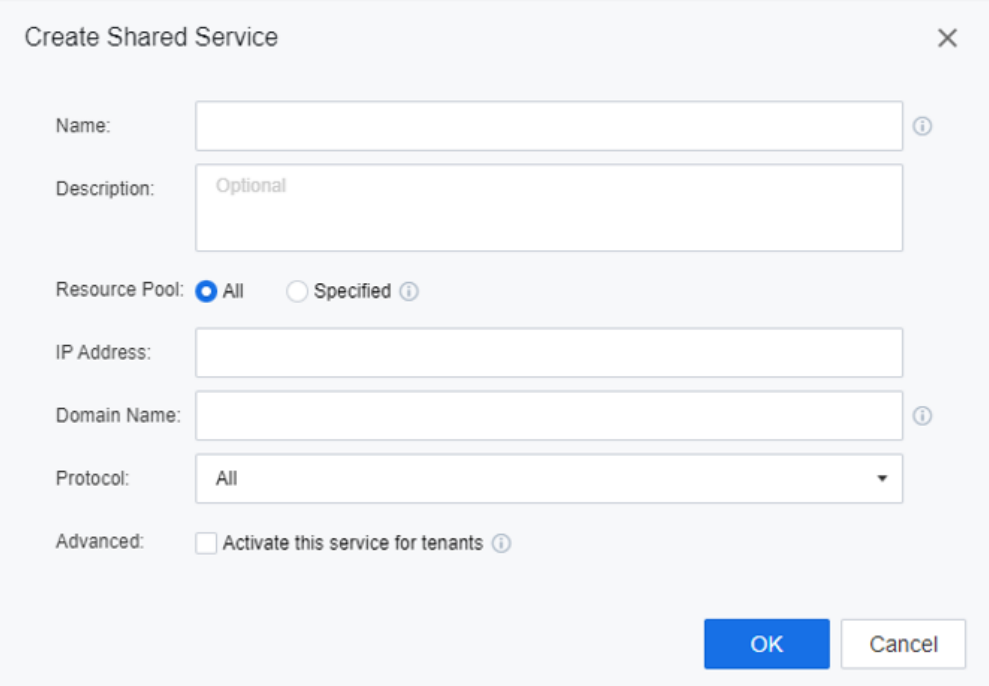
When it comes to operator lines, you need to plan the line type in advance.

Steps:

Step 1. Log in to the SCP platform, select **Resources** > **Networking** > **Shared Service Network** > **Shared Services**, and click **New.** Note: SCP 6.10.0 supports IPv6 elastic IP pools.



Step 2. Fill in the name and description of the elastic IP pool, select the tenant to be associated, line type, network egress, set the total bandwidth, add the elastic IP, and click **OK** to complete the creation.



NOTE

1. For versions earlier than SCP6.7.0, the elastic IP pool needs to be associated with a resource pool (one elastic IP pool can be bound to multiple resource pools, one resource pool can also be bound to multiple elastic IP pools, and the elastic IP bound to the resource pool, all VPCs under it are visible.)
2. In SCP6.7.0 and later versions, the elastic IP pool needs to be associated with the egress (the line type is an ordinary line, the VPC egress is associated, and the line type is public service network, the public service outlet is associated).

Step 3. After the elastic IP pool is created, the platform administrator can edit and delete it.

4.4.6.2 Virtual IP

Function Description:

SCP supports associating a unified virtual IP (VIP) to multiple virtual machines and then performs elastic IP association.

Precautions:

1. The virtual IP uses the tenant's subnet IP. If no IP is available on the network segment under the tenant's subnet, the creation of the virtual IP will fail.
4. The virtual IP associated with a virtual machine cannot be deleted.
5. It is not supported to set the virtual machine binding/unbinding relationship for application-type virtual IPs in the virtual IP list. However, if necessary, you can go to the application center.

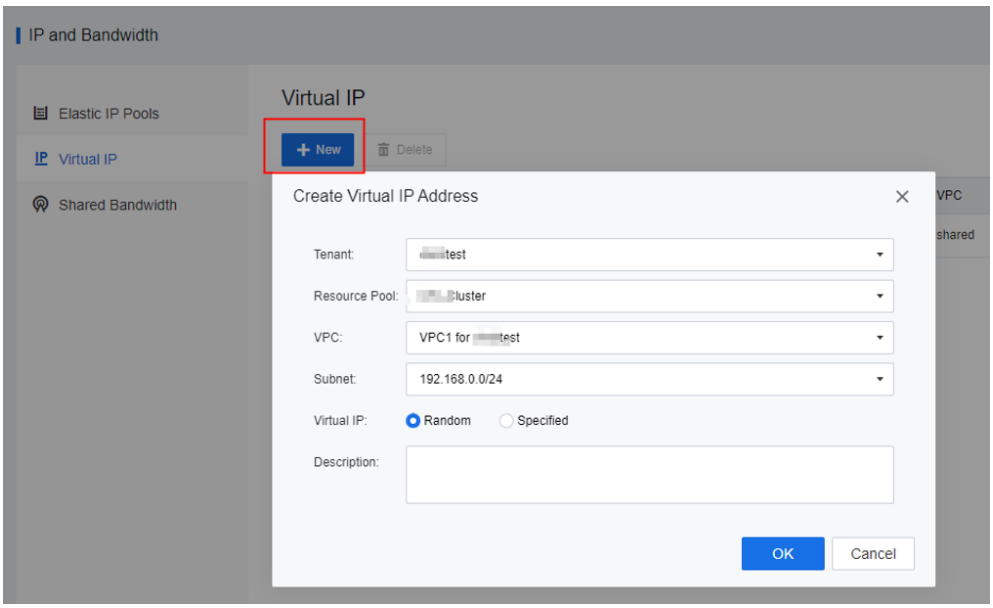
Prerequisite

None.

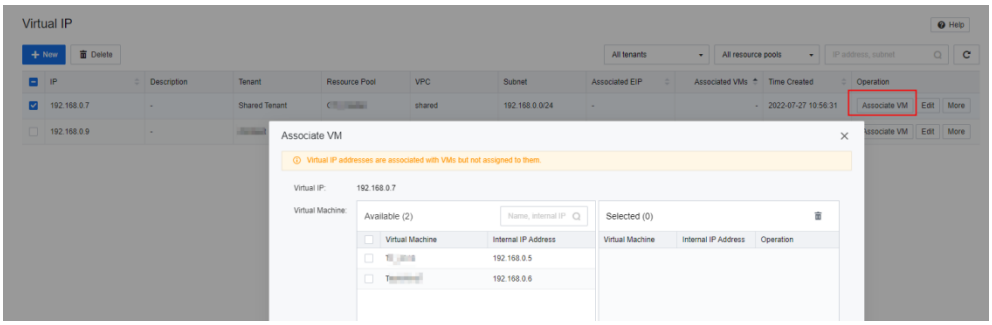
Steps:

Step 4. Navigate to **Resources** > **Networking** > **IP and Bandwidth,** then select **Virtual IP**.

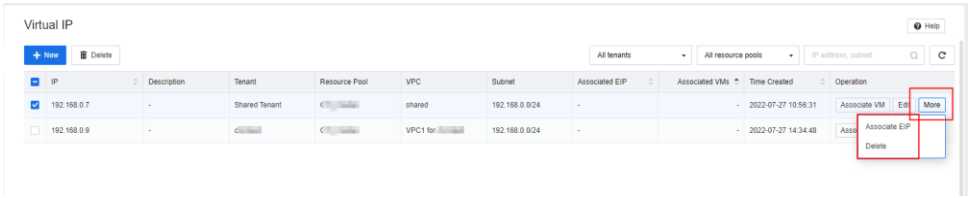
Step 5. Click **New** to create a new virtual IP, select the **Tenant**, **Resource Pool**, **VPC**, **Subnet**, **Virtual IP** support both **Random** and **Specified** and click **OK** to create the virtual IP.



Step 6. Click **Associate VM** to associate or disassociate the virtual IP.



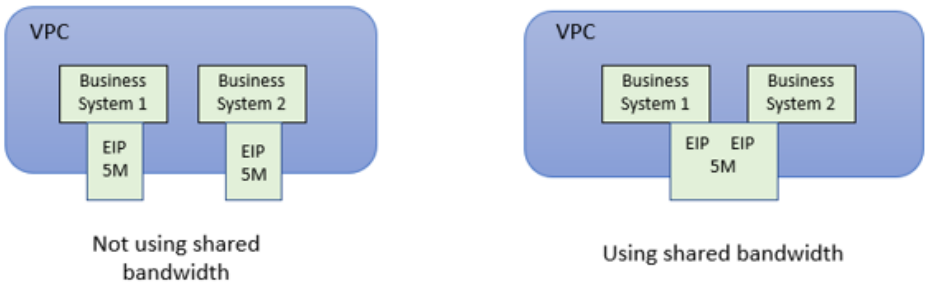
Step 7. Click **More** to associate EIP or delete the virtual IP.



4.4.6.3 Shared Bandwidth

Function Description:

Shared bandwidth enables multiple elastic IPs to share the same bandwidth: virtual machines, routers, and NFV instances bound to elastic IPs under the same tenant share the same bandwidth resources. It can improve the bandwidth utilization rate and facilitate administrators' management.



Precautions:

1. The administrator cannot add shared bandwidth but can only set and delete bandwidth. However, tenants can create shared bandwidth at the Tenant portal and bind it to an elastic IP.
2. If the elastic IP associated with the shared bandwidth is bound to a virtual machine or NFV device, the shared bandwidth cannot be deleted directly at this time. You need to unbind the elastic IP from the device to delete it.

Prerequisite

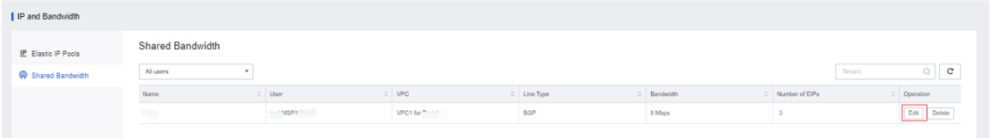
None.

Steps:

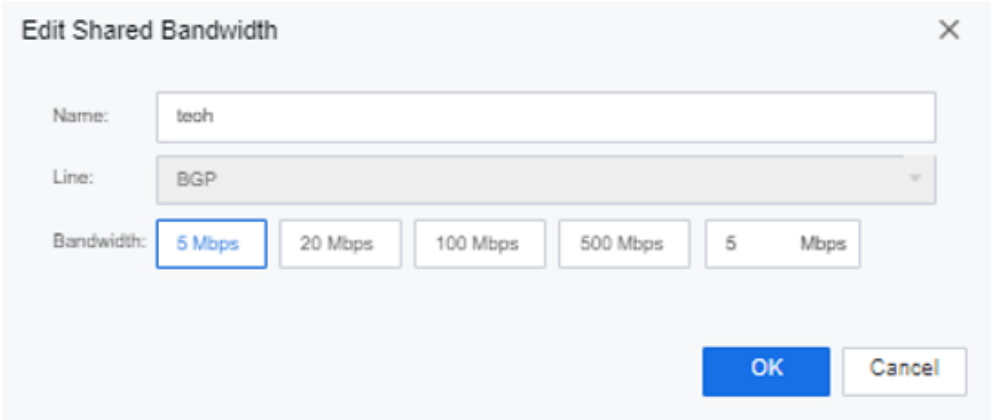
Step 1. Log in to the SCP platform, select **Network** > **IP and Bandwidth** > **Shared Bandwidth** to enter the shared bandwidth list. Note: SCP 6.10.0 supports IPv6 shared bandwidth.



Step 2. Select a shared bandwidth and click **Edit** to set the name and bandwidth of the shared bandwidth.



Step 3. Click **Delete** to delete the shared bandwidth.



4.4.6.4 IP Resource Statistics

Function Description

You can make statistics on IP resources, including physical machines, VMs, NFVs, routers, and IP conflicts.

Prerequisites

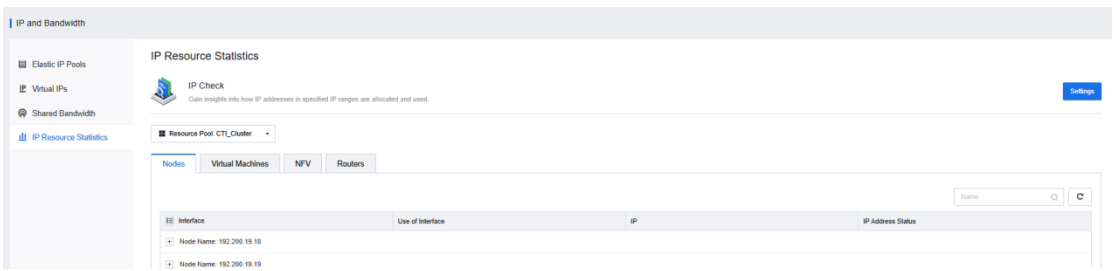
N/A

Precautions

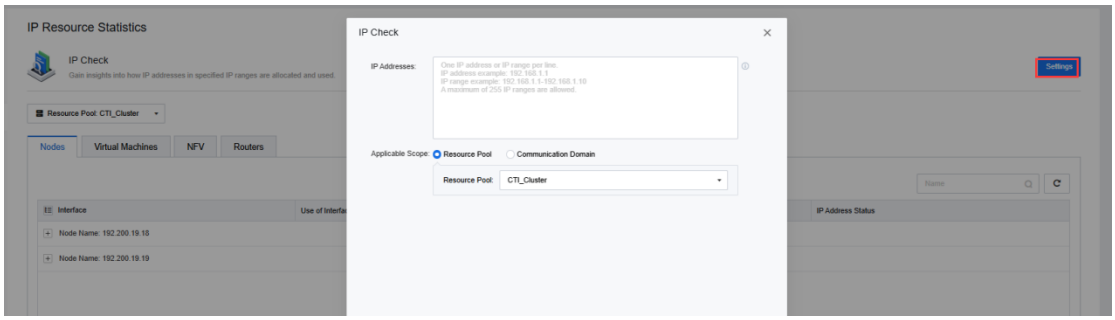
You can detect up to 255 IP addresses at a time.

Steps

1. Log in to the SCP console and go to **Networking** > **IP and Bandwidth** > I**P Resource Statistics**.
2. Select a resource pool to view the information about physical machines, VMs, NFVs, router IP addresses, and IP address statuses.



3. Click **Settings** and then click **Check Now** to view the allocation and usage of an IP address or each IP address in a range.



4.4.7 Enterprise Dedicated Line

Function Description:

The VPC of the SCP tenant can configure the enterprise private line on the operation page to communicate with the environment outside the VPC at Layer 2 and Layer 3. To use the enterprise private line function, you need to specify a fixed private line gateway for each resource pool.

Precautions:

1. The SCP cloud computing platform has planned a dedicated line export.
2. The SCP cloud computing platform has created a tenant and created a VPC.

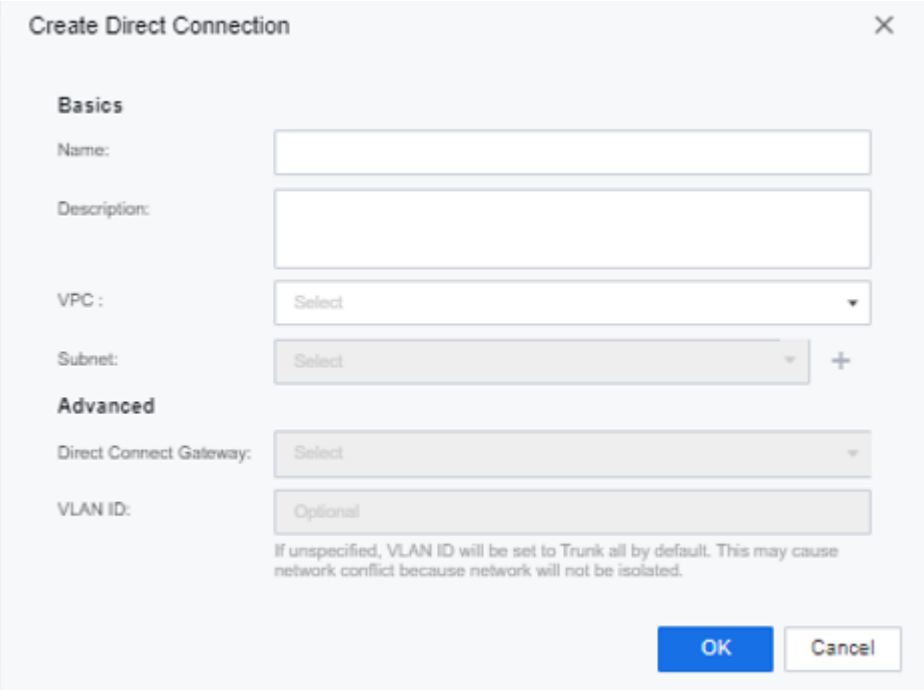
Prerequisite

To avoid IP address conflicts, it is recommended to configure different VLAN IDs for the enterprise private line of each subnet.

Steps:

Step 1. Select **Networking** > **Direct Connect** and click **New**.

Step 2. Configure the name and description, select the VPC, subnet, and Direct Connect Gateway, and configure the VLAN ID.



4.5 Security Services

4.5.1 Distributed Firewall

Function Description:

1. The distributed firewall protects all virtual machines in the data center.\ By creating and configuring distributed firewall policies, network isolation between virtual machines can be achieved, the internal traffic of the data center can be protected, and the impact of malicious attacks on the internal data center can be reduced.
2. If both VDI and HCI VMs exist on a tenant VPC network, an applicable scope can be configured to make the policy applicable to specified VMs only.

Precautions:

1. It is forbidden to bypass the SCP to directly execute the distributed firewall operation on the HCI, which may cause the firewall rules to take effect in the wrong scope, resulting in policy rule conflicts.
2. The distributed firewall supports creating up to 100 policies in the same effective scope.
3. The distributed firewall supports creating up to 1000 rules in the same policy.

4. The distributed firewall supports creating up to 50 IP groups in the same effective scope.
5. The distributed firewall supports creating up to 50 custom services in the same effective scope.

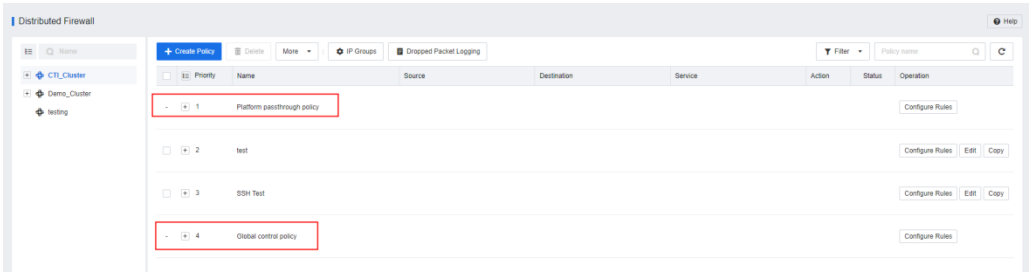
Prerequisite:

None.

Steps:

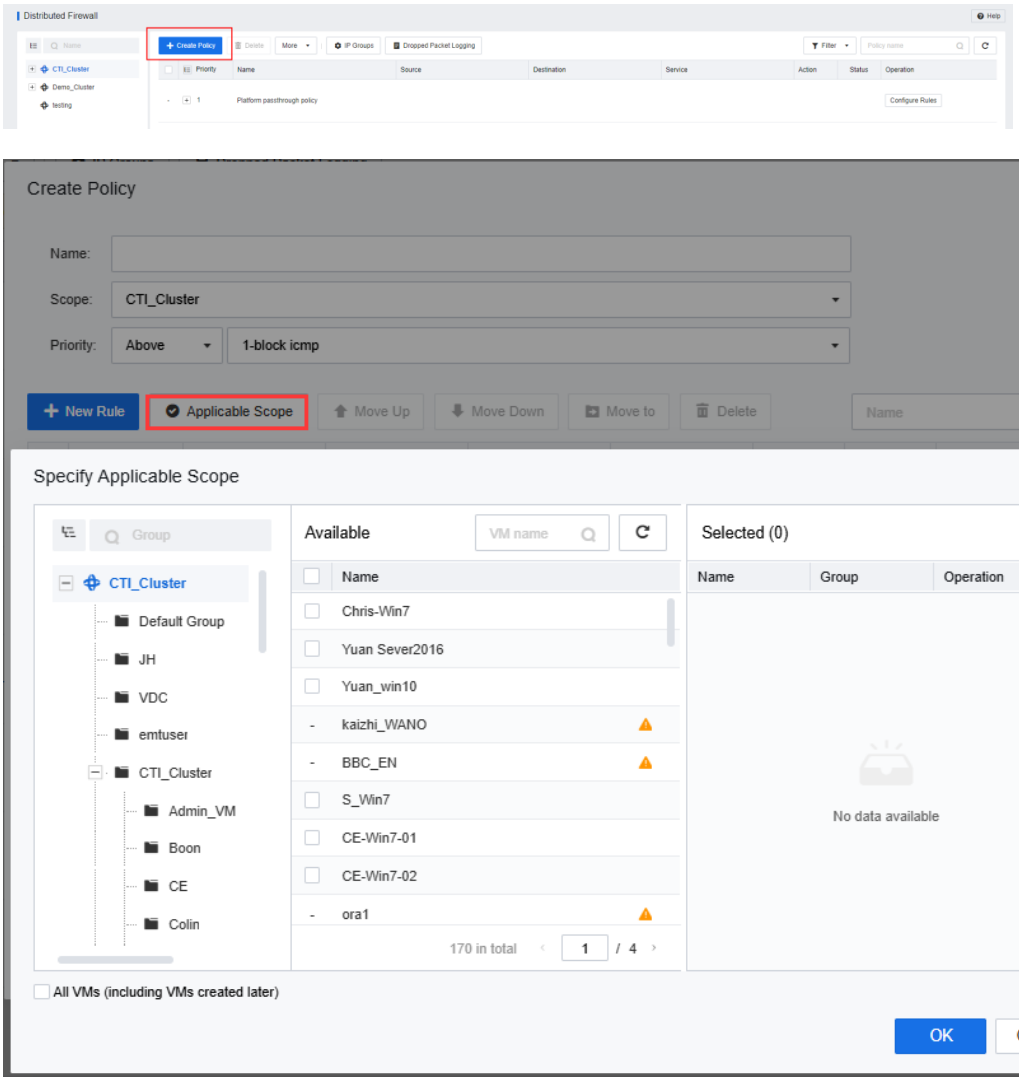
Step 1. Log in to the SCP admin platform and navigate **Resources** > **Security Services** > **Distributed Firewall** to enter the distributed firewall configuration page. The **Platform passthrough policy** and **Global control policy** are the default policies and cannot be edited.

- **Platform passthrough policy**: Contains the platform passthrough rule, which ensures the connectivity between the SCP and the resource pool.
- **Global control policy**: Contains global control rules, which ensure overall traffic is released.



Step 2. Select the resource pool name or tenant name on the left list to enter the corresponding page, and click the **Create Policy** button to create a firewall policy for the resource pool or tenant network.

- **Name:** The firewall policy name.
- **Scope**: The effective domain of the firewall policy. It can be the entire resource pool, the tenant's classic, or the VPC.
- **Priority**: The policy created by the administrator is between the platform default policies, and other policy priorities can be adjusted manually.
- Click **Applicable Scope** to set the applicable scope of the policy, which can be a custom group of VMs.



Step 3. You can manage firewall rules in groups after adding them to a created distributed firewall policy. Select a policy and click Edit. Then click New Rule. Note that all the rule configurations are within the applicable scope of the policy.

NOTE

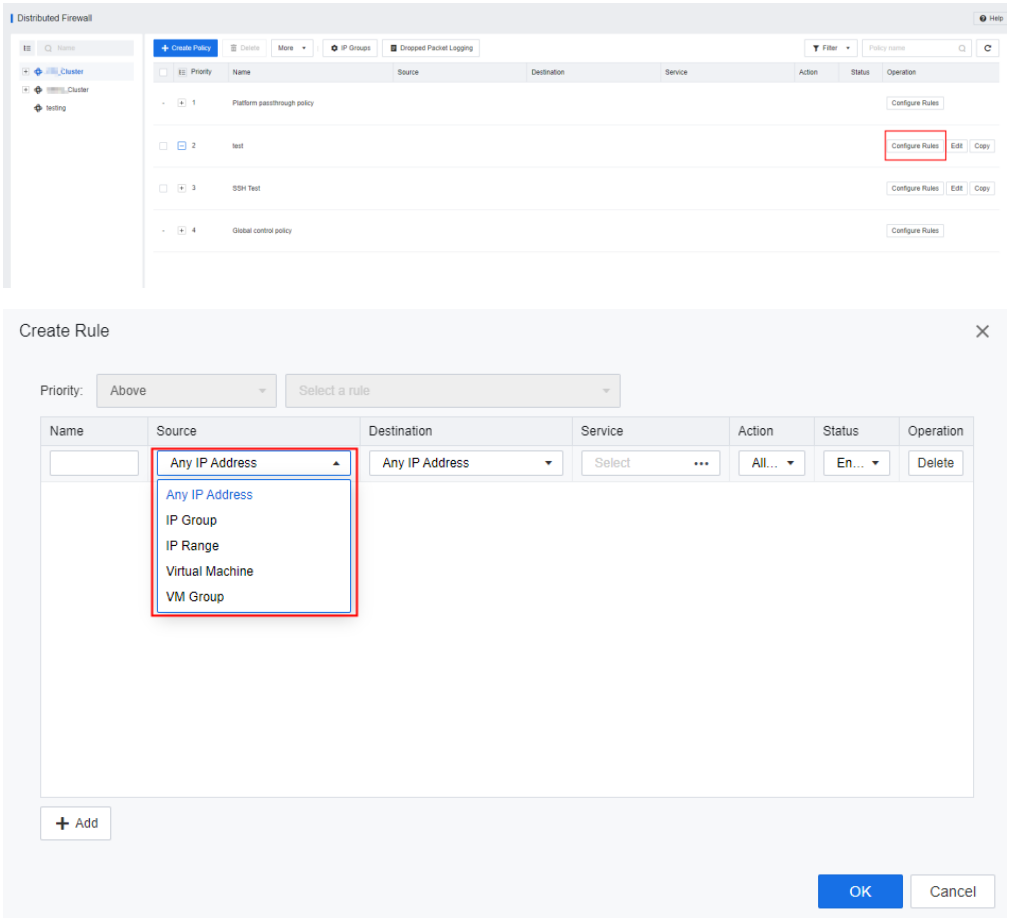
This applies to the effective scope where the policy is located.

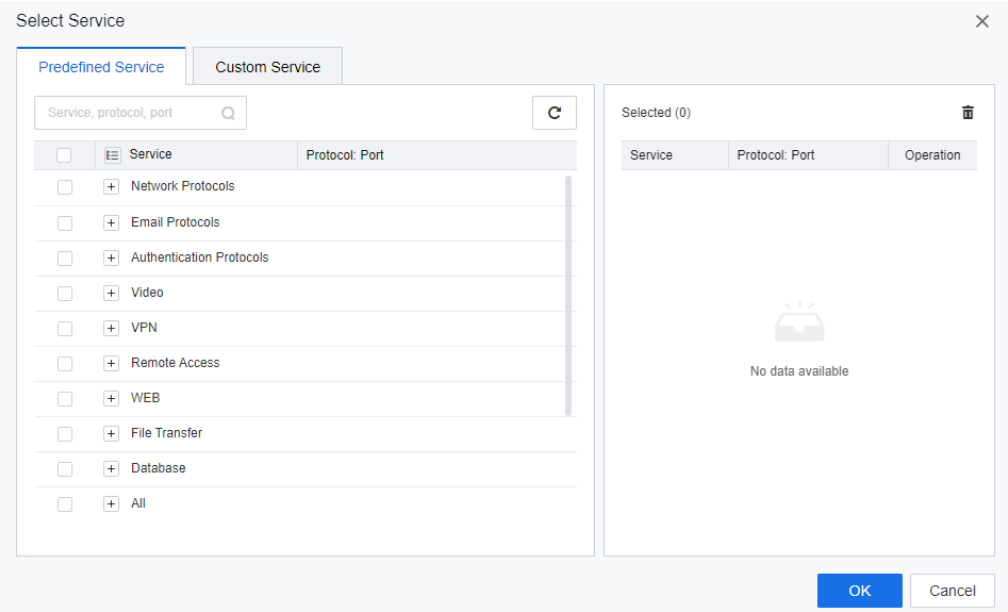
- **Source/Destination** condition: Support configuring **Any IP Address, IP Group and Range, Virtual Machine**, and **VM Group**.

NOTE

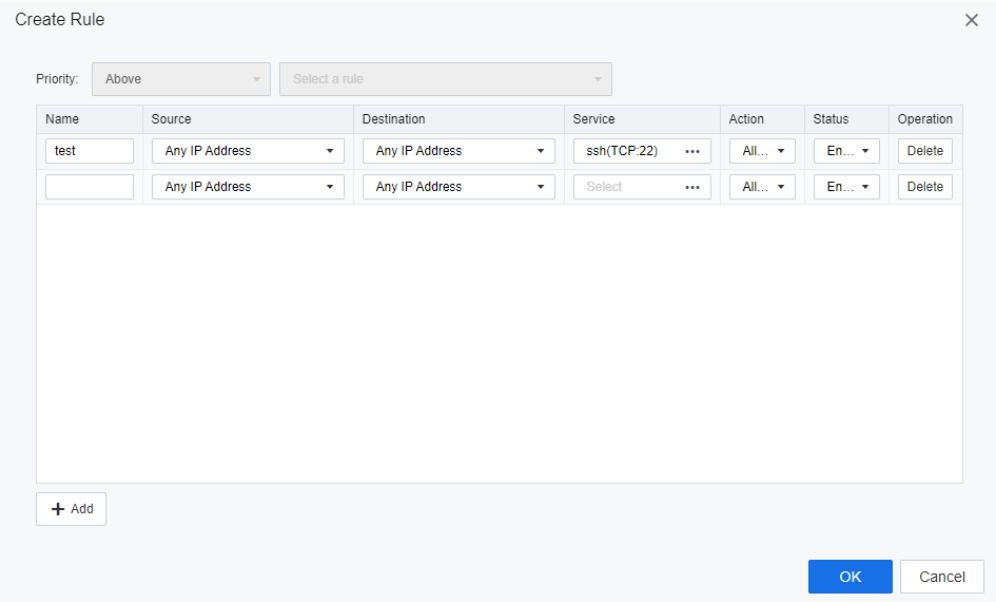
When the source/destination selects a virtual machine, if the virtual machine does not have vmTools installed, the system cannot automatically obtain the virtual machine's IP, and the underlying firewall rules cannot perform effective IP conversion. As a result, the rules are ineffective for the virtual machine. Therefore, in this case, you need to configure an IP for the virtual machine before using it as the source/destination of firewall rules.

- **Service**: It supports the selection of **Predefined Service** on the platform and **Custom Service** based on protocols and port numbers. Multiple rules can share custom services in the same effective scope.

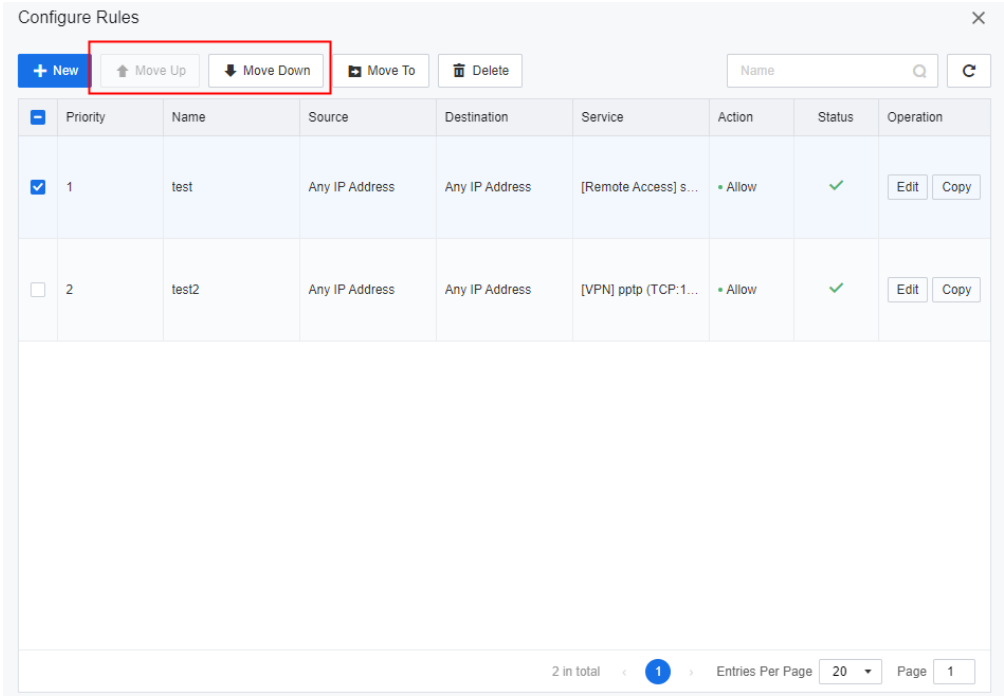


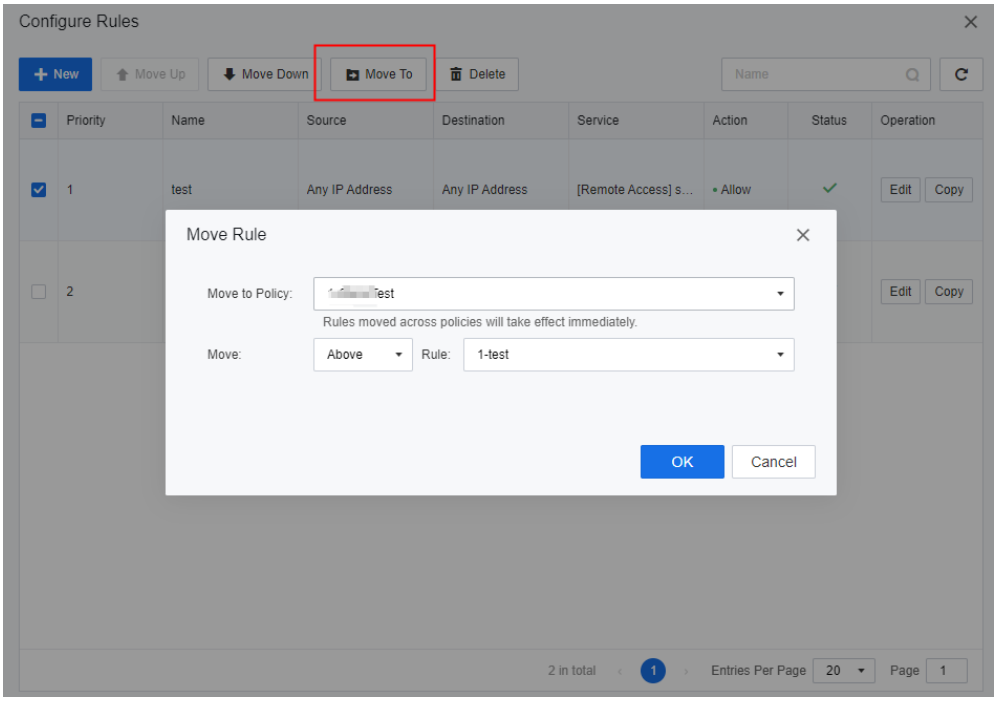


Step 4. Return to the **Create Rule** page, and click the **Add** button to continue adding other rules.

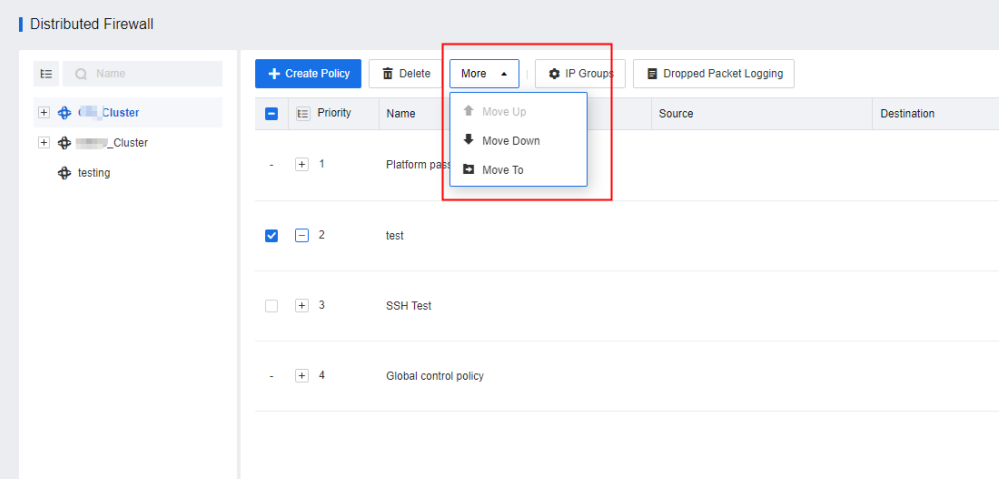


Step 5. After confirming that all rules are added correctly, click **OK** to create. On the **Configure Rules** page, select a rule record and click the **Move Up** or **Move Down** button to adjust the priority of the created rule. Click **Move To** to move the rule to another policy group.





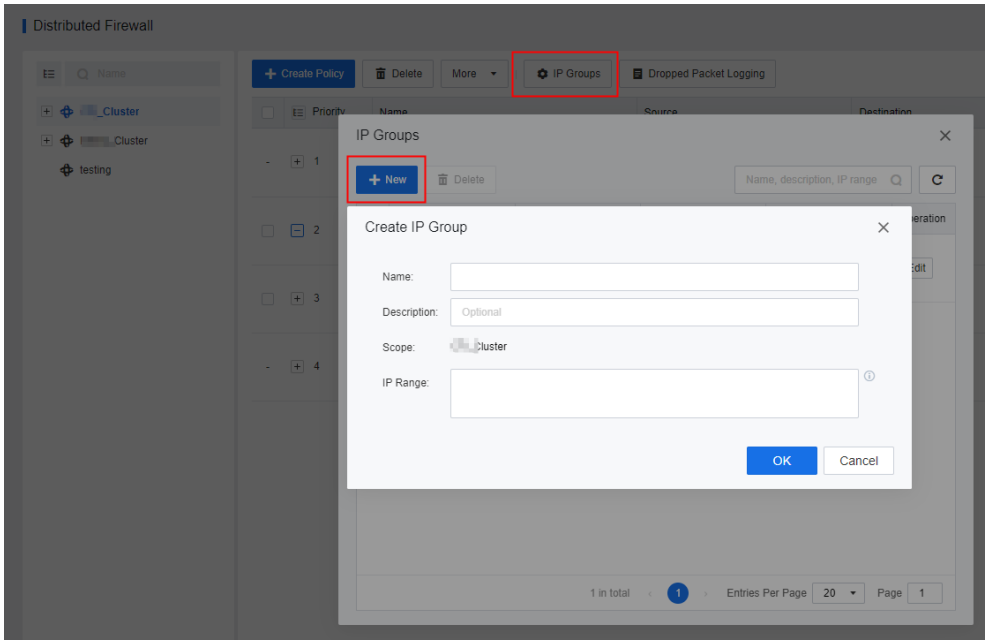
Step 6. It also supports the priority adjustment of distributed firewall policies. Select the policy's priority that needs to be adjusted in the list, and click **More** to adjust.



Step 7. **IP Groups:** The platform administrator can manage the IP groups in the distributed firewall policy. Click the **IP Groups** button, click the **New** button, and enter the **Name**, **Description,** and the **IP Range** to complete the IP groups creation.

NOTE

Multiple rules can share a custom IP group in the same effective domain.

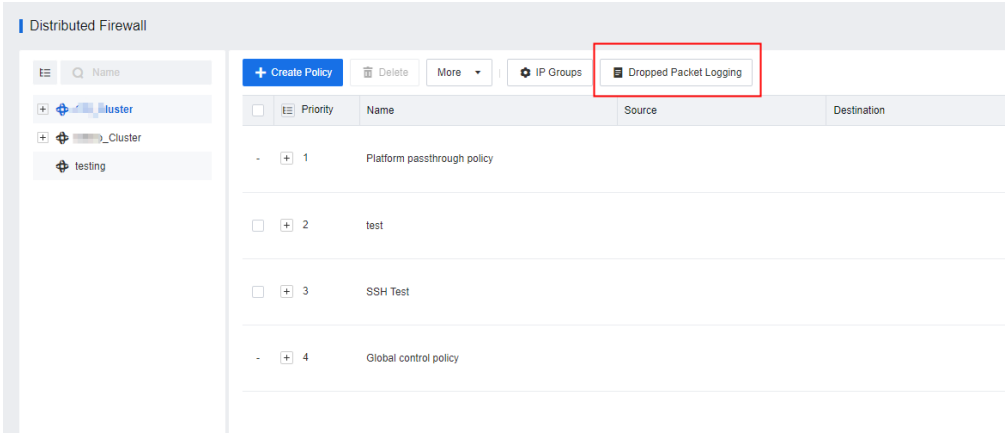


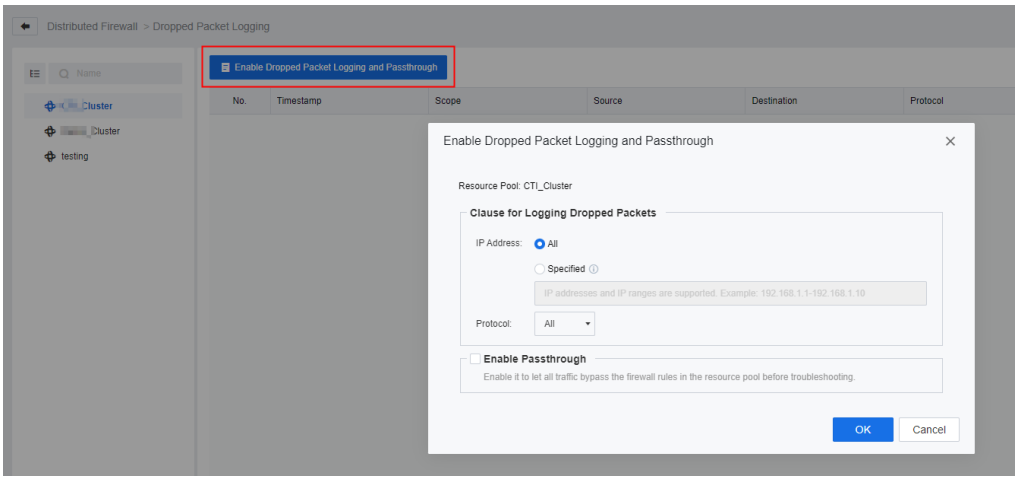
Step 8. After configuring the firewall policy, you can configure the **Dropped Packet Logging**.

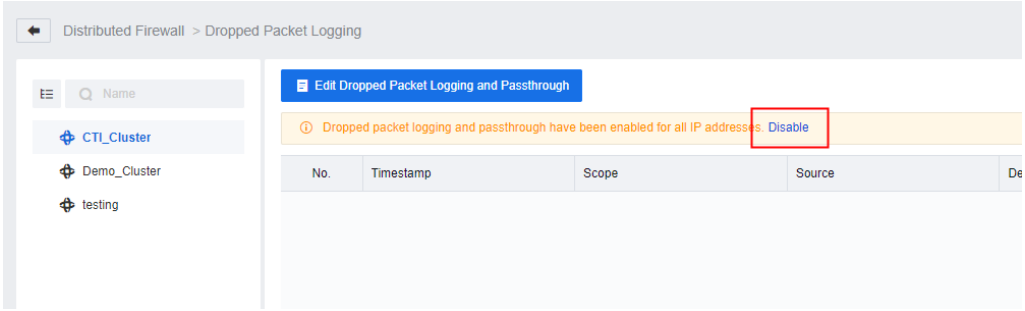
- Click the **Dropped Packet Logging** button to enter the dropped packet logging page. Then, click **Enable Dropped Packet Logging and**

Passthrough to configure the clause for logging dropped packets, only the logs that meet the clause will be recorded.

- Check the **Enable Passthrough** checkbox to enable dropped packet logging and passthrough at the same time. After enabling, all firewall policies in the resource pool will not take effect, which can be used for temporary troubleshooting.
- Click the **Disable** button on the interface to disable the dropped packet logging and passthrough feature.







4.5.2 VPC Boundary Firewall

Function Description

You can configure access control policies for routers at the tenant VPC boundary to establish a secure network boundary between the inside and outside of the VPC.

Precautions

1. One VPC tenant can create up to 1,000 access control policies.
2. A resource pool can have up to 20,000 dropped packet logs.

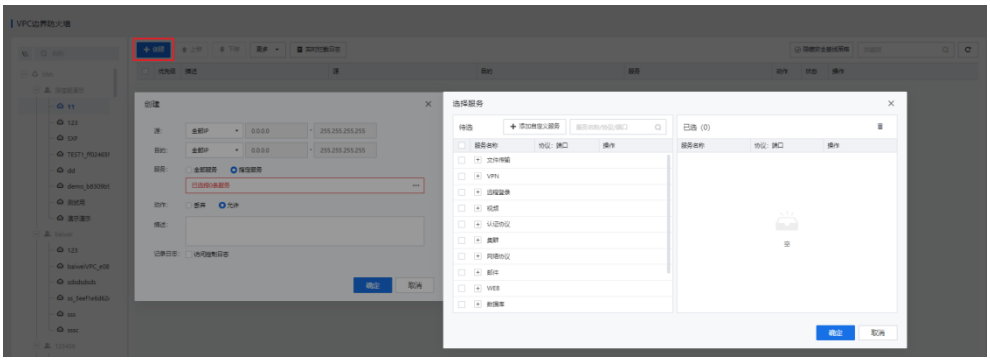
Prerequisites

N/A

Steps

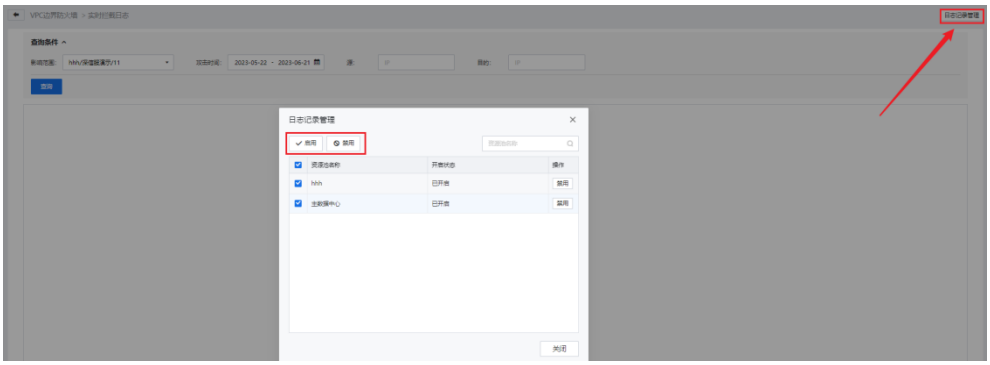
1. Go to **Security Services** > **VPC Firewall**, select a VPC from the tree menu on the left, and click **New**.

- Source/Destination: It can be set to **Any IP**, **Specified IP**, **Specified subnet**, or **Specified IP range**.
- Service: It can be set to **All**, **Specified**, or **Custom**.
- Action: It can be set to **Drop** or **Allow**.
- Log: Select **Access Control Log** as needed.



2. Click **Dropped Packet Logging** at the top of the page. On the page that appears, select the target VPC network and attack time and enter the source and destination IP addresses to query logs. Click **Log Management** in the upper-right corner of the page to enable or disable dropped packet logging

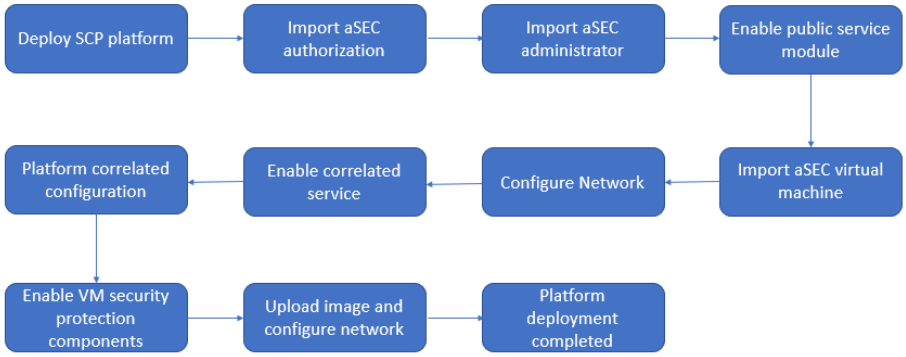
for a resource pool.



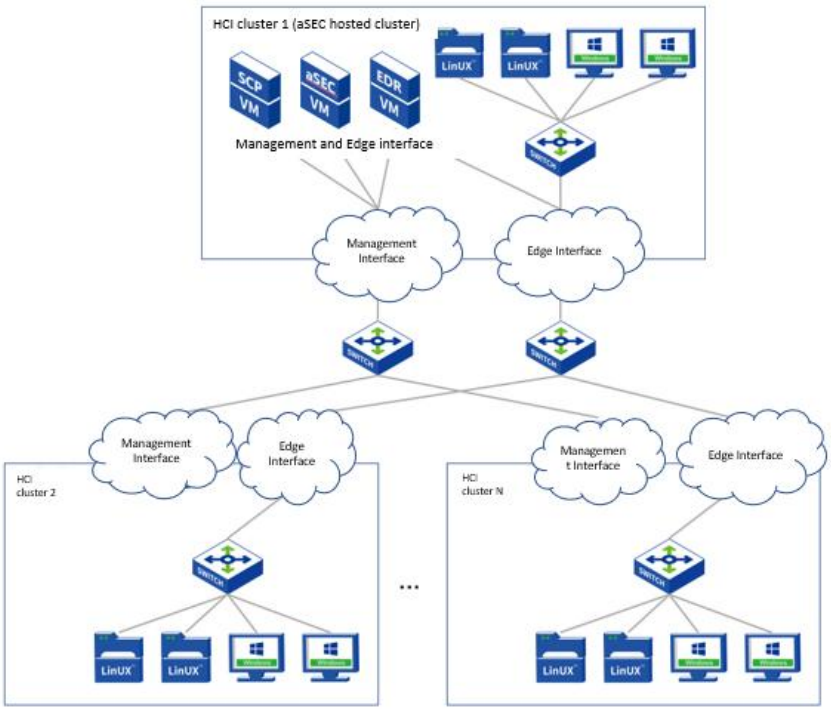
4.6 aSEC Installation and Deployment

Sangfor cloud computing platform SCP supports the deployment of the Cloud Security Center(aSEC) by importing virtual machines. This chapter mainly introduces the installation and deployment of the Cloud Security Center, including the installation of the virtual machine aSEC of the Cloud Security Center and the deployment of the security protection management platform.

- The installation and deployment process of aSEC Cloud Security Center is shown in the following figure.



- The deployment network topology plan of the aSEC cloud security center is shown in the following figure. The cloud security center platform needs to communicate with the management network of HCI and SCP (recommended to be on the same network segment as the HCI and SCP management network). It is mainly used for the cloud security center platform to call HCI and SCP. The API interface of SCP implements policies such as taking snapshots or creating distributed firewalls, the management port of the virtual machine security protection platform is configured to connect to the physical outlet of the management port (it is recommended to plan the same network segment as the HCI and SCP management network). The virtual machine security protection platform service communication port configuration (optional) is connected to the physical edge of the service network, which is used to connect security servers such as the virus database and cloud search service to realize automatic virus database updates.



- Refer to the following table for the recommended configuration instructions for aSEC Cloud Security Center.

aSEC virtual machine server recommended configuration			
Number of access terminals	**CPU**	**Memory**	**Disk**
1 – 300 (Default Specifications)	4 Cores	8 GB	300GB
300-1000	4 Cores	16 GB	300 GB
1000 – 2000	8 Cores	32 GB	300 GB
Recommended configuration of the virtual machine of the security protection management platform			
Number of access terminals	**CPU**	**Memory**	**Disk**
1 – 300 (Default Specifications)	2 Cores	2 GB	300GB
300-1000	2 Cores	4 GB	300 GB
1000 – 2000	4 Cores	8 GB	300 GB

Precautions

1. Tenants with no aSecurity quota in any resource pool cannot access aSecurity.
2. To ensure automatic defense against cyber attacks on the tenant VPC network, you need to ensure that cyber attack protection is enabled in the resource pool of the VPC.

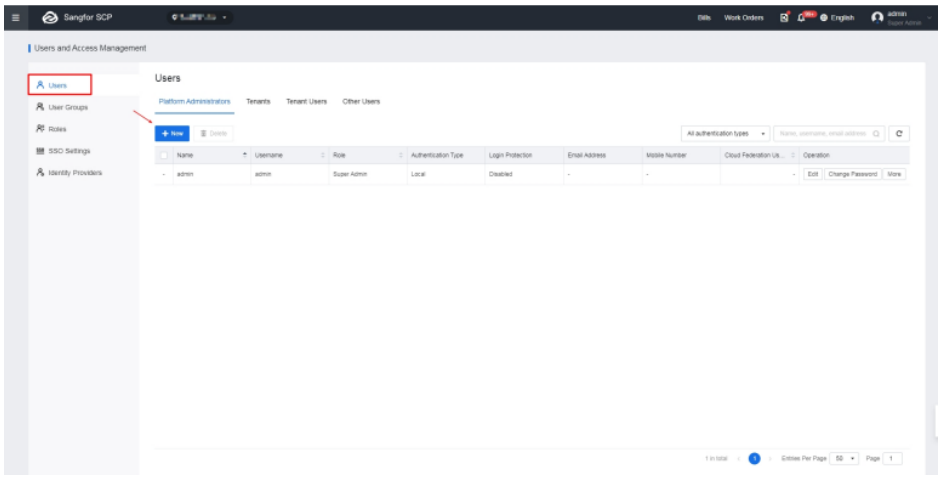
4.6.1 aSEC Cloud Security Center Platform Installation

Precautions:

1. aSEC Cloud Security Center can deploy on SCP6.8.0, and the HCI version must be 6.8.0 and above.
2. The licensing import of the aSEC Cloud Security Center has been completed.
3. You must change the aSEC password once every three months.

Steps

Step 1. Log in to the SCP platform as admin, select **User and Access Management > Users > Platform Administrators**, and click the **Create** button to create a platform administrator.



Step 2. Configure the following information to complete the creation of the platform administrator.

Name: asec_admin

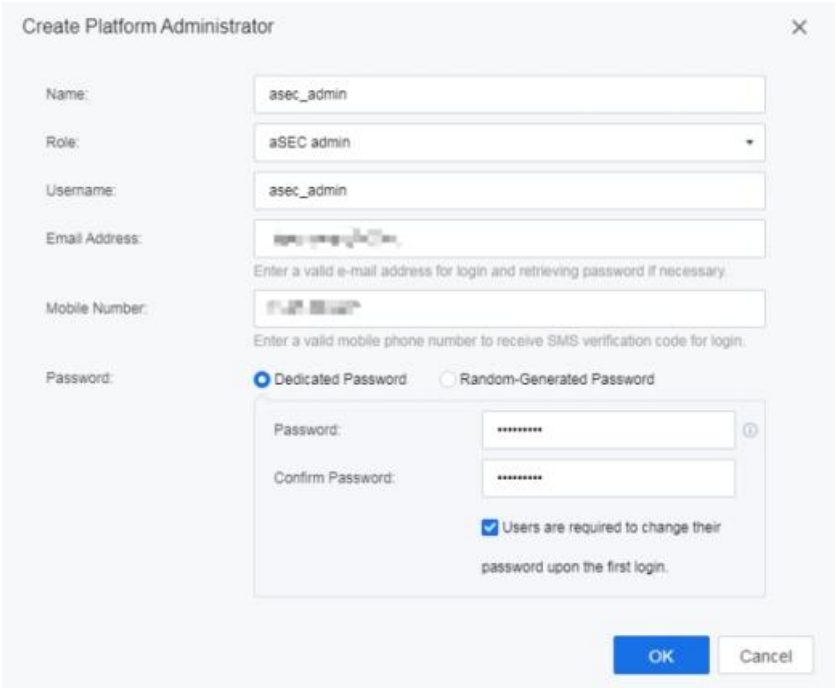
Role: aSEC Administrator

Login username: asec_admin

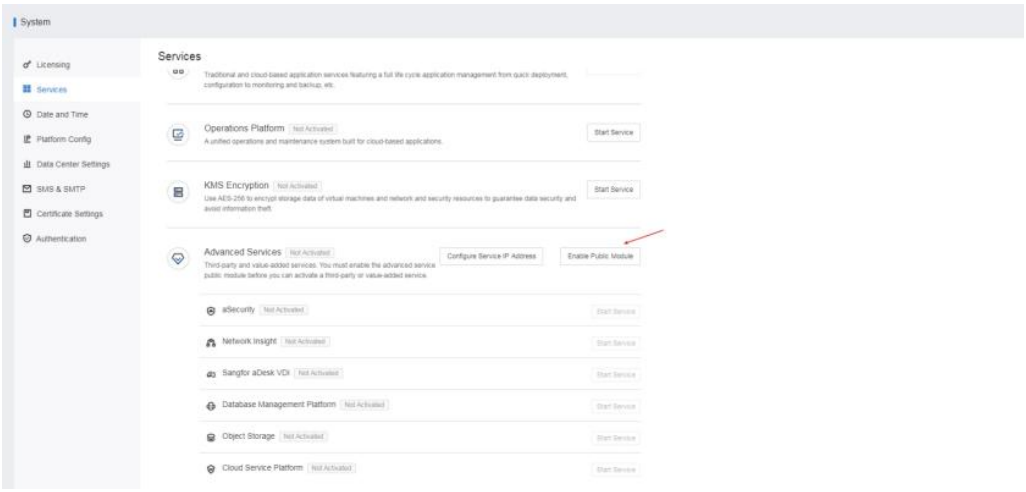
Email: Custom

Mobile: Custom

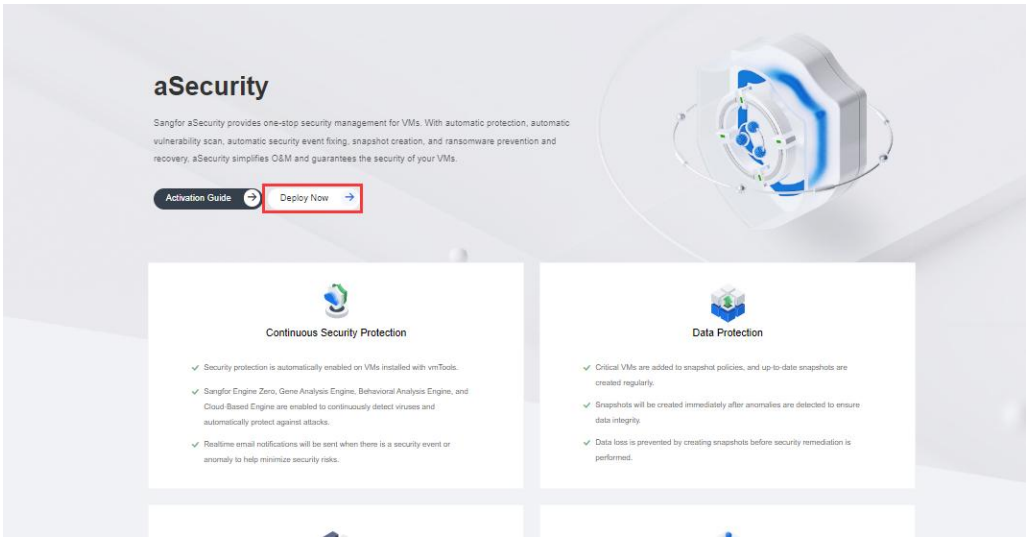
Password: custom



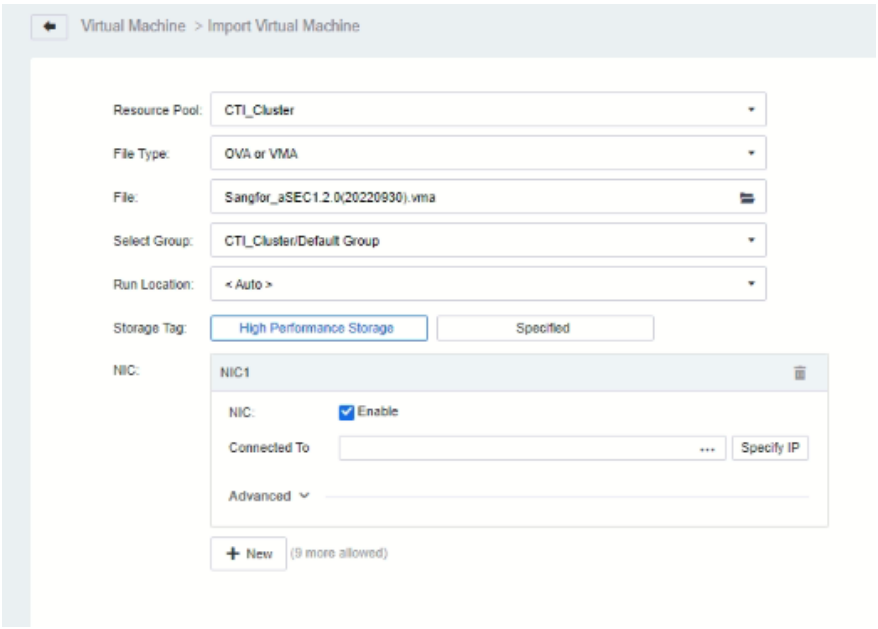
Step 3. Go to **System > Services**, and click **Enable Public Module of Advanced Services.**



Step 4. Go to the **Compute > Virtual machine**s page, click **Deploy Now**, and select **Import Virtual Machine**.

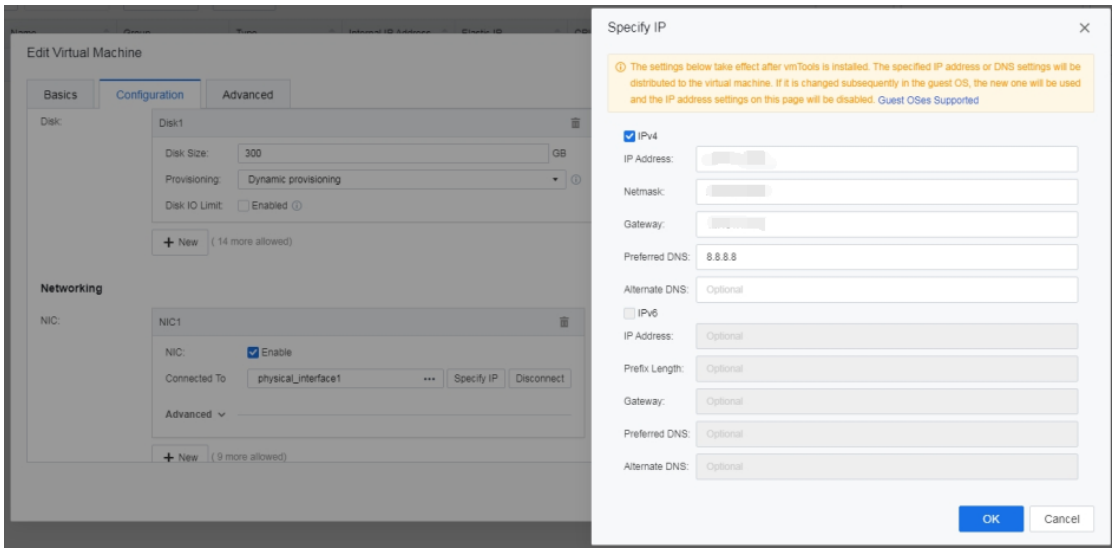


Step 5. Import the vma file, and select the resource pool, virtual machine group, running location, storage performance, and network card.

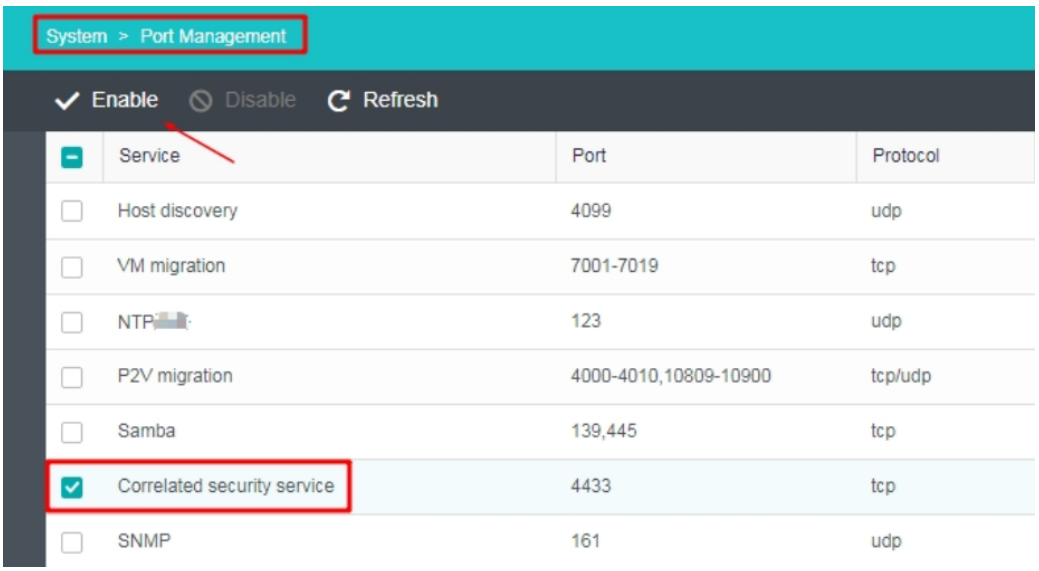




Step 6. After the import is successful, enter the **Edit virtual machine** interface to configure the network card. Check **Enable**, connect to the physical edge, click the **Specify IP** button, select **Use IPv4 Address**, configure the IP address of the aSEC virtual machine, and use it as the management network of the Cloud Security Center (it must be able to communicate with the SCP management network segment). It is recommended to be on the same network segment as the SCP management network.



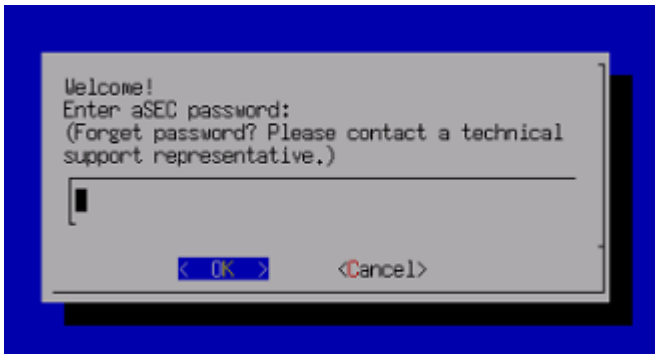
Step 7. Log in to the HCI cluster where the Cloud Security Center is located, enable the **Correlated Security Service** port, and enable the partner service. Otherwise, you will not be able to access the aSEC Cloud Security Center service.

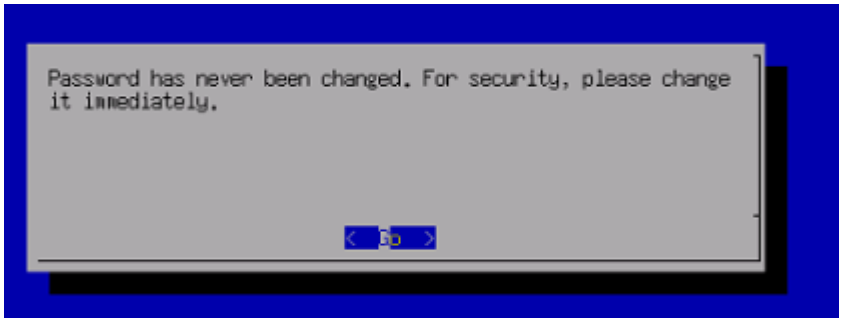


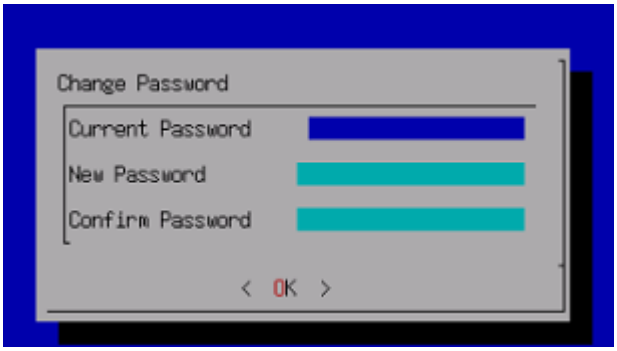
Step 8. Power on the virtual machine, enter the VM console and configure the platform security correlation.

Enter the password of the cloud security center to log in. You need to change the password for the first login. The default password is **Sfcsec@123**. The password change policy is as follows:

- The length is 8~64 characters.
- Must contain 4 items of uppercase letters, lowercase letters, numbers, and special characters, special characters support ~`@#%&<>"',;_-^$.*+?=!:|{}()[]/.
- It cannot be the same as or contain the username.
- The same character cannot appear consecutively, such as aaa, 11, etc.
- Common characters (including upper and lower case) of sangfor/sinfor/dlanrecover cannot be used.



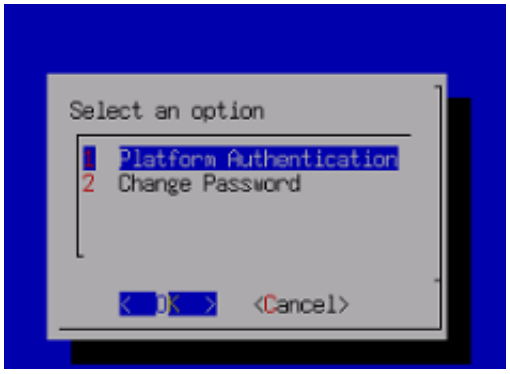


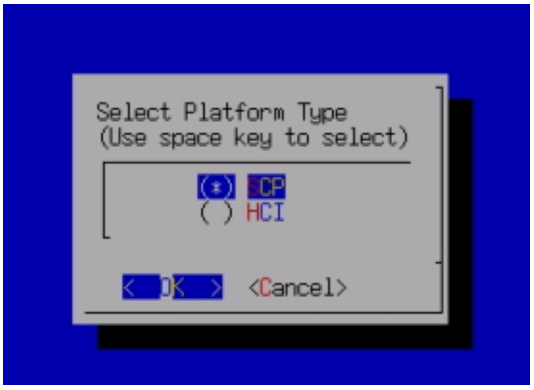


NOTE

If there is no modification within 10 minutes or the modification fails, an **"Internal Error"** will be displayed. In this case, the session has timed out, and you need to log in again before modifying it.

After successful login, click **Platform Authentication** and select the SCP platform.

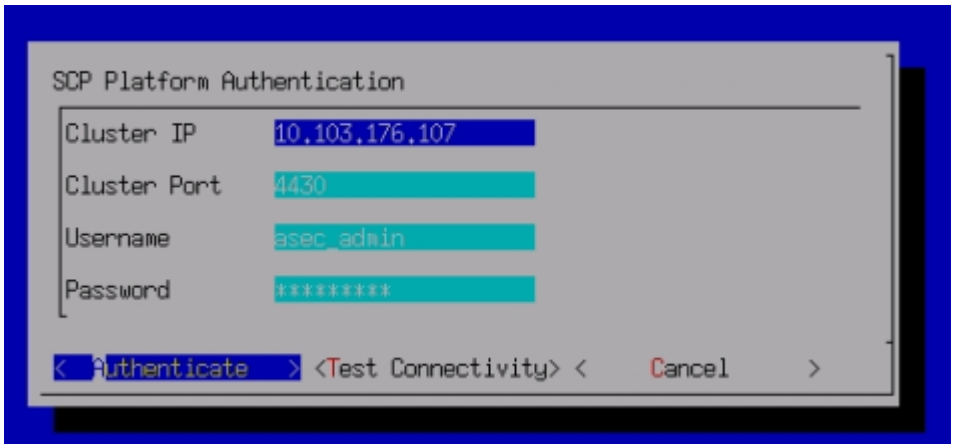




Enter the platform authentication page:

- Cluster IP: IP of the SCP management network.
- Username/Password: asec_admin/password.

Click **Authenticate** to complete the aSEC deployment.





4.6.2 VM security protection management platform installation

Prerequisite

Complete the deployment of aSEC platform.

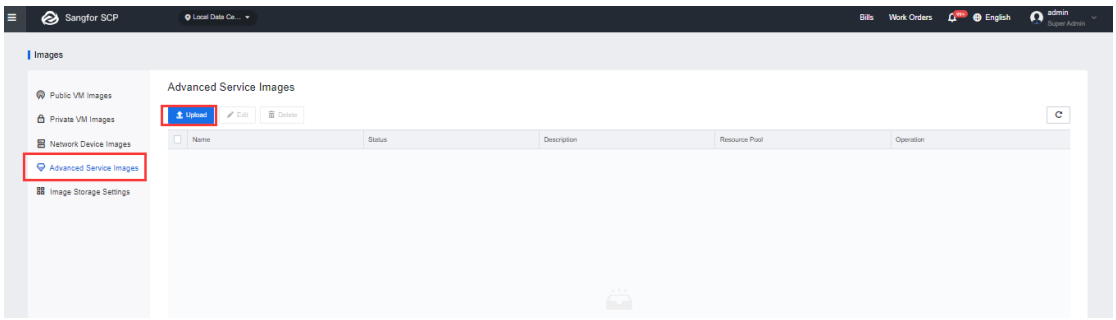
Precautions

1. Specification adjustment may generate the following impacts on your business: For access to services with cyber attack protection enabled, a small number of packets (one or two) may be lost, and a network jitter of no more than 10 seconds may occur. We recommend that you perform the operation during off-peak hours.
2. After modifying the cyber attack protection configurations, the cyber attack protection module will take effect after the restart, and the communication will become disconnected for a short time period. The restart can be completed within 1 minute. If any troubleshooting task exists, it will also be automatically closed.

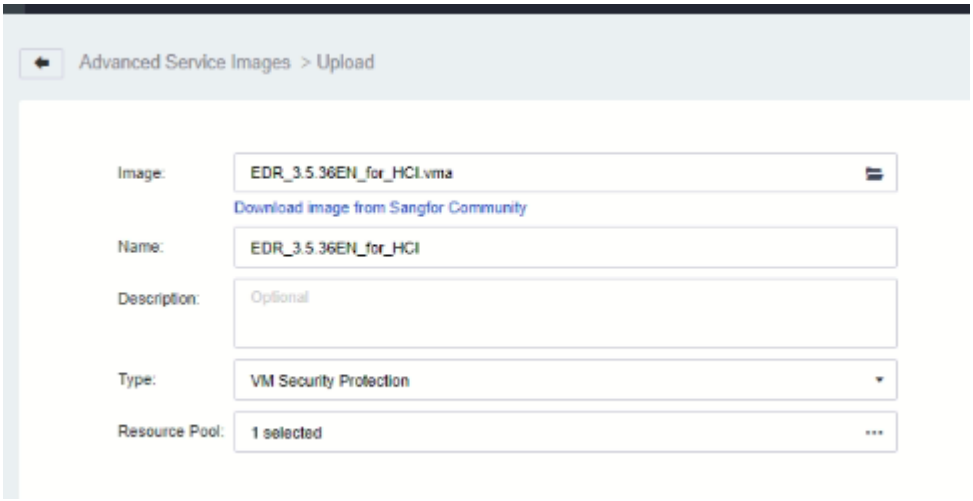
3. If cyber attack protection is enabled, it occupies the CPU and memory resources of each physical host, which can be 1 CPU core, 1 GB memory by default and 8 CPU cores, 8 GB memory at maximum.

Steps:

Step 1. Log in to the SCP platform, select **Compute > Image > Advanced Service Image**, and click the **Upload** button (the image file can be downloaded from the Sangfor community).



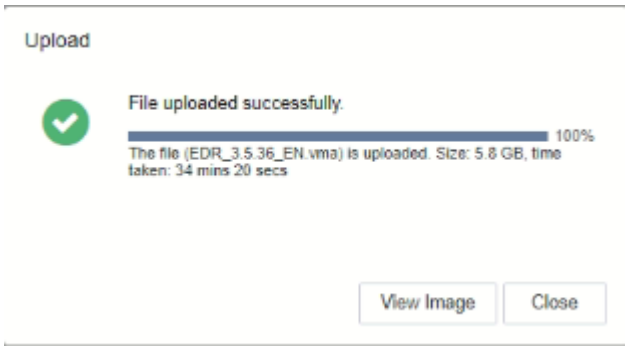
Step 2. Select the local advanced service image file (vma format) to be uploaded, select the service type and the resource pool, and click the **Upload** button.

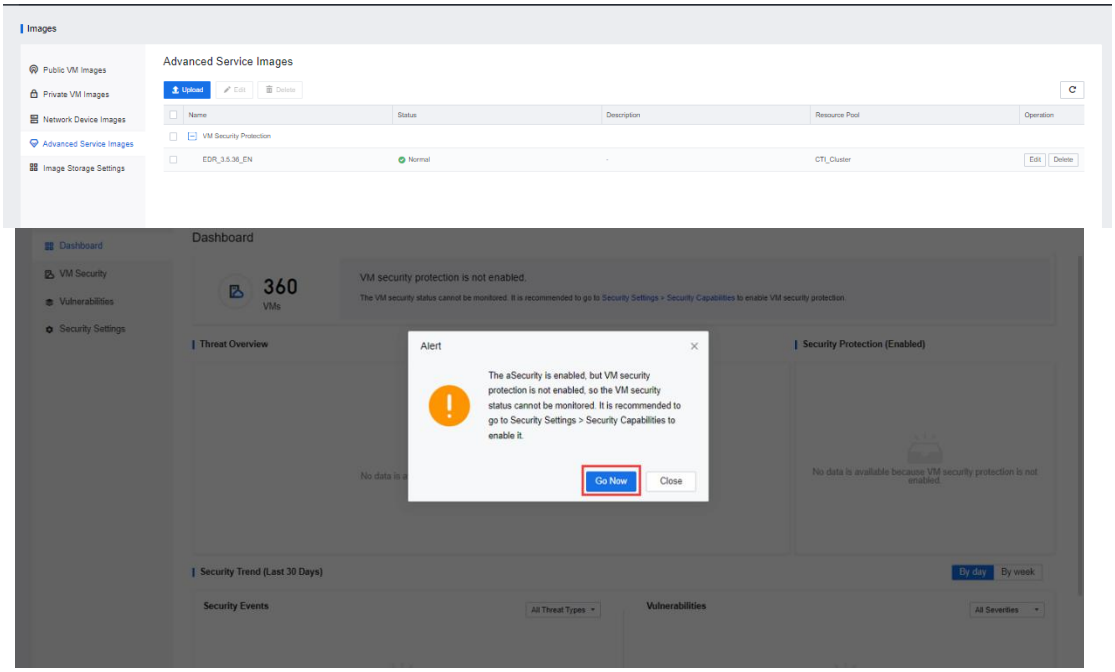


Type: cloud service security protection

Resource pool: The resource pool is run by the virtual machine of the Cloud Security Center.

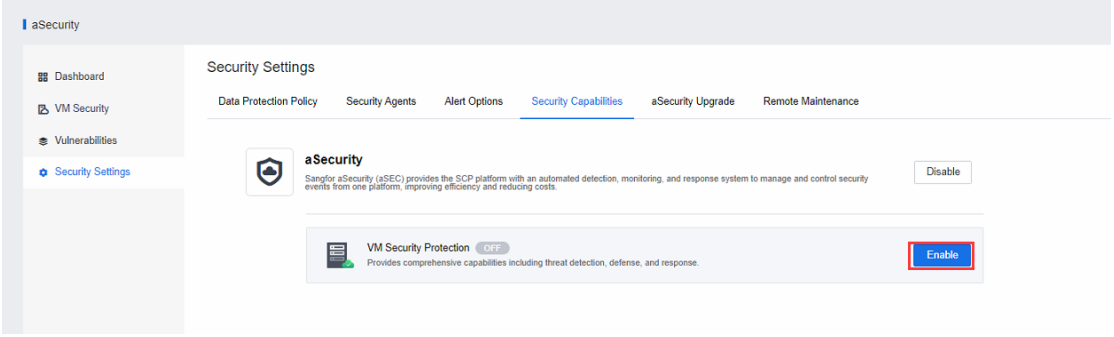
Step 3. After the upload is complete, click the **View Image** button to return to the **Advanced Service Image** page, or click the **Close** button.



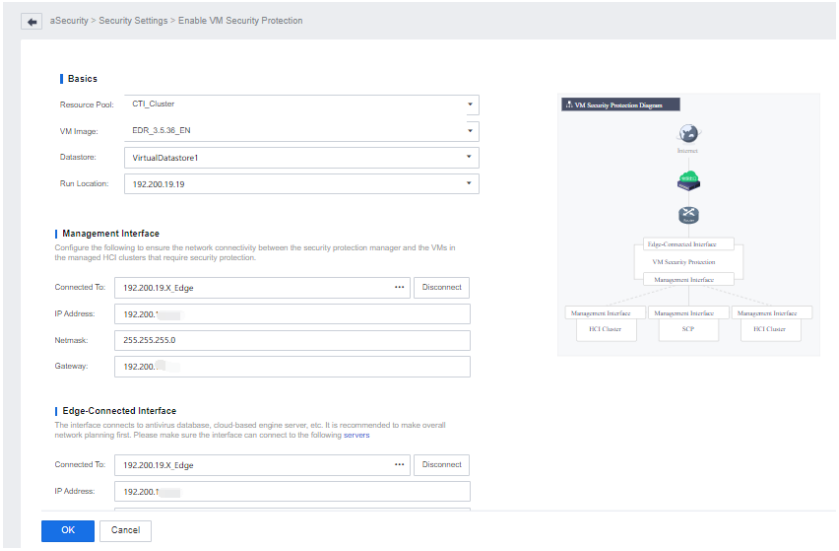


Step 4. After completing the aSEC installation, enter the aSecurity Center page and click **Go Now** on the pop-up message box to enable the cloud host security protection.

Step 5. Go to the **Security Settings > Security Capabilities** page, and click the **Enable** button of **VM Security Protection**.



Step 6. Configure and deploy the EDR_MGR management platform.



- **Basics**

  Resource Pool: cluster running on the virtual machine of the priority cloud security center.

  VM Image: The virtual machine security protection image imported from the advanced service image.

  Datastore: Prefer virtual storage volume.

  Run location: keep the default.

- **Management interface configuration**: connect to a physical edge (the physical edge must be able to access the HCI and SCP management interfaces, and it is recommended to plan the same network segment as the SCP management network).

- **Edge-Connected Interface configuration (optional)**: It is connected to the physical edge of the service network, which is used to connect to the security servers such as virus databases and cloud search service, and it must be ensured that the interface can be connected to the following servers:

  Virus database: http://download.sangfor.com.cn/download/product/edr

  Vulnerability patch:

Step 7. After successful deployment, go back to the **Security Capabilities** page and click **Add Resource Pool** to enable VM security protection and cyber attack protection for a resource pool.

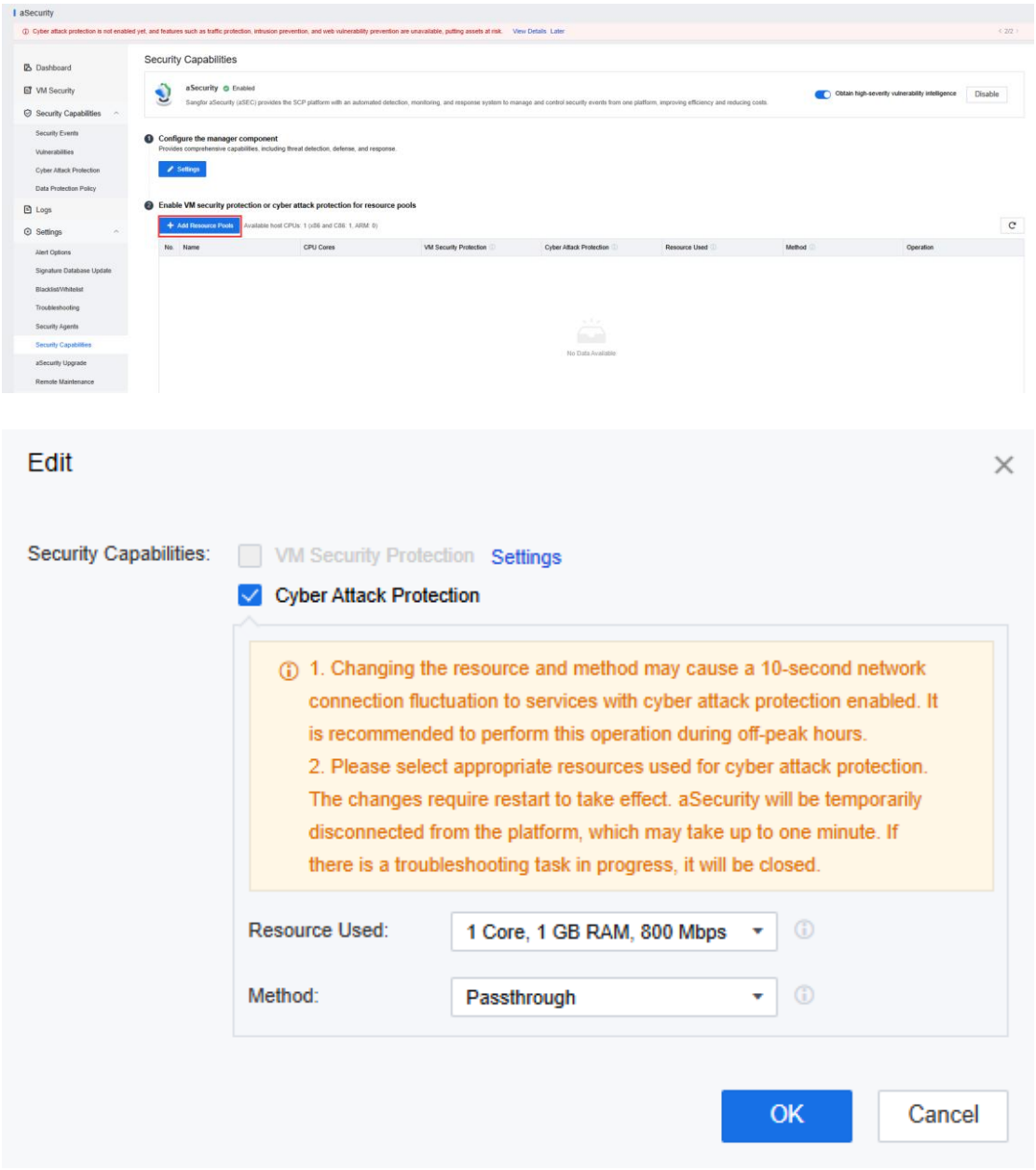
- Cyber attack protection specifications: Select the specifications as needed. If the specifications do not match the remaining resources of the physical host, that is, resources are insufficient, enablement may fail.

Container Instance Specifications	Maximum Traffic Throughput	vAF Reference Value	Remarks
1 vCPU core, 1 GB memory	800 Mbps	50 Mbps	1 CPU core, 2 GB memory for vAF
2 vCPU cores, 2 GB memory	1.8 Gbps	200 Mbps	2 CPU cores, 4 GB memory for vAF
4 vCPU cores, 4 GB memory	3.3 Gbps	400 Mbps	4 CPU cores, 8 GB memory for vAF
8 vCPU cores, 8 GB memory	5.2 Gbps	1.6 Gbps	8 CPU cores, 16 GB memory for vAF

- Processing for performance overload:

Passthrough: The platform automatically enables the policy passthrough mode if it is detected that the traffic limit is exceeded. This helps avoid business interruption.

Packet loss: The platform directly drops excessive packets if it is detected that the traffic limit is exceeded, which may cause business interruption.



4.6.3 Virtual Machine Security Agent Installation

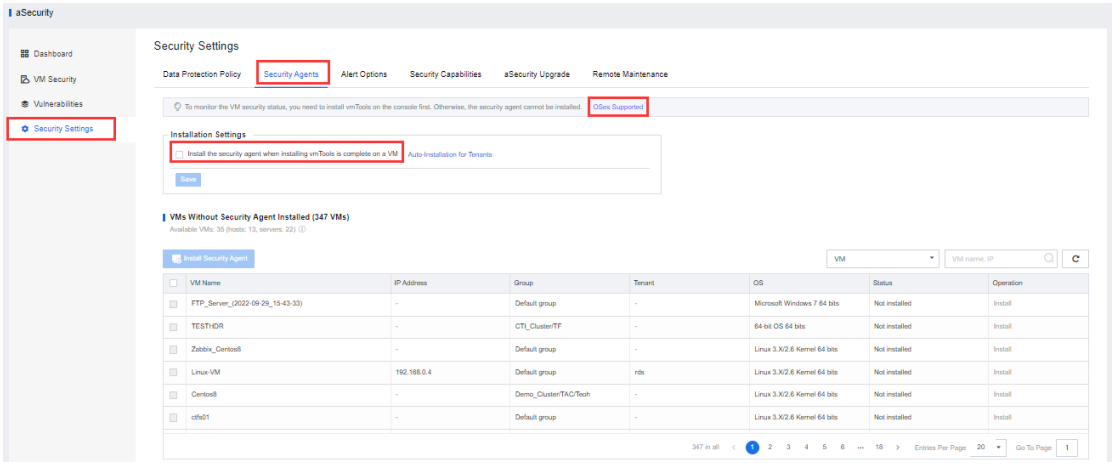
Precautions:

1. Supports automatic installation of security agent on the virtual machine, but when the number of remaining licensable virtual machines is insufficient, automatic installation cannot be triggered.
2. The time for the virtual machine to automatically install the security agent is expected to be within 10 minutes.
3. Operating systems that do not meet the compatibility whitelist cannot

install a security agent.

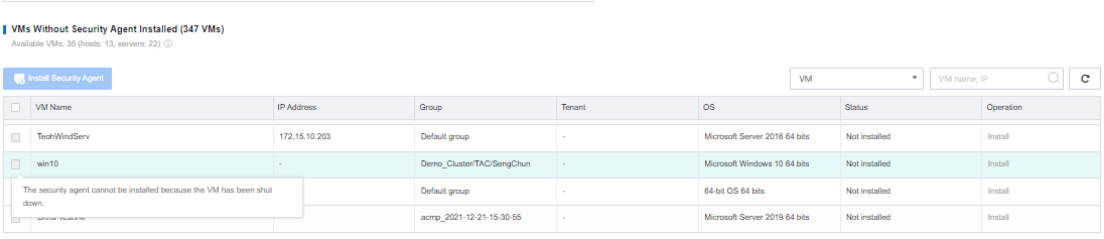
Steps:

Step 1. Go to the **Security Services > aSecurity** page, and check **the Install the security agent when installing vmTools is complete on a VM** checkbox. After checking the box, the Cloud Security Center module will automatically discover new assets online and automatically update the cloud via vmTools. . At the same time, the virtual machine security protection platform also supports the automatic update of security components through vmTools. The operating system compatibility whitelist can be viewed by clicking the **OSes Supported** button on the interface.



Step 2. Installation of the original virtual machine security agent of the Sangfor cloud computing platform.

- Suppose the automatic installation of security components is selected. In that case, the installation of the security agent will be automatically triggered for the virtual machines that have the vmTools installed and are powered on.



- If the automatic installation of security components is not selected, that is, the customer has a business in progress and only needs to monitor the security protection of some virtual machines temporarily, you can choose the virtual machine that needs to install security components in the list of virtual machines without security components. Then, click the **Install Security Agen**t button to perform the batch installation.

4.7 aSEC Configuration Guide

Sangfor aSecurity builds a unified security platform on the cloud based on unified security policies and security management. It provides targeted protection for different businesses based on accurate asset identification. Security capabilities are automatically enabled without deployment, and are deeply integrated with platform capabilities.

4.7.1 Dashboard

Function Description

The **Dashboard** page under **aSecurity** displays security information about HCI, including pending security risks, asset risk analysis, risk trend analysis, and security defense and response analysis.

Prerequisites

1. You have enabled security protection and cyber attack protection on the **Security Capabilities** page.
2. You have added the target VM to the data protection policy.
3. The platform has at least one cyber attack protection policy.

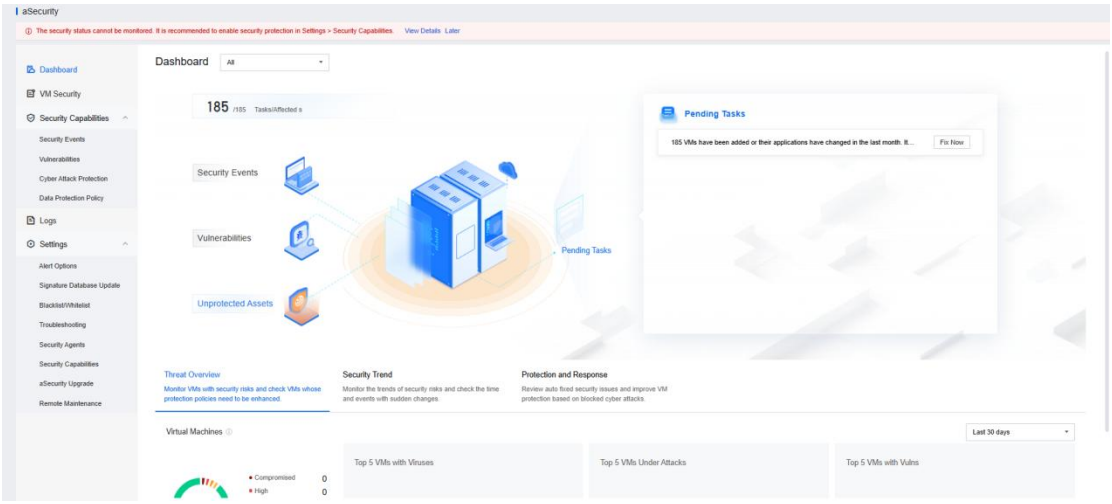
Precautions

1. Automatically fixed security events are updated at 0:00 every day but not in real time.
2. If virtual patching is enabled for a VM, the platform applies the virtual patch to all VMs with the same vulnerability by default.

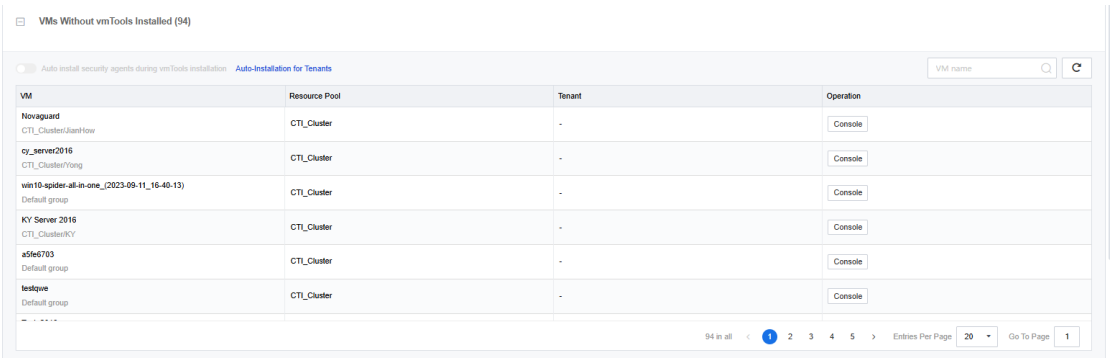
Steps

1. Go to **aSecurity** > **Dashboard** to get a security overview. In the upper area of the page, pending security risks are displayed, including security events,

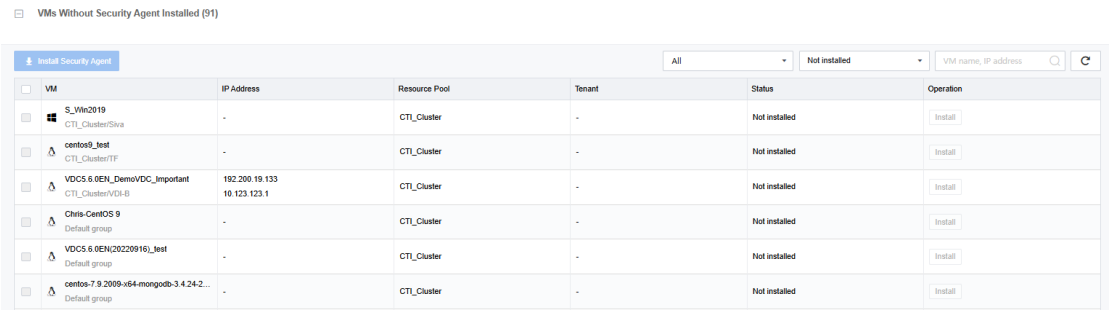
vulnerability events, and unprotected assets. You can click **Fix Now** next to an event to quickly go to the fixing page. Pending security risks include pending vmTools installation or security protection solution configuration for new assets, ransomware, ordinary risks, hot events, and ordinary vulnerabilities.



- vmTools: The platform helps you quickly locate new VMs without vmTools in the dashboard, and you can click **Console** in the **Operation** column for quick installation.



- Security protection solution: The platform helps you quickly locate new VMs without the security protection solution in the dashboard, and you can click **Configure Protection Solution** in the **Operation** column for configuration.



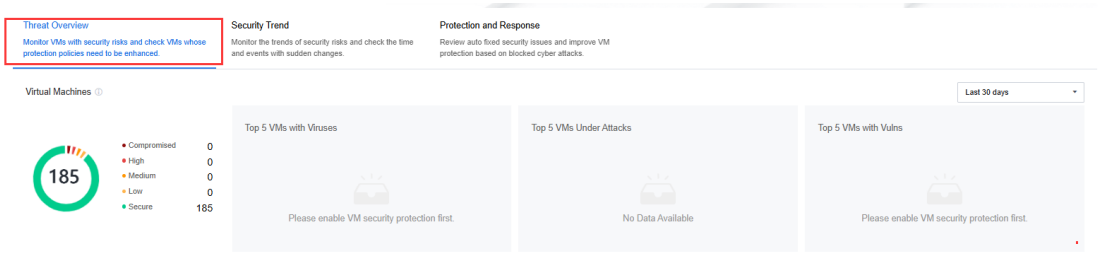
Install security components for VMs to enable the security protection feature.

Add VMs to data protection policies to implement snapshot creation for VMs every day and quickly recover business data in the case of virus infection.

Configure cyber attack protection policies for VMs to synchronize with all intrusion prevention system (IPS) policies in section 4.6.3.3 "Cyber Attack Protection."

- Ransomware: If ransomware is detected, the platform helps you quickly locate the VMs under risk in the dashboard and provides a fixing wizard.
- Ordinary risks: If an ordinary risk, such as a virus, brute-force attack, or cyber attack is detected, the platform helps you quickly locate the VMs under risk in the dashboard and provides a fixing wizard.
- Hot events: Indicate high severity vulnerabilities. On the details page of a hot event, virtual patches can be applied on the affected VMs based on the associated IPS rule for the vulnerability. A rule will be automatically created if not matched.
- Ordinary vulnerabilities: Indicate the vulnerabilities except for the above-mentioned ones. If vulnerabilities are detected, the platform helps you quickly locate them in the dashboard. Currently, Windows vulnerabilities can be quickly fixed, and Linux and application vulnerabilities can be prevented through virtual patching.

2. On the **Asset Risk Analysis** tab, view VMs with risks at different levels. You can click a risk level to go to the **VM Security** tab and filter VMs at this level quickly.



3. On the **Risk Trend Analysis** tab, view the trend of different risks, including virus events, cyber attacks, and vulnerabilities, helping you troubleshoot different security risks in a timely manner.
4. On the **Security Defense and Response Analysis** tab, view the VM security events that are automatically detected and fixed by Sangfor Engine Zero, Gene Analysis Engine, Behavioral Analysis Engine, and Cloud-Based Engine.

4.7.2 Virtual Machine Security

- aSecurity displays all HCI VMs and their basic and security information for asset management in an easy and unified manner.
- aSecurity allows you to deliver security scan tasks to specific VMs and provides virus fixing solutions to fix, trust, recover, untrust, or ignore security events.
- aSecurity supports one-click fixing of security events with a full-stack guide covering network isolation and snapshot fallback.
- aSecurity features the ransomware recovery capability based on a full-process guide covering emergency isolation and recovery without expert intervention.
- aSecurity provides cyber attack protection capability and Layer 7 network protection for business systems within the cloud.

4.7.2.1 Asset Management

Function Description

The asset management feature automatically obtains the basic and security information of VMs, including risk level, running status, VM name, IP address, operating system, application, VM protection status, and security events.

Prerequisites

N/A

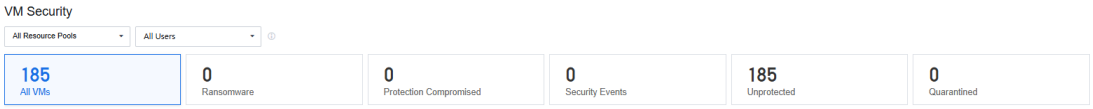
Precautions

The intervals for reporting basic, security, and application information are 1 minute, 5 minutes, and 4 hours, respectively.

Steps

1. Go to **aSecurity** > **VM Security** and manage platform assets by category.

- **Ransomware Detected**: Display the list of VMs with pending suspected ransomware events.
- **Protection Compromised**: Display the list of compromised VMs. When the security component of a VM is compromised, the security status of the VM is displayed as **Protection Compromised**.
- **Security Events Detected**: Display the list of VMs with pending security events.
- **Unprotected**: Display the list of unprotected VMs.
- **Quarantined**: View the list of quarantined VMs.



2. Go to **aSecurity** > **VM Security** > **VMs** to view the running status and information of all HCI VMs.

- Risk levels include **Protection Compromised**, **High**, **Medium**, **Low**, and **Protected**.

Protection Compromised: Indicate that ransomware exists or the VM has been compromised. Immediate fixing is required.

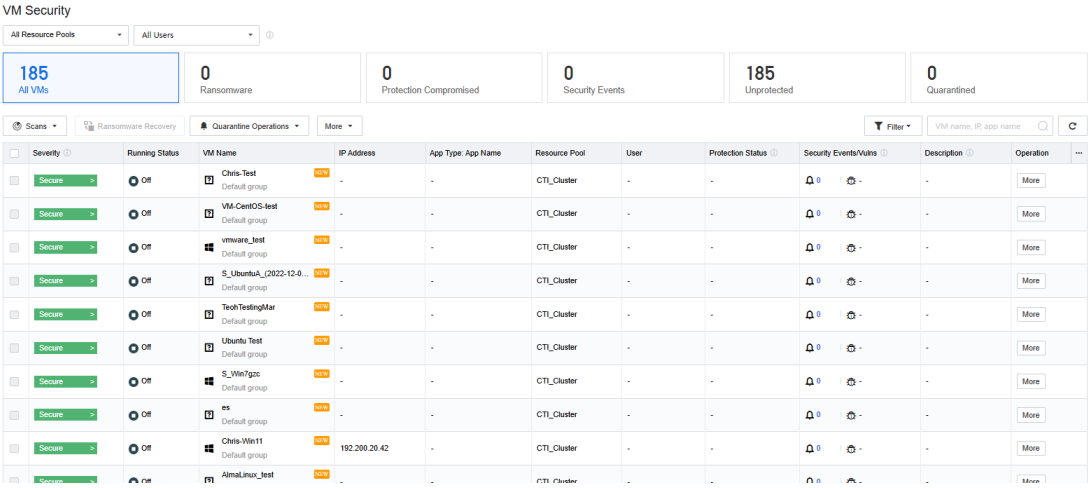
High: Indicate that a high-threat virus or a critical, high-severity attack event exists. Immediate fixing is required.

Medium: Indicate that a medium-threat virus, a low or medium-severity attack event, a brute-force attack, or a high-risk vulnerability exists. Related fixing is recommended.

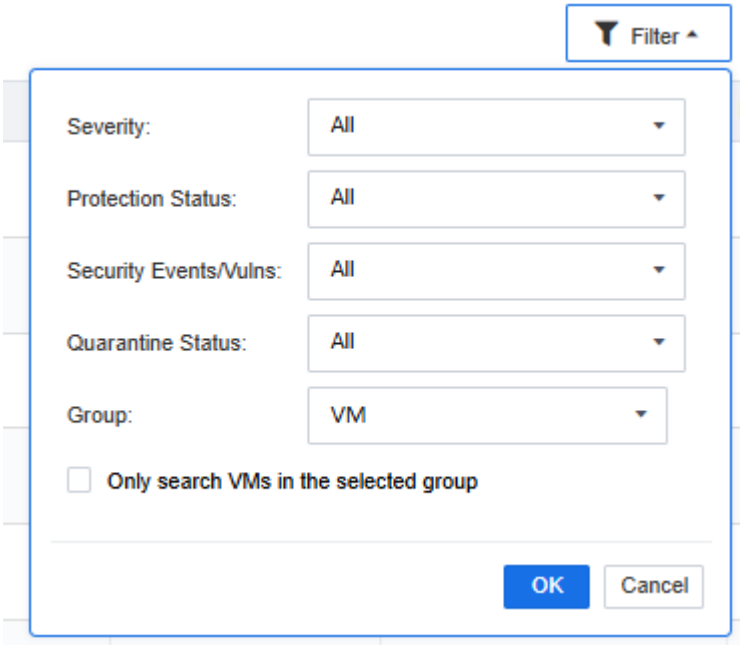
Low: Indicate that a low-threat virus or a low or medium-severity vulnerability exists. Fixing based on actual situations is recommended.

Protected: Indicate that no security risks exist.

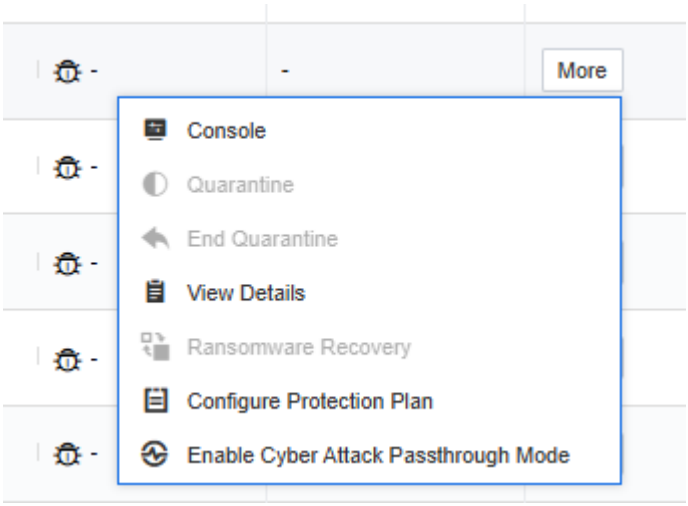
- Running status includes **On**, **Suspended**, and **Off**.
- Security risk events include security events and vulnerabilities.



3. Click **Advanced** to filter VMs by category.



4. Click **More** in the **Operation** column of a VM to go to the console, quarantine the VM, cancel quarantine, view security details, perform ransomware recovery, configure the protection solution, and enable passthrough mode for the VM.



4.7.2.2 Virus/Vulnerability Scan

Function Description

aSecurity leverages Sangfor Engine Zero, Gene Analysis Engine, Behavioral Analysis Engine, and Cloud-Based Engine to issue virus or vulnerability scan tasks to VMs and perform fixing.

Prerequisites

N/A

Precautions

1. You can scan up to 100 VMs for viruses at a time.
2. Only the scan records of the last 30 days are retained.
3. We recommend that you perform virus scans during off-peak hours, as they occupy certain CPU and memory resources.
4. Currently, Windows vulnerabilities can be fixed, and Linux and application vulnerabilities can be prevented through virtual patching.
5. If virtual patching is enabled for a VM, the platform applies the virtual patch to all VMs with the same vulnerability by default.

Steps

I. Virus Scan

1. On the **VM Security** page, select the target VM and select **Virus Scan** from the **Scans** drop-down list.
2. Select the scan method and click **OK**.

- **Quick Scan**: Scan critical system directories and registry items, memory, and running system processes, which takes a short period of time.
- **Full Scan**: Scan system memory, running system processes, critical registry items, and all disk partitions, which take a long period of time.

3. After the scan is completed, select **Vuln Scan History** from the **More** drop-down list.
4. On the page that is displayed, click **Details** in the **Operation** column of the VM and choose to fix, trust, recover, untrust, or ignore the security event.

II**.** Vulnerability Scan

1. On the **VM Security** page, select the target VM and select **Vulnerability Scan** from the **Scans** drop-down list.
2. On the **Vulnerability Scan** page, add or delete a VM, and click **OK**.
3. After the scan is completed, select **Vuln Scan History** from the **More** drop-down list.
4. On the page that is displayed, click **Details** in the **Operation** column of a VM and process the vulnerabilities that are detected. For Windows vulnerabilities, you can select **Marked as Fixed**, **Ignore**, or **Fix**. For Linux or application vulnerabilities, you can select **Marked as Fixed**, **Ignore**, or **Apply Virtual Patch**.

4.7.2.3 Quarantine

Function Description:

When virus damage occurs, the aSecurity center provides the ability to quarantine to prevent the virus from spreading. For assets that have been encrypted, the quarantine can be completed in seconds to ensure that the virus will not spread again.

Prerequisite

None.

Precautions:

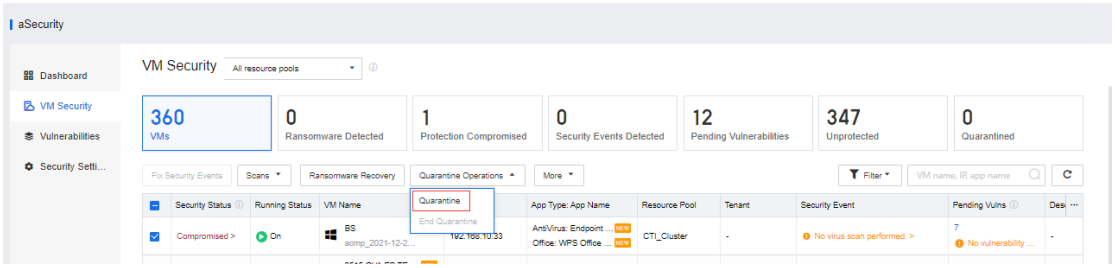
1. The quarantine will completely disconnect the virtual machine network, resulting in an interruption of services. For essential services, you can go to the **Distributed Firewall** to configure policies to avoid interrupting services

and isolating risks.

2. The virtual machine for emergency isolation will be added to the aSecurity quarantine policy. The policy will not take effect if the virtual machine is directly connected to the physical egress.

Steps:

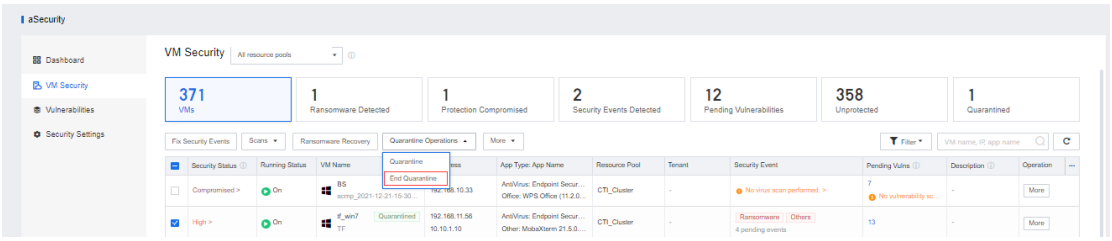
Step 1. In the VM Security list, select the virtual machines at risk of spreading the virus, and click **Quarantine Operations > Quarantine**.



Step 2. After the quarantine is complete, the virtual machine will be in the **Quarantined** state.



Step 3. When the isolated virtual machine eliminates the risk and can be released from isolation, click **Quarantine Operations > End Quarantine**.



4.7.2.4 Ransomware Recovery

Function Description:

1. The aSecurity center provides a guided ransomware recovery process, which can quickly and safely restore business without expert intervention.
2. The aSecurity center uses linked clones for business verification, which can be created in seconds. No additional storage space is occupied during the process, the environment is completely independent, and the virus will not

spread when the virus is restored during the process.

3. After the recovery point is determined and the recovery is performed, the entire process is strictly isolated from encrypted assets and other assets. The isolation is released after the recovery is completed and safe.

Prerequisite

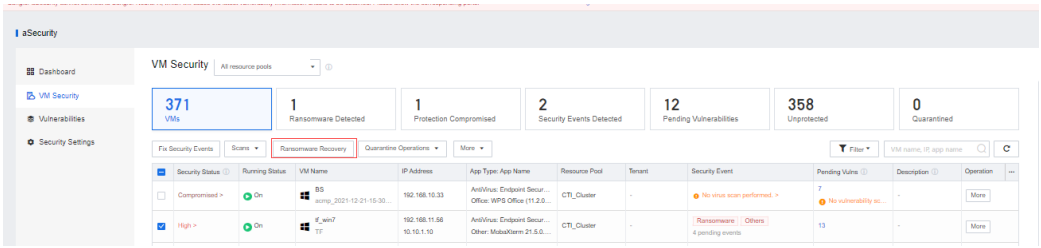
None.

Precautions:

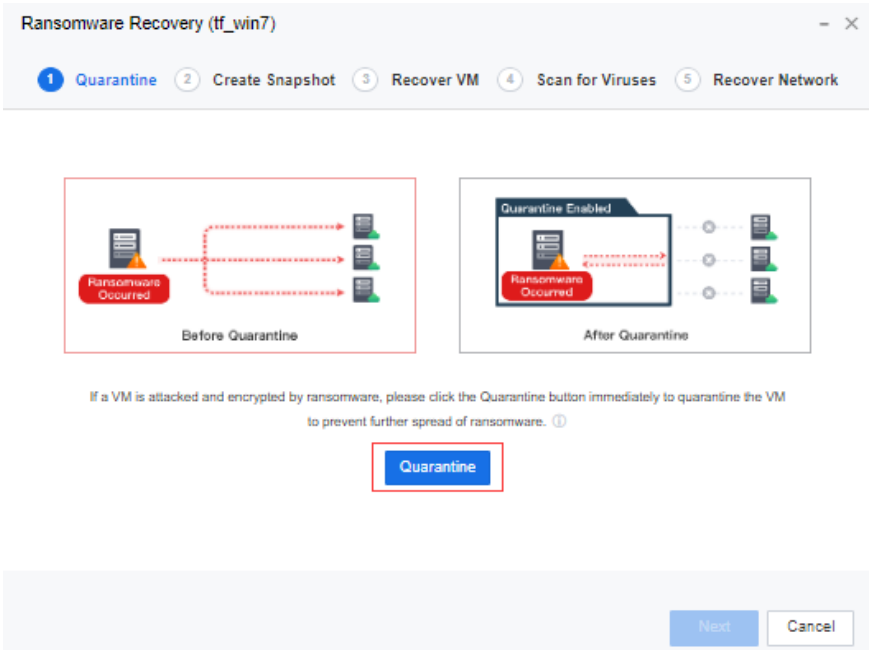
There is a time difference between the snapshot data of the recovery from ransomware and the current data. Rolling back the snapshot will cause data loss. In an actual business scenario, please evaluate the impact of ransomware and decide whether to roll back the snapshot.

Steps:

Step 1. In the VM Security list, select the virtual machine with ransomware virus, and click **Ransomware Recovery**.

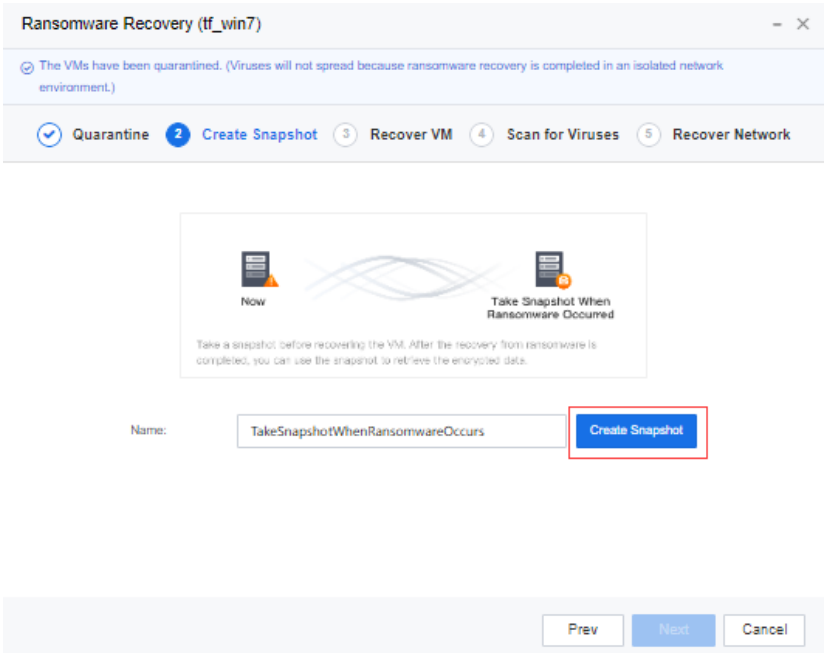


Step 2. First, it is necessary to conduct quarantine operations on the virtual



machine to prevent the further spread of ransomware. Click the **Quarantine** button, and after completing the isolation, click **Next**.

Step 3. Before performing ransomware recovery, click the **Create Snapshot** button to take a snapshot of the virtual machine. After the recovery is complete, you can try to retrieve the encrypted data through this snapshot.



Step 4. After the snapshot is created, click **Next** to restore the virtual machine. All snapshots of the virtual machine will be shown here. When the platform detects that the asset security protection component is abnormal and is suspected of being ransomware, it will automatically trigger a snapshot, creates a snapshot named **TakeSnapshotWhenRansomwareOccurs**, click the **Preview** button, and the platform will create a new linked-clone virtual machine. After cloning is complete, click the **Console** button to enter the virtual machine, and you can check whether the virtual machine is encrypted. If it is not encrypted, click **Start Recovery** and enter the admin password to recover.

Step 5. After clicking the **OK** button, the platform will automatically delete all linked-clone virtual machines created in the previous preview and restore the selected virtual machine snapshot.

Step 6. After restoring the snapshot, click **Next** to enter the virus scanning

page. It is recommended to perform a full scan on the restored virtual machine again. If a security event is found, it can be dealt with immediately.

Step 7. You can click the **Fix/Trust/Ignore** buttons for the scanned security events to handle the security events. After all security events have been dealt with, click **Next** to enter network recovery.

Step 8. Before restoring the network, since the current virtual machine data has been restored, it is recommended to check and confirm the security status of other connected virtual machines and then click the **Restore Network** button to avoid secondary infection. After the network is restored, the virtual machine will exit the isolation mode.

4.7.3 Security Capabilities

4.7.3.1 Security Events

Function Description

1. aSecurity supports the fixing of security events with a full-stack guide covering network isolation, snapshot fallback, and virus fixing.
2. This feature ensures that the RPO and RTO are the smallest. Before fixing, files are stored in a separate sandbox. In addition, a snapshot is automatically taken, so that files can be quickly recovered in the case of accidental deletion or system crash to ensure proper running of businesses.
3. It can block cyber attacks and blacklist source IP addresses to prevent network system crashes, data leakage, and information security threats caused by cyber attacks.

Prerequisites

N/A

Precautions

N/A

Steps

1. Go to **Security Capabilities** > **Security Events** > **Viruses**. Then, you can select an action on the target virus, which can be **Fix**, **Trust**, or **Ignore**.

2. Click **Fix**. In the pop-up dialog box, we recommend that you select **Create a snapshot before fixing to preserve the current VM data**.

- The virus is fixed after the snapshot is taken successfully. The snapshot suppression time is 1 hour, indicating that the earliest snapshot is retained if manual fixing is performed several times on a VM within an hour.
- A consistent group snapshot is taken for the VM if it is in a consistency group.

3. Click **OK**. After the fixing is completed, the number of virus events in the security events of the VM becomes 0.
4. Select **View Security Details** from the **More** drop-down list to enter the security event list and view the fixed virus events. If your business becomes abnormal after virus fixing, click **Recover**.

- **Recover File**: Recover the selected file to its original location, which overwrites the existing file with the same name and cannot guarantee the security of the file. By default, a recovered file will be marked as trusted. Please operate with caution.
- **Recover from Snapshot**: Recover the file from a VM snapshot. Note: This operation will recover the VM to the time point of the selected snapshot. Ensure that a snapshot or backup has been made for the VM; otherwise, unprotected data will be lost. Perform recovery during off-peak hours, as it will shut down the VM and interrupt your business.

5. Go to **Security Capabilities** > **Security Events** > **Brute-Force Attacks** and click **Block**, **Trust**, or **Ignore**.

- If you click **Block**, the attack source IP address will be added to the permanent blacklist. Traffic flowing to or from blacklisted IP addresses will always be discarded. If your business becomes abnormal after fixing, go to **Security Settings** > **Blacklist and Whitelist** > **Permanent Blacklist** to allow the blocked IP address by referring to section 4.6.5.3 "**Blacklist and Whitelist**."

6. Go to **Security Capabilities** > **Security Events** > **Cyber Attacks** and click **Block** or **Trust**.

- If you click **Block**, the attack source IP address will be added to the permanent blacklist. Traffic flowing to or from blacklisted IP addresses will

always be discarded. If your business becomes abnormal after fixing, go to **Security Settings** > **Blacklist and Whitelist** > **Permanent Blacklist** to allow the blocked IP address by referring to section 4.6.5.3 "**Blacklist and Whitelist**."

4.7.3.2 Vulnerabilities

Function Description

aSecurity provides a vulnerability monitoring view for all business VMs to help you comprehensively understand vulnerability risks in your business system. It also offers one-click bulk fixing of Windows vulnerabilities, ensuring better business security.

Prerequisites

N/A

Precautions

Currently, only Windows vulnerabilities can be fixed, and Linux and application vulnerabilities cannot be fixed.

Steps

1. Go to **aSecurity** > **Security Capabilities** > **Vulnerabilities**. The platform automatically detects and reports Windows, Linux, and application vulnerabilities, and you can also manually scan for vulnerabilities.
2. On the **Vulnerabilities** page, view the vulnerability information, including **Severity**, **Patch Name**, **Tags**, **Patch ID**, **First and Last Detected**, and **Pending/Affected VMs**. Click **Fix** in the **Operation** column to view the details of the vulnerability and the list of VMs it affects.
3. To fix a Windows vulnerability for one or more VMs, select the target VMs and click **Fix**. **We recommend that you select Create a snapshot before patching to preserve the current VM data, so that your business can be quickly recovered if fixing fails.**
4. Select one or more vulnerabilities and export the detection results as needed, including **Severity**, **Vuln/Patch Name**, **Tags**, **Patch/CVE ID**, **VM Name**, **IP Address**, **Status**, and **Remarks**.

4.7.3.3 Cyber Attack Protection

Function Description

aSecurity provides cyber attack protection policies for the virtual network topology and Layer 7 network protection for business systems within the cloud.

Prerequisites

N/A

Precautions

1. The backend aggregates cyber attack events by impact scope and attack source based on cyber attack log data once every 10 minutes.
2. You can configure up to 512 IPS policies and up to 512 web vulnerability protection policies.
3. You can configure cyber attack protection policies by resource pool or tenant VPC network but not tenant classic network.
4. A VM group can contain up to 100 IP addresses. If more IP addresses exist, a new group needs to be created.
5. To ensure automatic defense against cyber attacks on the tenant VPC network, you need to ensure that cyber attack protection is enabled in the resource pool of the VPC.

Steps

1. Go to **aSecurity** > **Security Capabilities** > **Cyber Attack Protection**, click **Create**, configure the basic, source, and destination information, and select applicable scenarios for the policy.

- **IPS**: Detect and defend against attacks exploiting operating system, application, and protocol vulnerabilities.
- **Web Vuln Protection**: Protect web servers from various attacks targeting web applications, such as SQL injections, XSS attacks, and command injections.

2. Go to **Cyber Attack Protection Policies** > **Templates** to view or manage intrusion prevention policies and web vulnerability policies.

- Click **Details** in the **Operation** column of the policy to view its details.

- Go to **Signature Database** and set **Action** (**Allow** or **Drop**) and **Status** (**Enable** or **Disable**).

4.7.3.4 Data Protection Policy

Function Description

aSecurity allows you to enable the data protection policy, where all VMs are snapshot every day for data protection. Snapshots are triggered immediately when security software is uninstalled or suspected of encountering ransomware risks. Scheduled snapshots are persisted so that they will not be overwritten by virus-infected data.

Prerequisites

The VMs have been added to the resource pool of the data protection policy, and the snapshot policy has been set to smart mode on HCI. In manual mode, you cannot enable the data protection policy. For more information about how to set the mode, see section 5.2.13 "Manage Snapshot Policies" of HCI User Manual.

Precautions

1. VM snapshots are created automatically every day according to the data protection policy. We recommend that you add critical VMs to the policy to quickly recover data in the case of severe issues such as ransomware.
2. In general, only the latest snapshot is retained. In the case of severe security events such as compromised VMs or suspected ransomware, the latest snapshot before the event occurrence is retained for 7 days.
3. The data protection policy has the following limits on the number of snapshots taken every day:

- Hybrid datastore: vm_num = [0.6 × (host_num - 3) × 4 + 12] × (capacity per SSD × 0.5 × number of SSDs/480 GB). Note: If storage capacities are heterogeneous, the smallest capacity is used for calculation.
- All-flash datastore: 2,048

4. If a selected VM or consistency group is added to a snapshot policy, the VM or consistency group will be removed from the original policy and added to the current data protection policy.

5. After being added to the data protection policy, the VM or consistency group will be snapshot once every day.

Steps

1. Go to **aSecurity** > **Security Capabilities** > **Data Protection Policy** and click **Add Resource Pool**.
2. Click **Add** on the **VM** tab or **Consistency Group** tab to add a VM or consistency group to the data protection policy.

4.7.4 Security Logs

Function Description

This feature allows you to query security logs, including virus scan logs, brute-force attack logs, cyber attack logs, and vulnerability scan logs, to facilitate security event analysis and processing.

Prerequisites

N/A

Precautions

N/A

Steps

Go to **aSecurity** > **Security Logs** and query logs. For cyber attack logs, you can add a detection rule to the whitelist to allow the cyber attack event. To modify the rule subsequently, go to **Security Settings** > **Blacklist and Whitelist**. For details, see section 4.6.5.3 "Blacklist and Whitelist."

4.7.5 Security Settings

4.7.5.1 Alerts

Function Description

aSecurity detects security events on VMs in real time, such as brute-force attacks, WebShell backdoors, ransomware, and Trojans. Then, it sends emails to the email address you specified to notify you of the detected security events.

Prerequisites

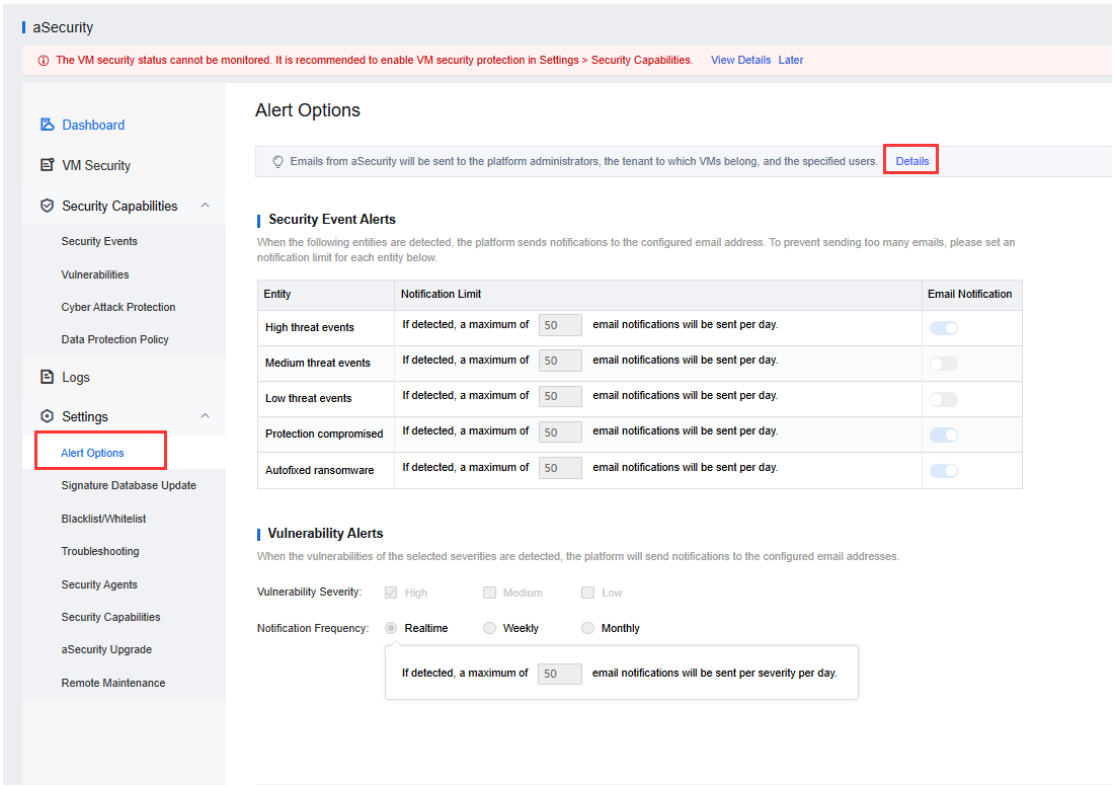
You have configured the Simple Mail Transfer Protocol (SMTP) server.

Precautions

aSecurity does not support alert notifications via SMS.

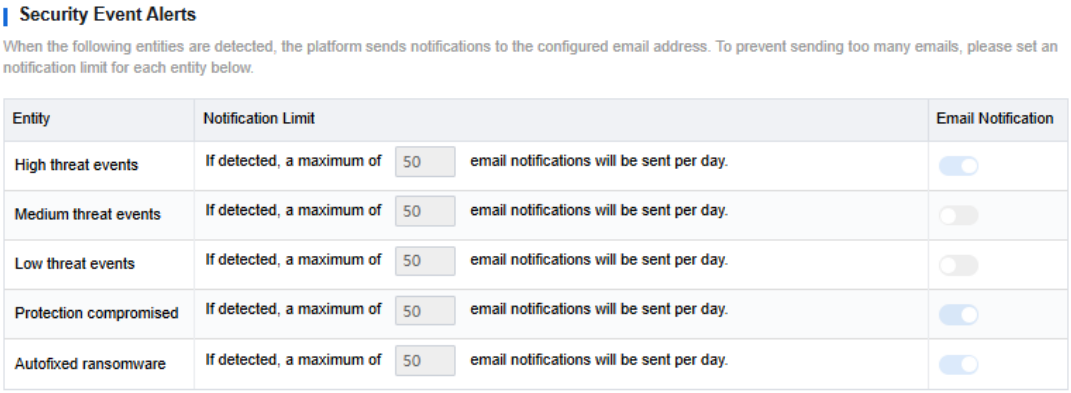
Steps

1. Go to **Security Settings** > **Alert Settings** and click **Change Email Address**. On the page that appears, click **New** and select **aSecurity Alert**. For more information about alert settings, see section 4.12.4.2 "Alerts."

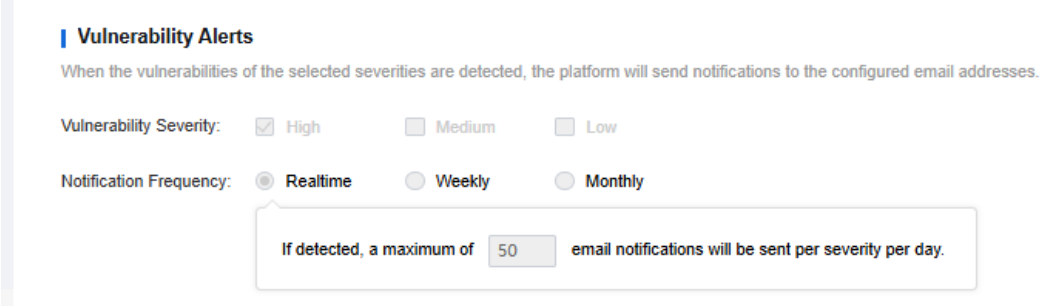


2. If the platform detects a security or a vulnerability event, it sends an alert email to the email address you specified according to the set alert condition.

- Security event alerts: You can set the maximum number of alert emails, which ranges from 1 to 1,000.



- Vulnerability alerts: You can set **Vulnerability Type** and **Alert Frequency**. If you select **Real-Time** for **Alert Frequency**, you can set the maximum number of alert emails, which ranges from **1** to **1,000**.



3. Click **Save**.

4.7.5.2 Signature Database Update

Function Description

aSecurity supports the automatic and manual updates of the web vulnerability signature database and IPS database, ensuring that new threats are identified and blocked in a timely manner and enhancing system security.

Prerequisites

The edge-connected interface of the aSecurity VM can connect to the following WAN servers, or the .zip file of the latest signature database has been obtained.

Cloud firewall signature databases:

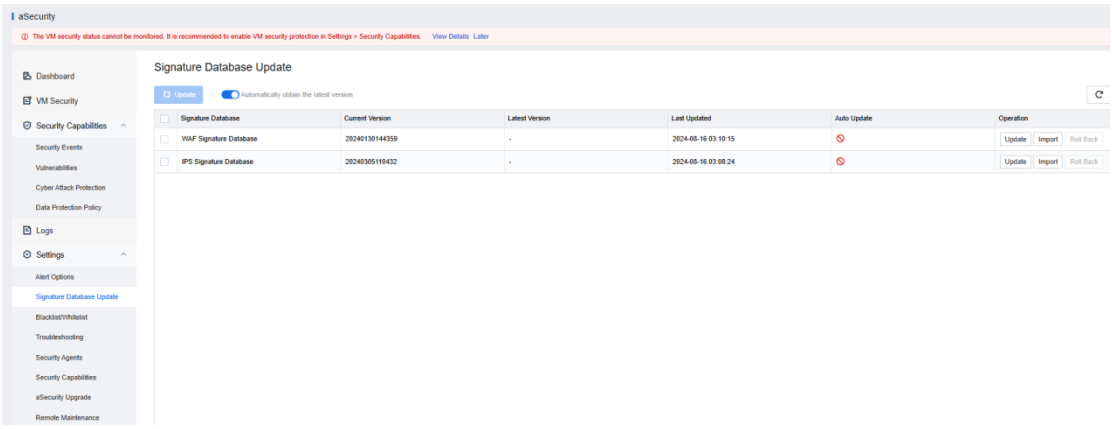
- Guangdong: upd.sangfor.com.cn
- Hong Kong: upd.snagfor.com
- Manual update: https://sec.sangfor.com.cn/index/abroad?lang=EN-US

Precautions

N/A

Steps

Go to **aSecurity** > **Security Settings** > **Signature Database Update**. On the page that appears, you can view the information of current signature databases, including **Name**, **Current Version**, **Latest Version**, and **Update Time**. You can perform operations such as online updates, manual import, and rollback.



4.7.5.3 Blacklist and Whitelist

Function Description

aSecurity supports blacklist management for attack protection or brute-force attack events and whitelist management for IP addresses, VMs, security policies, or threat events.

Prerequisites

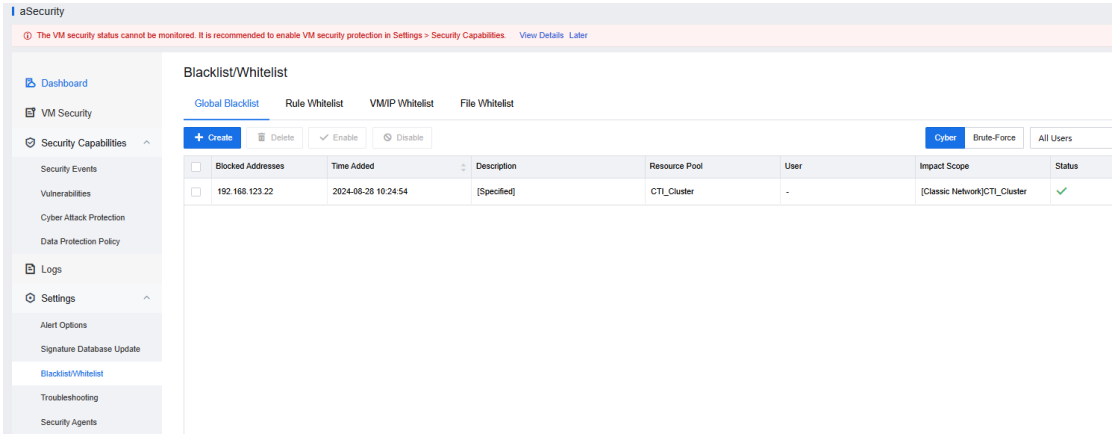
Allocate a quota and enable aSecurity for a tenant before creating a blacklist and whitelist for the tenant.

Precautions

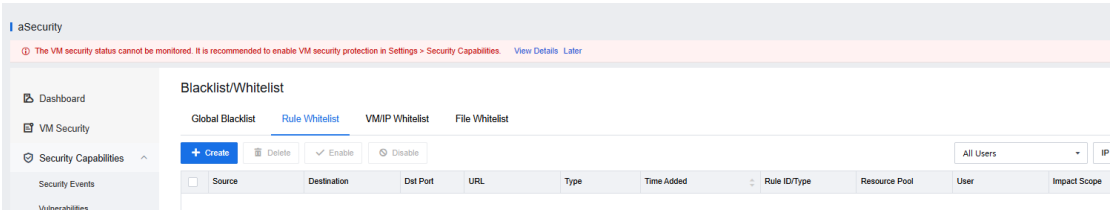
1. For the permanent blacklist, you can configure up to 2,048 items.
2. For the rule whitelist, you can configure up to 2,048 items.
3. For the VM/IP whitelist, you can configure up to 2,048 items.
4. When creating a blacklist or whitelist, you can specify the impact scope, resource pool, and tenant VPC network.

Steps

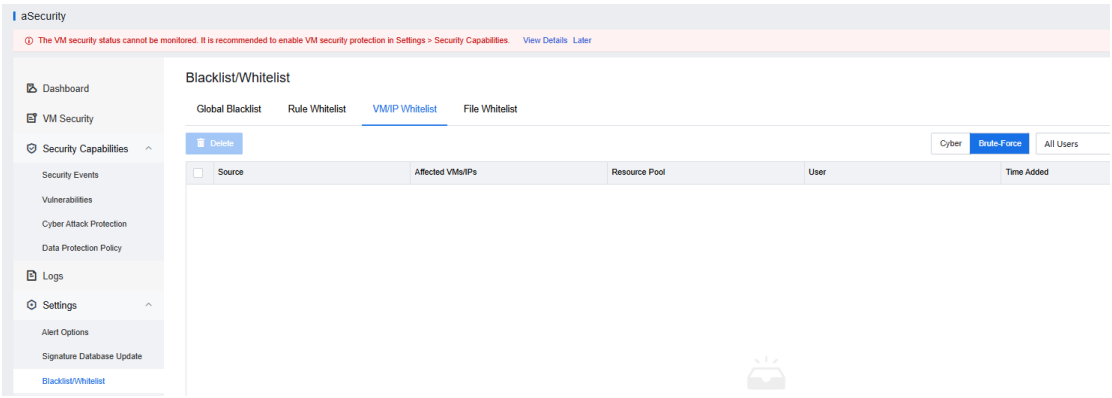
1. On the **Permanent Blacklist** tab, add or remove source IP addresses related to attack protection events and remove those related to brute-force attack events as needed.



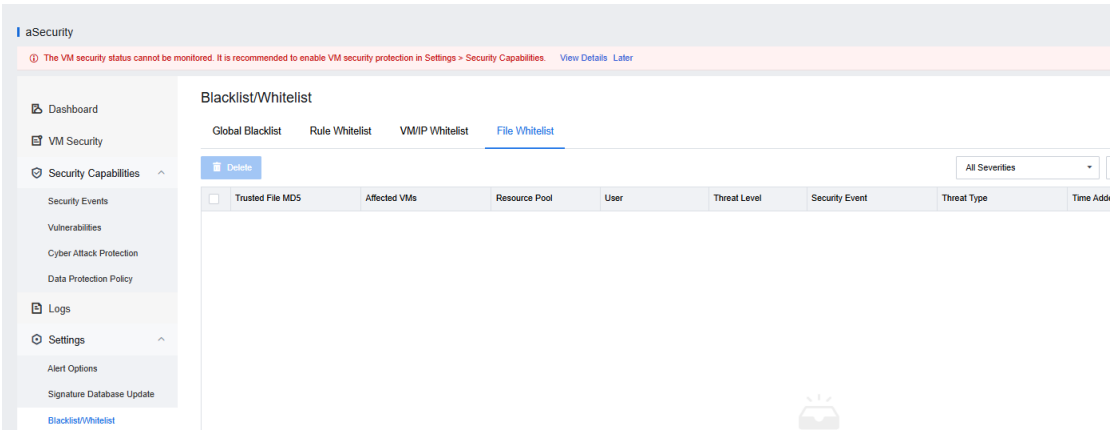
2. On the **Rule Whitelist** tab, add, remove, enable, or disable the enabled web vulnerability protection or IPS policies as needed.



3. On the **VM/IP Whitelist** tab, add or remove source IP addresses and destination IP addresses/VMs related to attack protection events and remove those related to brute-force attack events as needed.



4. On the **File Whitelist** tab, remove trusted threat events as needed, which will also remove files with the same MD5 value.



4.7.5.4 Troubleshooting

Function Description

This feature allows you to troubleshoot network disconnections or service or application inaccessibility on aSecurity. Currently, precise traffic analysis and global passthrough modes are supported.

- Precise traffic analysis: Data packets dropped due to the firewall policy are obtained based on the specified rules, which can be used for analysis of blocked access.
- Global passthrough: All firewall policies are ineffective within the specified scope. This mode is applicable in the case when the firewall policy that blocks the business access cannot be identified. It disables global firewall policies to ensure the proper connection of the business network.

Prerequisites

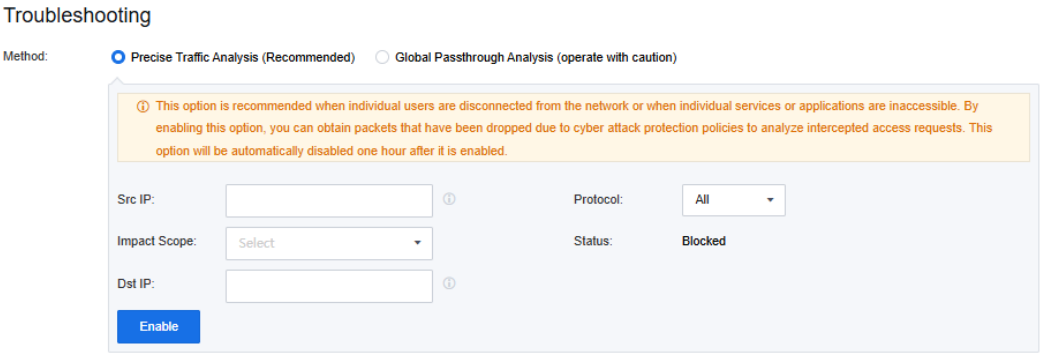
N/A

Precautions

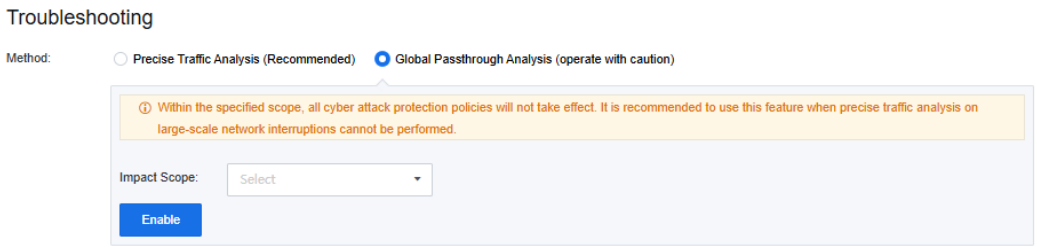
1. Precise traffic analysis will be automatically disabled 1 hour after it is enabled.
2. You can start only one precise traffic analysis task at a time.

Steps

1. Precise traffic analysis (recommended): Go to **Security Settings** > **Troubleshooting**, select **Precise Traffic Analysis** for **Mode**, set **Source IP** or **Destination IP**, select **Protocol** and **Impact Scope**, and click **Enable**.



2. Global passthrough (use with caution): Go to **Security Settings** > **Troubleshooting**, select **Global Passthrough** for **Mode**, select **Impact Scope**, and click **Enable**.



4.7.5.5 aSecurity Upgrade

Function Description

This section provides guides on how to upgrade aSecurity.

Prerequisites

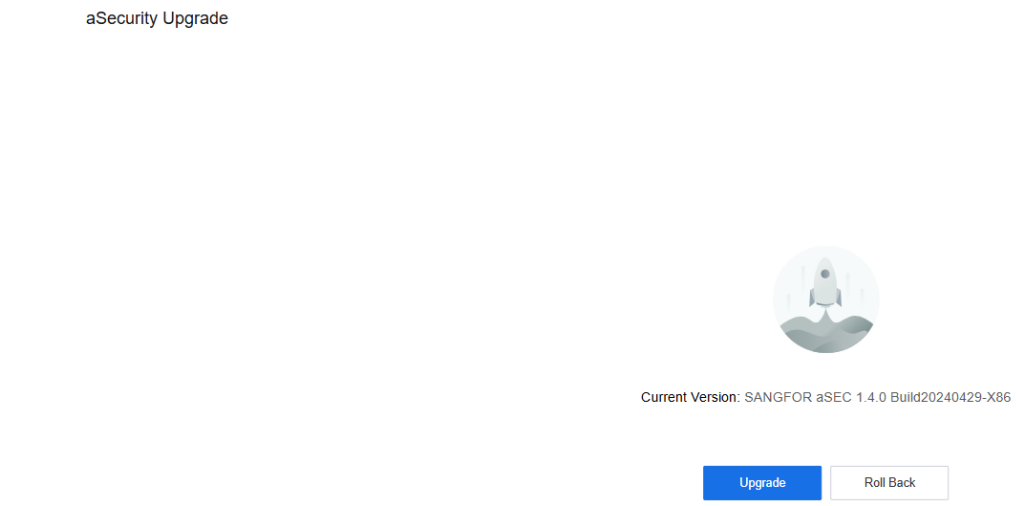
The latest service pack or upgrade package has been obtained.

Precautions

1. You can install up to 10 service packs for a version.
2. You can roll back one service pack at a time, in reverse order of the upgrade sequence.
3. Cold start is used for upgrade and rollback, that is, aSecurity VM restart.
4. If the upgrade or rollback is interrupted, the service pack is rolled back automatically.

Steps

Go to **Security Settings** > **aSecurity Upgrade**, click **Upgrade** or **Roll Back**, and perform operations as instructed.



4.7.5.6 Remote Maintenance

Function Description

You can contact technical support for remote diagnostics, troubleshooting, and fixing to improve system performance or recover businesses.

Prerequisites

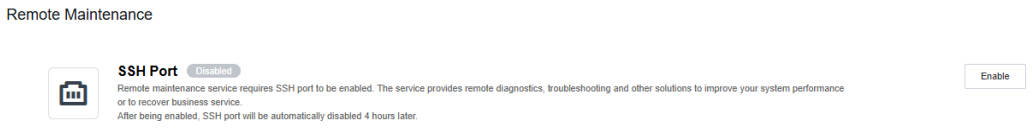
N/A

Precautions

SSH Port will be automatically disabled 4 hours after it is enabled.

Steps

Go to **Security Settings** > **Remote Maintenance** and click **Enable SSH Port**. Then, aSecurity can be remotely maintained via SSH.



4.8 Hybrid Cloud Services

4.8.1 Third-Party Public Cloud

Function Description:

Sangfor SCP supports AWS management and can add the resources on Alibaba

Cloud to SCP in the form of a cloud environment. After adding a cloud environment, you can directly use the SCP on the AWS cloud server (EC2). Besides, assigning it to the tenant is supported.

Precautions:

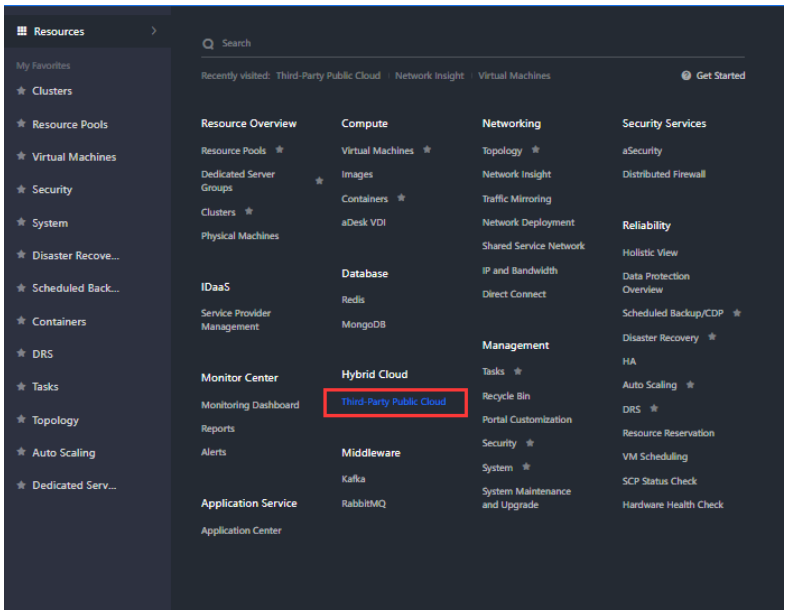
1. When an AWS account has multiple Access Keys, the Keys cannot be used to manage the same cloud environment.
2. Since AWS has a monthly limit on the number of free API queries, when using the same AWS account to add a cloud environment, it is not recommended that the number of cloud environments exceeds 10. If it exceeds 10, the user needs to pay.
3. If the AWS account is in arrears, it will report service unavailable when collecting cloud environment data, and you can recharge it in the Alibaba Cloud console.

Prerequisite

1. SCP configuration enables the SCP to have an internet connection.
2. The Access Key ID and Access Key Secret of the AWS account have been obtained. AWS Access Key ID and Access Key Secret are your only credentials for accessing Alibaba Cloud API. Access Key ID is similar to the identification of identity, and Access key secret is similar to your login password, which is used to sign your access parameters to prevent tampering.

Steps:

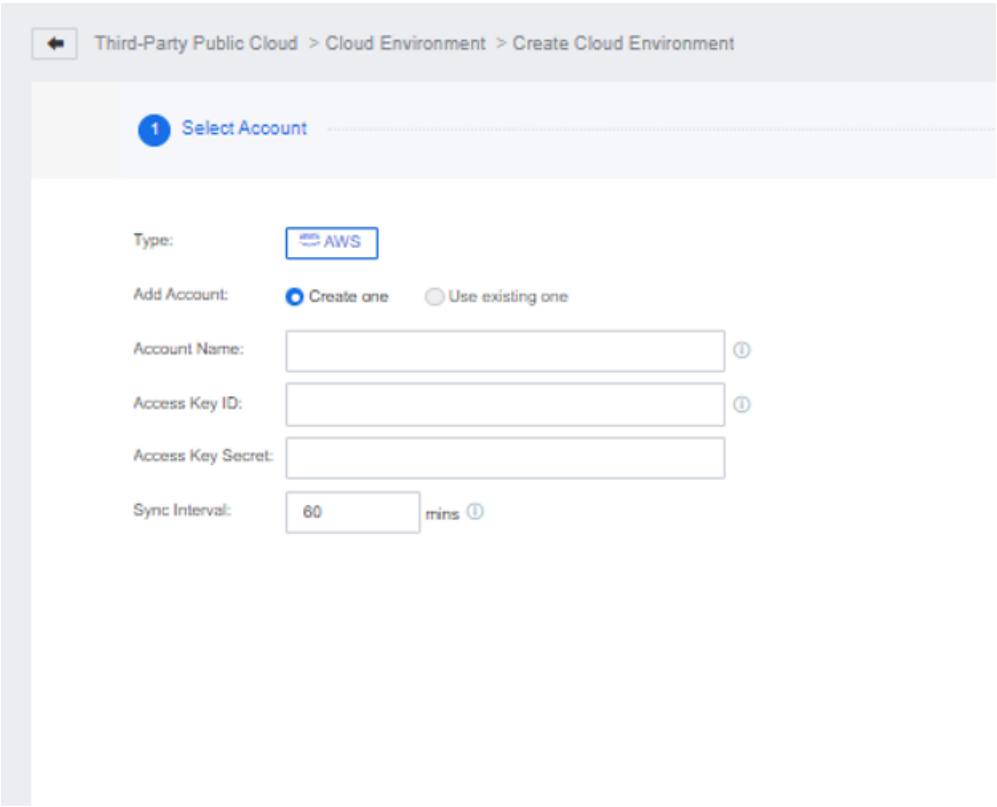
Step 1. Use the admin account to log in to the system management interface



of SCP and navigate to **Hybrid Cloud** > **Third-Party Public Cloud**.

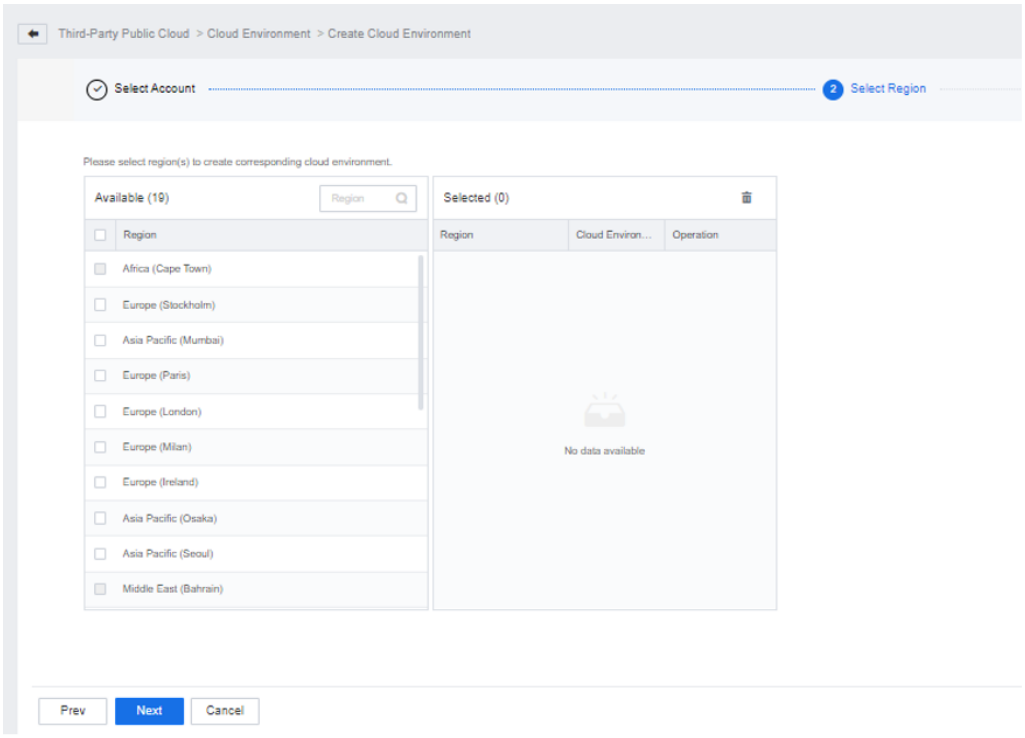
Step 2. Click **New** to add a new cloud environment:

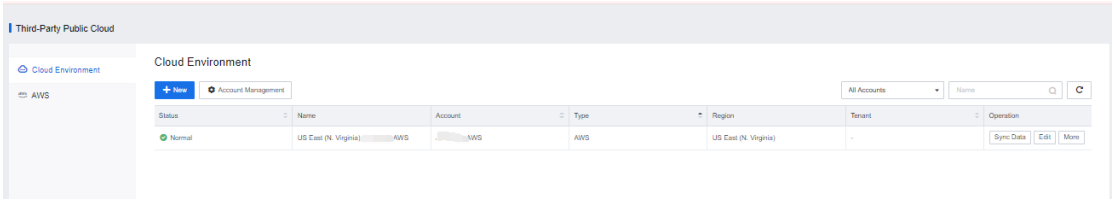
- **Type:** AWS
- **Add Account:** Select between **Create One** or **Use existing one** (for the user who previously added the account).
- **Account Name:** Custom cloud account.
- **Access Key ID:** Obtained from the client.
- **Access Key Secret:** Obtain from the client.
- **Sync Interval:** 60 minutes (the new resources added by the cloud account on the AWS platform will be automatically updated within the specified cycle. It is recommended to keep the default cycle. The shorter the cycle, the higher the SCP platform resources will be occupied).



Step 3. Click **Next** and select a region to create the corresponding cloud

environment. For example, if a customer has a virtual machine in Tokyo AWS, he can select Asia Pacific (Tokyo) and add it as a cloud environment.





4.8.1.1 Allocate Cloud Environment

Function Description:

The added cloud environment can be allocated to tenants according to actual needs. The cloud environment can be regarded as the tenant's exclusive resource pool, and other tenants cannot use the cloud environment.

Prerequisite

After a cloud environment is allocated to a tenant, the virtual machine in the cloud environment cannot be allocated to other tenants.

Precautions:

The cloud environment has been added successfully.

Steps:

Step 1. Use the admin account to log in to the system management interface of SCP and navigate to **Hybrid Cloud > Third-Party Public Cloud > Cloud Environment.**

Step 2. Select a cloud environment, click **More > Allocate**, select the tenant's name to be assigned to, and then complete the assignment of the cloud environment.

4.8.1.2 Deallocate Cloud Environment

Function Description:

After a cloud environment is assigned to a tenant, the platform administrator can deallocate it.

Prerequisite

After the cloud environment is de-allocated, the tenant will not be able to use the cloud environment.

Precautions:

The cloud environment has been successfully assigned to the tenant.

Steps:

Step 1. Use the admin account to log in to the system management interface of SCP and navigate to Hybrid Cloud > Third-Party Public Cloud > Cloud Environment.

Step 2. Select a cloud environment, click **More > Deallocate**, and confirm to complete the cloud environment deallocate.

4.8.1.3 Delete Cloud Environment

Function Description:

After a cloud environment is added to the platform, platform administrators can delete it.

Prerequisite

After the cloud environment is deleted, all cloud resources synchronized to the local cloud environment will be cleared, and cloud resources will not be affected.

Precautions:

None.

Steps:

Step 1. Use the admin account to log in to the system management interface of SCP and navigate to Hybrid Cloud > Third-Party Public Cloud > Cloud Environment.

Step 2. Select a cloud environment, click **Delete**, and delete the cloud environment after confirming.

4.9 Reliability Center

4.9.1 Holistic View

Function Description:

This function provides a visualized and simplified operation and maintenance method and one-click access to reliable resources and services. Through this interface, managers can obtain the overall operating status of the platform and can quickly locate specific problems.

Precautions:

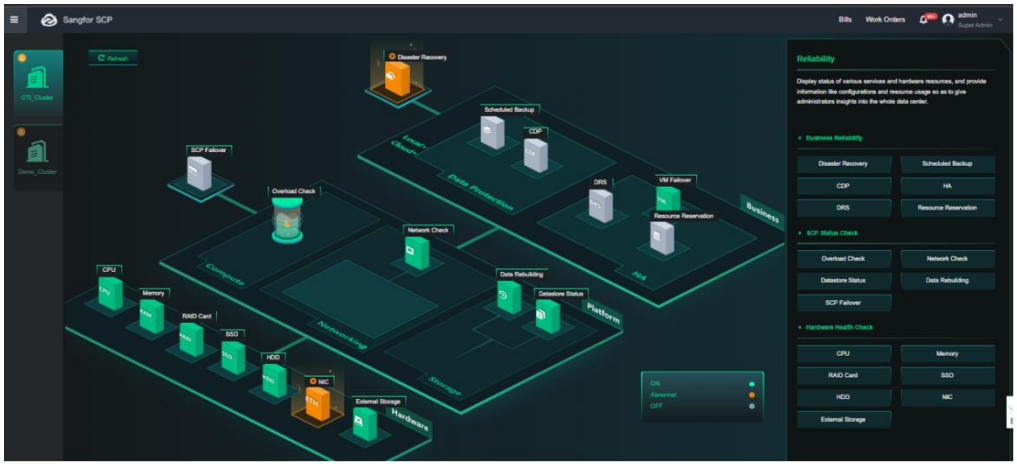
None.

Prerequisite

None.

Steps:

Step 1. Log in to the SCP platform and select **Reliability** > **Holistic View** to enter the **Holistic View** interface.

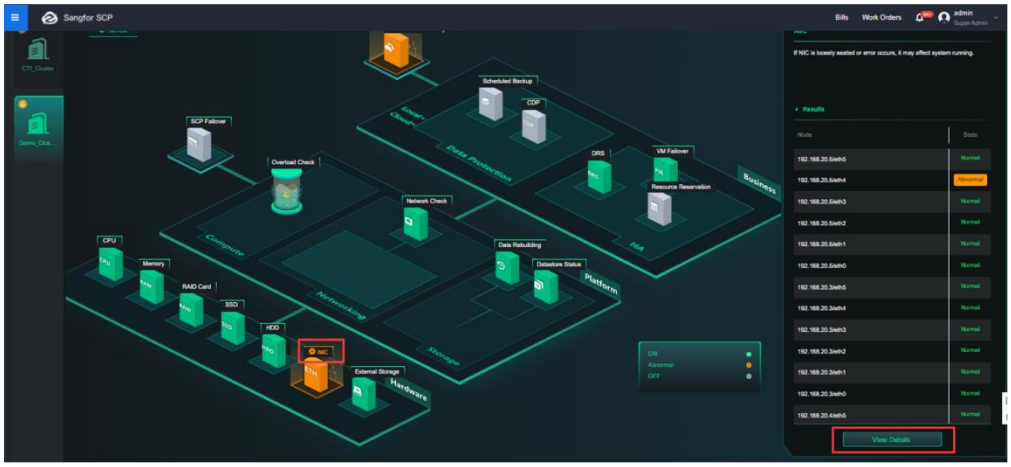


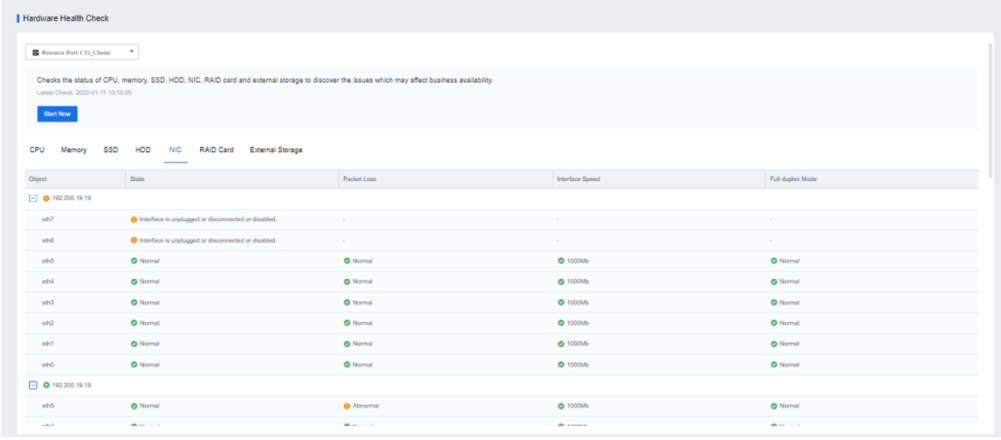
Step 2. You can see different sites on the left panel, click any service you want to view in the main interface, and you can view the corresponding detailed status.

NOTE

Gray indicates that the function is unavailable or the service is not configured, yellow indicates that an abnormal service is detected, and green indicates that the service is normal.

Step 3. Click the exception icon and **View Details** to enter the **Hardware Health Check** page.





Start Now: To detect and eliminate false positives.

Entity Description: You can view the judgment rule of each inspection item.

Suggestion: Provide suggestions for the current issues.

4.9.2 Data Protection Overview

Function Description:

This function provides a visual interface for data protection, including scheduled backup status, CDP backup status, and disaster recovery status information.

Precautions:

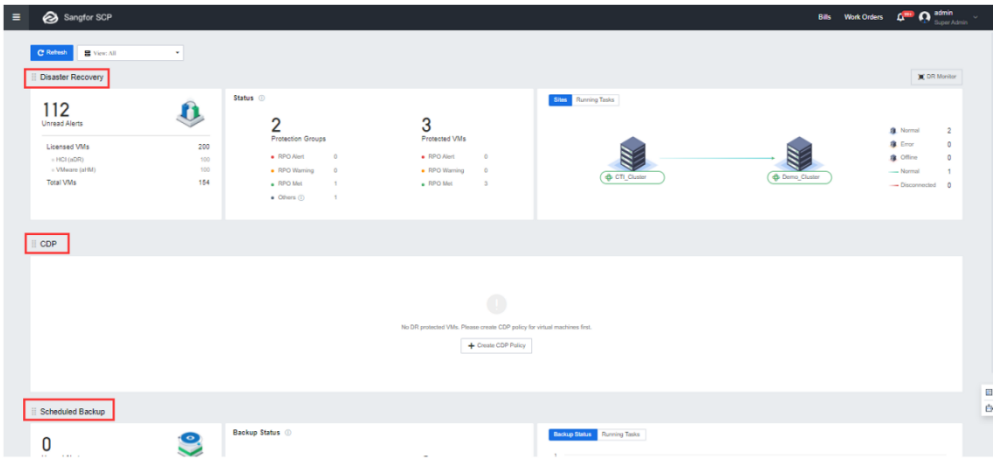
None.

Prerequisite

None.

Steps:

Step 1. Log in to the SCP platform, select **Disaster Recovery** > **Data Protection Overview**, and enter the data protection overview interface. You can see the status of the protected business group and the protected virtual machine for aDR and provide comprehensive monitoring and alarm capabilities.



4.9.3 Backup and CDP

4.9.3.1 Scheduled Backup

Function Description:

Provide scheduled backup services for the virtual machine to regularly back up data.

Precautions:

1. After the SCP manages the HCI resource pool, backup can only be performed on the SCP platform.

2. Backup protection of raw disks in virtual machines is not supported.
3. The virtual machine can be backed up when powered on or off.
4. The first backup is a full backup. Other backups within the backup retention period are incremental backups.
5. Only one full backup is retained in each backup retention period. At the start of the next backup retention period, the system will automatically merge the first full backup and multiple incremental backups into a new full backup.
6. The virtual machine can be quickly pulled up during backup and recovery when the backup repository is virtual storage, FC storage, or iSCSI storage.
7. Each virtual machine can only add one backup policy.
8. When compression is enabled for backup archives, the compressed archive time will increase by three times or more than the uncompressed case, and the data sorting time after recovery will increase by about three times or more than the uncompressed case. It is recommended to choose whether to compress according to the actual situation.
9. VMs from specified groups can be automatically added to a backup policy:

- This feature takes effect only when you create, clone, or import VMs on SCP. The backup policy does not change for original VMs in the group or when VMs are moved to other groups.
- A VM group can be added to the group list with only one backup policy.
- VMs of a tenant user are VMs in the default group of the tenant.

10. The backup in quiesced mode feature is available only to the following Windows operating systems.

Windows 7 32-bit/64-bit	Windows 8 32-bit/64-bit	Windows 10
Windows 11	Windows Server 2003 32-bit/64-bit	Windows Server 2008 32-bit/64-bit
Windows Server 2008 R2	Windows Server 2012	Windows Server 2016
Windows Server 2019	Windows Server 2022	

11. When the quiesced mode is enabled for a backup policy, if the target VM does not support this feature or fails to be quiesced, the backup will be created in non-quiesced mode and a description will be recorded in the

operation log file.

12. When backups are created in quiesced mode, consistency can be ensured for the NTFS and the applications that support this mode.
13. To ensure proper backup in quiesced mode, you need to verify the running status of the Windows services on which this feature depends to ensure that:

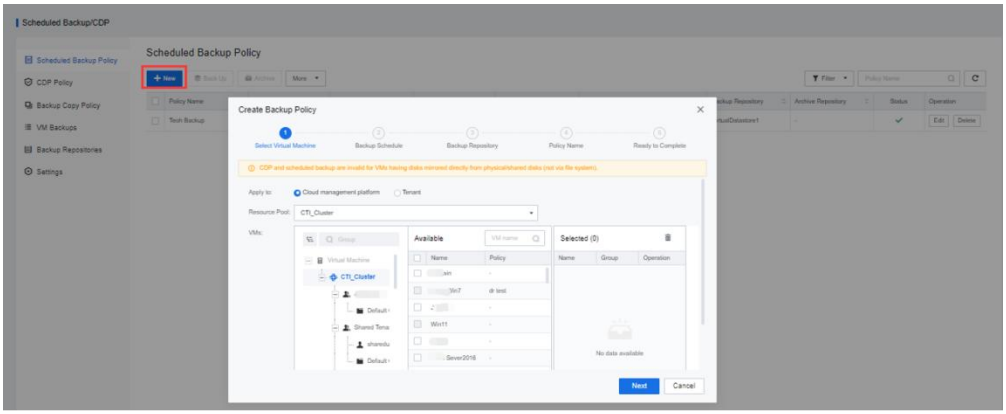
- The COM+ System Application service has been started, with the startup type set to **Manual**.
- The COM+ Event System service has been started, with the startup type set to **Automatic**.
- The Volume Shadow Copy service is not running, with the startup type set to **Manual**.

Prerequisite

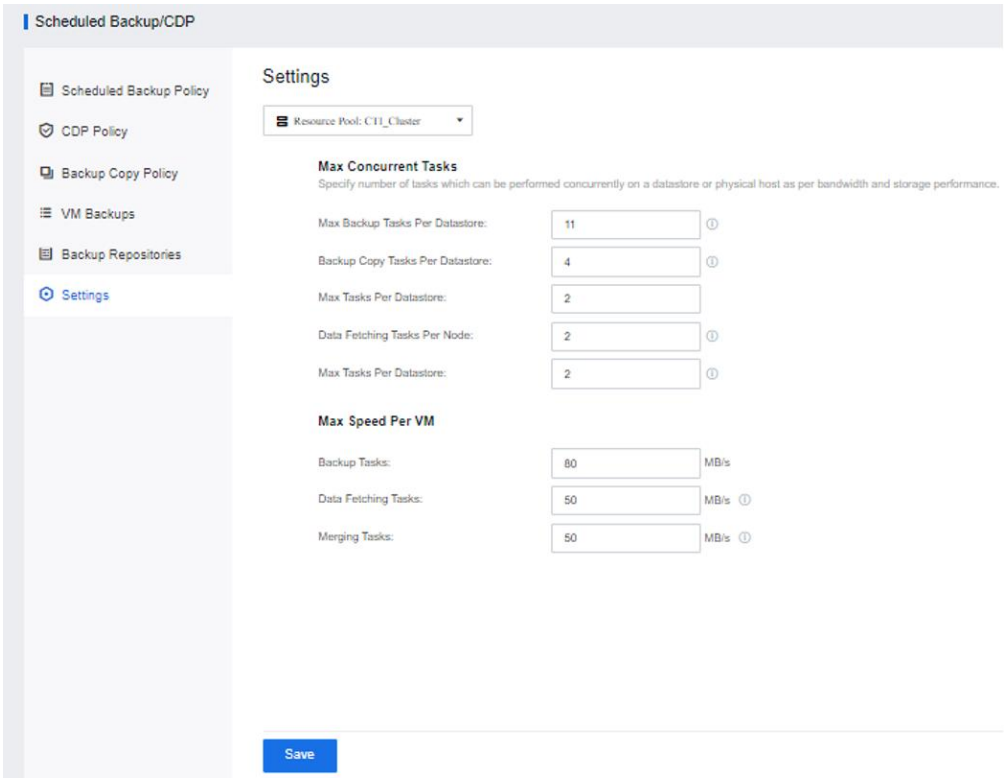
1. A third-party backup repository has been Backup Repositoryconfigured (it is recommended to configure a third-party backup repository).
2. When using the archive function, separate archive storage is required, and the archive needs to be added to the backup pool before configuring the archive. Windows shared folder, and the storage in the same repository as the backup repository cannot be selected for the archive storage.
3. Backup in quiesced mode is available for SCP 6.9.0 and later versions. Before enabling Quiesce Guest File System, you need to install vmTools for the VM, and the VM needs to be in the running status during backup.

Steps:

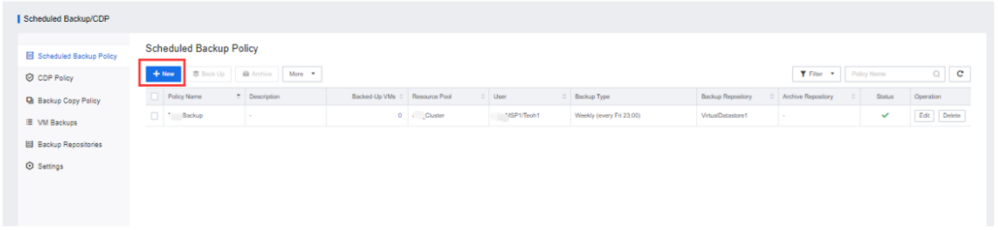
Step 1. Log in to the SCP platform, select **Disaster Recovery** > **Scheduled Backup/CDP**, and click **New** to add the planned backup repository to the backup repositories.



Step 2. Click **Settings** to limit the number of concurrent backups for the resource pool.

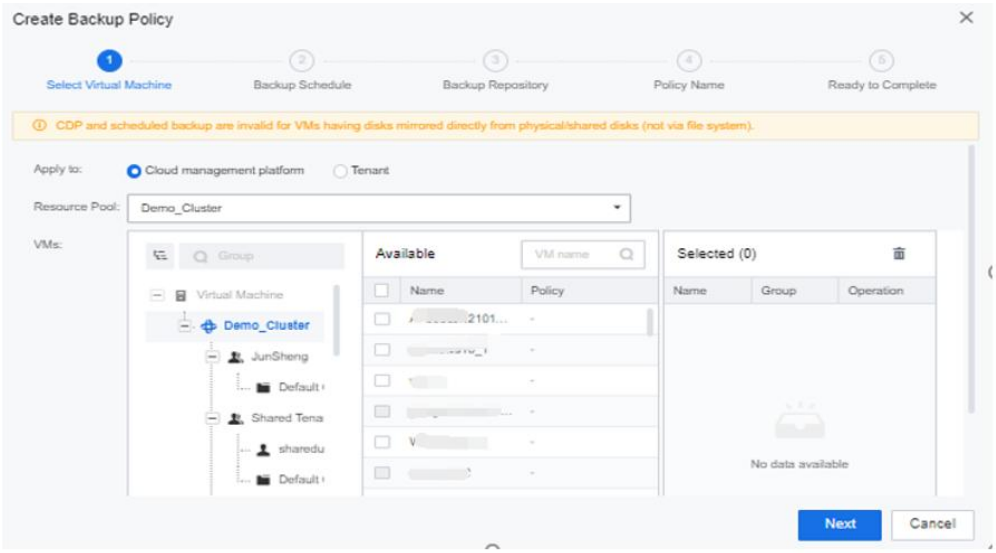


Step 3. Enter the **Scheduled Backup/CDP** interface and click **New** to add a new local backup policy.

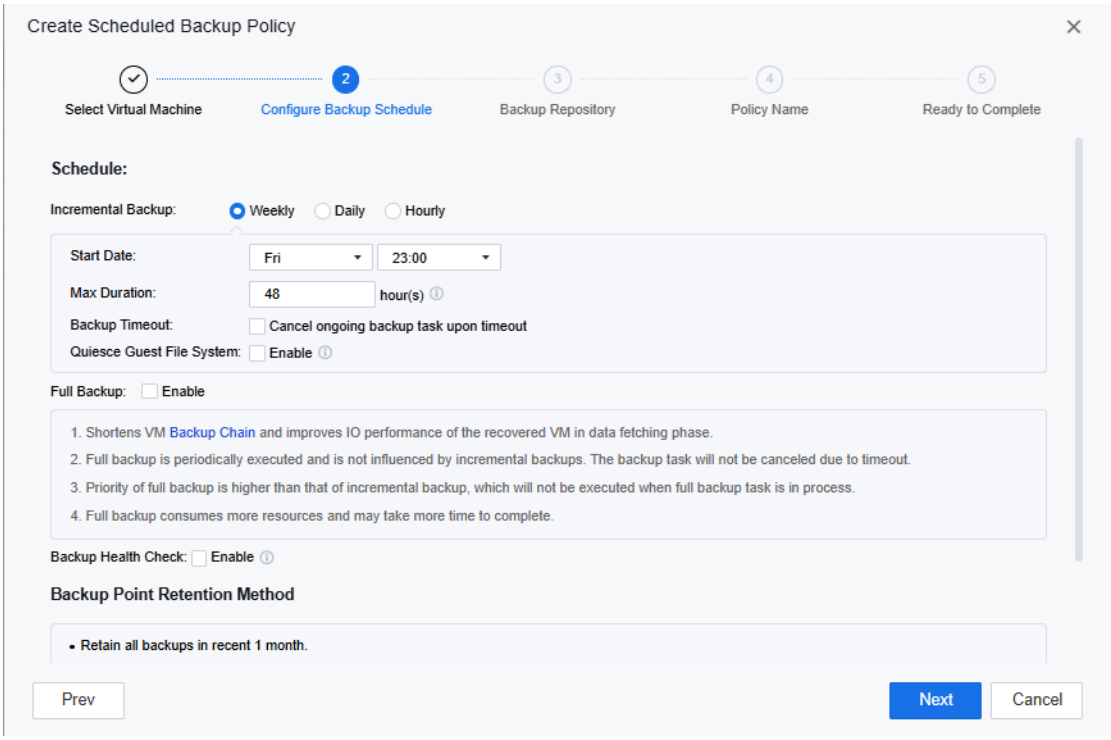


Step 4. Select the target resource pool, select the virtual machine to be backed up, and click **Next**.Or select Auto add VMs in specified groups as

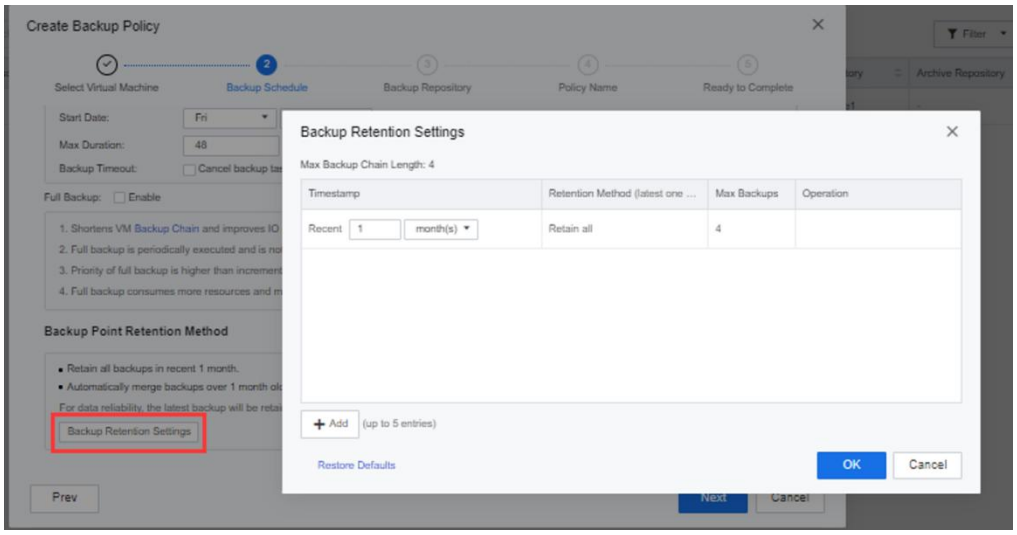
needed. If it is selected, newly created, cloned, and imported VMs in the group will be automatically added to the backup policy.



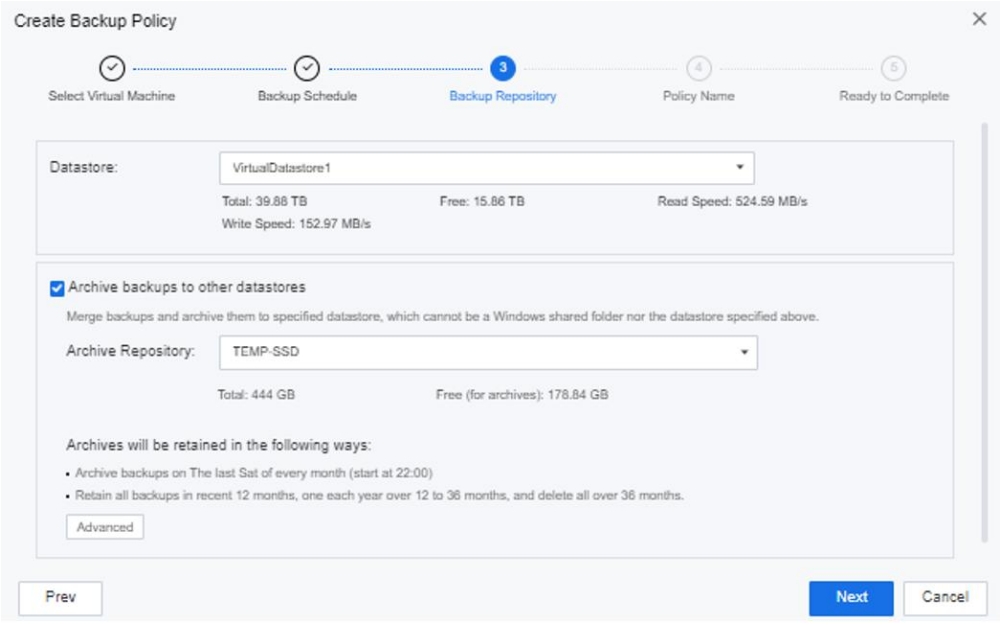
Step 5. Set the backup schedule, backup date, and duration. Choose to **Enable** the **Full Backup** according to actual needs.Or select Enable for Quiesce Guest File System as needed.



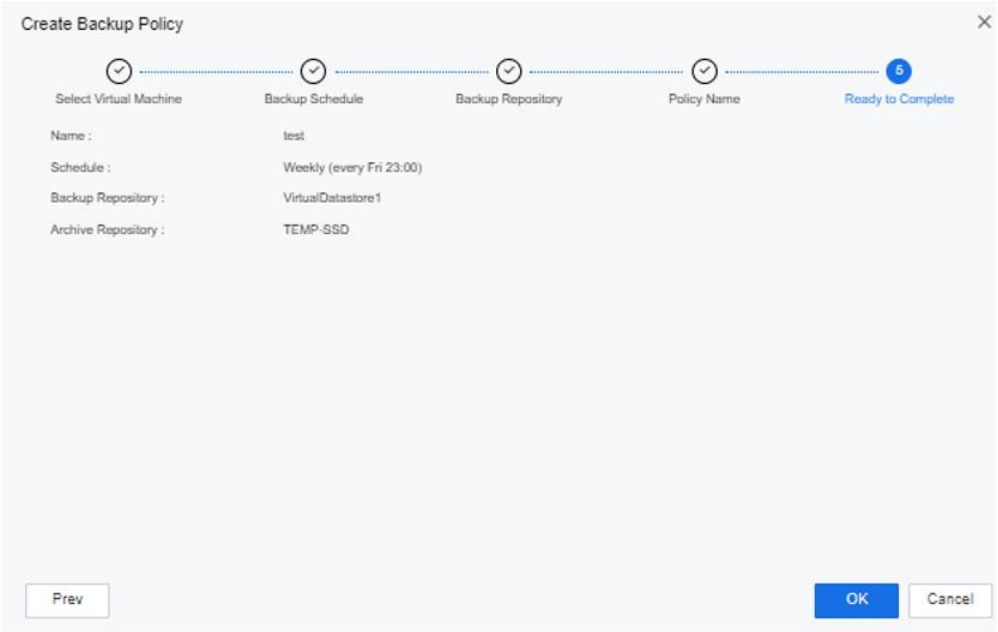
Step 6. Click **Backup Retention Settings** to manually set the backup retention mode as follows: keep all the backups of the last month, keep one backup per month for one month to six months, and keep backups over six months to two years. Keep one copy per year. Keep one copy per year.



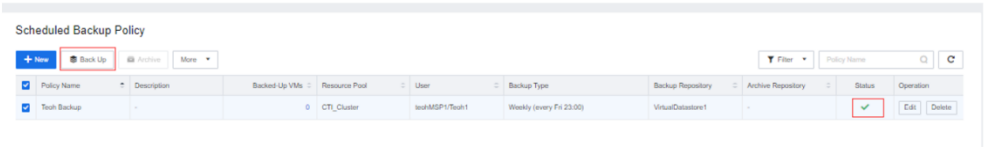
Step 7. Manually specify the backup repository, and choose virtual storage or external storage. Archiving is not allowed when there is only one backup datastore.



Step 8. Complete backup configuration.



Step 9. Select the created backup policy to enable, disable, and backup now.



Step 10. After the backup policy is added, you can see the backup virtual machine list and status on the **VM Backups** interface.

4.9.3.2 Backup Recovery

Function Description:

This task guides administrators in restoring backup files.

Precautions:

After restoring the virtual machine (whether it is a new one or overwriting the original virtual machine), the disk allocation mode changes to thin provisioning, which will lead to performance degradation. You can manually go to **Virtual Machine > More > Edit > Configuration > Storage** to adjust the disk settings to pre-allocation.

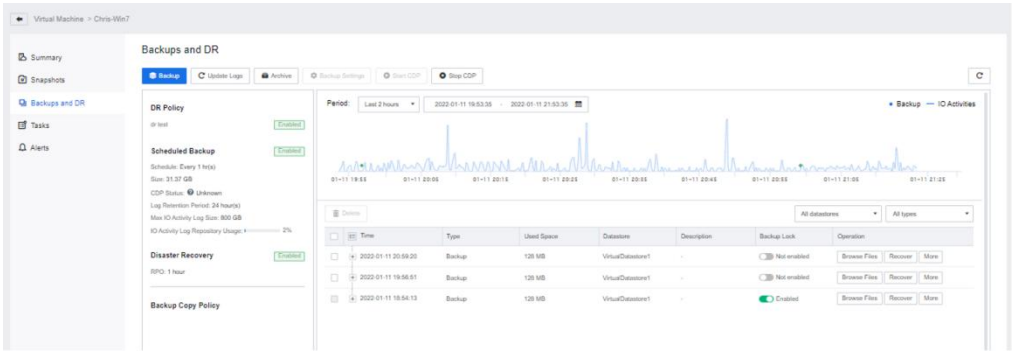
Prerequisite

1. The virtual machine that needs to restore the backup has backup files before the operation.
2. Manual recovery is not supported for backup files moved to the recycle bin.

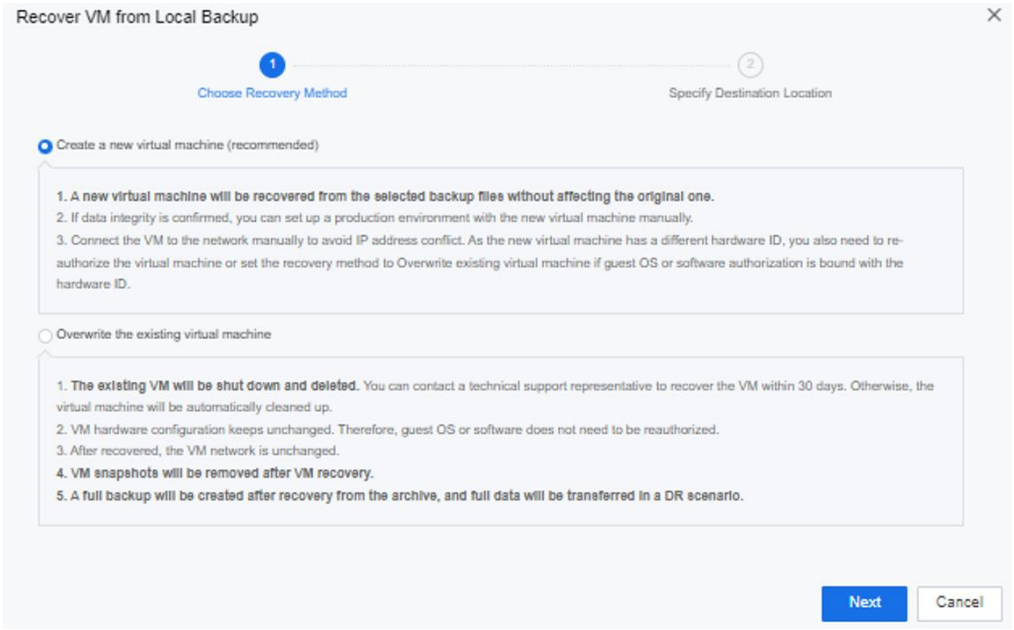
Steps:

Step 1. On the virtual machine page, click **More** in the virtual machine list, and then click **More** > **Backups**.

Step 2. Click **Backup and DR** to find the backup file of the virtual machine.



Step 3. Click **Restore** under **Operation** to restore the corresponding backup file. You can choose to **Create a new virtual machine** or **Overwrite the existing virtual machine**.



4.9.3.3 Backup Copy Policy

Function Description:

Provide backup replication policy services for the virtual machine and regularly replicate backups. Backups have copies on multiple storages to meet the data security requirements of some customers.

Precautions:

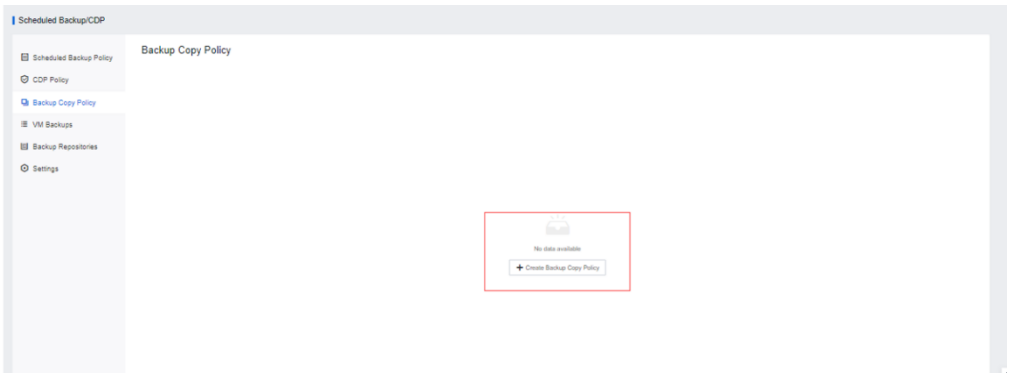
1. The destination storage for backup replication does not support local storage.
2. The source and destination storage of backup replication cannot be the same.
3. You can create multiple backup copy policies on multiple external datastores.

Prerequisite

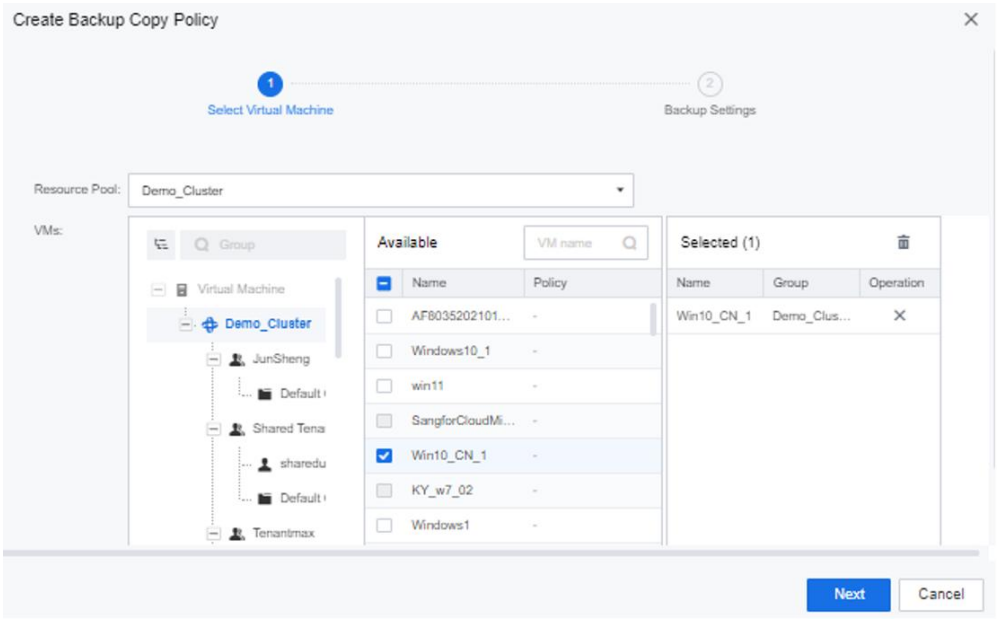
A local backup policy has been created for the virtual machine that needs to be backed up and replicated.

Steps:

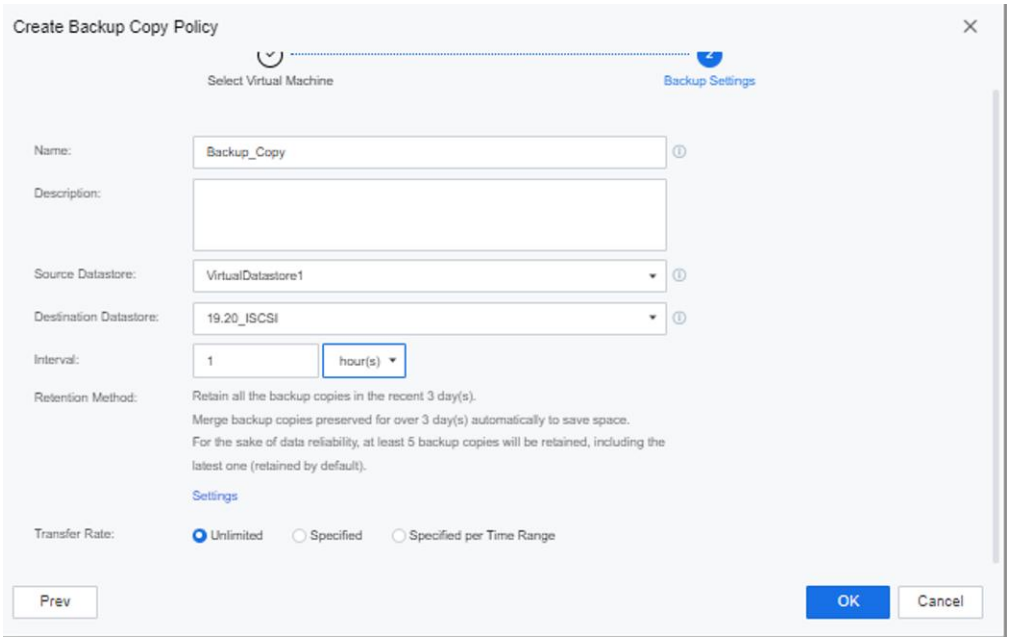
Step 1. Log in to the SCP platform, go to **Disaster Recovery** > **Scheduled Backup /CDP** > **Backup Copy Policy**, and click **New** to create a backup copy policy.



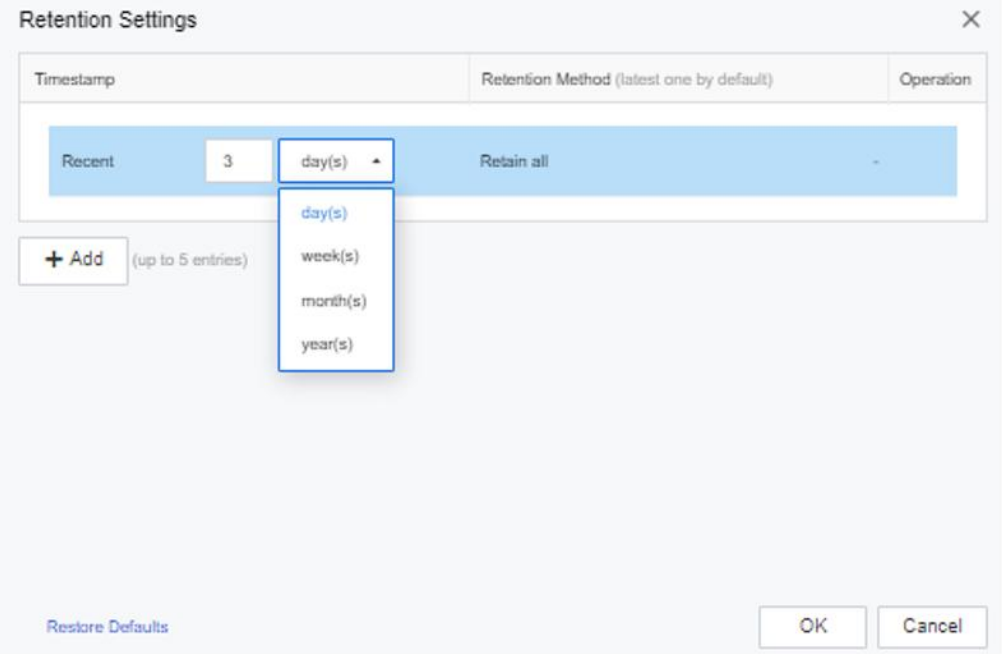
Step 2. Select the **Resource Pool**, select the **VMs** to which the backup replication policy needs to be added, and click **Next**.



Step 3. Select the **Source** and **Destination Datastore** and set the **Interval**. The backup replication frequency supports hourly or daily.



Step 4. You can manually set the backup retention mode, click the **Settings** button, and support setting the backup replication cycle by day, week, month, and year. Click the **Add** button to set up to 5-time plans. The last backup within the time plan will be retained by default if multiple time plans are added.



Step 5. Select whether to limit the data Transfer Rate according to the actual needs and click the **OK** button after the setting is complete.

Step 6. Select the created backup copy policy to Enable, Disable, and Copy now.

4.9.3.4 CDP

Function Description:

By distinguishing different service levels, provide CDP services for virtual machines and real-time data protection for businesses.

Precautions:

1. After the SCP manages the HCI resource pool, backup can only be performed on the SCP platform.
2. The formula for calculating the maximum space used by IO logs: Average write IO speed * 3600 (one hour and seconds) * retention time (hours) / 1024 = GB. For example, if the average writes IO speed of the business system is 10MB/s, the retention time is one day, and the interval is 1 hour, the maximum space used by the IO log is 10 * 3600 * 24 / 1024 = 844 GB.
3. CDP protection is not supported for raw disks mapped in the virtual machine.
4. Only the destination storage of CDP is supported to be configured on iSCSI,

FC, and aSAN.

5. Only NTFS and FAT32 file systems support file retrieval functions, and the Linux system does not support file retrieval operations.
6. Using the CDP function, if the backup and I/O logs are placed on the external storage because the I/O logs and backups occupy space, the I/O logs cannot be stored in time, and the I/O log buffer is exhausted, resulting in CDP interruption. Therefore, it is recommended not to place backups and logs in the same storage. Therefore, it is recommended not to place backups and logs in the same storage.
7. The backup in quiesced mode feature is available only to the following Windows operating systems.

Windows 7 32-bit/64-bit	Windows 8 32-bit/64-bit	Windows 10
Windows 11	Windows Server 2003 32-bit/64-bit	Windows Server 2008 32-bit/64-bit
Windows Server 2008 R2	Windows Server 2012	Windows Server 2016
Windows Server 2019	Windows Server 2022	

8. When the quiesced mode is enabled for a CDP policy, if the target VM does not support this feature or fails to be quiesced, the backup will be created in non-quiesced mode and a description will be recorded in the operation log file.
9. When backups are created in quiesced mode, consistency can be ensured for the NTFS and the applications that support this mode.
10. To ensure proper backup in quiesced mode, you need to verify the running status of the Windows services on which this feature depends to ensure that:

- The COM+ System Application service has been started, with the startup type set to **Manual**.
- The COM+ Event System service has been started, with the startup type set to **Automatic**.
- The Volume Shadow Copy service is not running, with the startup type set to **Manual**.

11. If the quiesced mode is enabled for the CDP policy, only CDP logs, but not

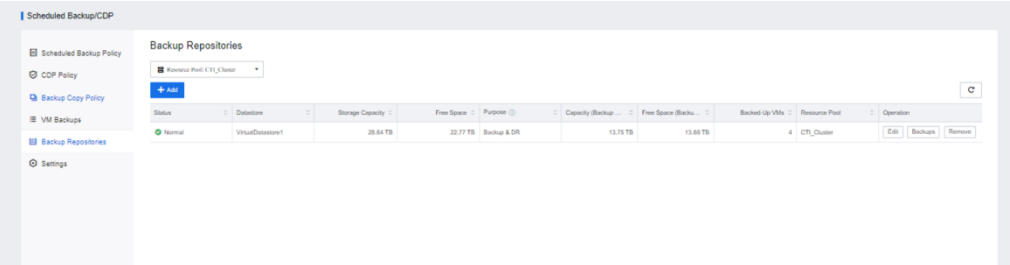
I/O logs, are backed up in quiesced mode.

Prerequisites

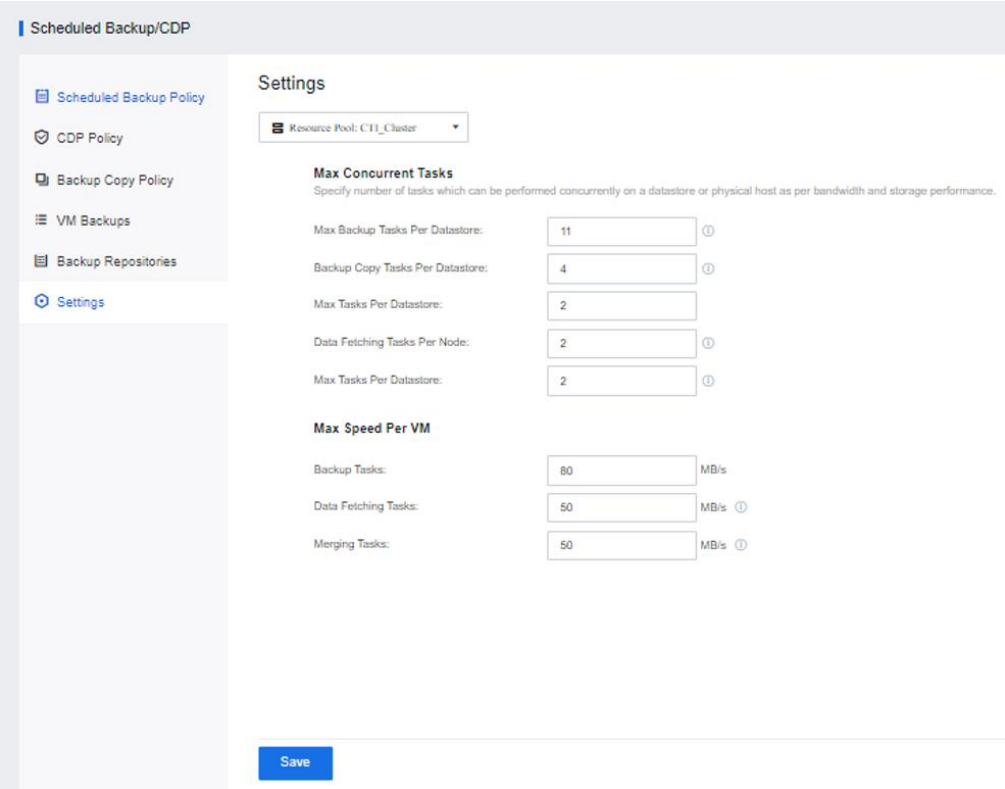
1. The backup datastore is added to the backup repository.
2. Backup in quiesced mode is available for SCP 6.9.0 and later versions. Before enabling Quiesce Guest File System, you need to install vmTools for the VM, and the VM needs to be in the running status during backup.

Steps:

Step 1. Log in to the SCP platform, select **Disaster Recovery** > **Scheduled Backup/CDP** > **Backup repositories**, and click **Add** to add the planned backup location to the backup repositories.

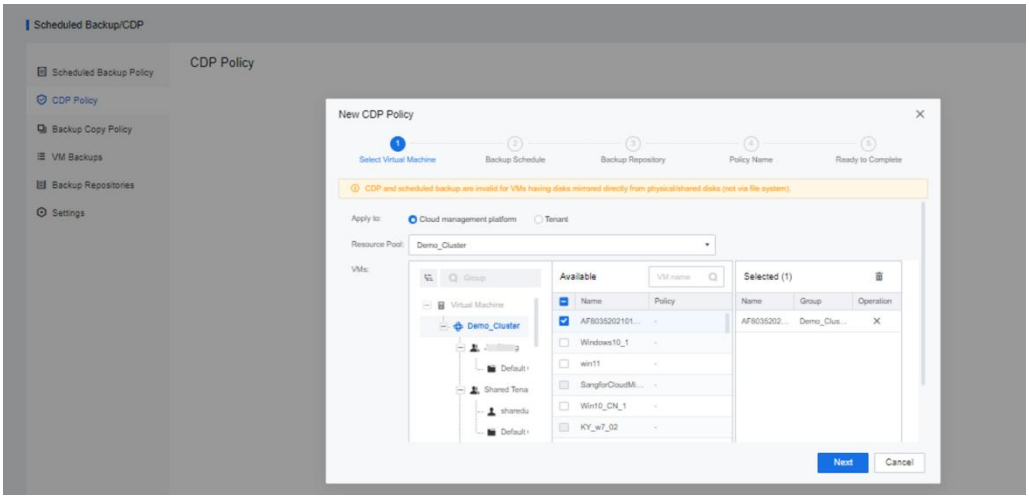


Step 2. Click **Settings** to limit the number of concurrent backups for the resource pool.

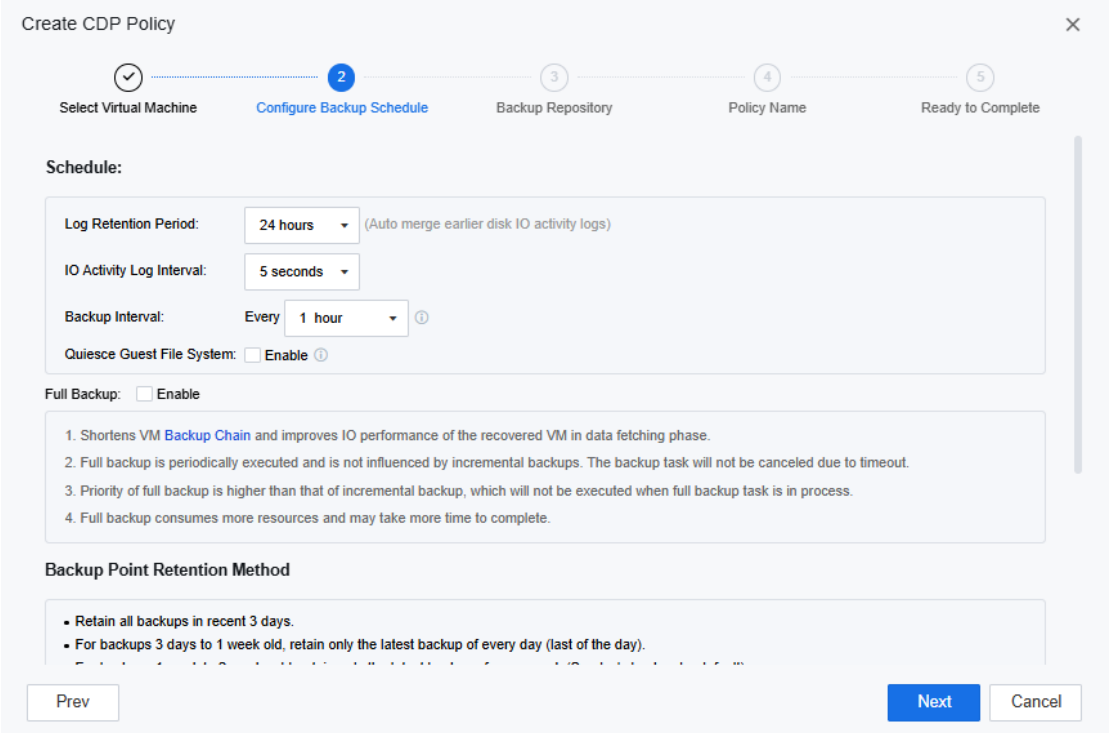


Step 3. Enter the **CDP Policy** interface, click **New**, and select the virtual

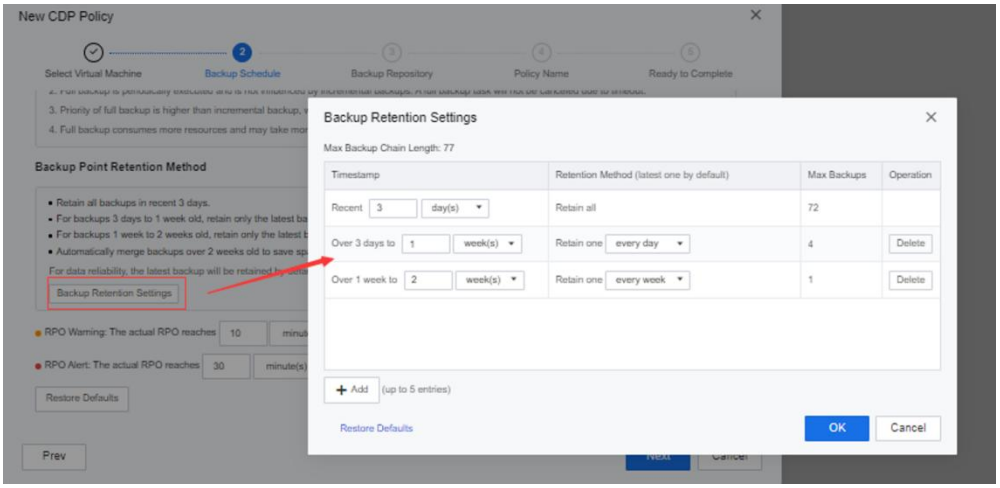
machine to be backed up.



Step 4. Configure the backup schedule, backup date, and duration. Then, select whether to check the **Enable** checkbox according to the actual needs to start a regular **Full Backup** or select **Enable** for **Quiesce Guest File System** as needed.



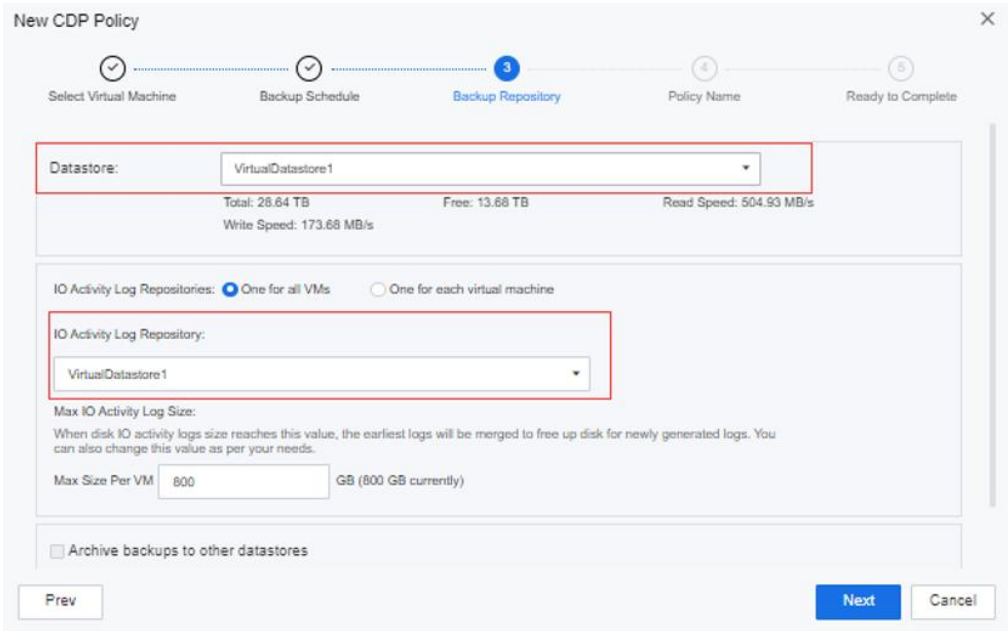
Step 5. Click **Backup Retention Settings** to manually set the backup retention mode as follows: keep all the backups of the last month, keep one backup per month for one month to six months, and keep backups over six months to two years. Keep one copy per year.



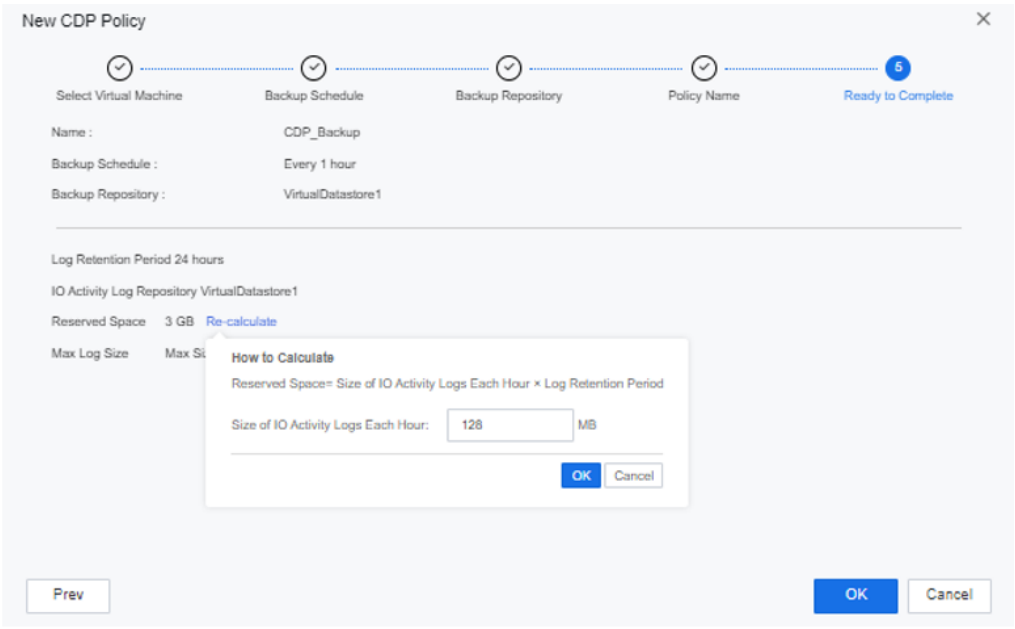
Step 6. Configure the early warning and alarm thresholds for RPO in CDP.



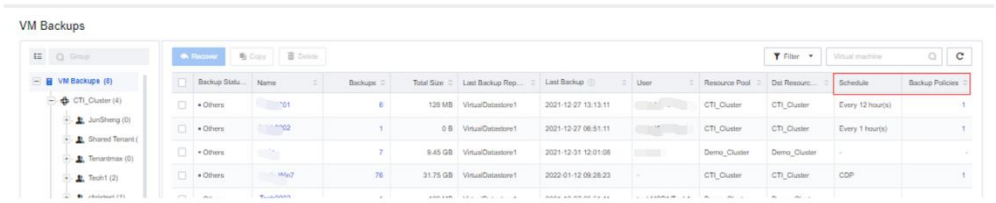
Step 7. Define the backup repository and IO Datastore for the CDP Policy.



Step 8. Complete the backup policy configuration. At this time, manually writing business increments will automatically calculate the estimated backup space.



Step 9. After the backup policy is added, you can see the backup virtual machine list and status on the **VM Backups** interface.



4.9.3.5 CDP Recovery

Function Description:

This task guides the administrator in restoring the backup file. CDP supports recording every IO of the business system and supports restoring to the business system state 5 seconds ago.

Precautions:

1. Support quick recovery of the virtual machines during backup and recovery.
2. After restoring the virtual machine (whether it is a new one or overwriting the original virtual machine), the disk allocation mode changes to thin provisioning, which will lead to performance degradation. You can manually go to **virtual machine** > **More** > **Edit** to adjust the settings to pre-allocation.

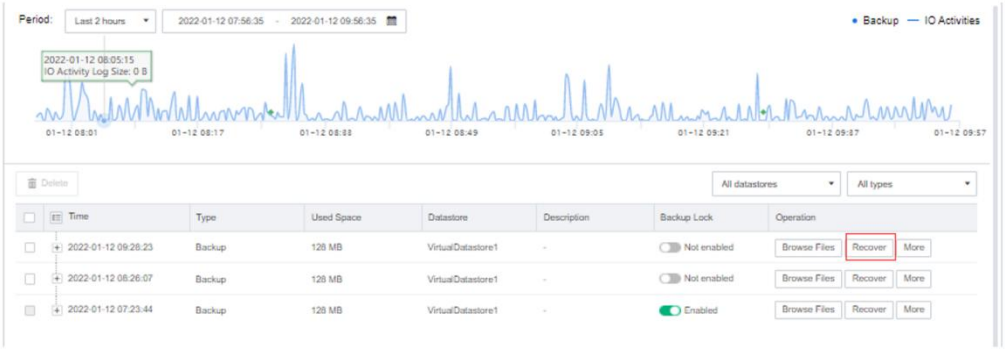
Prerequisite

The virtual machine that needs to be backed up has a CDP backup file.

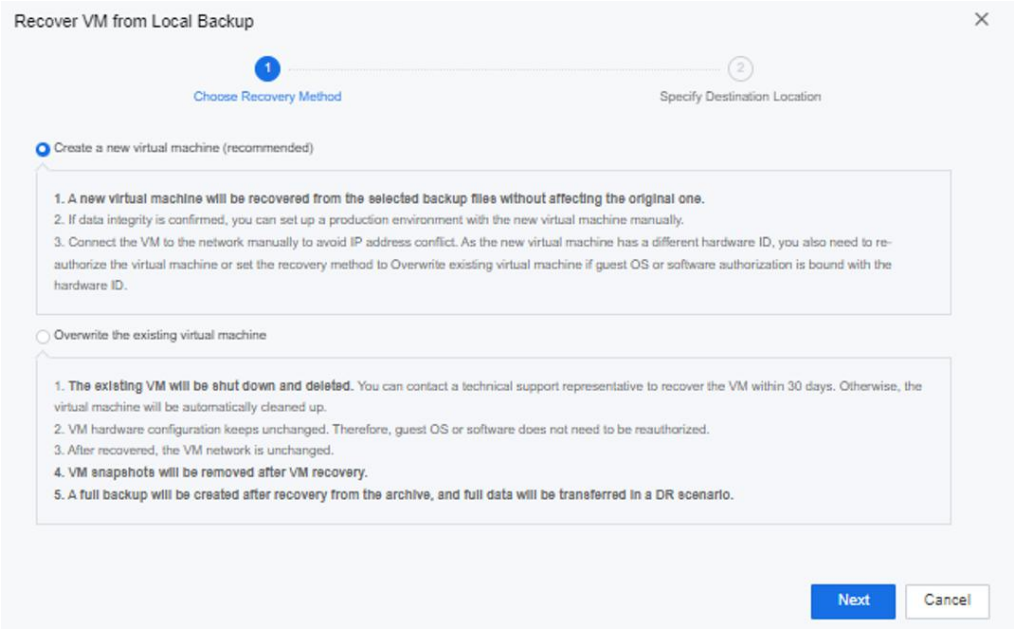
Steps:

Step 1. On the **Virtual Machine** page, click the virtual machine name in the virtual machine list and click **More** > **Backup**.

Step 2. Click **Backups and DR** to find the backup file point of the virtual machine, and click the arrow of the backup file point to see the recovery point.



Step 3. Click **Restore** under **Operation** to restore the corresponding backup file. You can choose to **Create a new virtual machine** or **Overwrite the existing virtual machine**.



4.9.3.6 Agentless Backup

Function Description:

By using the OpenAPI and disk data provided by Sangfor SCP and Sangfor HCI to access Sangfor Virtual Disk Development Kit (SFVDDK), third-party backup applications can configure VMs on SCP and their disks and manipulate disk

data to enable agentless VM backups and recovery, without installing plugins on SCP or VMs.

SFVDDK is a development kit consisting of SDKs and APIs written in the C programming language for accessing virtual disk files on SCP. Its APIs cover basic operations such as opening, closing, reading and writing to virtual disk files. SFVDDK accesses virtual disk data of VMs in LAN through Network Block Device (NBD) or NBDSSL protocols. The NBD protocol uses the storage on the remote host as a block device, and the NBDSSL protocol uses SSL to encrypt all the data transmitted through TCP with a high level of security.

SCP provides management of basic compute, network, and storage resources, including snapshots, backups, and other resources relevant to agentless backups, so that third-party users can standardize the management and operation and maintenance of SCP through existing APIs. The APIs are all Representational State Transfer (REST) APIs that can be called by HTTPS requests.

Precautions:

1. Agentless backup tasks have a lower priority than disaster recovery backup tasks and scheduled backup tasks of SCP and HCI. When there is an ongoing task with a higher priority, the agentless backup will be unavailable.
2. It is not supported to backup storage mounted on VMs, such as iSCSI, and NAS storage.
3. It is not supported to backup physical disks (including shared disks of Oracle RAC), USB disks of VMs.
4. This feature is not supported for VMs that have internal disk based snapshots.
5. It is not supported to backup component-based VMs, VM templates, NFV VMs, placeholder VMs, and VMs with Turbo mode enabled.
6. Up to 2 backup and recovery tasks can be concurrently executed per node, and up to 16 disks can be concurrently backed up and recovered per node. A datastore concurrently backs up and recovers 10 disks by default, and you can adjust it with **Max Tasks per Datastore** to meet the backup needs. Please configure the backup policy during off-peak hours.
7. It is recommended to manage agentless backups by a dedicated account

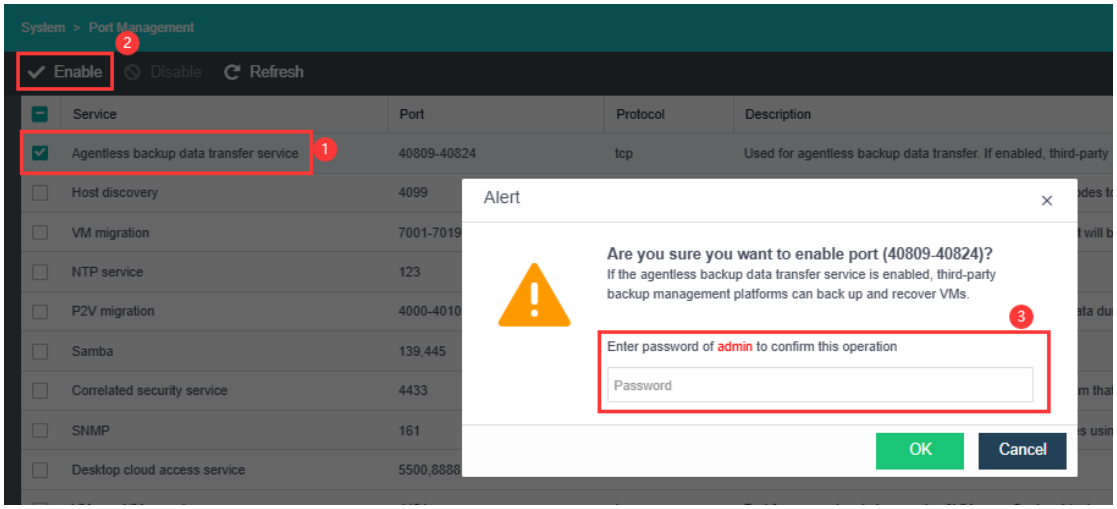
with necessary permissions. It is not recommended to use a super administrator account for security reasons.

Prerequisite:

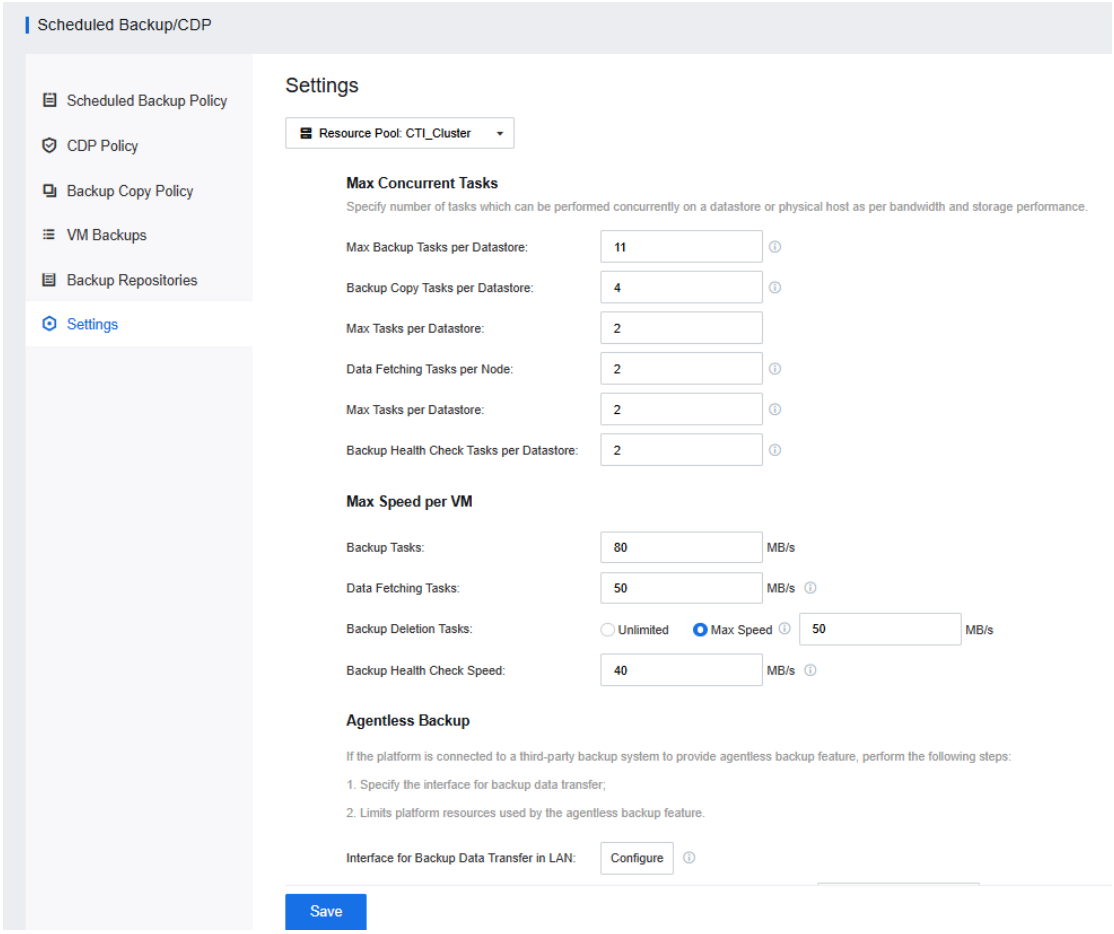
1. Only SCP 6.10.0 and higher and HCI 6.10.0 and higher support this feature.
2. The third-party backup application version supports being connected to SCP or HCI.

Steps:

Step 1. Log in to HCI, go to **System** > **Port Management**, check **Agentless backup data transfer service**, enter the admin password, and click **OK**.



Step 2. Log in to SCP, and go to **Disaster Recovery** > **Scheduled Backup/CDP** > **Settings** > **Interface for Backup Data Transfer in LAN** > **Configure** to configure a suitable backup data transmission interface (a dedicated interface is recommended).



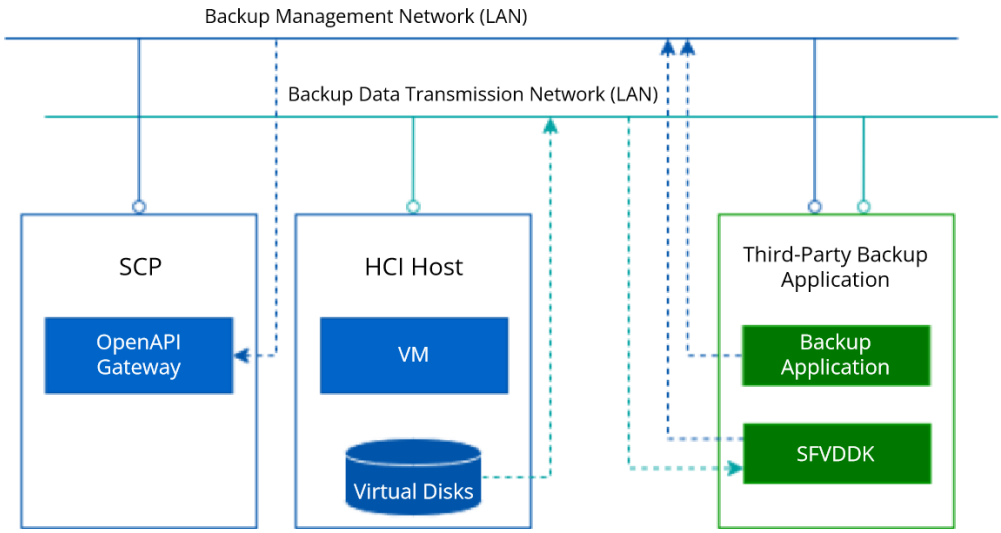
- **Interface for Backup Data Transfer in LAN**: Used for backup data transfer between a third-party backup system and the HCI node. The management interface is used by default. You can also select an idle interface or reuse other interfaces. The network connection between the backup data transfer interface and the third-party backup system must be normal; otherwise, backup tasks will fail.
- **Merging Speed for External Snapshot Deletion**: Used to configure a maximum merging speed for external snapshot deletion to reduce the impact of data merging on the VM services. Default value is recommended.
- **Transmission Speed per Node**: Used to configure a maximum network bandwidth for agentless backups. Other interfaces (such as management interface) of HCI nodes can be reused as the backup data transfer interface. If the maximum transmission speed is not specified, backup transfer may consume too many network resources, affecting the network performance of other services.

- **Data Transfer Speed per Backup Task**: Used to configure the maximum network bandwidth for agentless backups to read disks through SFVDDK, and here limits the data transfer speed for a single backup task. Default value is recommended.
- **Max Tasks per Datastore**: Used to configure the number of disks that can be concurrently backed up on a single datastore, and here limits the storage IO usage by agentless backups to reduce the impact of third-party backup applications on other services. You can configure this item as needed.

When deploying the network, make sure that third-party backup application can access HCI to connect to OpenAPI, and that the third-party backup application is connected to the backup data transmission interface of the HCI node for SFVDDK to access the VM disk data.

Prerequisites for Network Deployment:

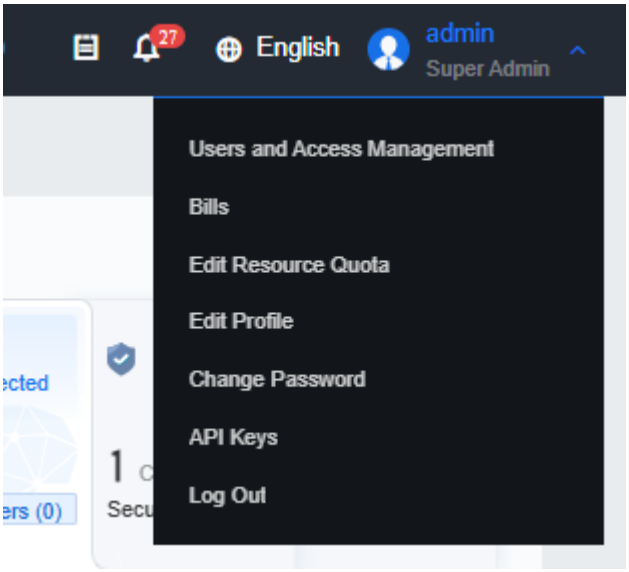
1. The third-party backup platform is connected to the management networks of SCP and HCI at layer 3.
2. The third-party backup platform is connected to the backup data transmission network of HCI at layer 3 without going through a NAT device.
3. If the third-party backup platform is not connected to the backup data transmission network, log in to HCI, and go to **Nodes** > **Physical Interfaces** > **Advanced** > **Other** > **Static Route** > **Add New Static Route** to configure a next-hop IP address for HCI.



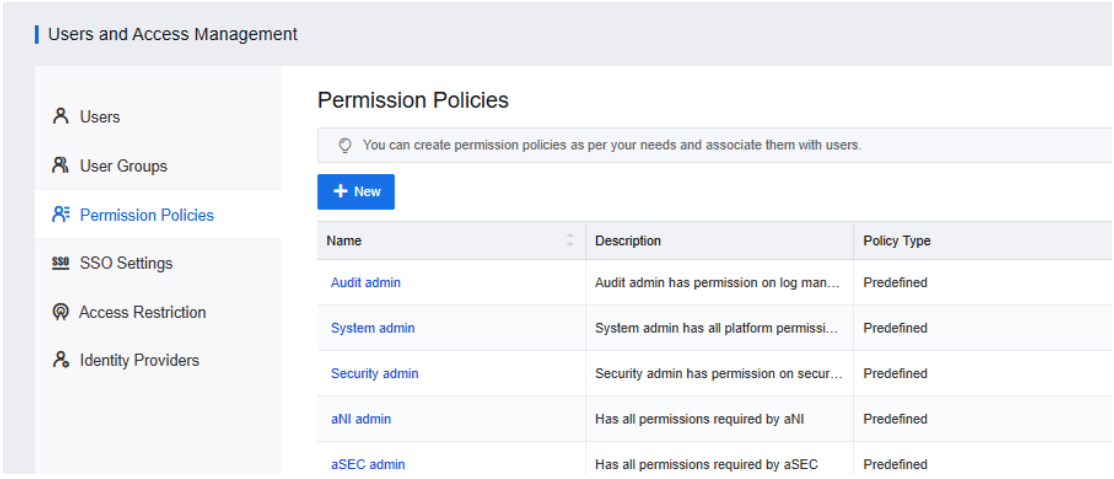
It is recommended to create an account and grant it with necessary permissions to manage agentless backups.

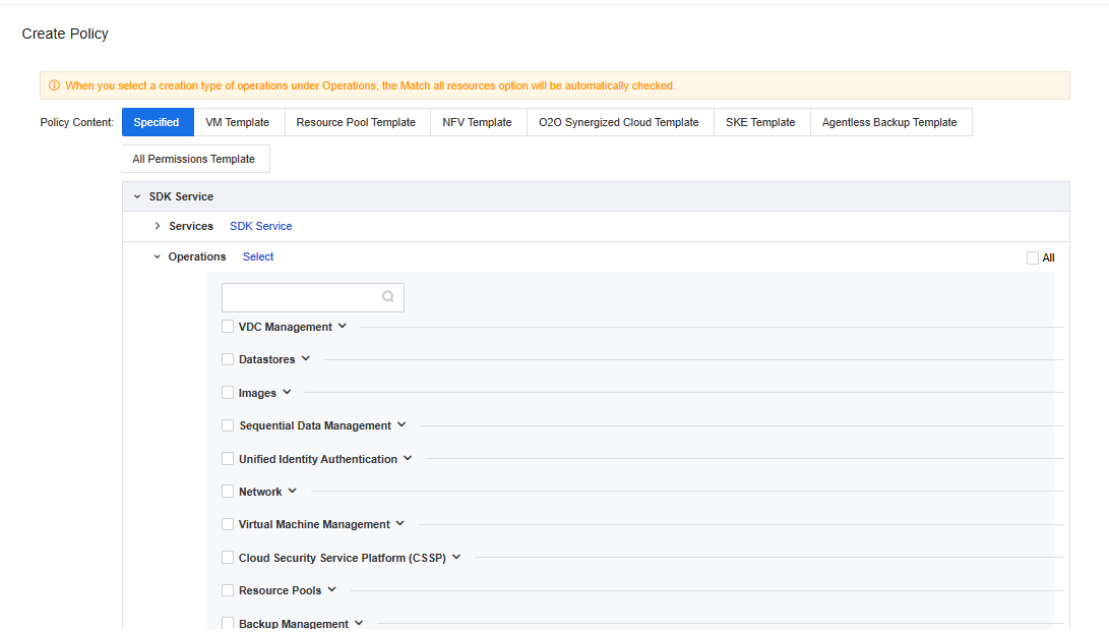
Steps for Account Creation:

Step 1. Click **admin** at the upper right corner on SCP, and then click **Users and Access Management**.



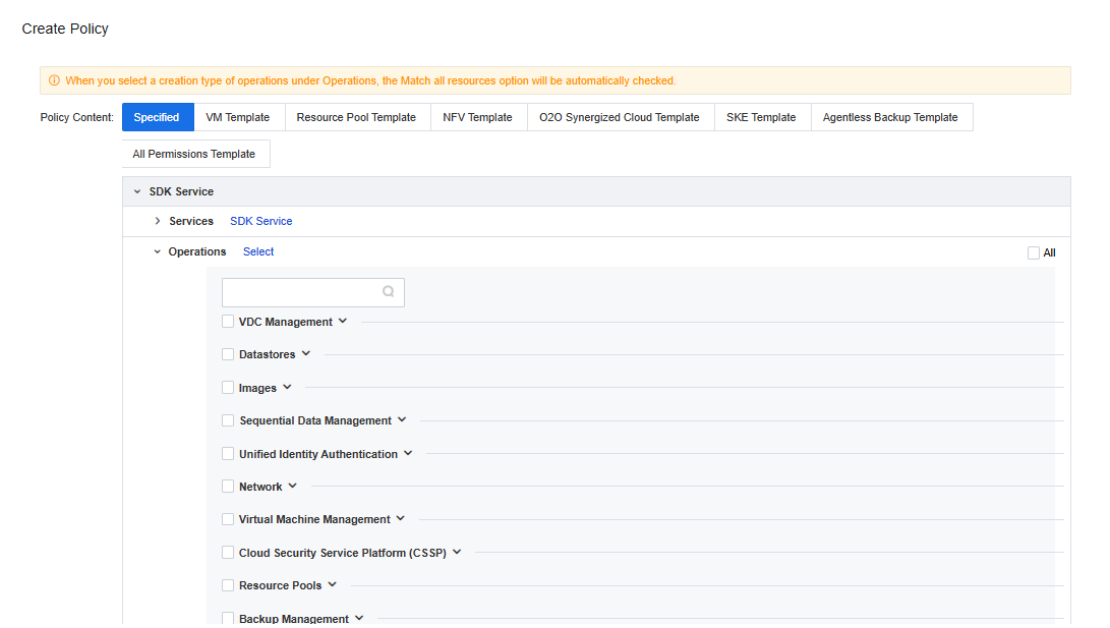
Step 2. Go to **Permission Policies** > **New** to create a permission policy for agentless backups. Go to **Policy Content** > **Services**, and select **SDK Service**.





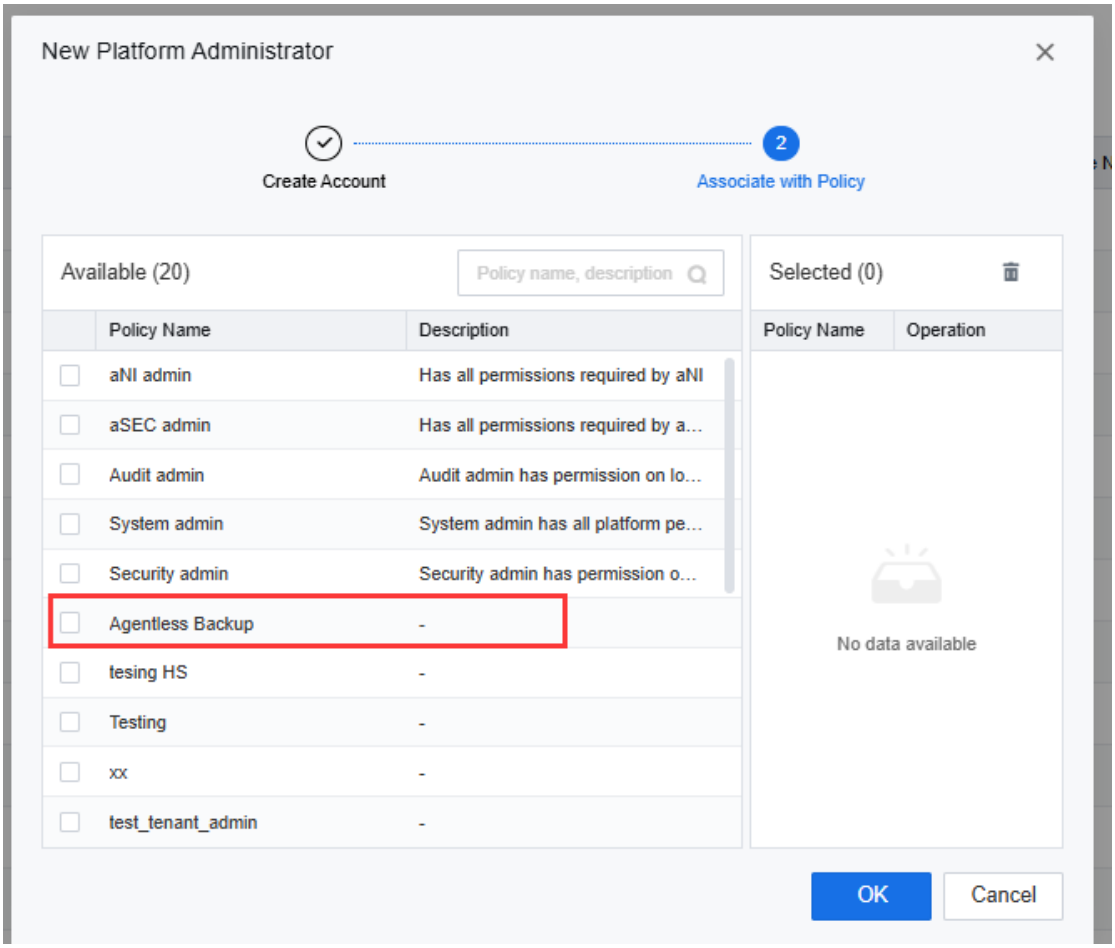
Step 3. Select at least the following operations for **Operations**:

- All operations of **Backup Resource Management**.
- Needed operations of **Virtual Machine Management**, such as **Create VM**, **Update VM**, **Start VM**, **Shut down VM**, **Restart VM**, **Allocate VM**, **Delete VM**, **Create VM snapshot**, **Obtain VM snapshot**, **Delete VM snapshot**, **Enable backup data merging for the "repidly-recovered VM"**, **Modify base image of VM disk, Create VM using configurations**, and **Edit VM configuration details**, etc.
- All operations of **VM CBT Management**.
- All operations of **Cluster File Management**.



Step 4. Remain **All** for **Resources** as default, specify the **Name** (e.g., Agentless Backup), and click **Finish**.

Step 5. Go to **Users and Access Management** > **Users** > **Platform Admins/Users** > **New** to create a platform administrator. Complete the basic information of the platform administrator, and associate the administrator with the permission policy created above.



NOTICE

Only platform administrators can manage agentless backups in SCP 6.10.0.

4.9.4 aDR (Cross-Site Disaster Recovery)

Function Description:

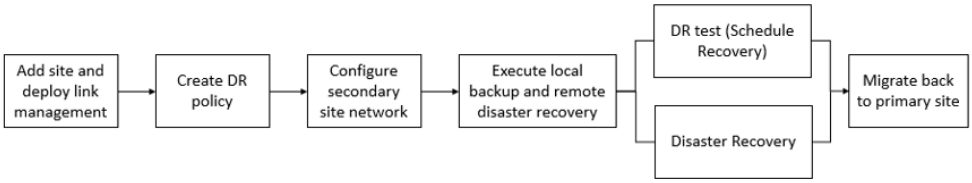
The Sangfor disaster recovery solution adopts the Scheduled **backup/aDR** solution, and both the primary and standby sites are Sangfor enterprise cloud platforms.

Provide common backup or CDP backup solutions locally, and back up the virtual machine to the primary site backup repository. When the virtual machine fails, the entire virtual machine can quickly recover from the local protection data. The best can achieve RPO=1s and RTO=2 minutes (when the customer's RPO requirement is at the second or minute level, the CDP backup solution is recommended. When the customer's RPO requirement is at the

hour level or more, the ordinary backup solution is recommended).

Provide virtual machine-level disaster recovery functions with different RPOs (minimum 1s) in different places. Based on local backup, the data of the primary site is asynchronously replicated to the secondary site. As a result, when the primary site fails, the virtual machine can be quickly pulled up at the secondary site. The minimum RTO is 10 minutes, significantly shortening the business interruption time.

The main configuration process of disaster recovery is shown in the following figure.



4.9.4.1.1 Add A Disaster Recovery Site

Function Description:

SCP supports multi-site DR and supports synchronization between the primary site and the secondary site. In this case, business can be quickly recovered from the secondary site when the primary site fails.

Precautions

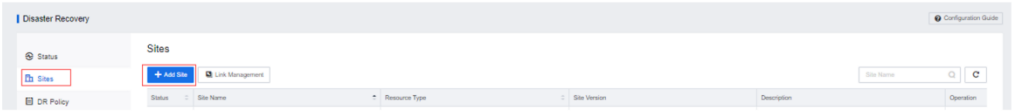
Ensure that the time of the HCI primary and secondary sites are in synchronization with that of SCP. We recommend that you deploy an NTP server.

Prerequisite

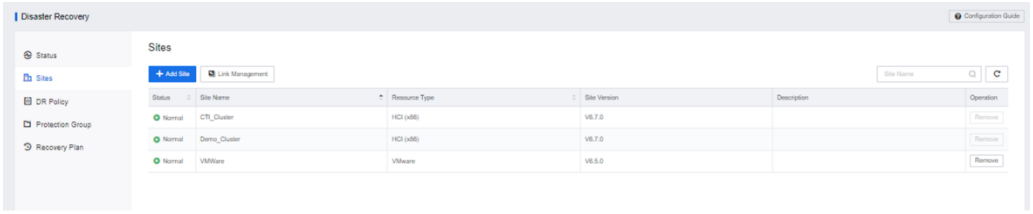
The primary and secondary DR sites have been added to the resource pool.

Steps:

Step 1. Go to **Disaster Recovery > Disaster Recovery > Sites** to add the resource pool as a disaster recovery site.



Step 2. The disaster recovery site is added successfully.



4.9.4.1.2 Add A Disaster Recovery Link

Function Description:

This section specifies the connection relationship of all sites through disaster recovery links and supports modification of transmission rates, disaster recovery interface, transmission encryption, and link alarms.

Precautions:

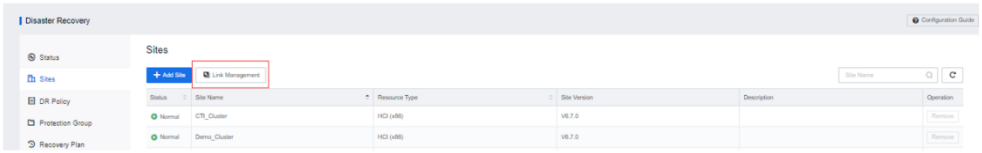
1. The time of the active and secondary sites and the SCP must be synchronized. It is recommended to deploy an NTP server.
2. Disaster recovery data transmission will take up a large amount of bandwidth. It is necessary to plan the disaster recovery interface separately. Reusing the disaster recovery interface with the management and service interfaces is not recommended.

Prerequisite

The DR primary and secondary sites have been added to the resource pool, and the DR site has been added successfully.

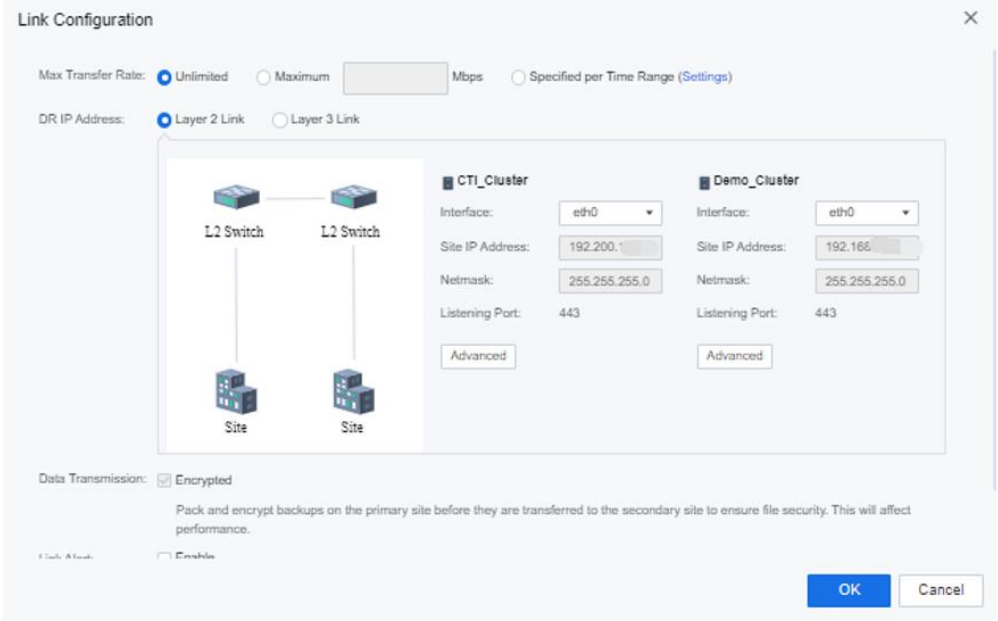
Steps:

Step 1. Go to **Disaster Recovery** > **Disaster Recovery** > **Sites** interface. Click **Link Management** to configure a DR link for the DR site.

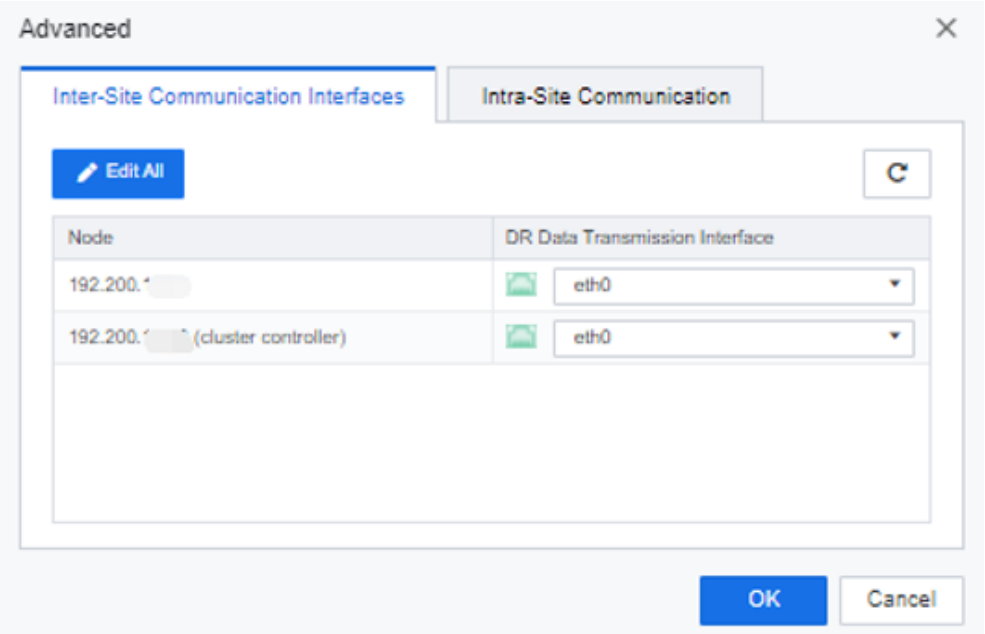


Step 2. Configure the link:

1. Configure the link transmission bandwidth limit, which can limit the disaster recovery bandwidth when the disaster recovery link is multiplexed.
2. When the primary and secondary sites are on the same network segment, select the **Layer 2 link.** When the primary and secondary sites are on different network segments, select **Layer 3 link**.
3. Select the disaster recovery communication interface for the primary and secondary sites, and the disaster recovery data is transmitted through the cluster controller of each site.
4. Click **Advanced** to configure the DR transmission interface of each node in the cluster.



Step 3. Click **Advanced** to configure the interface for the disaster recovery link. **Inter-Site Communication Interfaces** refer to the interface that transmits disaster recovery data when the node acts as the cluster controller.

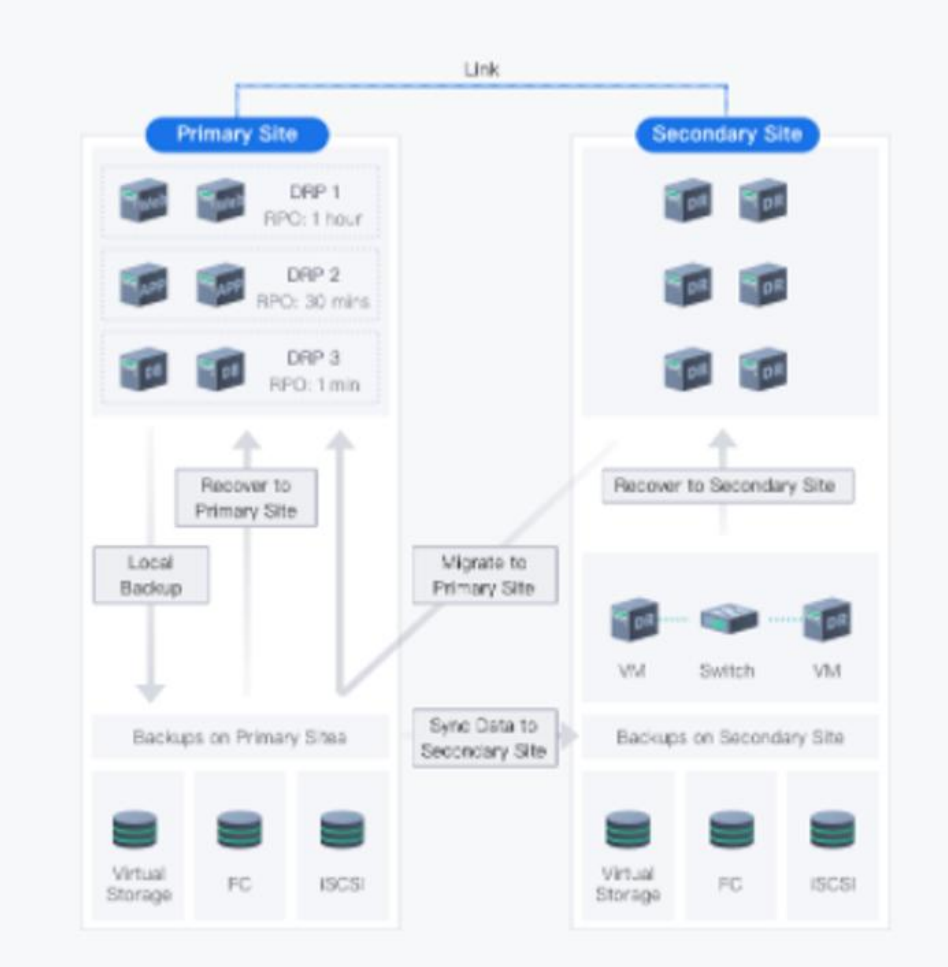


Step 4. **Intra-Site Communication Interfaces** refer to the interfaces through which the non-active node in the cluster transmits disaster recovery data to the cluster controller.

4.9.4.1.3 Configure The Disaster Recovery Policy

Function Description:

It supports setting disaster recovery strategies for virtual machines and configuring parameters such as backup schedule and transmission frequency. It also supports setting disaster recovery strategies for virtual machines with different RPO requirements, such as WEB systems, application systems, and database systems, to meet the needs of data-tiered protection.



Precautions:

1. It is forbidden to use file storage to save CDP IO log files.
2. The IO log files and disaster recovery data of the standby site are stored in the same storage.
3. The backup in quiesced mode feature is available only to the following Windows operating systems.

Windows 7 32-bit/64-bit	Windows 8 32-bit/64-bit	Windows 10
Windows 11	Windows Server 2003 32-bit/64-bit	Windows Server 2008 32-bit/64-bit
Windows Server 2008 R2	Windows Server 2012	Windows Server 2016
Windows Server 2019	Windows Server 2022	

4. When the quiesced mode is enabled for a DR policy, if the target VM does not support this feature or fails to be quiesced, the backup will be created in non-quiesced mode and a description will be recorded in the operation

log file.

5. When backups are created in quiesced mode, consistency can be ensured for the NTFS and the applications that support this mode.
6. To ensure proper backup in quiesced mode, you need to verify the running status of the Windows services on which this feature depends to ensure that:

a. The COM+ System Application service has been started, with the startup type set to **Manual**.

b. The COM+ Event System service has been started, with the startup type set to **Automatic**.

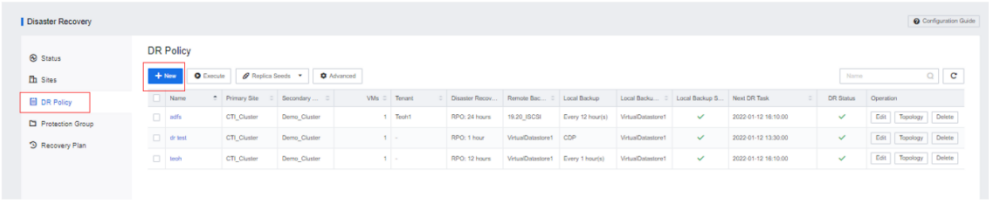
c. The Volume Shadow Copy service is not running, with the startup type set to **Manual**.

Prerequisite

1. The backup repositories of the primary and secondary sites have been planned and configured.
2. The DR site and DR link have been successfully configured.
3. Backup in quiesced mode is available for SCP 6.9.0 and later versions. Before enabling Quiesce Guest File System, you need to install vmTools for the VM, and the VM needs to be in the running status during backup.

Steps:

Step 1. Enter the **Disaster Recovery** > **Disaster Recovery > DR Policy** and click the **New** button.

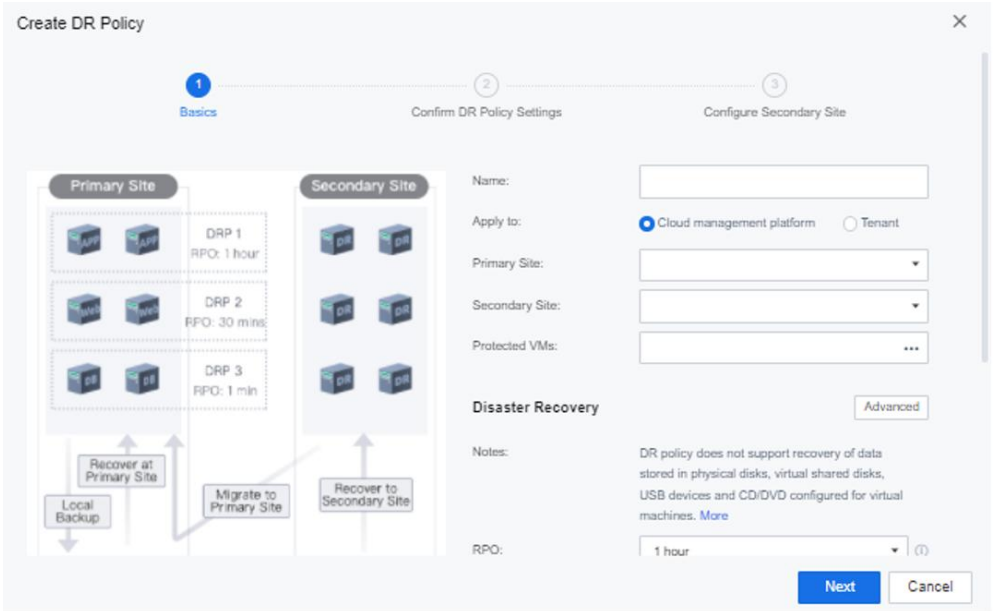


Step 2. Configure the disaster recovery policy:

1. Configure a name for the disaster recovery policy.
2. Select the applicable scope.
3. Select the primary disaster recovery site.
4. Select the primary disaster recovery site.
5. Select the protected virtual machine, which is the virtual machine that needs

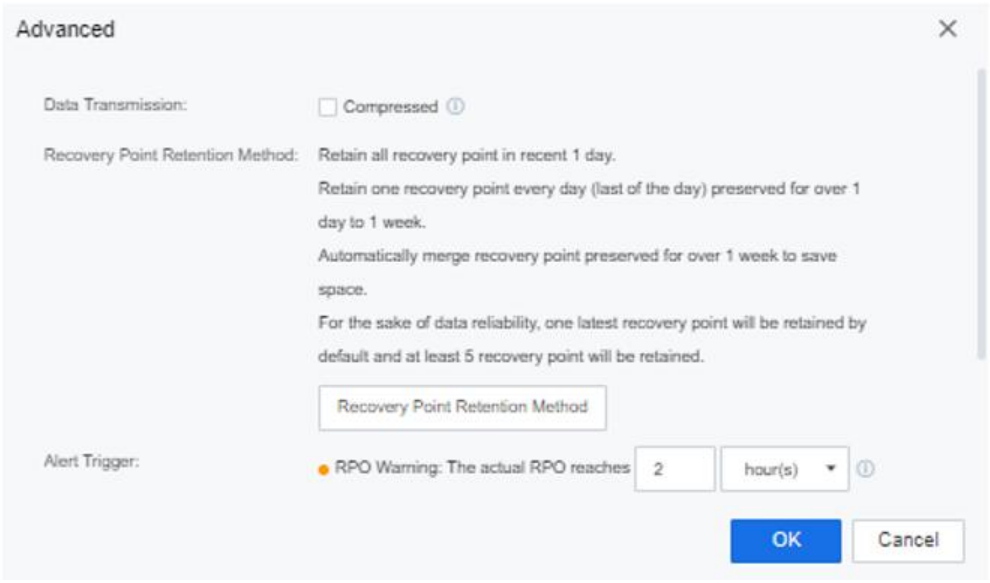
disaster recovery.

6. Set the Disaster Recovery **RPO.** **RPO** refers to the acceptable amount of data loss when the application goes down. The more important the data, the higher the frequency of data backup and synchronization, and the shorter the RPO time, which will have higher pressure on the production environment and network.
7. Configure the off-site disaster recovery location, usually select the backup repositories of the disaster recovery site.
8. Configure the local backup mode. The local backup interval must be less than the configured disaster recovery RPO. When the disaster recovery RPO is less than or equal to 1 hour, the local backup mode can only be selected for continuous data protection (second-level CDP).
9. Select the primary site backup location.
10. When the local backup method is Continuous Data Protection (CDP), you need to select the repository for the IO log files. It is recommended to select the second storage, and a virtual repository is allowed.Select **Enable** for **Quiesce Guest File System** as needed.





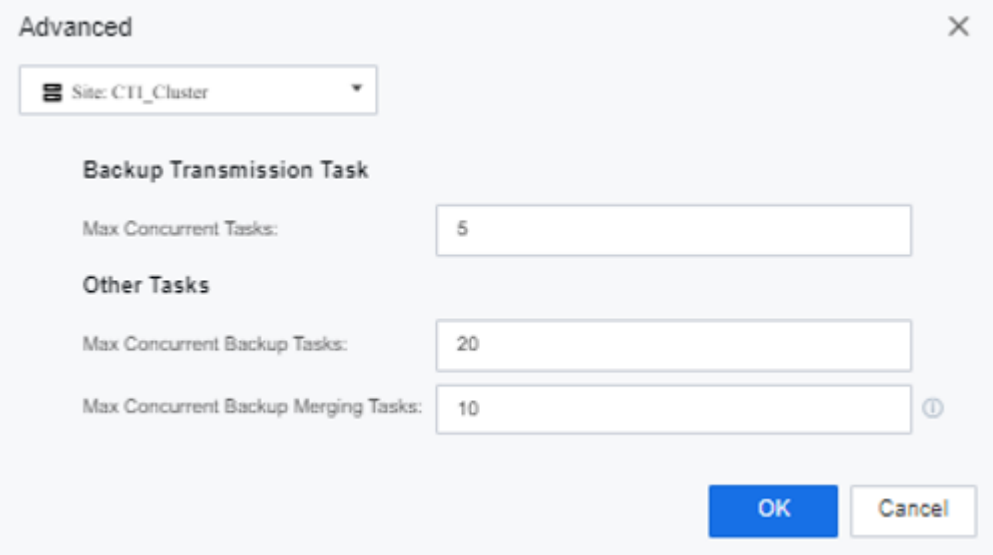
Step 3. Click **Advanced** of the **Disaster Recovery** to configure whether to compress the transmission, the recovery point retention mode and the alarm threshold for the disaster recovery policy.



Step 4. Create different disaster recovery policies for the different VM groups according to the required RPO. After the disaster recovery policy is configured, you can select the disaster recovery policy and click **Execute** to complete the first data backup and disaster recovery transmission. Or use the **Replica Seed** function to export the full data of the virtual machine at the primary site and import it to the secondary site through the manual transmission to complete the first data backup and disaster recovery transmission. After completing the configuration, click the green button to enable or disable the disaster recovery policy.

Step 5. On the **Advanced** Settings page, it is possible to configure DR limits for different resource pools. The number of concurrent backup transmission tasks is the number of concurrent data transfers from the primary site to the standby site.

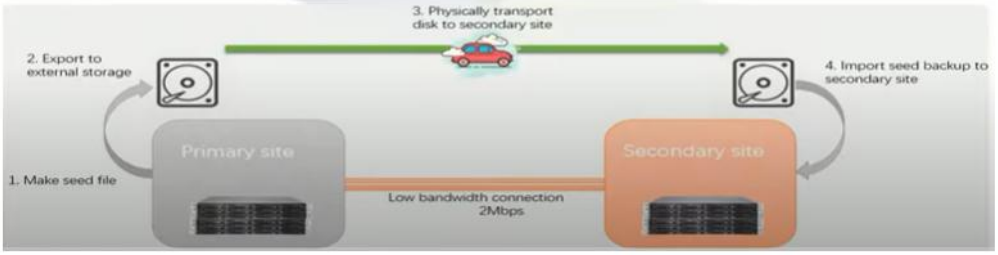
Number of concurrent tasks: The number of concurrent backups and merge tasks is the number of concurrent tasks that can be performed at the same time when multiple VM trigger a backup and merge task.



4.9.4.1.4 Replica Seed

Function Description:

After creating a disaster recovery policy, you can export and save the full backup of the virtual machine to a disk (such as a mobile hard disk, mechanical disk, low-capacity NAS, etc.) through a seed file and transport it to the disaster recovery site to complete the initial replication of the virtual machine. For subsequent data sync, transferring the full backup is unnecessary. Only the incremental data based on the seed backup can be transferred.



Precautions:

1. When the disaster recovery project is implemented for the first time, if the amount of data is particularly large (such as 100TB level), it is often impossible to provide a disk with sufficient capacity. At this time, it is not recommended to use a seed file. You can choose to deploy the hyper-convergence of the disaster recovery site at the primary site. Configure the disaster recovery task and complete the first disaster recovery replication through the local network (Gigabit or 10 Gigabit). Then manually stop the disaster recovery task, move the hyper-converged devices at the disaster recovery site to the disaster recovery site for storage, and then enable the disaster recovery task again for subsequent incremental data replication.
2. The hard disk will be formatted as the sffs file system during the mounting process for the hard disk used to make the seed file. Please backup the data on the hard disk in advance to avoid data loss.
3. Before creating a replica seed, please disable the relevant disaster recovery policy to avoid triggering the backup transfer and affecting the import of the replica seed file.
4. After inserting the USB device, HCI will recognize and prompt to configure the USB. Since the disk is not for the use of VMs, there is no need to configure a USB. Just close the prompt.
5. Since the seed file is used for initial replication, the disaster recovery site must have no backup file of the protected virtual machine. Therefore, before importing the seed file, it is recommended to delete the backup file corresponding to the occupied virtual machine on the disaster recovery site HCI.
6. 6. Exporting a seed file consists of two operations: Creating a seed backup file and exporting a seed file. The backup speed can be limited as needed to avoid affecting business. The backup rate of the primary site virtual machine can be limited in SCP **Disaster Recovery** > **Scheduled Backup /CDP** > **Settings**.
7. For virtual machines with small capacities (such as less than 1TB), when creating and exporting seed files, SSD disks can be used to save replica seeds, which helps improve the export speed. For an HDD disk with a capacity of 8TB (inserted into the server panel as local storage), the rate of

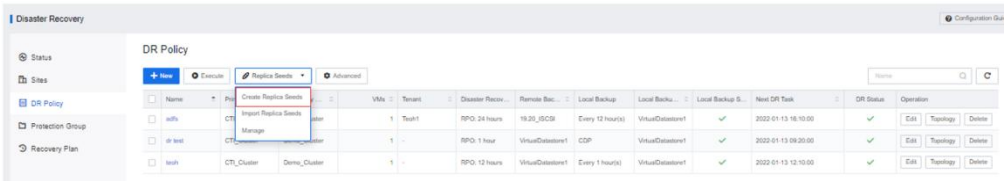
exporting torrent files is about 100MB/s, and the rate of importing replica seeds to the secondary site is about 50MB/s (the values are for reference only).

Prerequisite

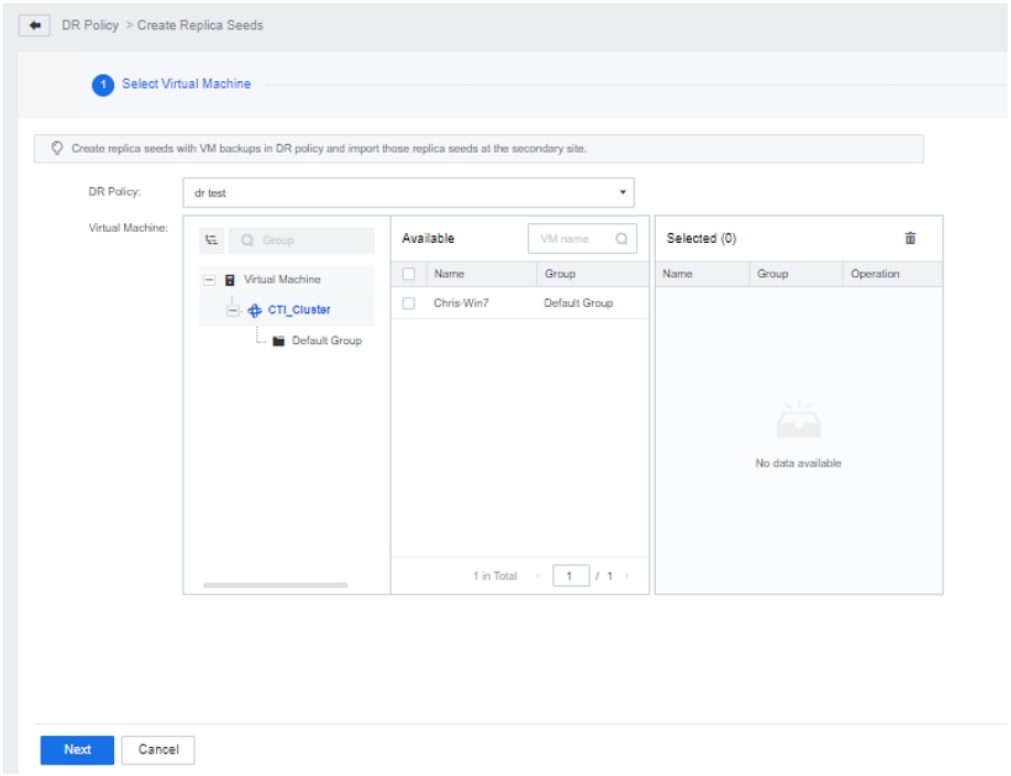
1. When the bandwidth of the disaster recovery link is small, the amount of full backup data is relatively large, and the network replication time is much longer than the physical transportation, it is recommended to use the seed file method.
2. Prepare removable storage media with suitable capacity and backup data.
3. Stop the related disaster recovery task on the SCP and delete the backup file corresponding to the occupied virtual machine on the disaster recovery site HCI.
4.

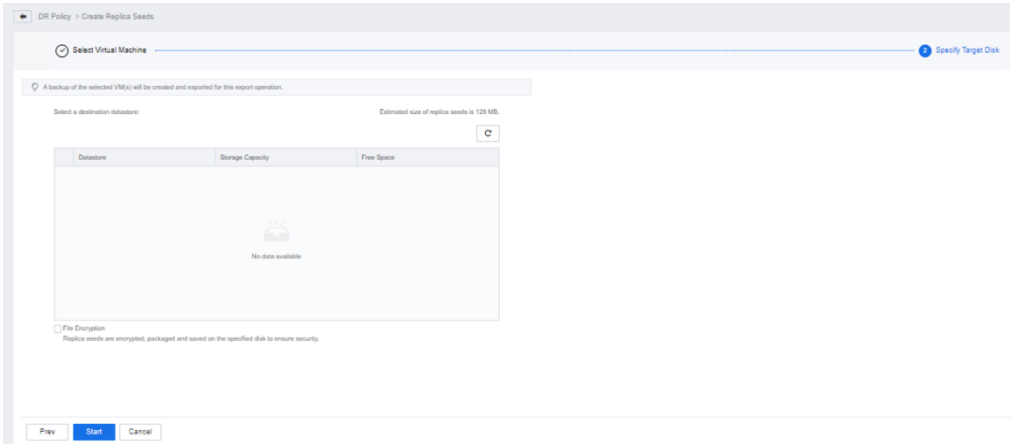
Steps:

Step 1. Connect the medium used to transmit seed files to the HCI platform of the primary site, navigate to **Disaster Recovery > DR Policy**, and click **Replica Seeds** > **Create Replica Seeds**.



Step 2. Select a disaster recovery policy and click **Next**.





Step 3. Select the export destination datastore as the transmission medium of the replica seed file and check the **File Encryption** checkbox to encrypt and pack the replica seed file and save it to the specified hard disk to ensure the security of the file. Exporting the replica seed file will perform a backup on the virtual machine and then export it and will not affect the original backup chain.

Step 4. Click **Start** to enter the export process.

4.9.4.1.5 Add Protection Group

Function Description:

The virtual machine in multiple disaster recovery policies is supported to form

a protected group. Add WEB1, APP1, and DB1 to the protected group 1. You can perform drills on different RPO virtual machines in protected group 1. Migrate and restore actions. It supports manually configuring the priority order according to the dependencies of the virtual machine in the protection group to ensure that the business can be started. At the same time, it supports configuring the priority for multiple protection groups and guarantees the vital business first during the recovery.



Precautions:

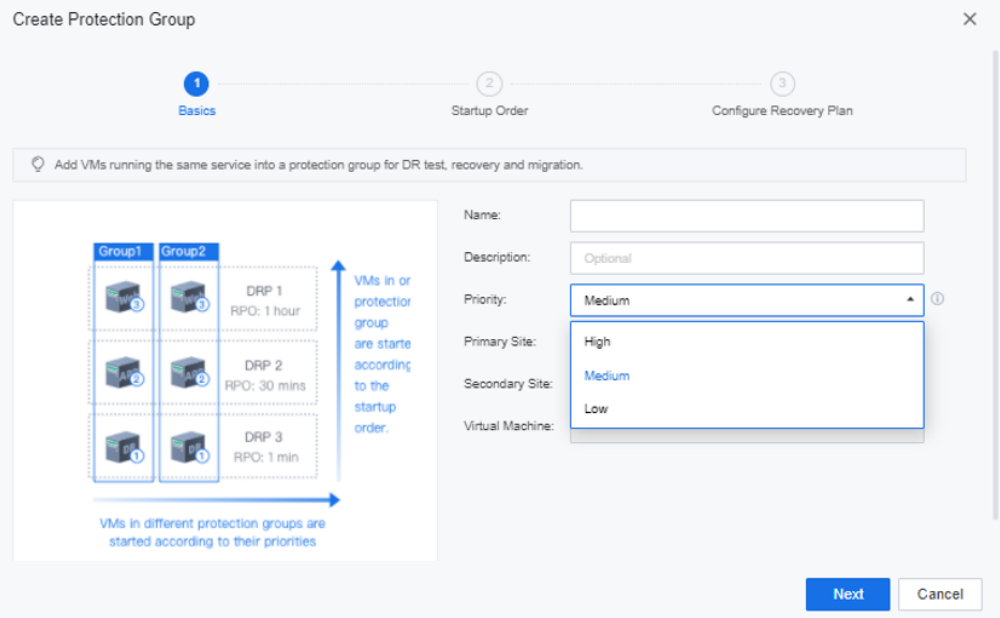
None.

Prerequisite

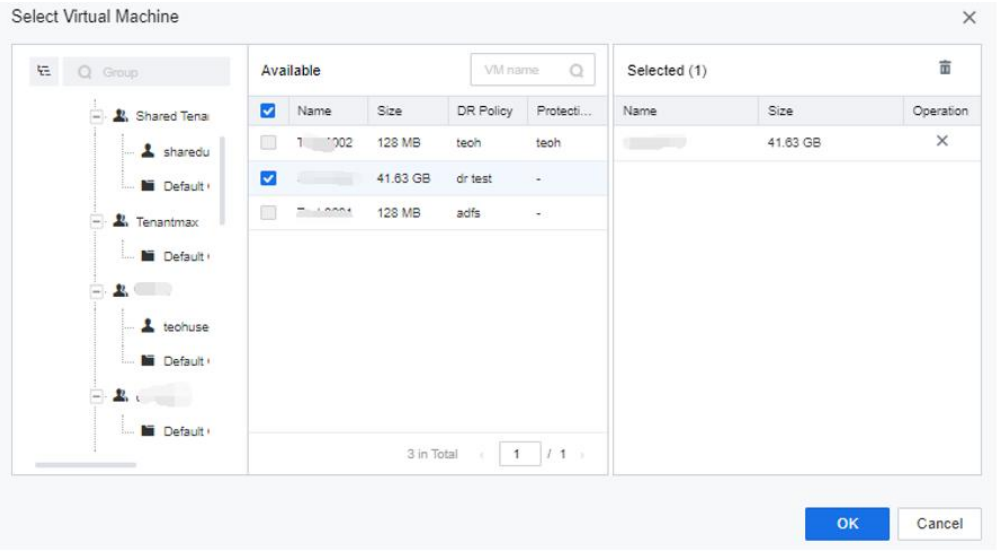
The disaster recovery policy has been successfully created, and the disaster recovery virtual machine has been added.

Steps:

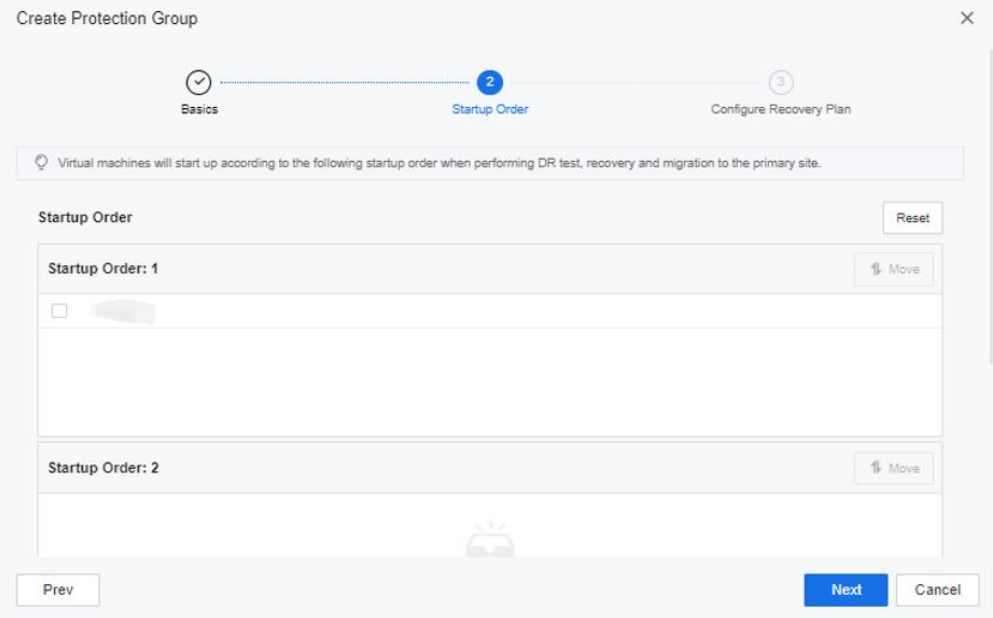
Step 1. Enter the **Disaster Recovery** > **Disaster Recovery** > **Protected Group** interface and click the **New** button to create a protection group. Select the importance level for the group. The group with a higher priority can perform tasks such as backup, data transfer, recovery, drill, and relocation.



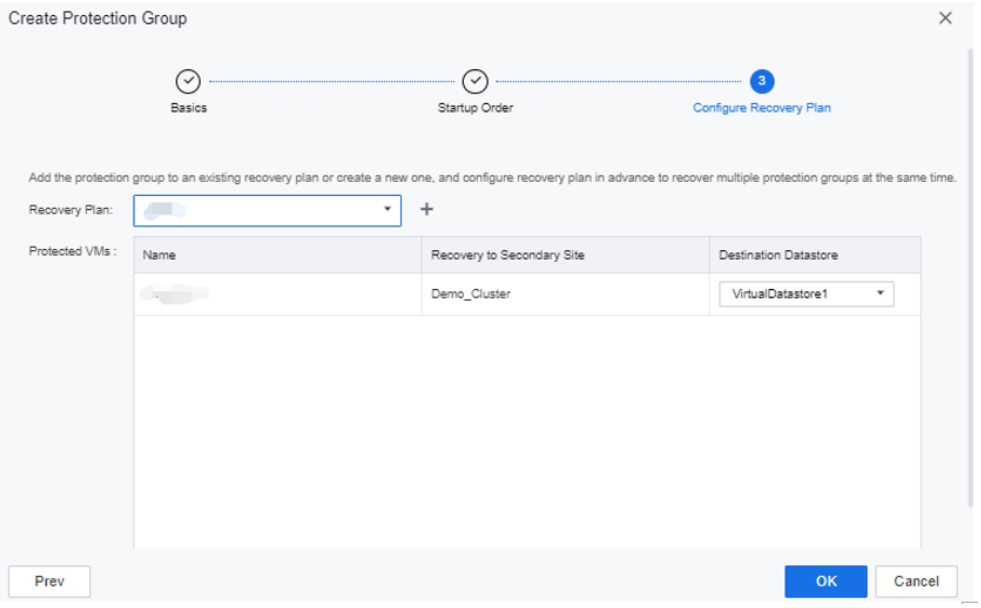
Step 2. Configure the virtual machine and add the virtual machine of the same business group to the disaster recovery business group 1.



Step 3. Configure the boot sequence in the group and select a safe boot sequence according to the business architecture logic. For example, start the database virtual machine first and the OA and APP application virtual machine after the waiting time.



Step 4. You can choose to add a group to an existing or newly created recovery plan, allowing multiple protection groups to perform disaster recovery drills, data transmission, and disaster recovery relocation operations at the same time.



Step 5. The protection group configuration is complete.

4.9.4.1.6 Recovery Plan

Function Description:

Create a recovery plan for the disaster recovery virtual machine. When multiple services need to be drilled, multiple protection groups can be added to the

same recovery plan, and the recovery plan can be drilled, restored, and relocated. The group will prioritize the recovery and retrieving actions for businesses with high priority.



Precautions:

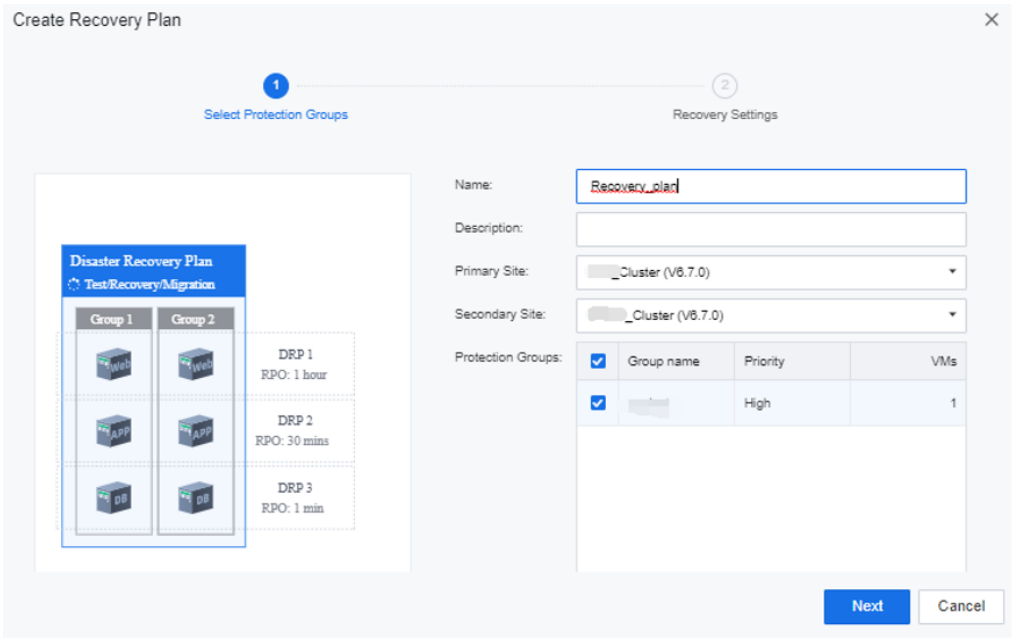
1. When the virtual machine is restored, the power on sequence takes effect only for the virtual machine with the vmTools installed.
2. A protection group supports only one recovery plan.

Prerequisite

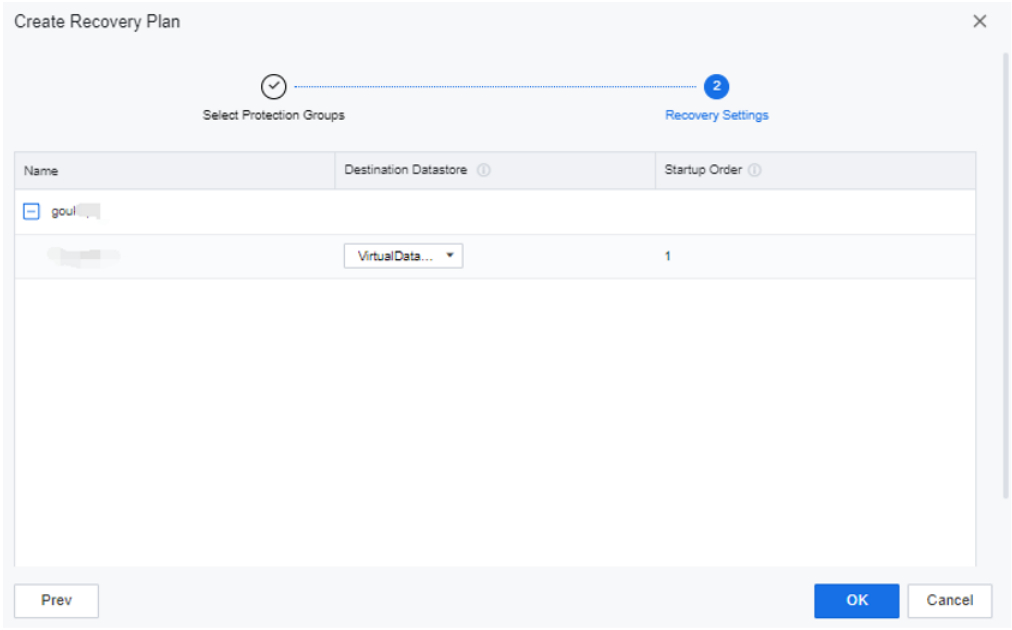
The disaster recovery virtual machine has been successfully added to the protection group.

Steps:

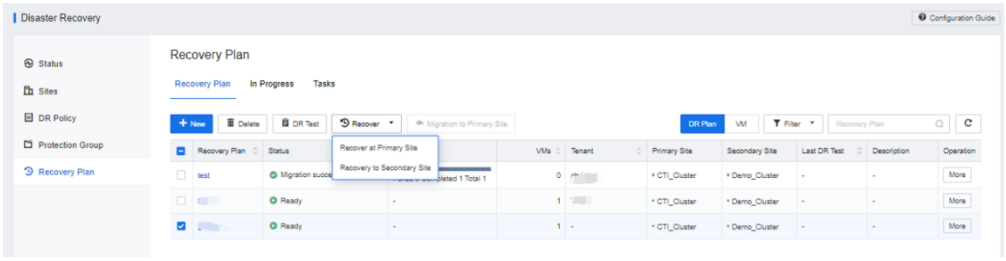
Step 1. Enter the **Disaster Recovery** > **Disaster Recovery** > **Recovery Plan,** and click the **New** button to create a protection group. Select the importance level for the business group. The business group with a higher priority can perform tasks such as backup, data transfer, recovery, drill, and relocation.



Step 2. In **Recovery Settings**, you can see the destination storage location and the startup order during restoration.



Step 3. Select a recovery plan and perform operations such as DR Test, Recover, and migrate to the primary site at the top of the page.



4.9.4.1.7 DR Test

Function Description:

Supports disaster recovery drills for the virtual machines in the protection group. During the disaster recovery drill, a new drill virtual machine will be generated at the secondary site, which has no impact on the virtual machine at the primary site and the disaster recovery standby machine.

Precautions:

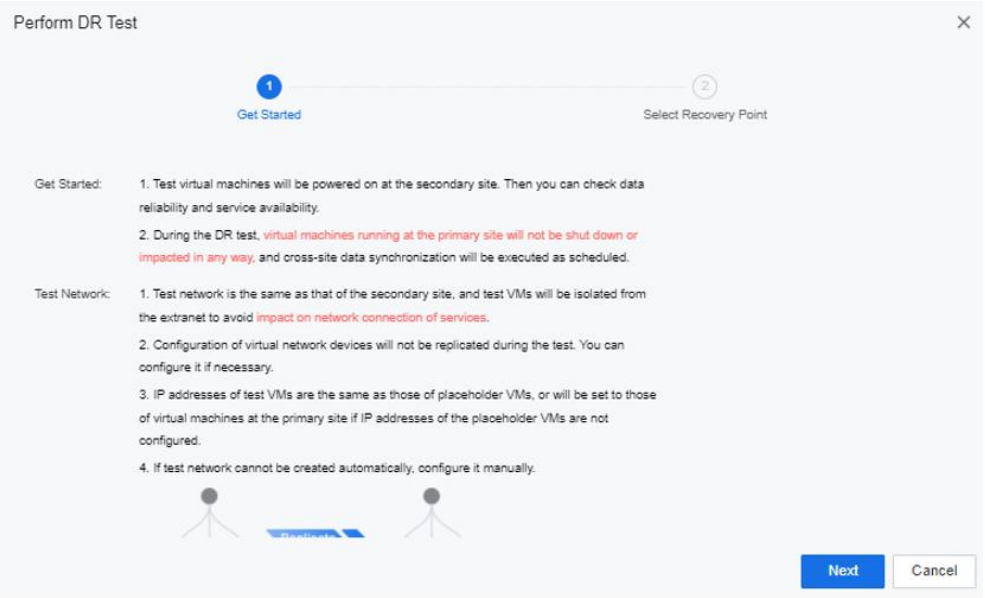
In order not to affect services, the drill virtual machine-generated by the disaster recovery drill is not connected to the virtual network. To perform post-drill service verification, you need to separately plan the drill network and manually connect the drill virtual machine to the drill network.

Prerequisite

The protection group has been successfully added to the recovery plan.

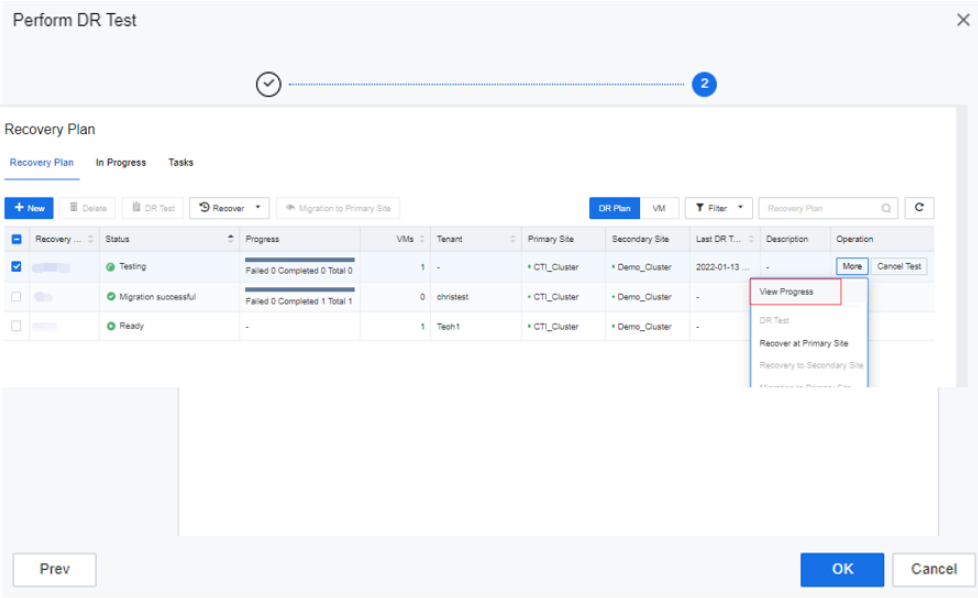
Steps:

Step 1. Go to the **Disaster Recovery** > **Disaster Recovery** > **Recovery Plan** interface, select the recovery plan that needs to be drilled, and click the **DR Test** button above to view the description of the drill function and choose whether to use the reserved node resources to perform the drill on the virtual machine.



Step 2. Click **Next** to select the recovery point of the virtual machine. Next, you can choose whether to synchronize the data of the primary site for the

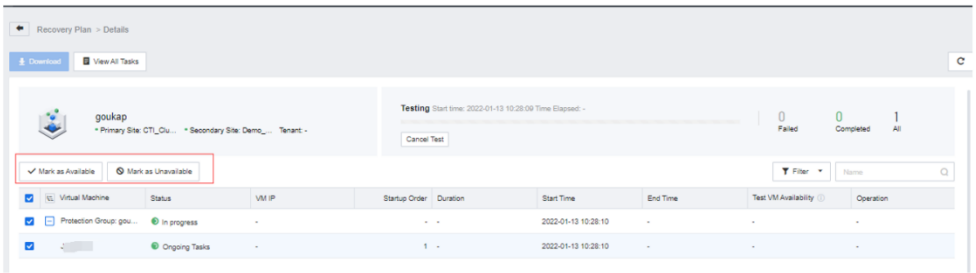
drill. If you choose **Start DR test without syncing data**, the drill virtual machine will be directly launched at the secondary site, and the drill virtual machine can choose the recovery point saved on the secondary site. If you choose to **Sync data before testing**, the current virtual machine state of the primary site will be synchronized. After arriving at the secondary site, start the virtual machine with the current status of the virtual machine at the primary site.



Step 3. Click **OK** to start the test. During the test, you can click **More** > **View Task Progress** to see the progress of the test.

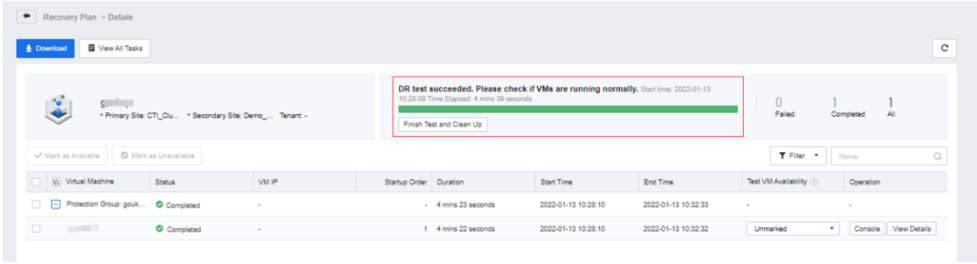
Step 4. After the DR test is completed, a corresponding DR test virtual machine (non-disaster recovery backup machine) will be added to the standby site. The drill virtual machine is not connected to the physical edge.

Step 5. Enter the **View Progress** interface, verify the virtual machine's services and mark it as available. The virtual machine not marked as **Available** or **Unavailable** will be recorded in the DR test report.

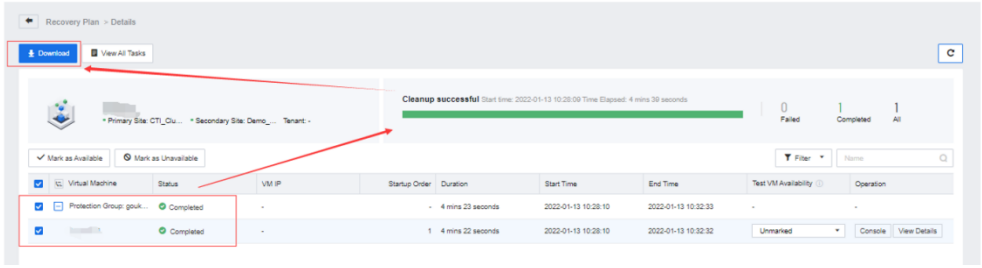


Step 6. After the DR test is complete, click **Finish Test and Clean Up** to delete the DR test virtual machine and data, including all the available and unavailable

DR test virtual machines, and delete the network devices and VM groups generated during the DR test.



Step 7. After the DR test is cleaned up successfully, select the disaster recovery business group and click **Download** to obtain the detailed DR Test report.



4.9.4.1.8 Recover At Primary Site

Function Description:

When data loss occurs on the virtual machine at the primary site, you can select **Recover at Primary Site** to restore the disaster-tolerant virtual machine from the primary site through backup. There are two ways to restore to a new virtual machine and to overwrite the original virtual machine. **Create a new virtual machine** will create a new virtual machine from the backup point, and the original virtual machine will not be affected. **Overwrite the existing virtual machine** will shut down and delete the original virtual machine.

Precautions:

1. To avoid the IP address conflict with the existing virtual machine, you need to manually connect the newly created virtual machine to the network.
2. The newly generated virtual machine will have a new hardware ID. If the Guest OS or software is bound with hardware information for licensing, it must be re-licensed or use the **Overwrite the existing virtual machine**

method.

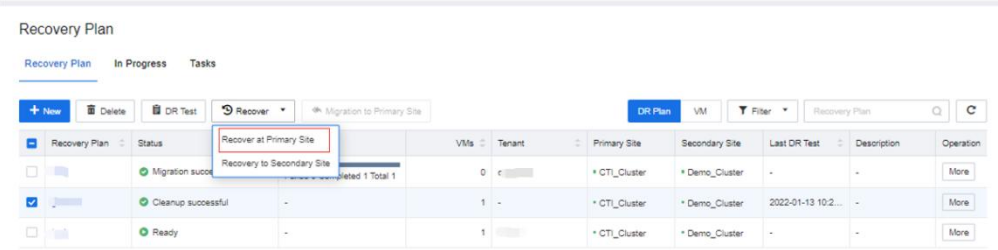
3. **Overwrite the existing virtual machine** will close and delete the original virtual machine.
4. **Overwrite the existing virtual machine** will not change the hardware and network information of the original virtual machine.

Prerequisite

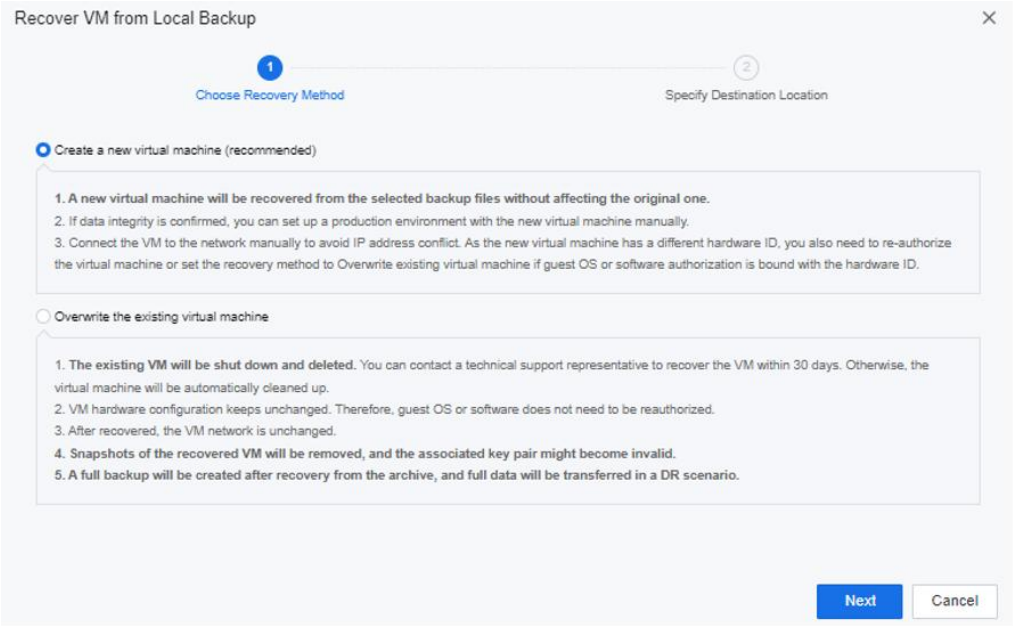
The protection group has been successfully added to the recovery plan.

Steps:

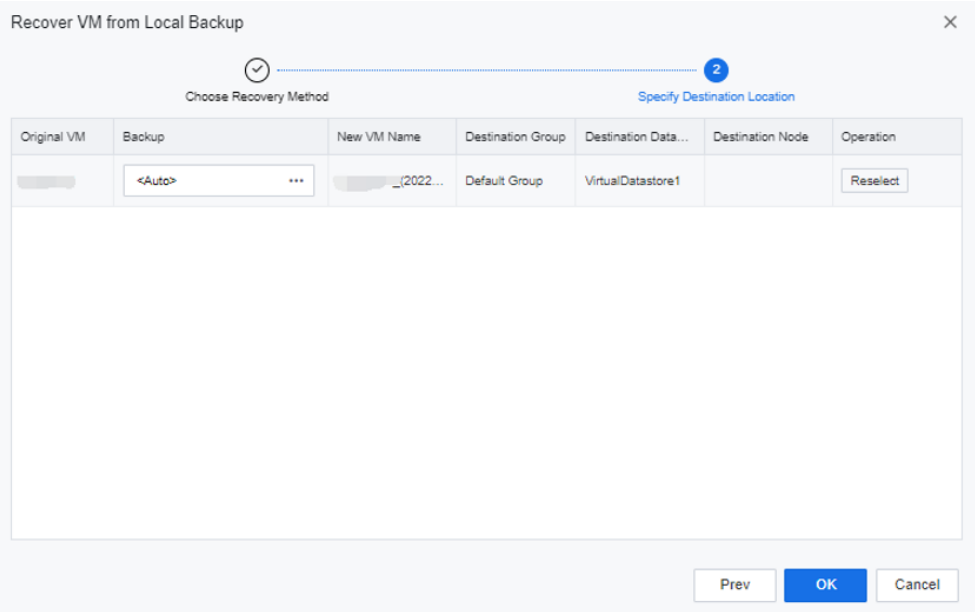
Step 1. Navigate to the **Disaster Recovery** > **Disaster Recovery** > **Recovery Plan**, select the recovery plan that needs to be drilled, and click on the **Recover at Primary Site** button.



Step 2. Select the recovery method. It is recommended to choose to generate a new virtual machine. This method's virtual machine must be manually connected to the production network. **Overwrite the existing virtual machine** will close and delete the original virtual machine.



Step 3. Select the backup point and destination location of the recovered virtual machine.



Step 4. Click **OK** to start restoring the virtual machine.

4.9.4.1.9 Recover To Secondary Site

Function Description:

When a disaster occurs at the primary site, select **Disaster Recovery** to pull up the disaster recovery standby machine from the secondary site. The data not synchronized to the secondary site will be lost.

Precautions:

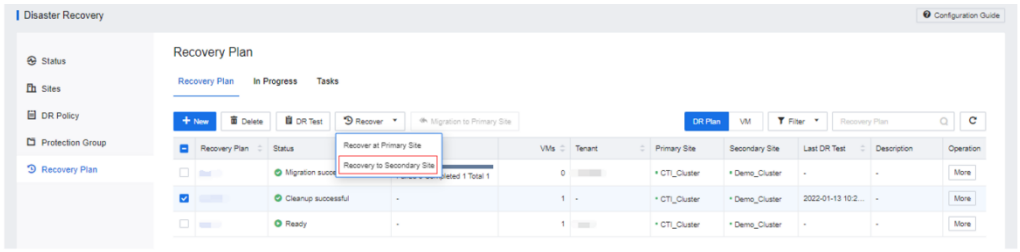
During post-disaster recovery, if the virtual machine at the primary site is still online, the DR at the secondary site may cause IP conflicts.

Prerequisite

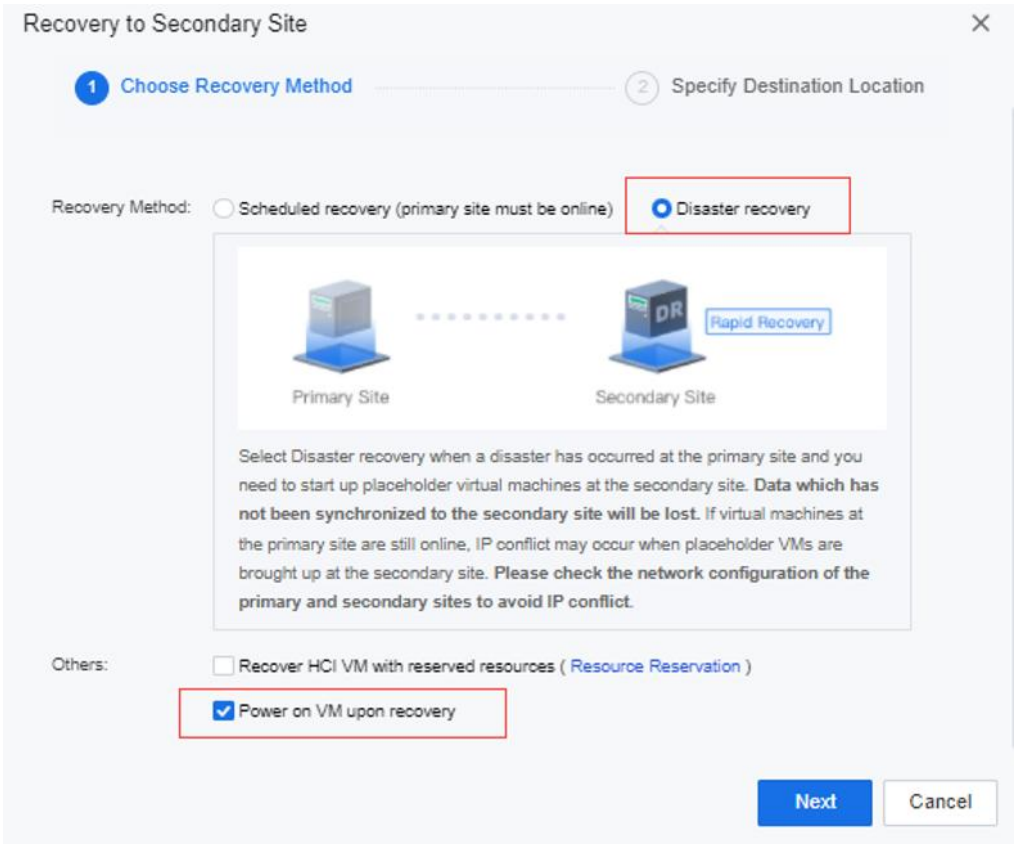
The protection group has been successfully added to the recovery plan.

Steps:

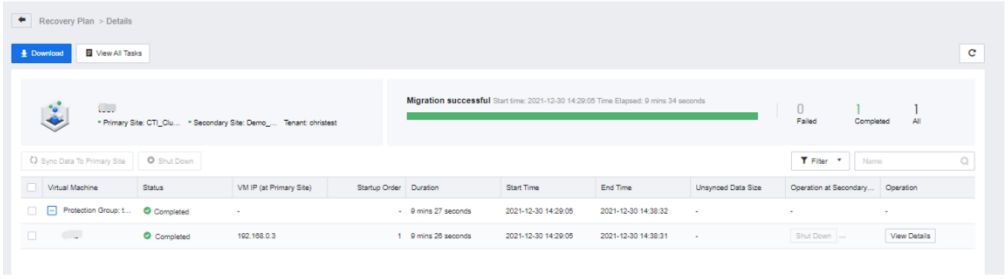
Step 1. Go to the **Reliability** > **Disaster Recovery** > **Recovery Plan** interface, select the recovery plan that needs to be drilled, and click the **Recover to Secondary Site** button.



Step 2. Select **Disaster recovery** as the recovery method and select **Power on VM upon recovery** for others. You can also configure resource reservations and select **Recover HCI VM with reserved resources**.



Step 3. Click the corresponding recovery plan **More** > **View progress** button. You can see the detailed information about the recovery.



Step 4. After the secondary site is successfully restored, select the disaster recovery protection group, and click **Download** to obtain the detailed disaster

recovery report. It supports the configuration of subscription to the report and sends the report to the specified mailbox via email.

4.9.4.1.10 Migration To Primary Site

Function Description:

When the primary site is recovered from a disaster, the virtual machine data of the secondary site is relocated to the primary site.

Precautions:

During the migration, you need to manually shut down the virtual machine at the secondary site according to the task prompts.

Prerequisite

The primary site recovered from the disaster.

Steps:

Step 1. Navigate to **Disaster Recovery** > **Disaster Recovery** > **Recovery Plan**, select the recovery plan that needs to be drilled, and click the **Migration to Primary Site** button.

Step 2. Support to modify the data synchronization interval, trigger synchronization threshold, and wait for manual shutdown timeout during the migration phase.

Step 3. Select the datastore for the virtual machine to be relocated and click **OK**.

Step 4. The interface will display the Waiting for shutdown prompt during migration to the primary site. You need to manually shut down the disaster recovery virtual machine at this time, and the migration task can continue.

4.9.5 High Availability (HA)

Function Description:

This function provides high-availability services for virtual machines. When any one of the node's hardware, storage, or network fails, the HA mechanism will automatically restore the virtual machine (including virtual network devices) to run on other nodes to ensure business continuity.

Precautions:

When the management interface and edge port are disconnected simultaneously, only the virtual machine HA in the two-node scenario takes effect, and the HA in the three-node scenario does not.

Prerequisite

The virtual machine needs to enable the HA function, and other hosts have sufficient resources.

Steps:

Log in to the SCP platform, and navigate to **Reliability** > **HA**. You can set the **Monitoring Sensitivity**, and the setting is set for the entire cluster. Example: If the fault sensitivity level is high and the fault status is detected for 30 seconds, HA will shut down the virtual machine on the faulty node and try to restore the virtual machine to other nodes in the cluster.

4.9.6 Dynamic Resource Scheduling (DRS)

Function Description:

Cluster Dynamic Resource Scheduling (DRS) is a technology for balancing and scheduling cluster resources. Traditional DRS ensures business service continuity by detecting the resource usage of hosts and migrating VMs in time to prevent resource shortage or load imbalance. However, its effectiveness is not guaranteed, such as the inability to predict the time of threshold triggering, the lag of suggestions, only based on the computing busyness of hosts but not VMs, and only based on resources but not on the performance and reliability after scheduling.

Sangfor HCI DRS 2.0 predicts the load on cluster resources for the next two hours based on the resource history of hosts and VMs over the past five days and performs intelligent scheduling based on the resource rating results to improve both the performance score and the reliability score after the migration, thus, to optimize business services.

Precautions:

1. DRS 2.0 is not supported for the VMs of the following types: non-clustered VMs, NFV VMs, rapidly-recovered VMs, VMs with a specified run location, VMs with a specified fault domain, VMs with CDP enabled, VMs with CPU exclusive mode enabled, VMs that are using a GPU, and VMs with USB

mapping.

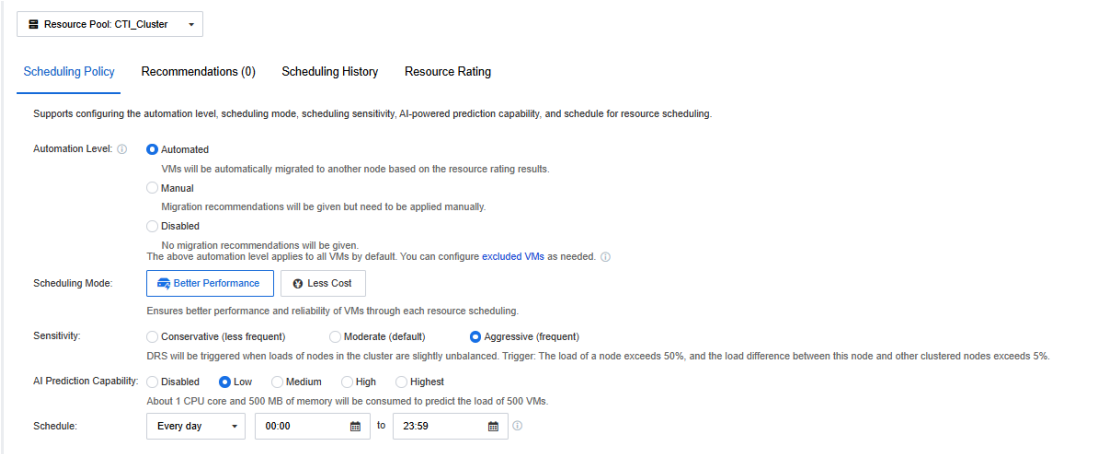
2. DRS 2.0 is not supported for the nodes whose UPS-powered VM shutdown policy is triggered.
3. It is only supported to perform disk failure detection for Seagate and Western Digital SATA disks (HDDs). The deduction deviation for the detection of unsupported disks is between 5 and 10 points (Labeled as Level 3).
4. It is only supported to perform memory failure detection for x86 architectures (not ARM architecture due to lack of training data and models).
5. After DRS is configured, disk failure detection is unavailable for the first 10 days, and memory failure detection for the first 30 days because these features require historical data for training.
6. It is only supported to perform RAID card failure detection for MegaRAID and SAS3008 RAID cards.
7. It is not supported to generate all scheduling recommendations for a cluster at a time. Up to 50 recommendations can be generated in 10 minutes.

Prerequisite:

1. A cluster of multiple HCI nodes already exists.
2. VMs are located on external storage or virtual storage.
3. **Run Location** of VMs is configured as **Auto**.

Steps:

Step 1. Log in to SCP, go to **Resources** > **Reliability** > **DRS**, select a resource pool, and click **Scheduling Policy**.



Step 2. Select an **Automation Level**. If **Automated** is configured, VMs will be

automatically migrated to another node based on the resource rating results. If **Manual** is configured, migration recommendations will be given but need to be manually applied. If **Disabled** is configured, no migration recommendations will be given.

Step 3. Select a **Scheduling Mode**, based on which the optimal destination nodes and recommendations are given to optimize the cluster. The **Better Performance** mode balances the load on each node, and the **Less Cost** mode saves node resources by centralizing VMs to run on one or more nodes as much as possible.

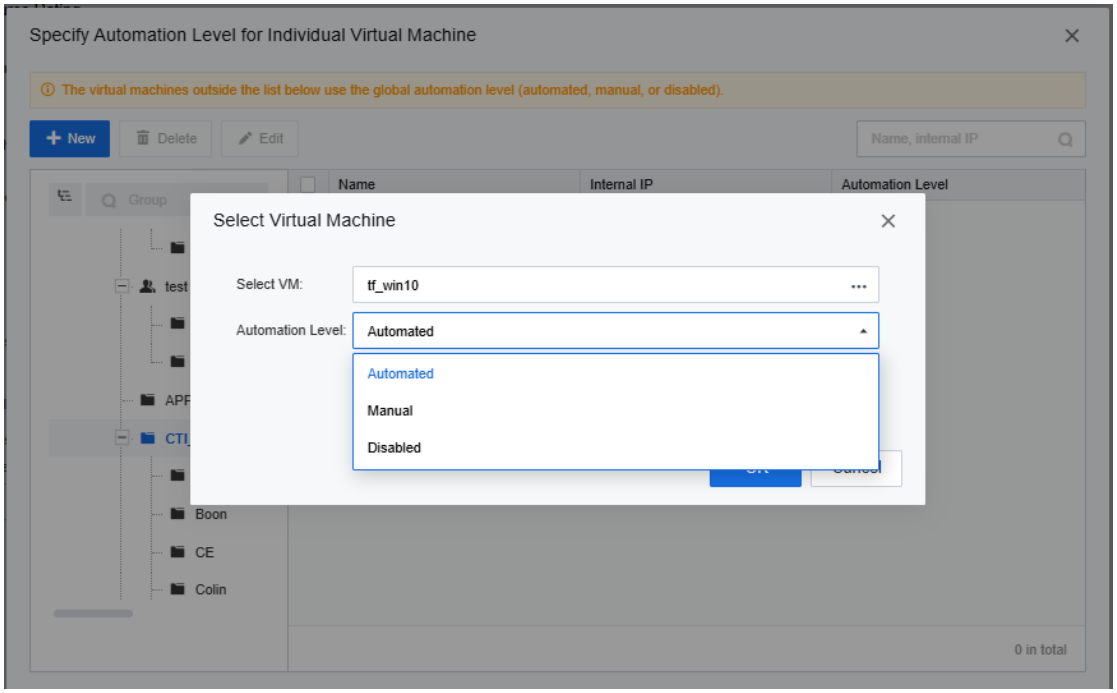
- **Better Performance**: Migrates VMs on nodes with high loads to nodes with low loads to improve the performance of the nodes and VMs. The reliability level of the destination nodes cannot be lower than that of the source nodes.
- **Less Cost**: Migrates VMs in order of node memory load from the lowest to the highest to nodes with high loads. The VM performance score decrease after the migration cannot exceed the threshold and the reliability level of the destination nodes cannot be lower than that of the source nodes.

Step 4. Select **Conservative (less frequent)**, **Moderate (default)**, or **Aggressive (frequent)** for **Sensitivity**. The node load threshold depends on **Sensitivity** and **Scheduling Mode**.

Step 5. Select **Disable**, **Low**, **Medium**, **High**, or **Highest** for **AI Prediction Capability** based on the number of VMs. If this feature is enabled, AI algorithms will be used to predict the loads of the nodes and VMs for the next two days and schedule resources based on the load trends of the past seven days.

Step 6. Configure the **Schedule** to prevent DRS from being performed during the off-peak hours.

Step 7. Configure **Automation Level** (**Automated**, **Manual**, **Disabled**) for specific VMs as needed.



4.9.7 Resource Reservation

Function Description:

Resource reservation means that a certain amount of resource space is reserved on some nodes. The system and other virtual machines will not use this part of the resources. When a node fails or is switched for disaster recovery, the reserved node resources can be used to immediately restore the virtual machine, reducing the risk of business failure recovery due to insufficient resources.

Precautions:

None.

Prerequisite

None.

Steps:

Step 1. Log in to the SCP platform and select **Reliability** > SCP **Status Check** > **Overload Check.**

Step 2. You can see the current reservation status on the main interface. Click the **Add Resource Reservation** button to enter the host resource reservation configuration interface.

Step 3. Select the **Resource Pool** for reserved resources and the **Node** for reserved resources, configure the **Reserved Memory**, and click **OK**.

Step 4. You can see the reserved item you just added to the interface, and you can **Edit** or **Delete** it.

4.9.8 VM Resource Limit

Function Description

You can configure upper limits for the CPU clock speed, disk I/O, and NIC QoS for the VM. Platform administrators can configure upper limits for the resources used by all VMs in a specific resource pool according to the business importance.

Precautions

1. The CPU clock speed ranges from 100 MHz to 1,000 GHz. Note that if this limit is too low, for example, 100 MHz, VM report data may not be updated in time, and the VM may restart.
2. The outbound or inbound traffic of the VM NIC ranges from 1,000 Kbps to 20,000 Mbps.
3. The disk I/O read or write speed of the VM ranges from 128 KB/s to 102,400 MB/s, and the read or write count ranges from 16 to 2,147,483,647. Note that if the I/O limit is too low, for example, 128 KB/s, the VM may restart due to poor system disk I/O.

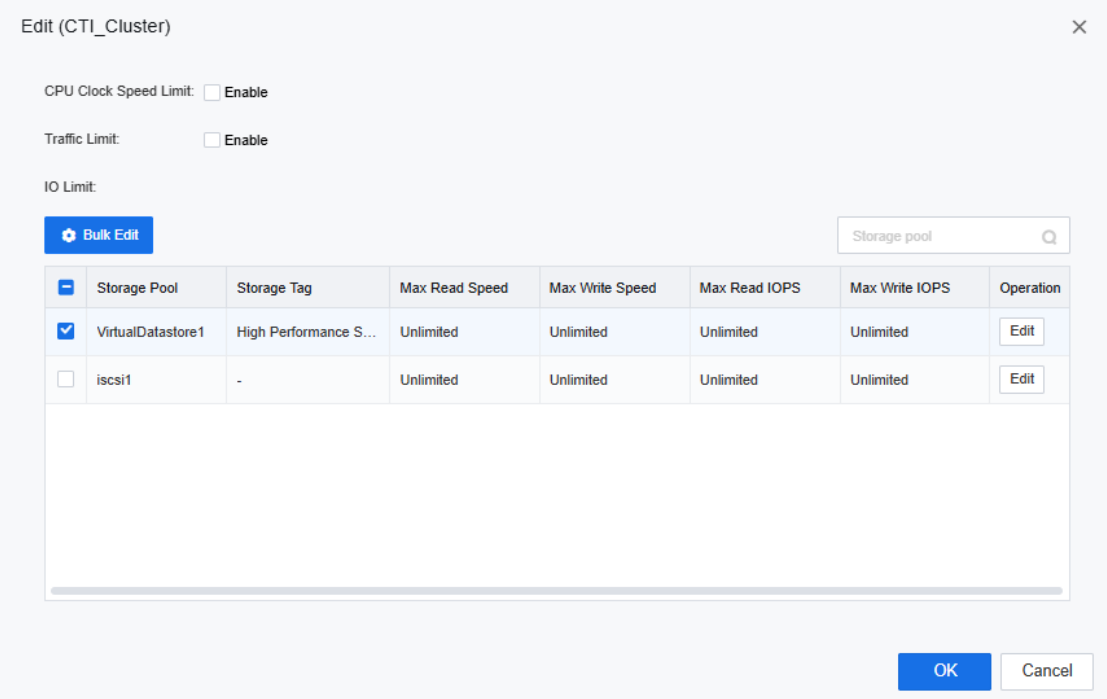
Prerequisites

N/A

Steps

Go to **Reliability** > **VM Resource Limit**, select the target resource pool, and click **Bulk Edit**. Bulk configure the CPU clock speed, NIC traffic, and disk I/O of VMs in different storage pools within the resource pool. After the configuration is completed, newly created VMs in the storage pool inherit the QoS policy of the resource pool. You can edit the default QoS configurations on the VM editing

page.



4.9.9 VM Scheduling

The VM scheduling policy supports the configuration of mutual exclusion or aggregation policies for multiple virtual machines and clusters. Through the scheduling policy, the running location of the virtual machine can be precisely controlled to meet the needs of virtual machine business tuning.

1. VM-VM Affinity

Function Description:

Aggregated VM allows multiple VM to be bound and run on a physical node. For example, VM with frequent business visits or virtual machine in the same business group is bound to the same server to improve business access performance.

Precautions:

1. The running virtual machine does not support modifying the Running Location configuration.
2. After the scheduling policy is created on the running virtual machine, the virtual machine needs to restart to take effect.
3. Supports configuring boot orders for VMs when SCP 6.10.0 is connected to

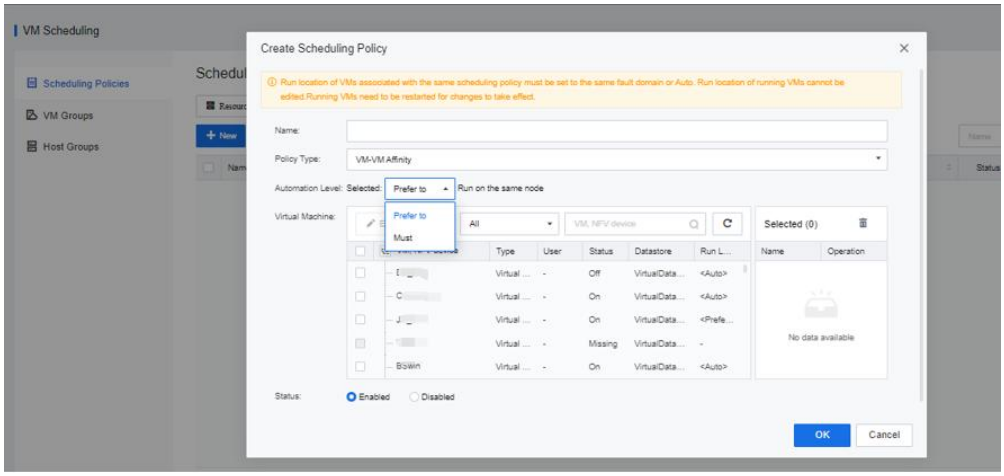
HCI 6.10.0 and higher.

Prerequisite

None.

Steps:

Enter the **Reliability** > **VM Scheduling** > **Scheduling Policies**, and click **New to configure an aggregation policy for the virtual machines in the same Run Location.**



2. VM-VM Anti-Affinity

Function Description:

Mutually exclusive virtual machines run the selected virtual machine on different physical nodes. For example, cluster systems such as Oracle RAC are mutually exclusive on different physical servers to ensure business reliability.

Precautions:

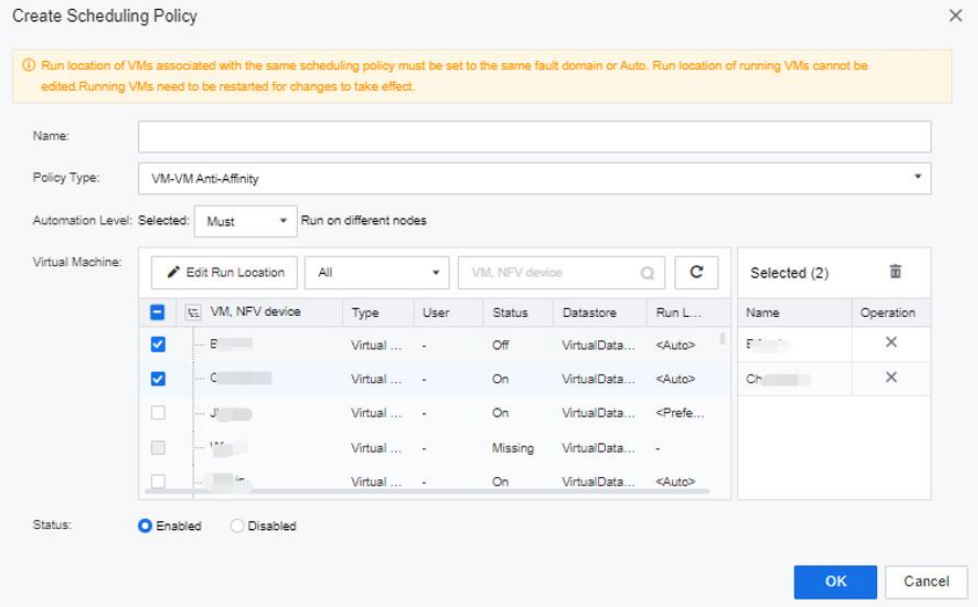
- The running virtual machine does not support modifying the **Running Location** configuration.
- After the scheduling policy is created on the running virtual machine, the virtual machine needs to restart to take effect.

Prerequisite

None.

Steps:

Go to **Reliability** > **VM Scheduling**, and add the virtual machine whose run locations are mutually exclusive to the mutual exclusion policy.



1. VM Group Anti-Affinity

Function Description:

Virtual machine group mutual exclusion supports running multiple selected VM groups on different physical nodes. For example, suppose the three VM of business A and the three VM of business B are configured to be mutually exclusive in VM groups when the physical node running business A fails. In that case, business B will not be affected, improving business availability.

Precautions:

- The run location must be configured in the same fault domain or automatically selected for the same virtual machine group.
- The running virtual machine does not support modifying the **Running Location** configuration.
- After the scheduling policy is created on the running virtual machine, you need to restart the virtual machine for it to take effect.
- The virtual machine in the same virtual machine group will not be aggregated by default, and the aggregation policy needs to be manually configured.

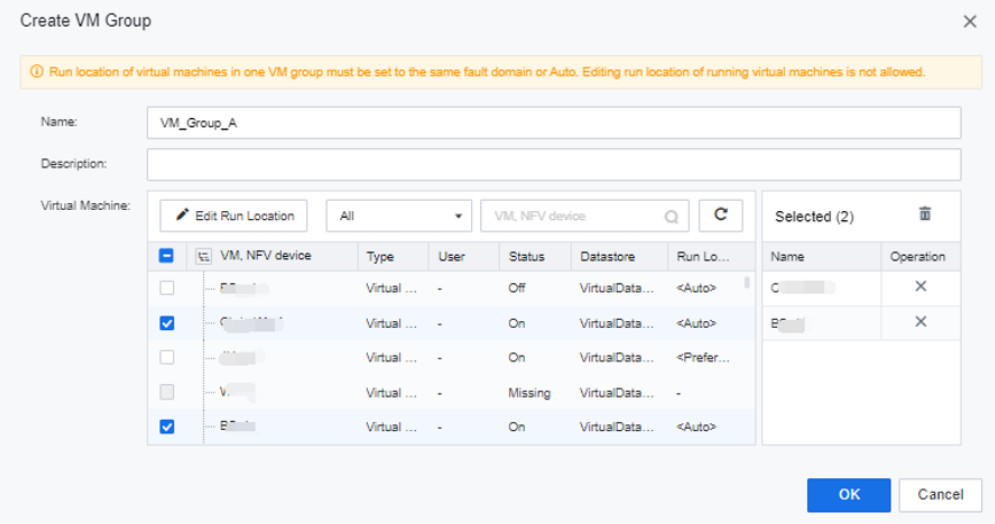
Prerequisite

None.

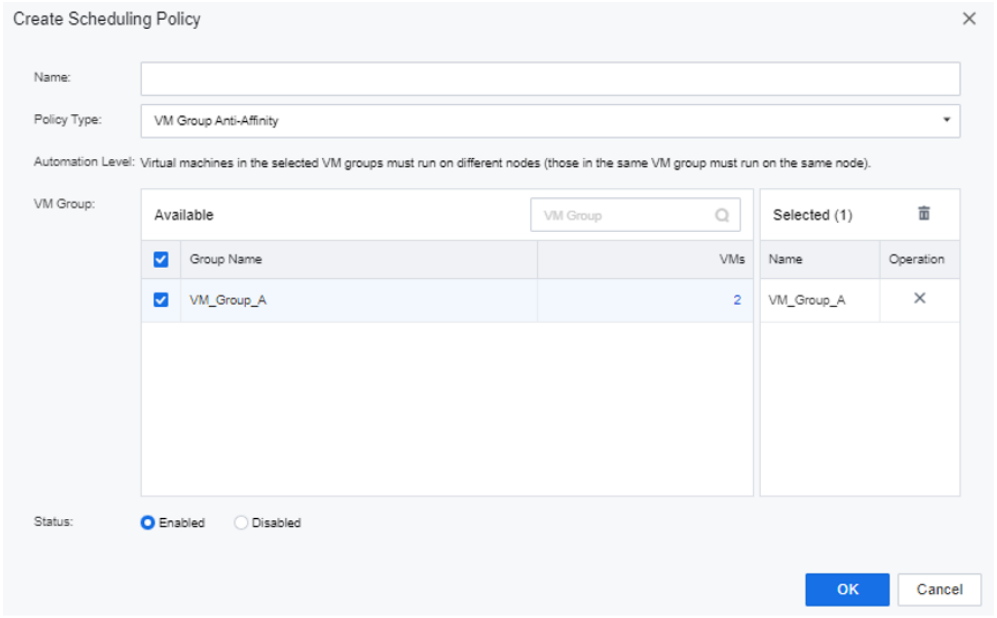
Steps:

Step 1. Go to the **Reliability** > **VM Scheduling** Policy > **VM Groups** interface

and add the **VM** planned to run at the same location to the virtual machine group.



Step 2. Enter the **Reliability** > **VM Scheduling**, click **New**, select **VM Group Anti-Affinity** for the policy type, select the mutually exclusive virtual machine group, and click **OK**.



2. VM-Host Affinity

Function Description:

VM group to host group supports running selected virtual machine groups on different physical host groups. For example, run service group A of the active-active service in the main fault domain of the extended cluster and run service group B of the active-active service in the standby fault domain of the extended cluster. It is to ensure that data and services are active-active simultaneously.

Precautions:

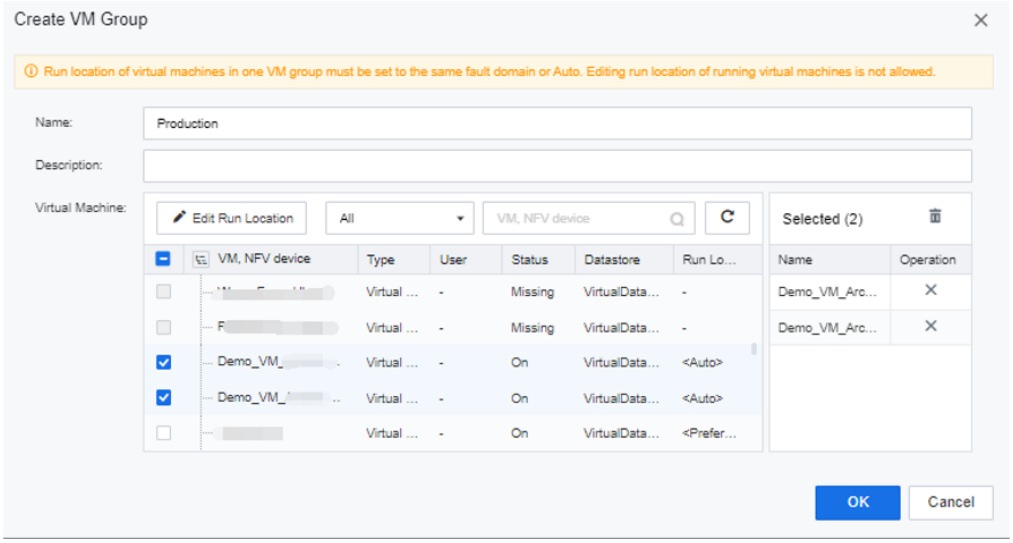
1. For the same VM group, the operating location must be configured in the same fault domain or automatically selected.
2. The running VM does not support modifying the **Running Location** configuration.
3. After the scheduling policy is created on the running VM, you need to restart the VM for it to take effect.
4. A stretched cluster group hosts in the same fault domain into the same host group by default.

Prerequisite

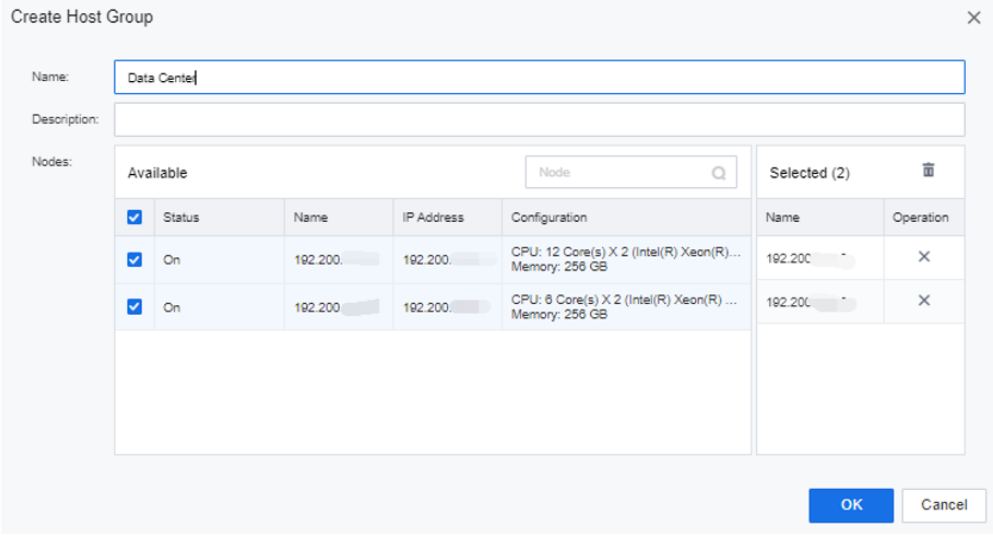
None.

Steps:

Step 1. Go to the **Reliability** > **VM Scheduling Policy** > **VM Groups** interface and add the VM planned to run at the same location to the virtual machine group.

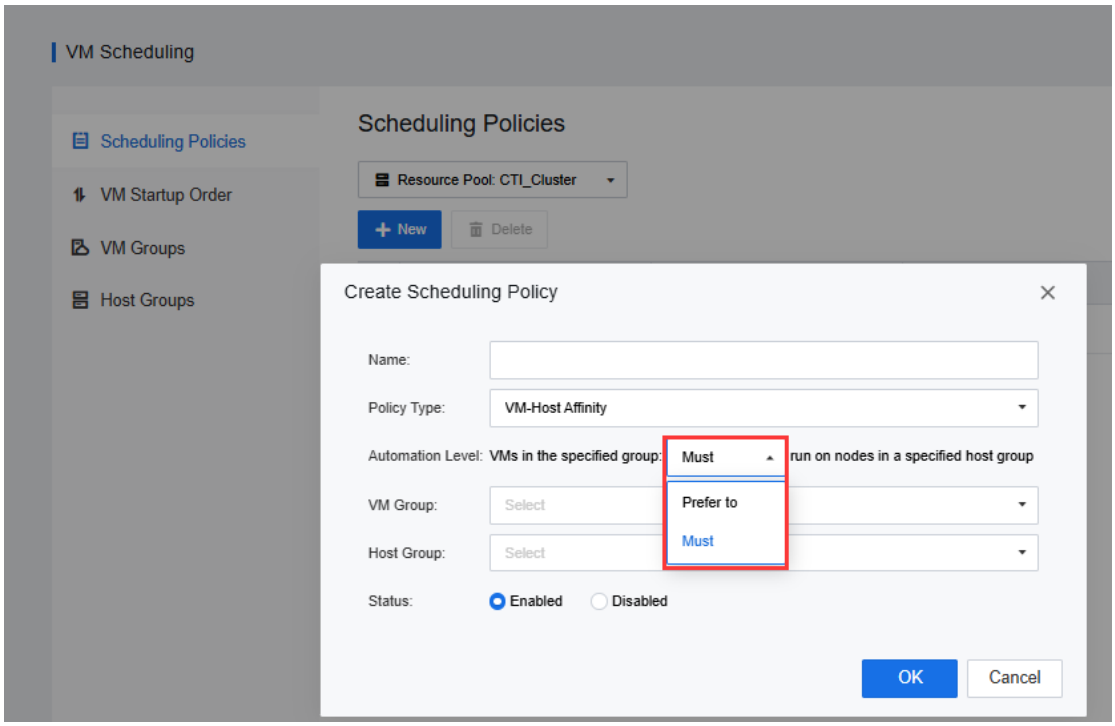


Step 2. Go to the **Reliability** > **VM Scheduling Policy** > **Host Groups.** Add the hosts in the primary and secondary fault domains to their respective host groups.



Step 3. Select **VM-Host Affinity** for **Policy Type**.

- If you select **Must** for **Automation Level**, VMs in VM group A will always run in the primary fault domain, and those in VM group B will always run in the secondary fault domain.
- If you select **Prefer to** for **Automation Level**, you can set a standby host group. In this case, if no host is available in the selected host group, VMs will be scheduled to hosts in the selected standby host group.



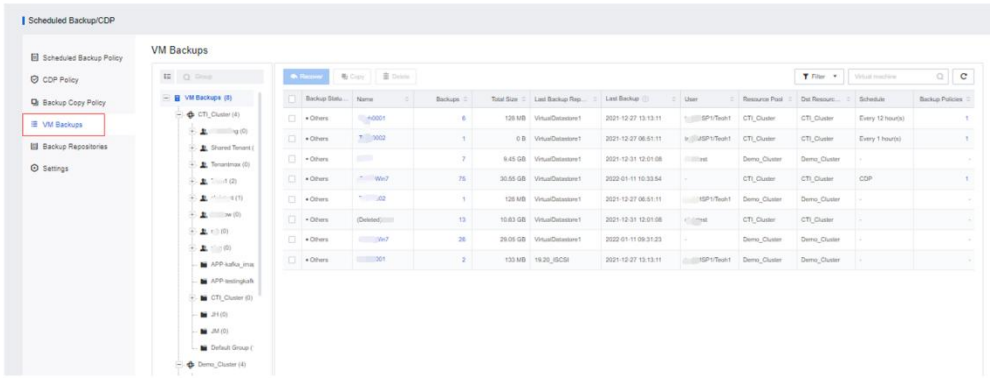
4.9.10 Business Reliable Service

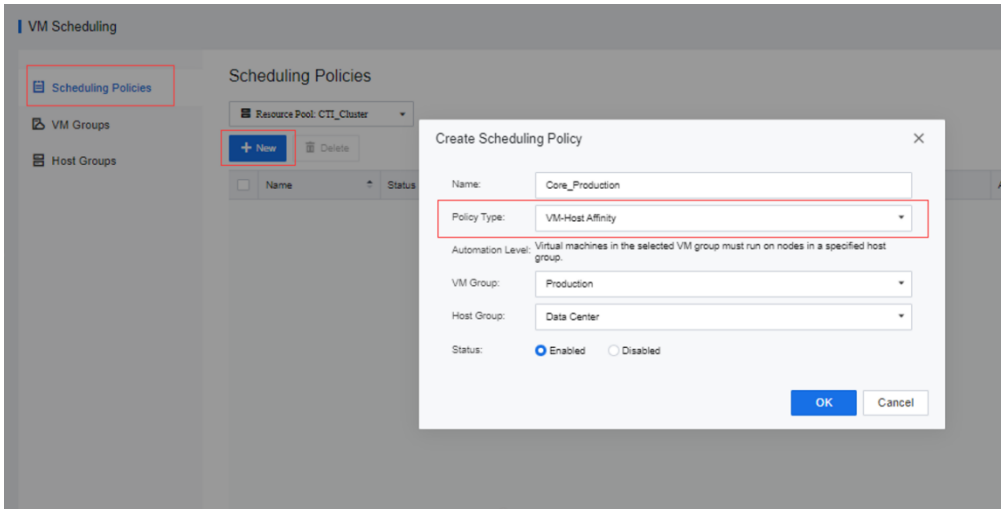
Function Description:

Sangfor SCP provides high service reliability, ensuring that services can operate under various abnormal conditions or return to normal in the shortest possible time.

First, suppose a node in the cluster shuts down abnormally or goes offline. In that case, you can set **HA** to ensure that the virtual machine running on the faulty node can be automatically pulled up on other suitable nodes to ensure the high availability of the virtual machine.

Secondly, **Resource reservation** can ensure that the reserved resources of the clustered node can support the normal startup of all virtual machines on the faulty node. Finally, suppose the CPU or memory resources of the virtual machine cannot support the normal operation of the current business. In that case, the specific virtual machine can be set as **Dynamic Resource Scheduling**, which can automatically allocate more computing and memory resources to the virtual machine when the CPU or memory usage reaches a certain threshold, ensuring the reliability of the virtual machine business.





4.9.11 Platform Reliable Service

Function Description:

Generally, the operating status of equipment is often overlooked, and it is only discovered by managers when it causes an accident. Sangfor SCP can conduct holistic operation and maintenance of cluster operation status and hardware by building a reliability center platform. The operation and maintenance personnel do not need to check each device's hardware status and platform operation status one by one, but only through the SCP reliability center. The holistic view is the entry point, and you can intuitively view the overall running status and hardware status of the cluster, helping managers to find problems in time and issues in advance.

The following mainly introduces how to view the platform resource overload status, network configuration status, storage volume status, and data rebuilding status and briefly describes the key parameters.

4.9.11.1 Overload Check

Function Description:

This function checks the resource usage of hardware CPU, memory, storage, and interface traffic status and whether there is overload.

Precautions:

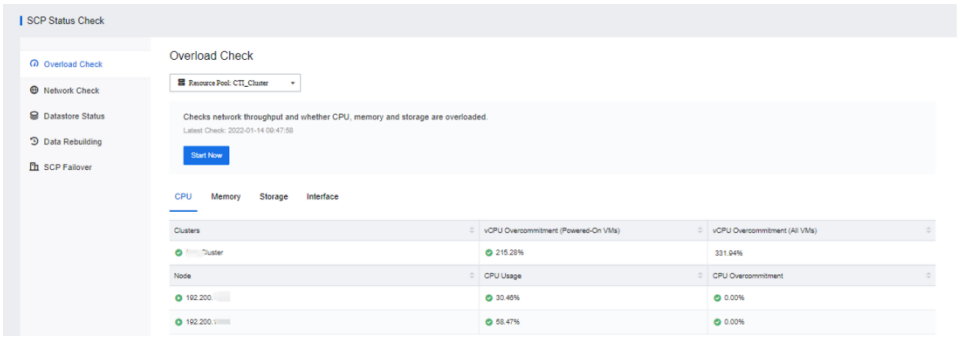
None.

Prerequisite

None.

Steps:

Step 1. Log in to the SCP platform and select **Reliability** > **Platform Status Check** > **Overload Check**. You can view the resource usage of **CPU, Memory, Storage**, and **Interface** traffic status.



NOTE

CPU overcommitment is the ratio of the CPU resources configured by the powered-on virtual machine to the total CPU resources of the server. The memory occupied by virtual network devices and platforms is not calculated here.

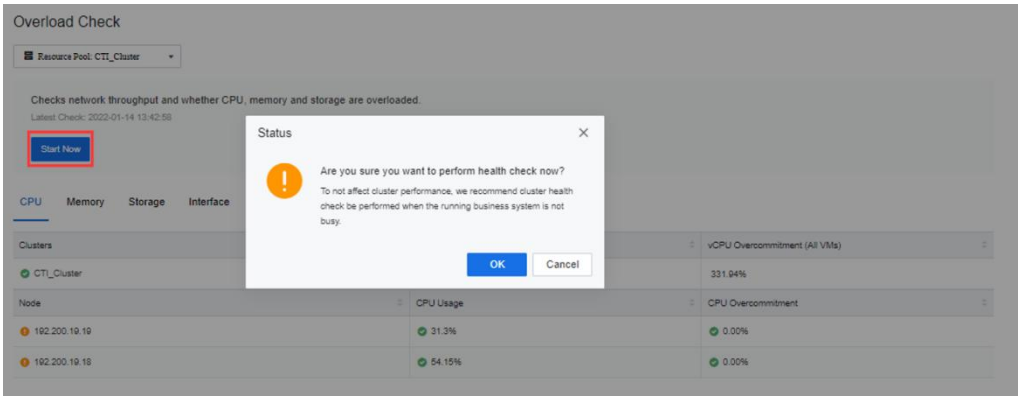
NOTE

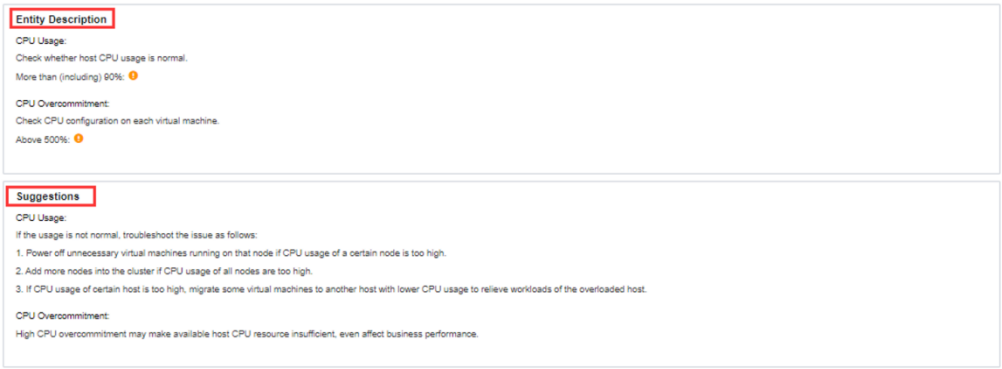
Memory over commitment ratio refers to the ratio of the actual configured memory resources of the powered-on virtual machine to the total server memory resources. The memory occupied by virtual network devices and platforms will not be calculated here.

NOTE

Storage overcommitment ratio refers to the ratio of the actual configured virtual machine storage resources to the total virtual storage resources of the server.

Step 2. You can click the **Start Now** button to get the latest status, click **Entity Description** to view the detection threshold of the corresponding detection item, or click **Suggestions** to view the corresponding suggested solution.





4.9.11.2 Network Check

Function Description:

This function checks the redundancy and connectivity status of the node management interface, overlay interface, and virtual storage interface.

Precautions:

None.

Prerequisite

None.

Steps:

Step 1. Log in to the SCP platform, select **Reliability** > **Platform Status Check Status Check** > **Network Check**, or click **Reliability** > **Holistic View** to enter the **Network Check** page. You can view the detected nodes' connectivity status of **Management Interfaces, Overlay Network Interface**, and **Storage Network Interface**.

NOTE

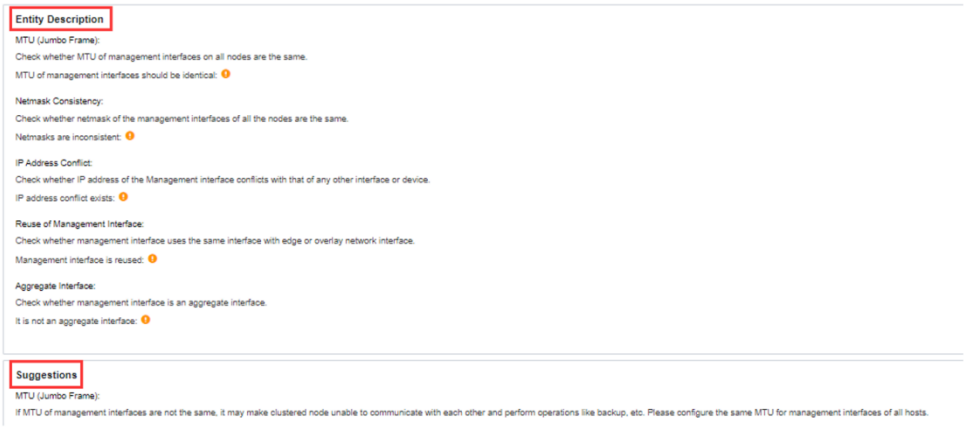
Interface multiplexing detection detects the multiplexing state of the edge port and the management interface, and multiplexing is not recommended here.

NOTE

Reuse interface detection detects whether the corresponding interface has redundant configurations such as aggregation.

Step 2. You can click the **Start Now** button to get the latest status, click **Entity Description** to view the detection threshold of the corresponding detection

item, or click **Suggestions** to view the corresponding suggested solution.



4.9.11.3 Datastore Status

Function Description:

Multiple copies across nodes ensure that the data in the cluster will not have a single point of failure of the node. Check the health status of multiple copies to ensure the reliability of platform data.

Precautions:

None.

Prerequisite

None.

Steps:

Log in to the SCP platform, select **Reliability** > **Platform Status Check** > **Datastore Status**, or click **Reliability** > **Holistic view** > **Datastore Status** > **View Details.** You can view virtual storage **Replicas**, the virtual datastore **Status**, **Cache Disks**, **Data Disks**, etc.

4.9.11.4 Data Rebuilding Status

Function Description:

When a node or hard disk fails and not responding, if the remaining storage space is sufficient, no spare disk or manual intervention is required to replace the disk/node, and the replicas are automatically rebuilt to the remaining hard disks/nodes in the cluster to restore the validity of the data copy.

Precautions:

None.

Prerequisite

None.

Steps:

Log in to the SCP platform, select **Reliability > Platform Status Check > Data Rebuilding**, or **click Reliability > Holistic View > Data Rebuilding > View Details** to enter the data rebuilding status viewing interface to view the data rebuilding status.

4.9.12 Hardware Reliability Service

Function Description

Sangfor SCP's hardware health detection can help managers clearly perceive the platform's hardware status. Managers do not need to check the hardware detection information of each server one by one. Still, they only need to use Sangfor SCP's reliable hardware services to monitor the entire platform at any time. The hardware health check mainly detects hardware such as CPU, memory, SSD, HDD, network card, RAID card, and external storage of each node. Any alarm or exception will be displayed on the interface.

4.9.12.1 Hardware Health Check

Function Description:

This function is used to check the health status of hardware CPU, memory, SSD, HDD, network card, RAID card, and external storage and to discover possible availability problems in advance.

Precautions:

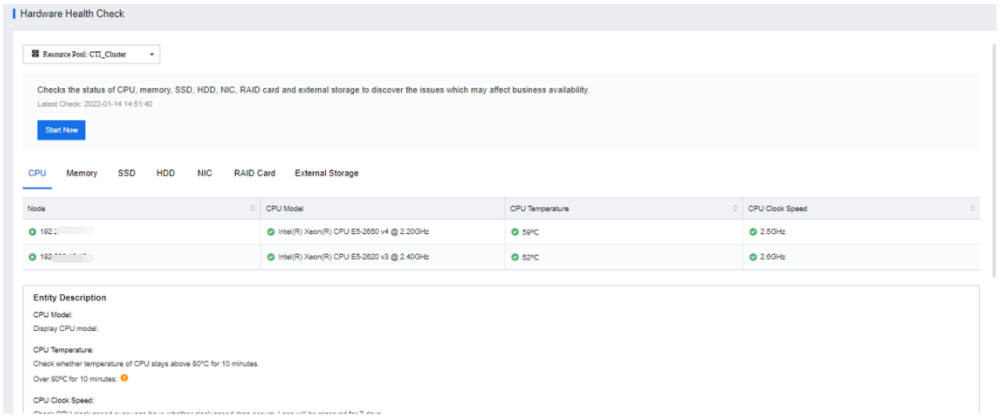
None.

Prerequisite

None.

Steps:

Step 1. Log in to the SCP platform, select **Reliability** > **Hardware Health Check**, or click **Reliability** > **Holistic View** > **Any Hardware** > **View Details** to view the hardware status.



Step 2. You can click the **Start Now** button to get the latest status, click **Entity Description** to view the detection threshold of the corresponding detection item, or click **Suggestion** to view the corresponding suggested solution.

4.9.13 Host Health Monitoring

4.9.13.1 Host Health

Function Description:

HCI can automatically identify and display unhealthy nodes (hung nodes or nodes with the hang risk) and does not prefer them for VM startup, HA, and other tasks. For cluster capacity expansion, node replacement, and other scenarios, SCP will detect the hardware to prevent node crash or system hang due to hardware failure to reduce the business service risks.

Precautions:

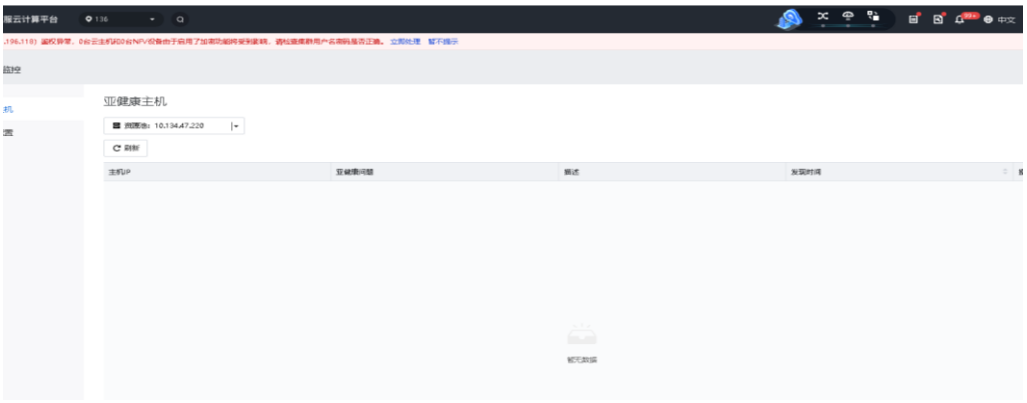
1. Only supports identifying and fixing node hangs caused by hardware failures.
2. For a node hang caused by a memory failure, if the node restarts without using the memory at the location where the failure occurred, it will remain unhealthy.

Prerequisite:

None.

Steps:

Step 1. Log in to SCP, and go to **Resources** > **Reliability** > **Host Health Monitoring** > **Unhealthy Nodes** to view unhealthy physical hosts.



Step 2. Go to **Health Monitoring** to configure **Host Health** and **Network Health**.



- **Unhealth Metrics**: If **Host hardware (CPU, memory, system disk or RAID card) anomaly** is enabled, the following will be checked: ECC Memory, UECC Memory, Bad Sector in System Disk, System Disk Read-Only, Short System Disk Lifetime Remaining, and RAID Card Failure. You can customize the crash frequency to identify unhealthy nodes that meet the criteria.
- **Check Schedule**: If **Health Monitoring** is enabled, the check will be automatically performed at each host startup or restart. You can also customize the check interval.
- **Notification Method**: You can go to **Resources** > **Monitor Center** > **Alerts** > **Notification Policies** to configure the email notification by referring to Section 4.12.3.2 Alert Options. When an unhealthy node is detected, the platform will send an email to notify the check results.

- **Recovery Method**: You can go to **Resources** > **Reliability** > **HA** to configure recovery methods for host hardware failures.
- **Fixing Method**: This mechanism will only migrate VMs on unhealthy nodes to healthy nodes. VMs that have been configured with a scheduling policy are prioritized to be scheduled based on the scheduling policy, and VMs without a scheduling policy will only be migrated to unhealthy nodes that are relatively healthy. This mechanism does not take effect if there are no healthy nodes in the cluster and does not apply to NFV devices.
- **Auto Removal**: If enabled, unhealthy nodes will be automatically removed from the **Unhealthy Nodes** list when they are healthy again.

4.9.13.2 Network Health

Function Description:

The network health check of HCI detects the packet loss and latency of the network links through messages sent between nodes. When the packet loss rate or latency reaches the threshold, an alert will be generated to effectively prevent service interruptions due to link issues.

Precautions:

None.

Prerequisite:

1. It is not supported to identify whether an interface is healthy within 15 minutes after the SCP environment is deployed.
2. Supports configuring VLAN ID for the interfaces for the network health check. For edge-connected interfaces, their VLAN ID cannot be the VLAN ID of their subinterfaces.
3. Supports checking the latency of physical links external to the servers (including NICs, optical modules, physical transmission media, and switches), which is independent of the latency of the operating system process scheduling. For aDesk Communication Interfaces, only links between servers can be checked.
4. The scenarios that support network health checks are as follows:

	Aggregated	Non-Aggregated	Aggregated and Non-Aggregated

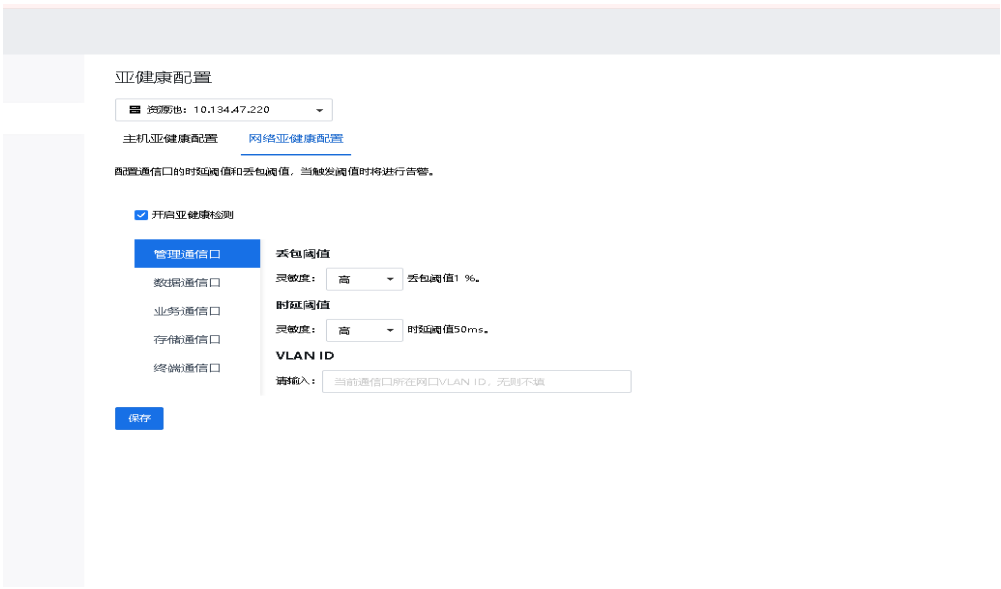
Management Interface	√	√	√
Overlay Network Interface	√	√	√
Edge-Connected Interface	√	√	√
Storage Network Interface	√	√	×
aDesk Communication Interface	√	√	√

5. Supports separating health check results for member interfaces with the following aggregation modes: master-standby aggregation, load sharing, and LACP. Load sharing of Mode 0 (round-robin policy), link aggregation with one switch, and link aggregation with two switches are not supported. If overlay network interfaces between clusters probe across the layer 3 network, the check results will not be separated for member interfaces.
6. The scenarios that do not support network health checks are as follows:

- Network links between SCP and HCI.
- Communication network of witness nodes (2+1 witness nodes, stretched cluster + witness node).
- Heterogeneous clusters (VMware) either links between HCI clusters and heterogeneous clusters.
- Physical hosts managed by SCP.

Steps:

Step 1. Log in to SCP, go to **Resources** > **Reliability** > **Host Health Monitoring** > **Health Monitoring** > **Network Health** to configure **Packet Loss** and **Latency** for interfaces. When their thresholds are reached, alerts will be generated.



The following are the interface configuration references:

Interface Type	Low Sensitivity	Medium Sensitivity	High Sensitivity	Check Time Range	Alert Interval	Max Alert Cancellation Time after Network Recovery
Management Interface	Packet Loss Rate ≥ 10% Latency ≥ 120 ms Check Interval=1 time/s	Packet Loss Rate ≥ 5% Latency ≥ 75 ms Check Interval=1 time/s	Packet Loss Rate ≥ 1% Latency ≥ 50 ms Check Interval=2 times/s	3 minutes	1 minute	4 minutes
Overlay Network Interface	Packet Loss Rate ≥ 10% Latency ≥ 120 ms Check Interval=1 time/s	Packet Loss Rate ≥ 5% Latency ≥ 75 ms Check Interval=1 time/s	Packet Loss Rate ≥ 1% Latency ≥ 50 ms Check Interval=2 times/s	3 minutes	1 minute	4 minutes
Edge-Connected Interface	Packet Loss Rate ≥ 10% Latency ≥ 120 ms Check Interval=1 time/s	Packet Loss Rate ≥ 5% Latency ≥ 75 ms Check Interval=1 time/s	Packet Loss Rate ≥ 1% Latency ≥ 50 ms Check Interval=2 times/s	3 minutes	1 minute	4 minutes

Storage Network Interface	Packet Loss Rate ≥ 0.2% Latency ≥ 1.2 ms Check Interval=10 times/s	Packet Loss Rate ≥ 0.1% Latency ≥ 850 us Check Interval=10 times/s	Packet Loss Rate ≥ 0.04% Latency ≥ 500 us Check Interval=10 times/s	15 minutes	1 minute	4 minutes
aDesk Communication Interface	Packet Loss Rate ≥ 2% Latency ≥ 50 ms Check Interval=1 time/s	Packet Loss Rate ≥ 1% Latency ≥ 25 ms Check Interval=1 time/s	Packet Loss Rate ≥ 1% Latency ≥ 5 ms Check Interval=2 times/s	3 minutes	1 minute	4 minutes

4.10 Operations Center

Sangfor SCP platform has multi-level management functions, providing three roles, including platform administrator, tenant, and tenant user, which can realize hierarchical and decentralized management of a company and an organization.

4.10.1 User Management

4.10.1.1 Platform Administrators

Function Description:

Sangfor SCP cloud management platform requires administrators to manage the platform, and the platform has a built-in super administrator admin. Super administrators can create three administrator roles: system administrator, security administrator, and audit administrator, assign different permissions to manage the cluster, and assist super administrators in managing the SCP platform.

Precautions:

1. The system administrator has all the business permissions of the platform

but not user and role management or operation audit permissions.

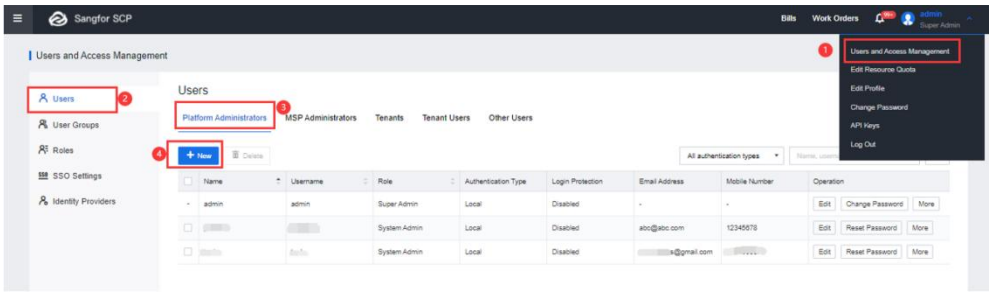
2. Security administrators have security management rights such as account authorization, role management, password policy, two-factor authentication, and IP address control policy.
3. Audit administrators only have log management rights.

Prerequisite

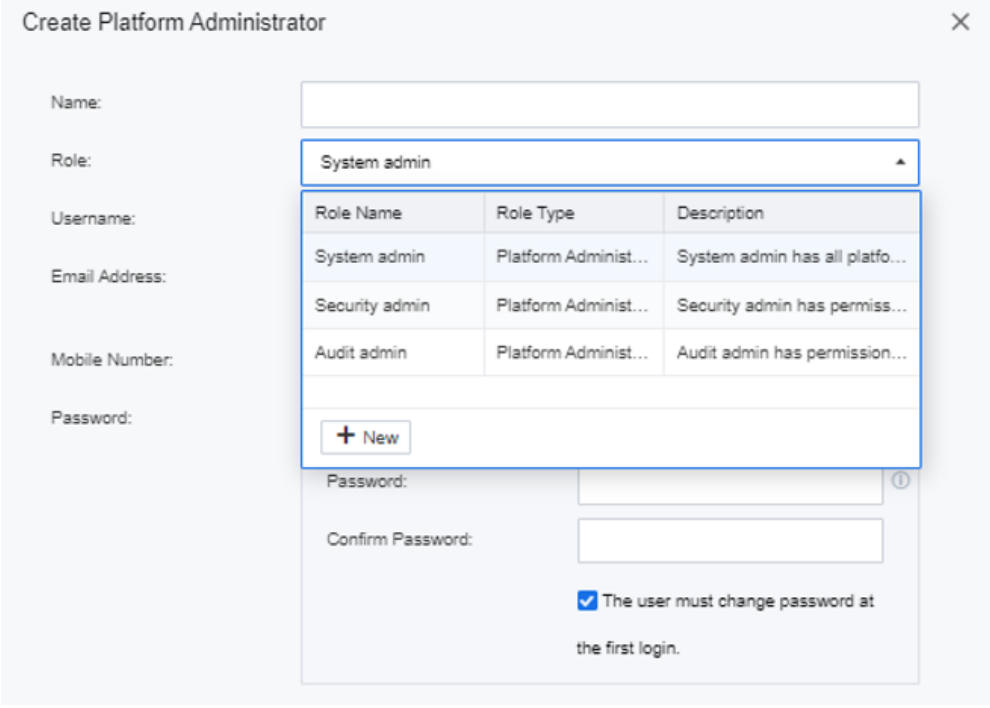
None.

Steps:

Step 1. Log in to the SCP platform as admin, select **User and Access Management** > **Users** > **Platform Administrators**, and click the **New** button to create a platform administrator.



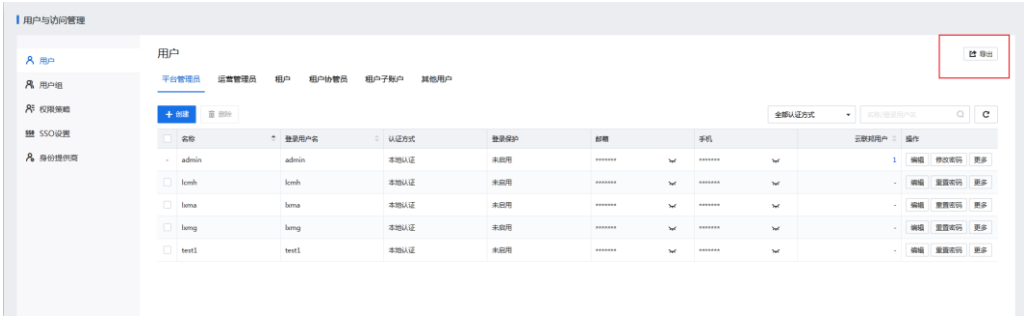
Step 2. Enter the name of the platform administrator, select the appropriate role, and enter the username, email, mobile phone number, and password.



Step 3. The super administrator admin can edit, reset the password, and

delete the platform administrator. The super administrator can click **Edit** to modify the platform administrator's name, role, email, and mobile phone number. The super administrator can reset the password when the platform administrator forgets the password.

Step 4. Click **Export** in the upper-right corner to bulk export user information.



4.10.1.2 MSP Administrator (Optional)

Function Description:

Sangfor SCP platform supports the role of the MSP administrator. The platform administrator establishes the role of the MSP administrator and issues resource pool quotas to the operation administrator, allowing the MSP administrator to assign them himself. For example, in a hosting cloud/operator scenario, the company headquarters has purchased a large-scale resource pool, and resources need to be allocated to each branch. The branch needs to create tenants for each department or group.

Precautions:

1. The system administrator needs to manually switch to the operation mode and enable the MSP operation management system, but it cannot be rolled back after the switch. Please evaluate the usage scenarios and operate with caution.
2. After the platform administrator converts the platform to the MSP operation mode, when creating a new tenant, must designate an MSP administrator for the tenant. It would not affect the existing tenants. It would not affect the existing tenants.
3. After the MSP administrator is assigned to a tenant, the quota used by the tenant is not allowed to exceed the quota of the MSP administrator to which he belongs.

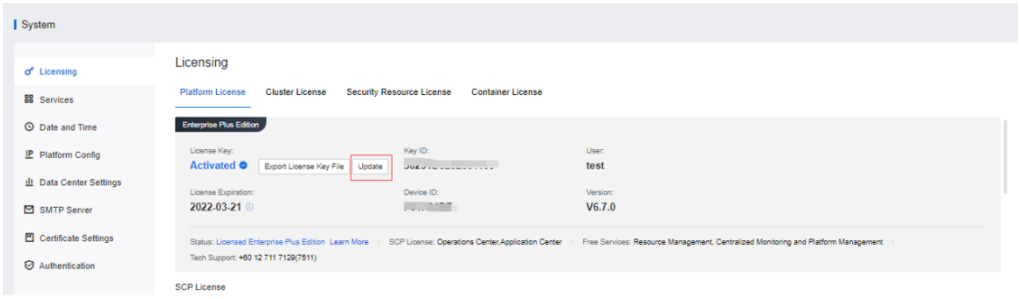
4. The MSP administrator's name, email address, and phone number cannot be reused by other users.
5. MSP administrator login address: https://{SCP-IP}/msp-login.

Prerequisite

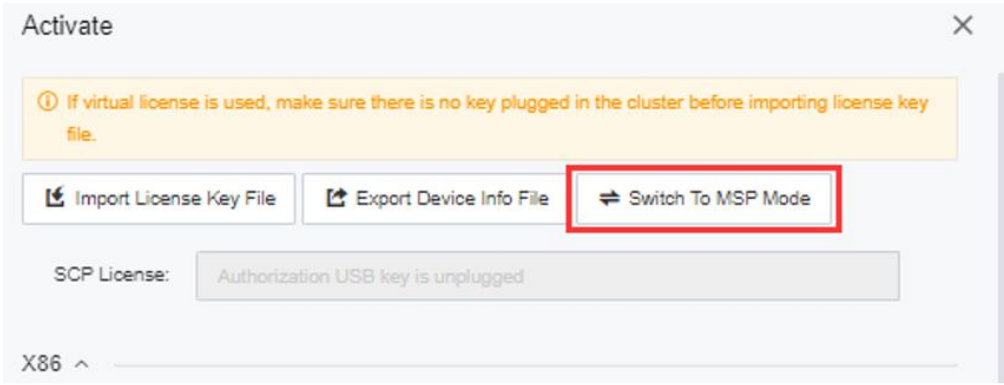
None.

Steps:

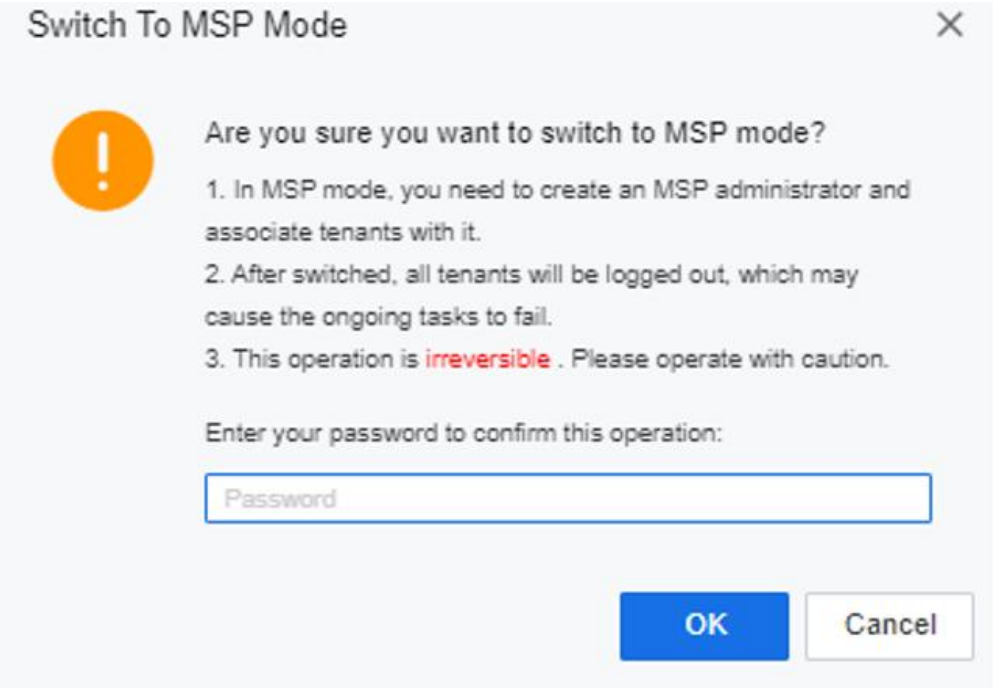
Step 1. Enter the **System** > **Licensing > Platform License,** and click the **Update** button.



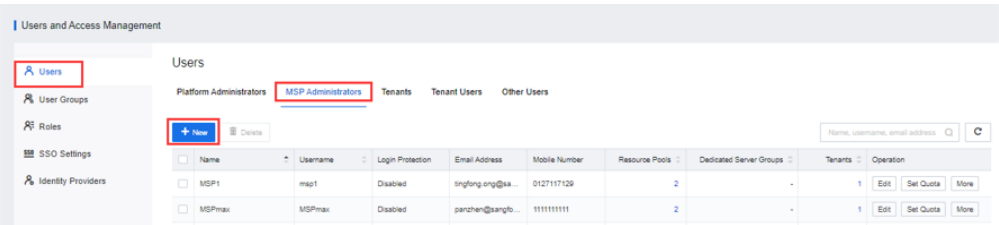
Step 2. Click **Switch to MSP Mode** in the pop-up window.

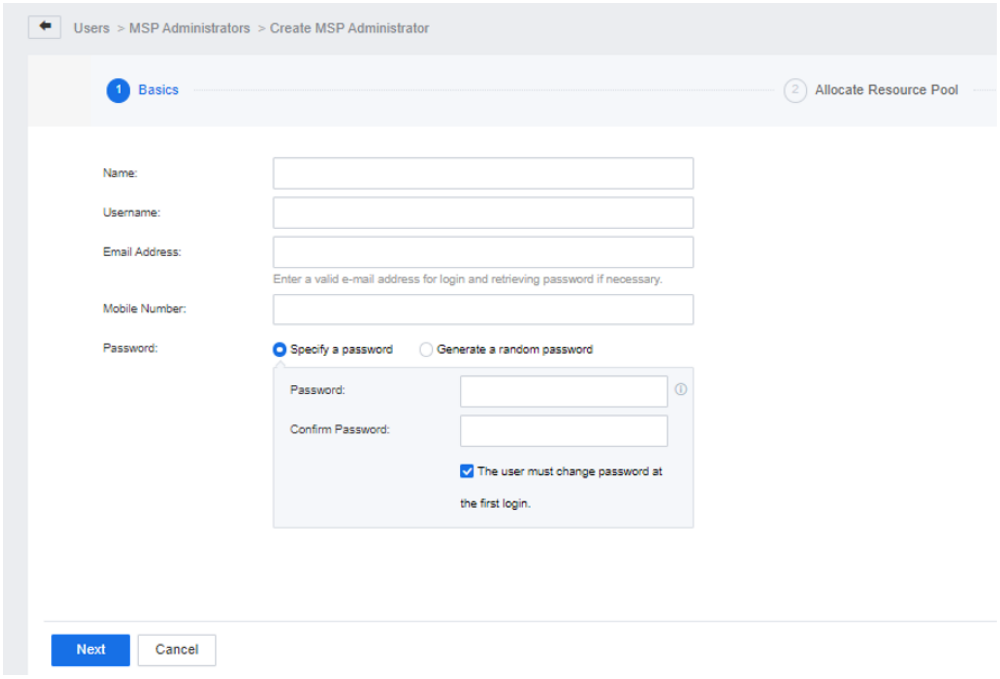


Step 3. Enter the administrator password.

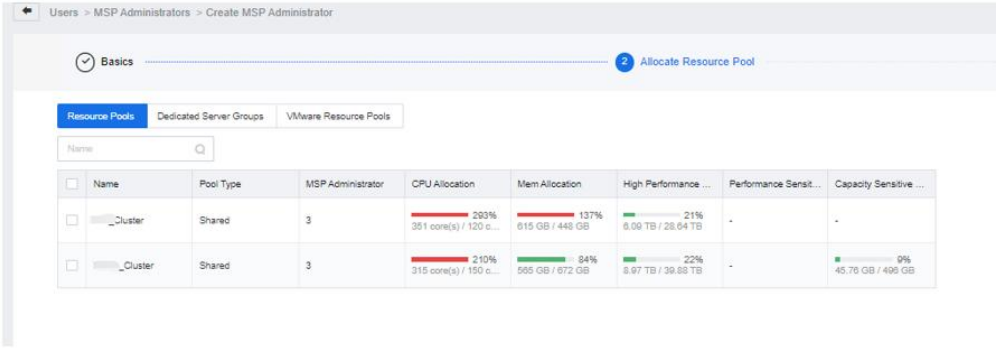


Step 4. The conversion to operation mode is completed. You can see the MSP Administrator page in the **User and Access Management** interface and the MSP Administrator Quota page in the **Quota Management** interface. Enter the MSP Administrator interface and click the **New** button to create a new operation administrator.

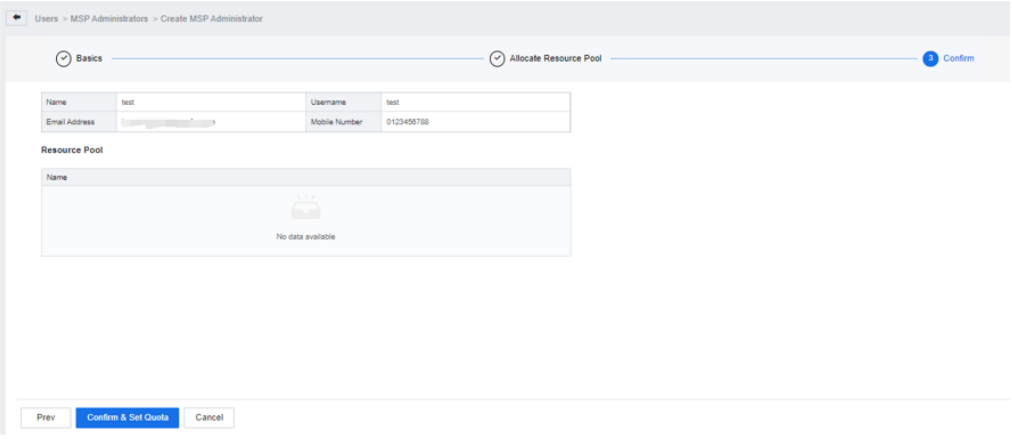




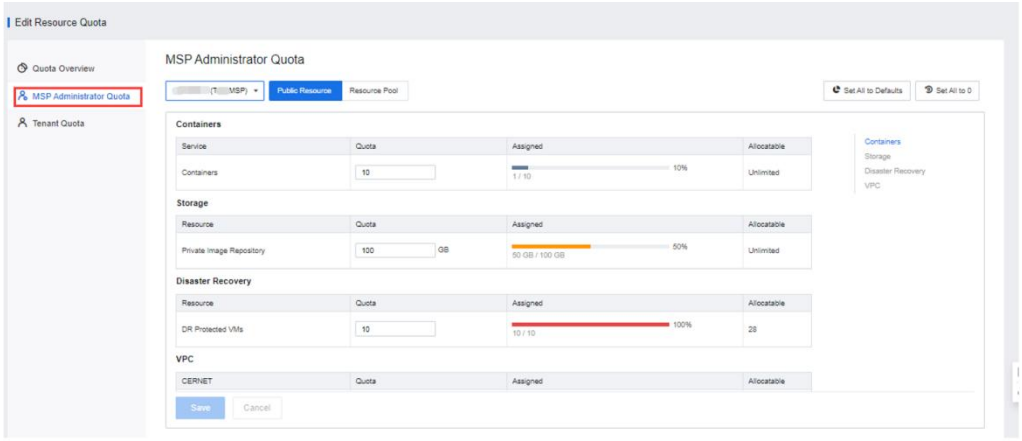
Step 5. Click **Next** to allocate resource pools. It supports the allocation of **HCI Resource Pools, Dedicated Server Groups**, and **VMware Resource Pools** for MSP administrators.



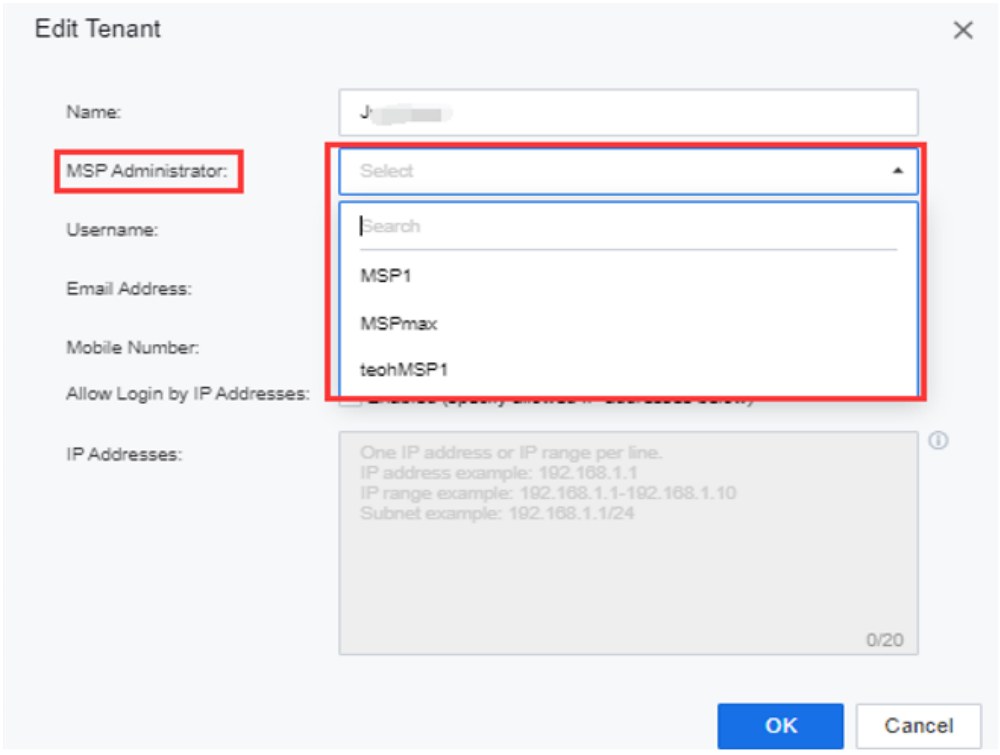
Step 6. Click **Confirm and Set Quota** to complete the operation administrator creation.



Step 7. After the MSP administrator is created, enter the **MSP Administrator Quota** interface to set the quota for the operation administrator.



Step 8. Go to the **User and Access Management** > **User** > **Tenant** interface, find the tenant for which an operation administrator is not specified, and click **Edit** to specify an MSP administrator.



4.10.1.3 Permission Policies

Function Description

Super admin can grant different users and organization administrators more than 100 permissions on resources such as VMs, resource pools, and NFVs.

Precautions

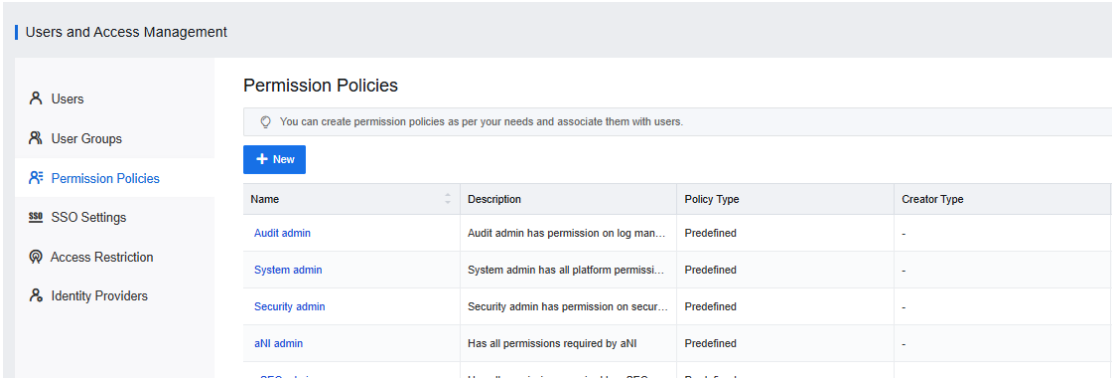
Super admin can grant permissions to platform administrators but not tenants. The tenant can grant permissions to tenant co-administrators but not tenant users.

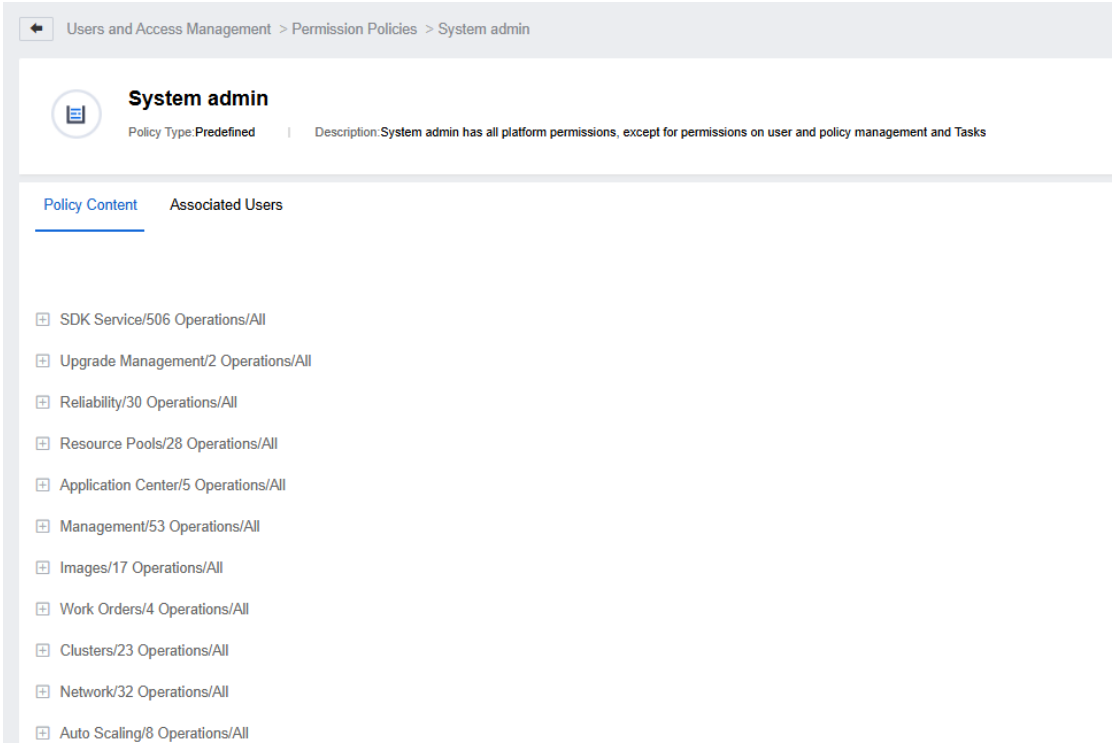
Prerequisites

Permission policies are available on SCP 6.9.0 and later versions.

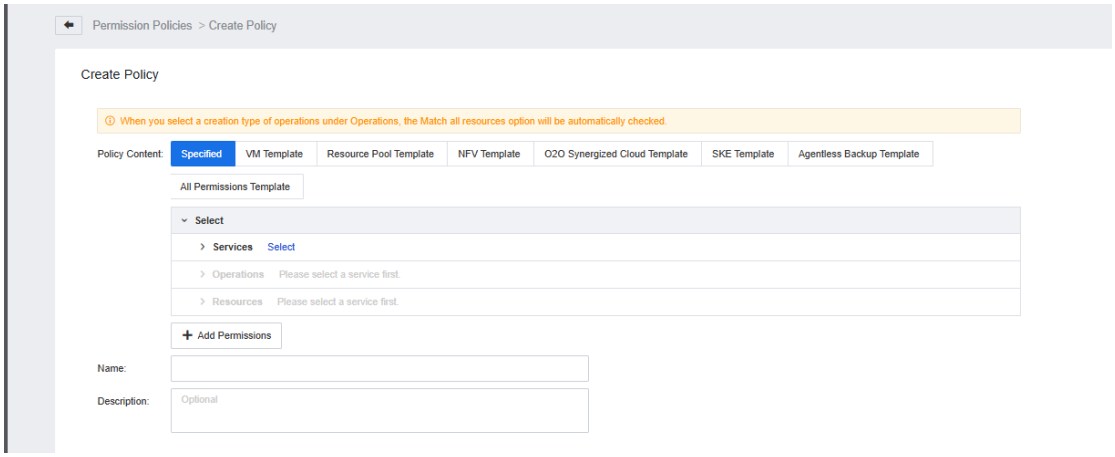
Steps

1. Go to **Users and Access Management** > **Permission Policies** to view the five permission policy templates, namely security administrator, aSEC administrator, audit administrator, aNI administrator, and system administrator. Click one of them to view the associated permissions.





2. Click **New** to create a policy and associate it with a user.



4.10.1.4 Tenant Management

There are three roles in SCP's multi-tenant management model: platform administrator (admin), tenant, and tenant user account. For example, a company (platform) has multiple departments (tenants), and each department has several employees (tenant user). Several tenants can be allocated on the Sangfor cloud computing platform, corresponding to each department. Several tenant sub-accounts can be allocated under the tenants, corresponding to the department's employees. The company needs to designate a platform administrator (admin), and each department needs to designate a tenant.

1. Create Tenant

Function Description:

Guide the platform administrator to create a tenant.

Precautions:

None.

Prerequisite

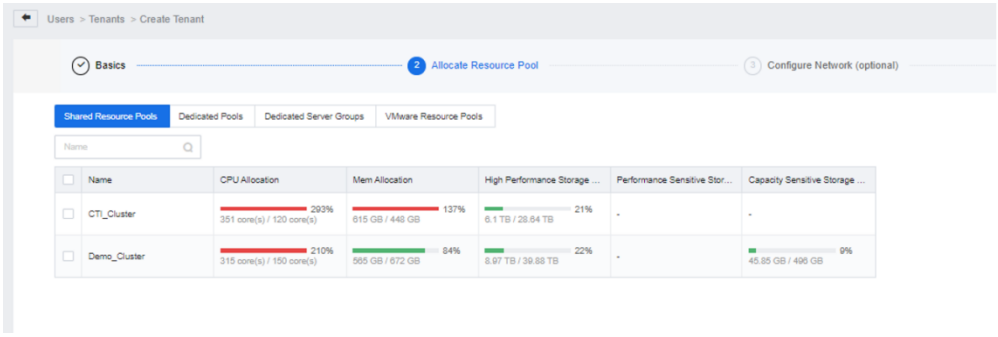
- Sangfor SCP has managed the cluster and created the resource pool.
- When creating a tenant VPC network, you need to plan the VPC network egress of the resource pool associated with the tenant in advance.

Steps:

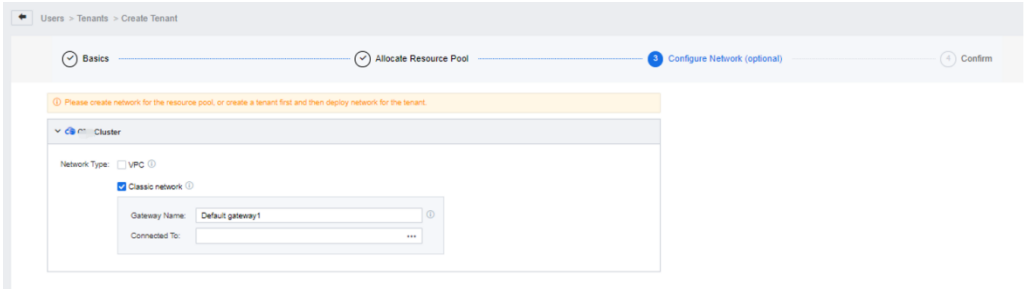
Step 1. Log in to the SCP platform, and select **User and Access Management** > **User** > **Tenants.** Then, click the **New** button to create a tenant.

Step 2. Enter the tenant's name, login username, email address, mobile phone number, and password, and click **Next**.

Step 3. Allocate resource pools and select the resource pool resources that the tenant can use. The resource pool attributes are divided into **Shared Resource Pools** and **Dedicated Pools**. A shared resource pool can be assigned to multiple tenants, and one tenant can be associated with multiple shared resource pools. However, a dedicated pool can only be assigned to one tenant, and a tenant can only be associated with one dedicated resource pool. (VMware resource pools can only be used as shared resource pools, not dedicated pools)



Step 4. Configure the network type of the tenant. VPC is selected by default. You can select the **Classic network** if you want to, fill in the **Gateway Name**, and select the **Connected To** device.



Step 5. Set quotas for tenants based on actual needs.

Step 6. Confirm the information. Click **OK** to create the static route.

2. Edit User

Function Description:

The platform administrator can edit the tenant and modify the tenant's name, email, and mobile phone number.

Precautions:

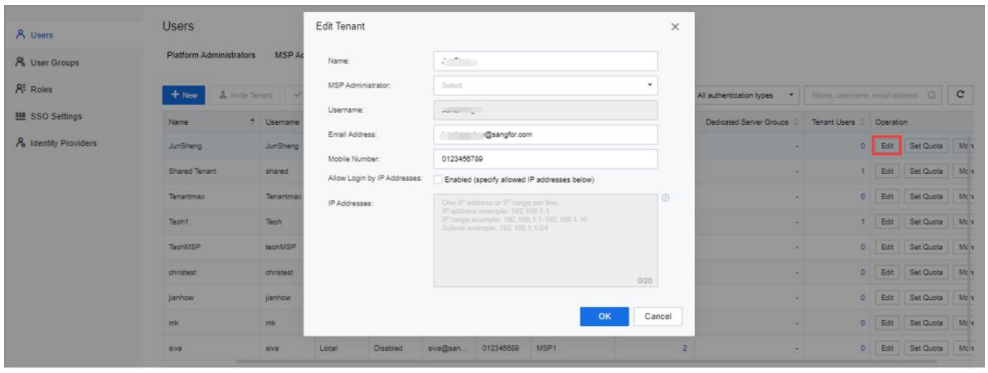
None.

Prerequisite

None.

Steps:

Log in to the SCP platform, and select **User and Access Management > User > Tenants.** Then, click **Edit** to edit the tenant.



3. Set Quota

Function Description:

Platform administrators can **Set Quota** for tenants. Quotas are subdivided into **Public Resource** and **Resource Pool**. Resource pool quotas are related to virtual devices running on resource pools, such as computing, storage, and security devices. Public resource quotas are those unrelated to resource pools, such as elastic IP, disaster recovery licensing, and container.

Precautions:

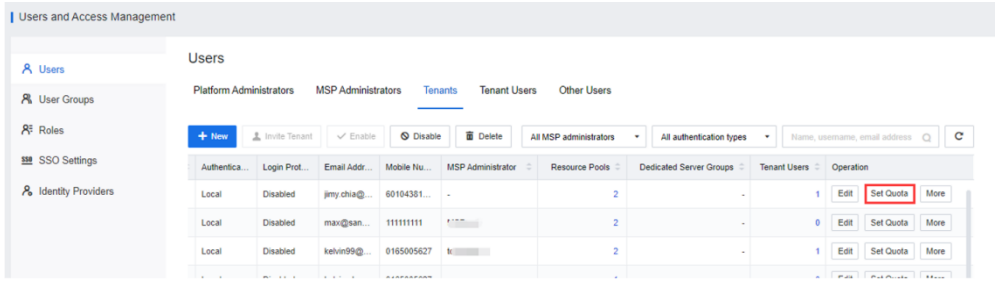
None.

Prerequisite

None.

Steps:

Log in to the SCP platform, select **User and Access Management** > **User** > **Tenant**, and click **Set Quota** to modify the tenant's quota.



4. Reset Password

Function Description:

The platform administrator can reset the password of the tenant.

Precautions:

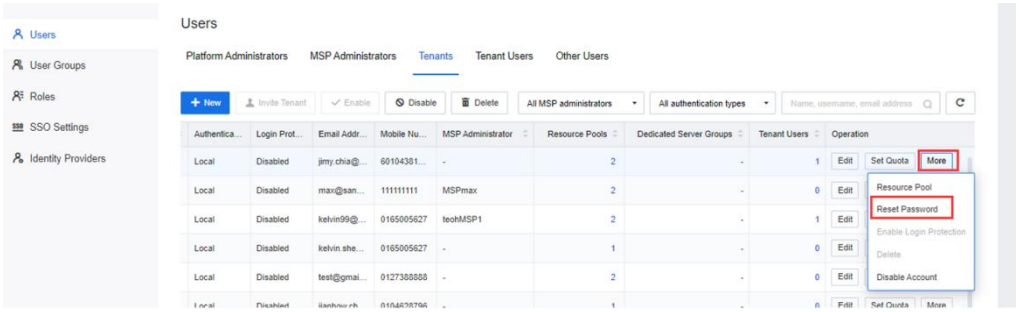
None.

Prerequisite

None.

Steps:

Log in to the SCP platform, select **Users and Access Management** > **Users** > **Tenants**, click **More,** and select **Reset Password.** Then, enter a new password and click **OK**.



5. Disabled Tenant

Function Description:

Platform administrators can disable tenants.

Precautions:

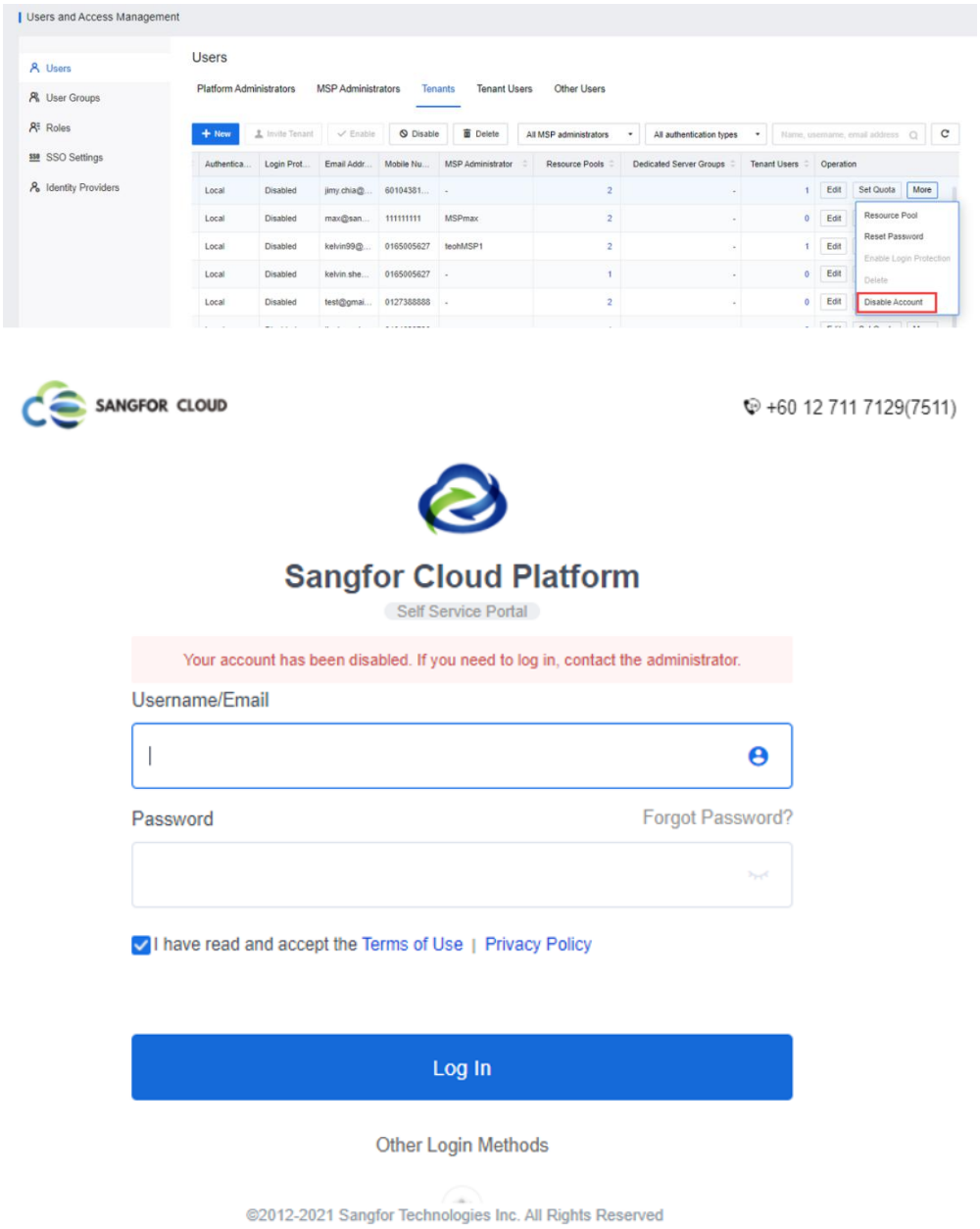
After the tenant is disabled, the tenant and all users under the tenant are not allowed to log in to the SCP platform, which does not affect the normal operation of the virtual machine.

Prerequisite

None.

Steps:

The platform administrator logs in to the SCP platform selects **User and Access Management** > **Users** > **Tenants**, clicks **More**, selects **Disable Account**, and enters the platform administrator's password to confirm and disable it.



6. Delete Tenant

Function Description:

Platform administrators can delete tenants.

Precautions:

A tenant cannot be deleted when there are tenant users.

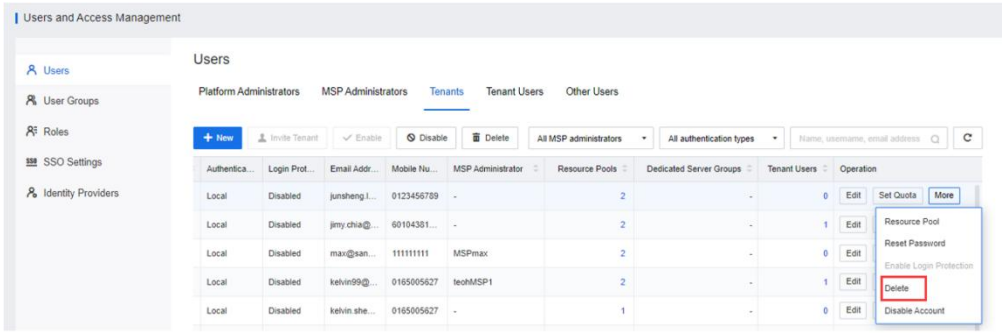
Prerequisite

None.

Steps:

The platform administrator logs in to the SCP, selects **User and Access**

Management > **User** > **Tenant**, clicks **More**, selects **Delete**, and enters the platform administrator's password to delete.



4.10.1.5 Tenant User Management

1. Create a tenant user

Function Description:

Platform administrators can delete tenant users.

Precautions:

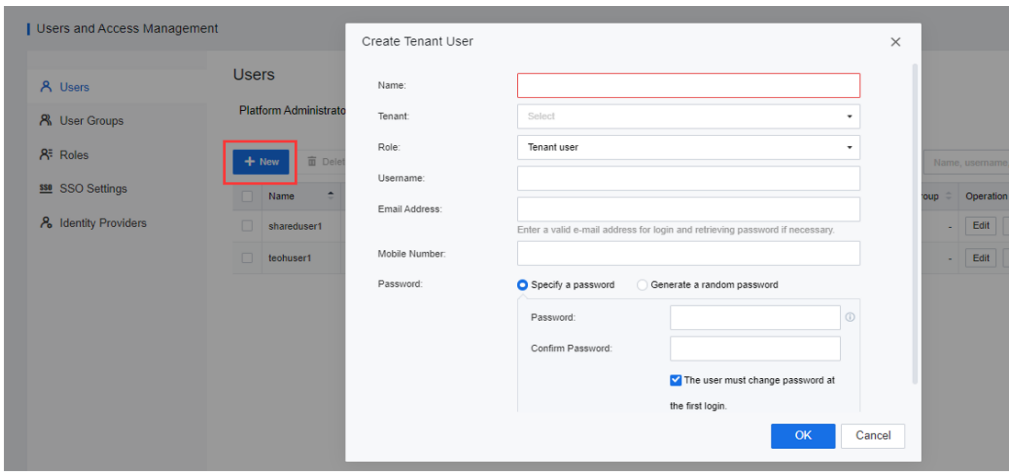
None.

Prerequisite

None.

Steps:

The platform administrator logs in to the SCP platform, selects **User and Access Management** > **User** > **Tenant Users**, clicks **New**, enters the corresponding information, selects the tenant to be associated with, and clicks **OK**.



2. Edit Tenant User

Function Description:

The platform administrator can edit the tenant user and modify the name, email, mobile phone, and the tenant of the tenant user.

Precautions:

None.

Prerequisite

None.

Steps:

The platform administrator logs in to the SCP platform, selects **User and Access Management** > **User** > **Tenant User**, and clicks **Edit** on the tenant user you wish to edit.

3. Reset password

Function Description:

The platform administrator can reset the password of the tenant user.

Precautions:

None.

Prerequisite

None.

Steps:

The platform administrator logs in to the SCP platform selects **User and Access Management** > **User** > **Tenant User**, selects the tenant user who needs to reset the password and clicks **Reset Password**.

4. Delete Tenant User account

Function Description:

Platform administrators can delete tenant users.

Precautions:

None.

Prerequisite

It cannot be deleted when the tenant user has a virtual machine. However, you can delete or deallocate the virtual machine to the tenant and platform and then delete the tenant user account.

Steps:

The platform administrator logs in to the SCP platform selects **User and Access Management** > Users > **Tenants**, clicks More, selects **Disable Account**, and enters the platform administrator's password to confirm and disable it.

4.10.2 Quota Management

4.10.2.1 Quota Overview

Function Description:

Platform administrators can view the quota overview to understand the allocation of basic platform resources and NFV resources.

Precautions:

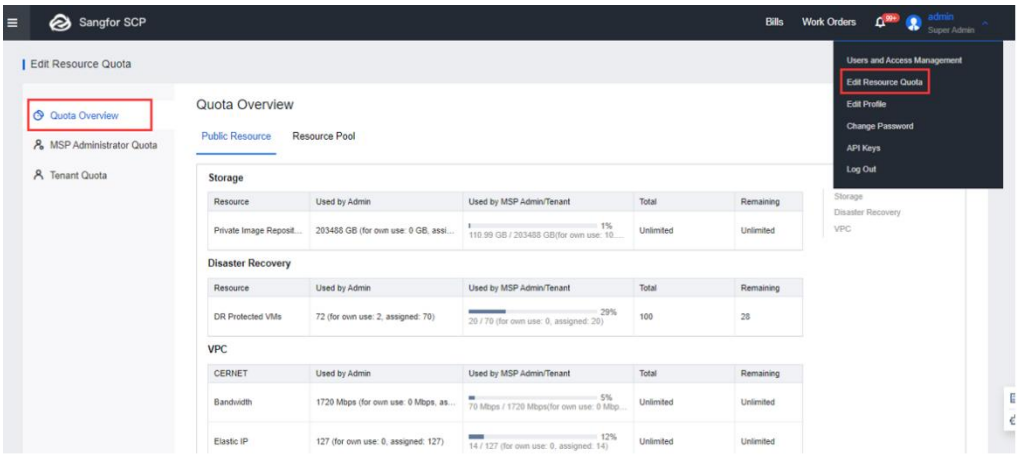
None.

Prerequisite

None.

Steps:

The platform administrator logs in to the SCP platform and selects **Edit Resources Quota** > **Quota Overview.**



4.10.2.2 Tenant Quota

Function Description:

Platform administrators can set tenant quotas and export tenant quota reports to understand the allocation of basic tenant resources and NFV resources.

Precautions:

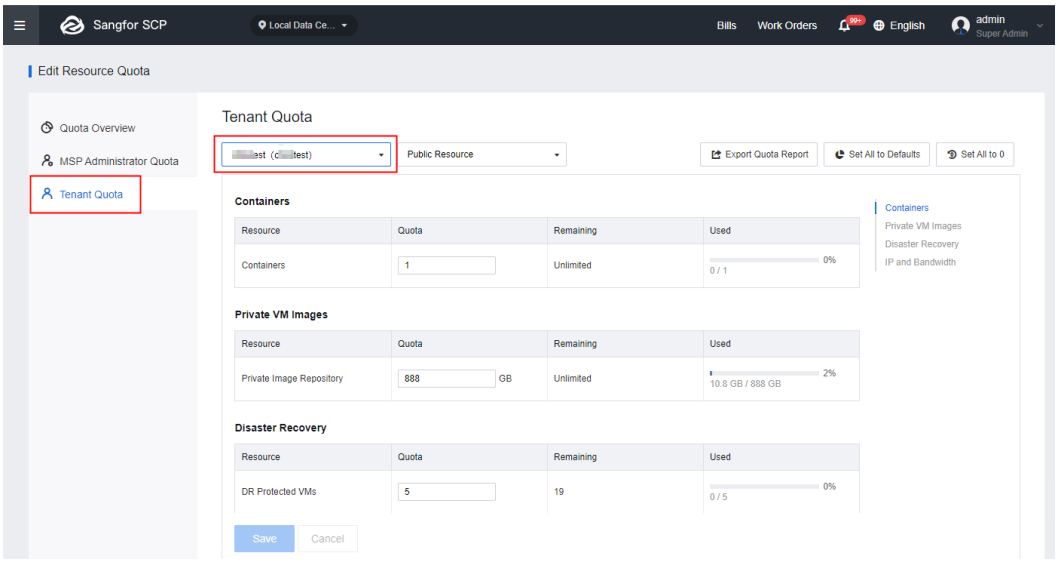
None.

Prerequisite

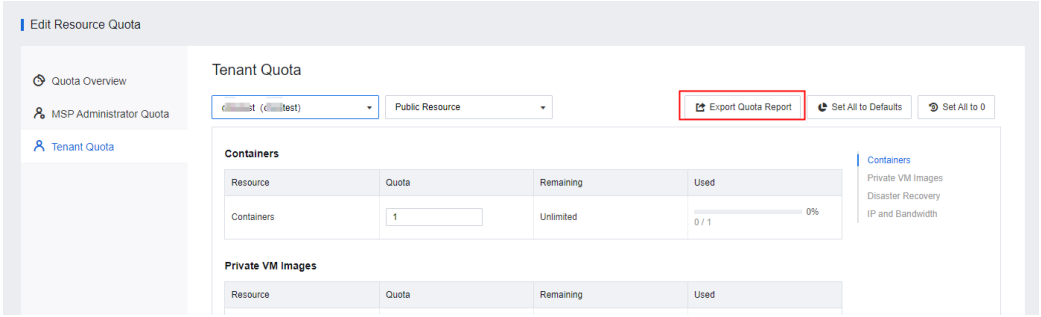
None.

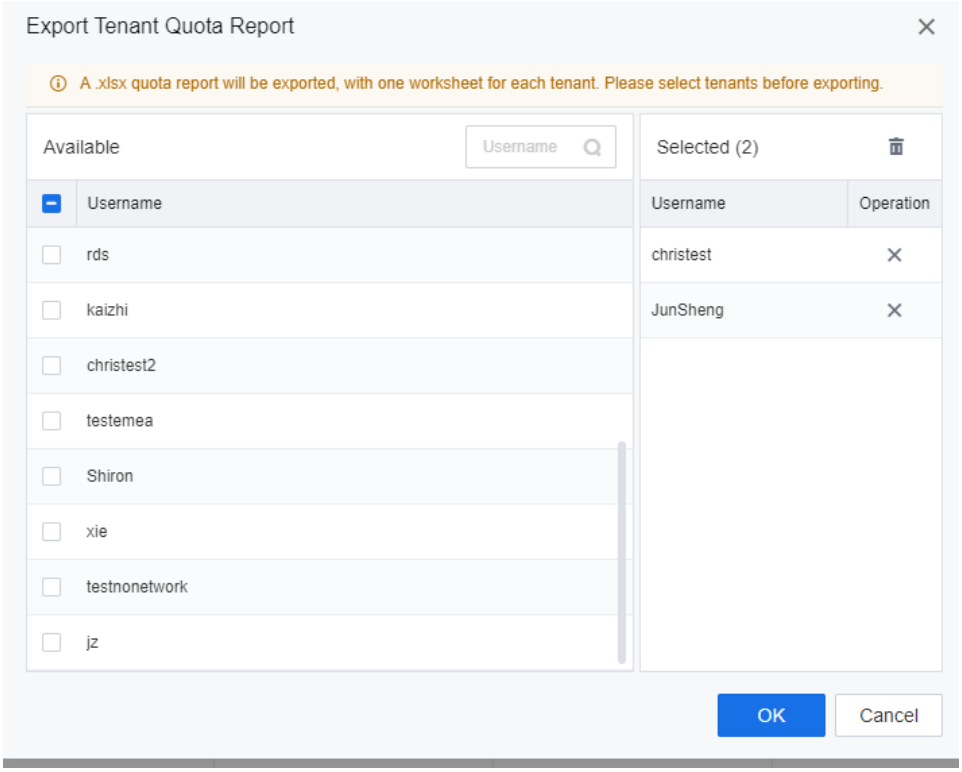
Steps:

Step 1. The platform administrator logs in to the SCP platform and selects **Edit Resource Quota > Tenant Quota** to view the usage and allocation of all resources of the currently selected tenant.



Step 2. Click **Export Quota Report** to export tenant quota information to the local computer.





4.10.3 Work Order Management

4.10.3.1 Create an Workflow Template

Function Description:

When a tenant or tenant user applies for quota change, application, or change of virtual machine, it needs to apply through a work order, and the corresponding administrator can approve it after receiving the work order. The admin administrator can set the approval process of the work order according to the actual situation.

Precautions:

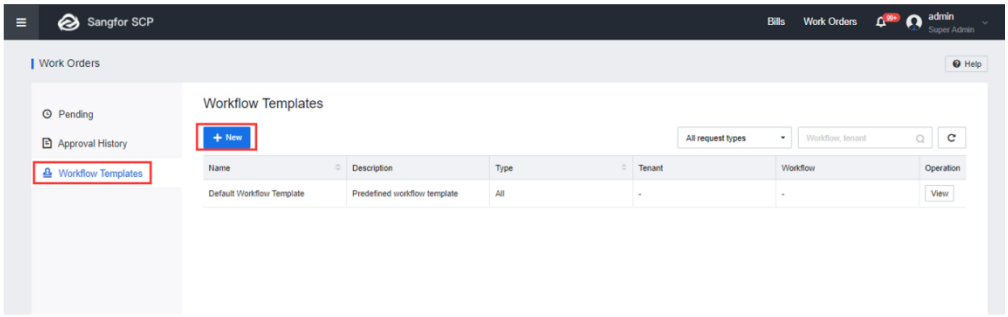
1. When no custom workflow template is created, it will use the platform's default workflow template.
2. After customizing the workflow template, the custom workflow template will be prioritized over the default template.

Prerequisite

The corresponding approver account is created.

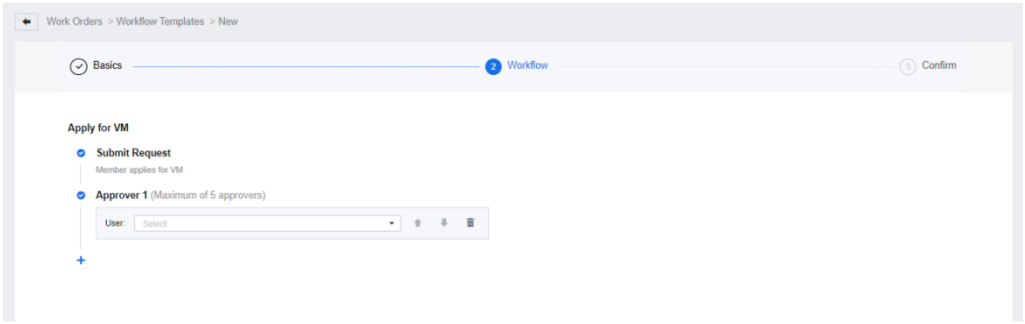
Steps:

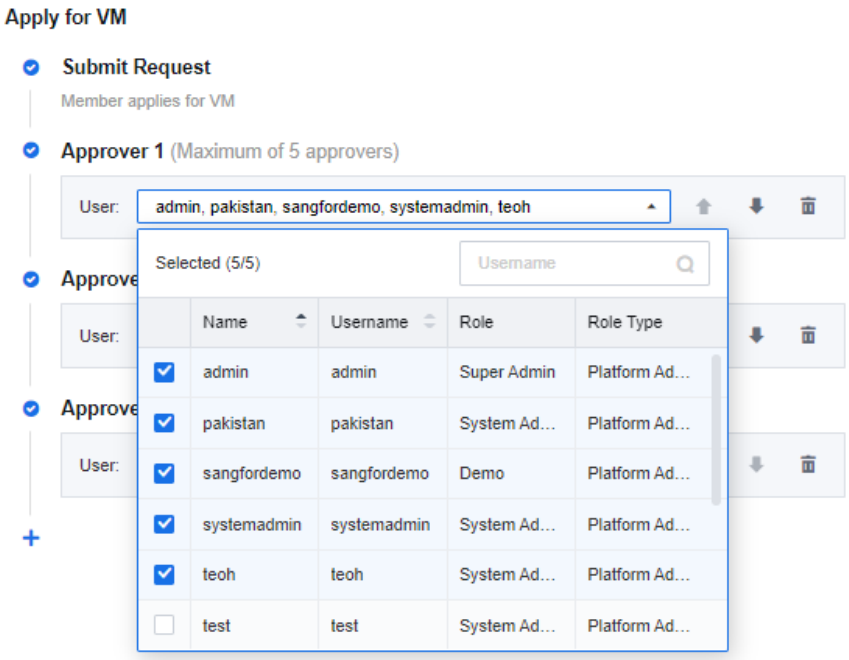
Step 1. Log in to the SCP platform, select **Work Orders** > **Workflow Templates (**the system has a built-in default template before the workflow template is created, all work orders are approved according to the default template), and click **New**.



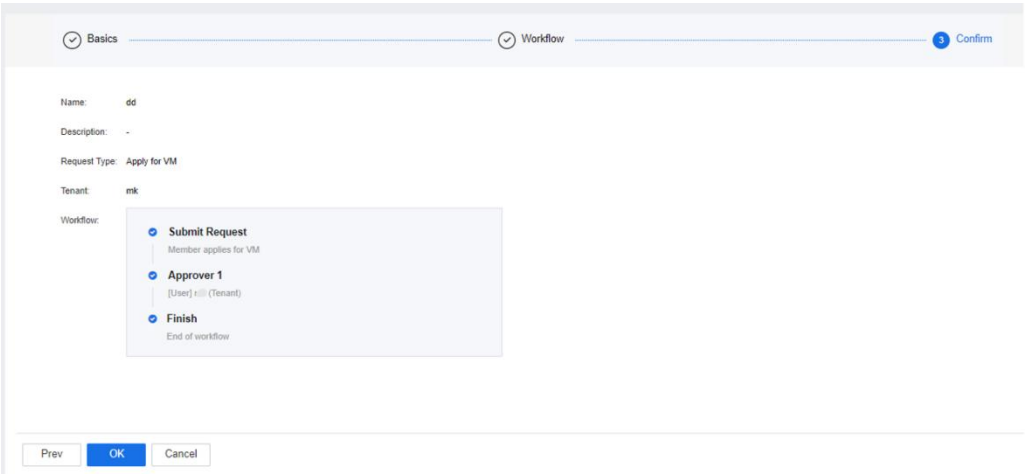
Step 2. Enter the name and description of the workflow template, select the **Request Type** and **Tenant**, and click **Next**.

Step 3. Select an approver. If multi-level approval is required, click **+** to add an approver. The position of each level of approver can be adjusted by clicking ↓↑, and up to 10 levels of approvers can be added. The current version supports parallel approval. A maximum of 5 approvers can be selected for every request.





Step 4. Click **OK.**



4.10.3.2 Create Work Order

Function Description:

1. When a tenant applies for a quota change, a work order needs to be created.
2. A work order must be created when a tenant user applies for or changes a virtual machine.

Precautions:

None.

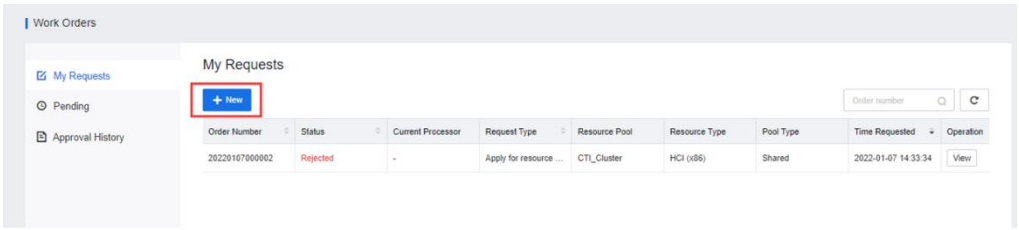
Prerequisite

None.

Steps:

Step 1. Apply for quota

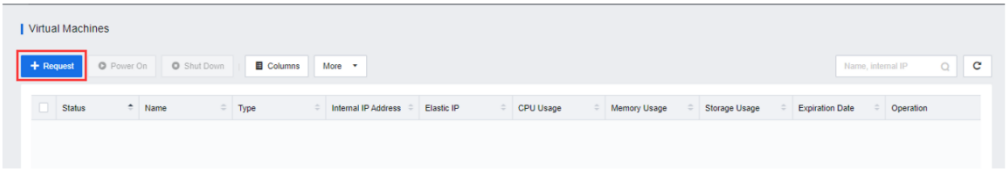
- From the IP address of https://SCP, log in to the tenant administrator, select **Work Order** > **My Requests**, and click **New** to create a work order.



- Enter the application's content and the reason for the application, and click **Apply Now** to complete the work order creation.

Step 2. Apply for virtual machine

- From the IP address of https://SCP, log in to the tenant user account, select **Virtual Machines**, and click **Request**.



- Select the resource pool to which the virtual machine belongs, the appropriate image, and the number of virtual machines, configure computing, storage, and network parameters, and enter the basic information of the virtual machine, the period of use, and the reason for the application, and click **OK** to complete the application.

Step 3. Change Virtual Machine

- From the IP address of https://SCP, log in to the tenant user account, select Virtual Machine, find the virtual machine that needs to be changed, click **More**, select **Change Configuration**, and configure computing, storage, network, etc. change.

4.10.3.3 Approve/Review Tickets

Function Description:

If the platform administrator and tenant account are added to the workflow template as approvers, they can view the approval application to approve and reject the work order and can modify the virtual machine configuration applied by the requester.

Precautions:

1. If the workflow template includes multiple levels of administrators, each administrator from a different level needs to approve.
2. When applying for a virtual machine, after the work order is approved successfully, it will take a certain amount of time for resources to be issued. The tenant user will need to wait for some time to see the applied virtual machine.

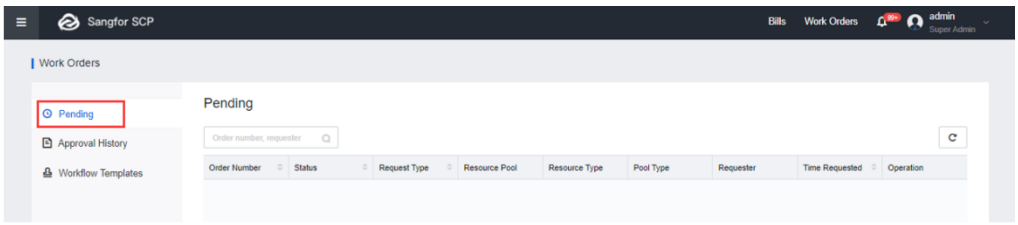
Prerequisite

1. An approver has been added to the ticket process.
2. The ticket has been correctly created and submitted.

Steps:

Step 1. The platform administrator approves/checks the work order.

- Log in to the SCP platform, click **Work Order** at the top right, and enter the workflow approval interface. On the **Pending** page, you can see the work orders that the platform administrator has not approved.



- Select a work order, and click **Approve.** Select a work order, and click Approve. You can see the work order's basic information and application content, modify the approval content according to the actual situation, and fill in the approval comments. The approval result can be **Rejected**, **Approved**, and **Cancel(for Work Order Initiator only).**

Step 2. Tenant approval/check work order.

- From the IP of https://SCP, log in to the tenant and select **Work Order** > **Pending.** You can see the currently unprocessed work order, select the work order, click **Approve**, and see the basic information of the work order according to the actual content of the application, modify the approval content and fill in the approval comments. The approval result can be **Rejected**, **Approved**, and **Cancel** (for Work Order Initiator only).

4.10.4 Billing Center

Function Description:

The admin can set the unit price for the resources of the platform. The current version supports basic pricing and tenant pricing. Different pricing can be set for different resource pools according to the actual needs of customers. Tenants can also be priced individually. Tenants can also be priced individually.

The SCP platform counts the tenant resource usage every 10 minutes, calculates the cost based on the usage and unit price, and updates the resource usage cost on the interface every 1 hour. Through billing management, resource management between tenants is quantified.

Precautions:

1. Pricing policy priority: Tenant individual pricing priority > MSP administrator pricing > Resource pool individual pricing > Resource pool default pricing.
2. The MSP administrator can view and export the consumption overview of all tenants under the tenant's name and account details and supports setting the unit price.

Prerequisite

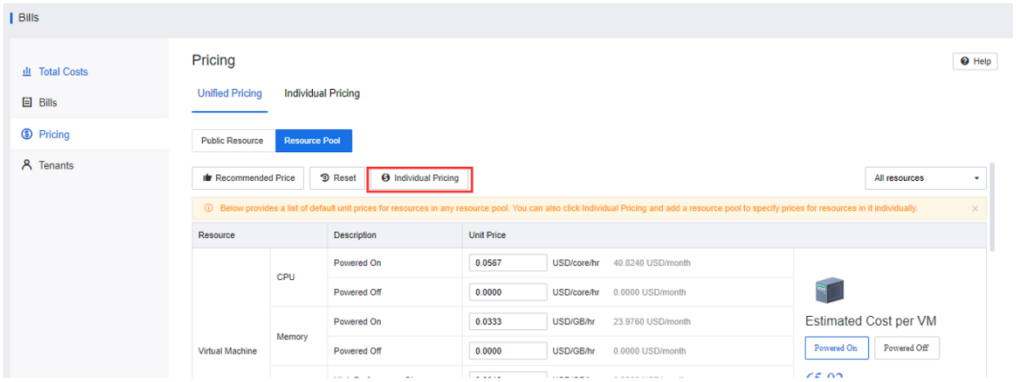
None.

Steps:

Step 1. Log in to the SCP platform and click the **Bills** button in the upper right corner to enter the **Pricing** interface.

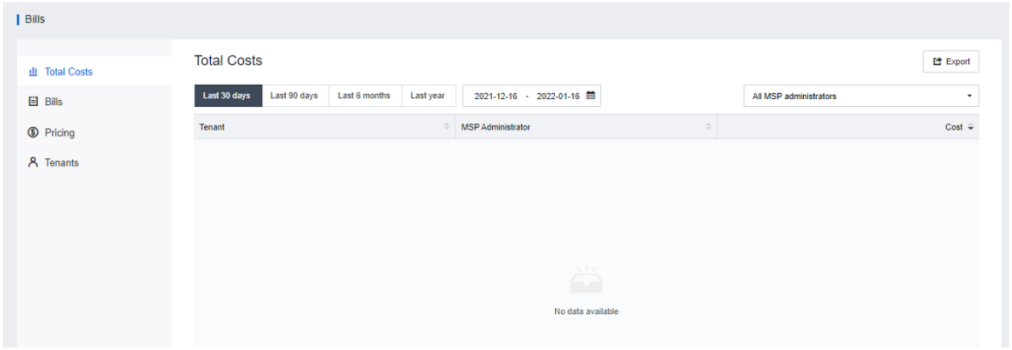
Step 2. You can set the price for the **Public Resources**: **Elastic IP**, **Private VM Images**, and **Disaster Recovery**. You can also set the price for **Resource Pool** resources: **Virtual Machine, Backup Repository**, and **NFV Resources**).

Step 3. Click **Resource Pool > Individual Pricing** to set separate pricing for resource pools with different performances.

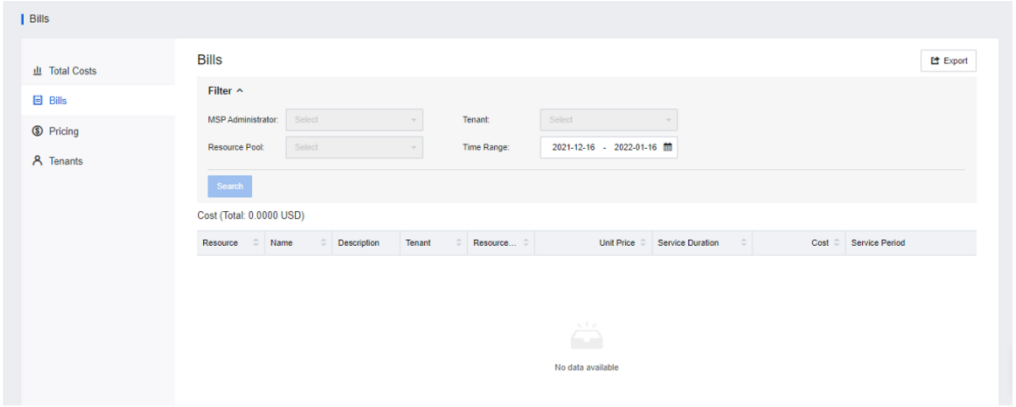


Step 4. Enter the **Individual Pricing** page to set the unit price for a tenant individually. Then, click **Add**, select the tenant whose unit price needs to be set and set the unit price.

Step 5. Select **Total Costs**, and set the period for statistics. Then, you can view the consumption profiles of tenants in the selected period and export reports (excel documents).



Step 6. Select **Bills** and set the **Time Range.** Then, you can query the consumption details of different tenants in the current period and export reports (excel documents).



4.10.5 Federal Authentication

Function Description:

Sangfor SCP supports SAML 2.0-based SSO (Single Sign-On) federal identity authentication.

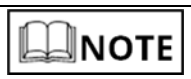
1. Administrators can connect with enterprise identity providers to support single sign-on of enterprise users to the SCP platform.
2. Support administrators or tenants to configure third-party service providers to extend the platform's users and user systems to third-party platforms to expand service catalogs.

- **Identity Provider (IdP for short):** Provides user authentication to ensure that users are who they claim to be.
- **Service Provider (SP for short):** An entity that provides formal services to users and usually needs to authenticate the identity of a user.
- **Assertions:** A collection of user authentication information, including when and how a user is recognized, and can also include some extended information, such as the user's email address and phone number.
- **MetaData:** SAML metadata is configuration data, which contains information about the parties involved in SAML communication, such as the ID of the other party in the communication, the IP address of the Web Service, the supported binding types, and the passwords used in the communication key, etc.

Precautions:

1. Service port configuration

   The federal identity authentication function requires that the Sangfor SCP can connect with enterprise identity providers or third-party service providers. The local data center information needs to be configured before connecting. For detailed configuration, kindly refer to **Chapter 4.11.5.5 Data Center Settings**.



The SCP cloud computing platform federal identity authentication is implemented based on the service port. Please ensure that the platform service port configuration is stable. Please update the data center configuration in time if there is any change.

2. Time Settings

7. In the process of federated identity authentication, most protocols need to verify the timestamp in the request. The single sign-on will fail if the time difference between the two communication parties is too significant. It is necessary to ensure that the SCP and the NTP server are networks reachable. For detailed configuration, please refer to **Chapter 4.11.5.3 Date And Time**.

4.10.5.1 SCP As An Identity Provider

Function Description:

SCP supports service providers configuring the SAML 2.0 protocol, where SCP acts as an identity provider. Once configured, tenants and tenant subaccounts can access third-party services through single sign-on.

Precautions:

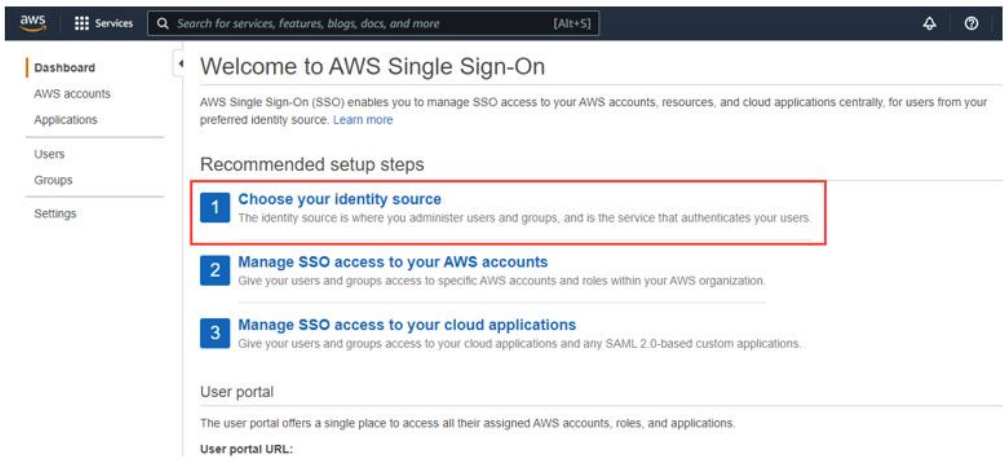
1. Only support the creation of service providers for tenants, each tenant can create up to 10 service providers, and the entire platform can create up to 500 service providers.
2. As an identity provider, SCP only provides two types of Issuer entries, HTTP-POST and HTTP-Redirect, and only supports service providers of HTTP-POST type.
3. If the SCP has active/standby, you need to reconfigure the service provider after the active/standby switchover.

Prerequisite

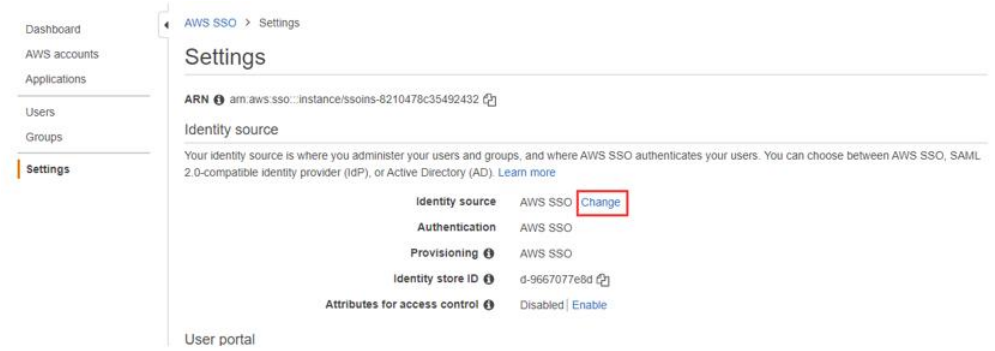
1. The metadata file of the target service provider has been obtained.
2. The client can access the SCP and the target service provider normally simultaneously.

Steps: (We take AWS as the service provider SP as an example)

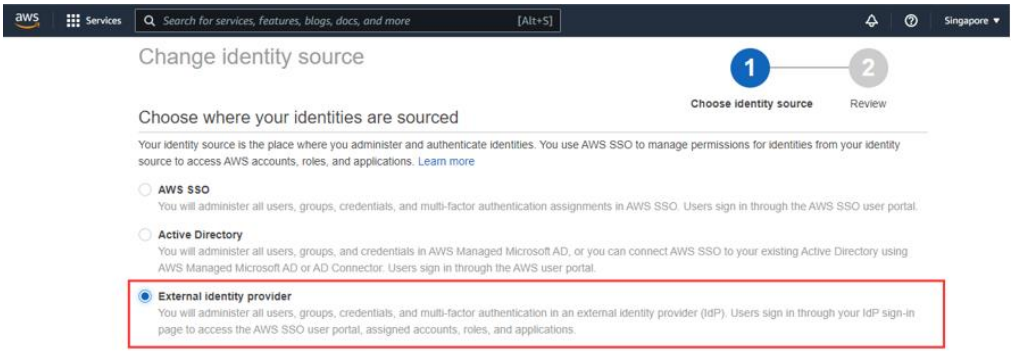
Step 1. Log in to the AWS SSO portal and click **Choose your Identity Source**.

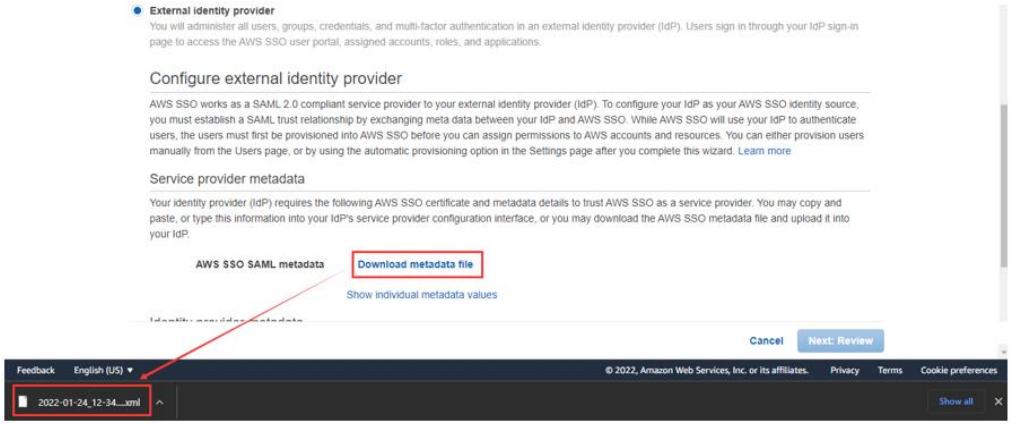


Step 2. Under **Settings**, click the **Change** button to change the Identity source.



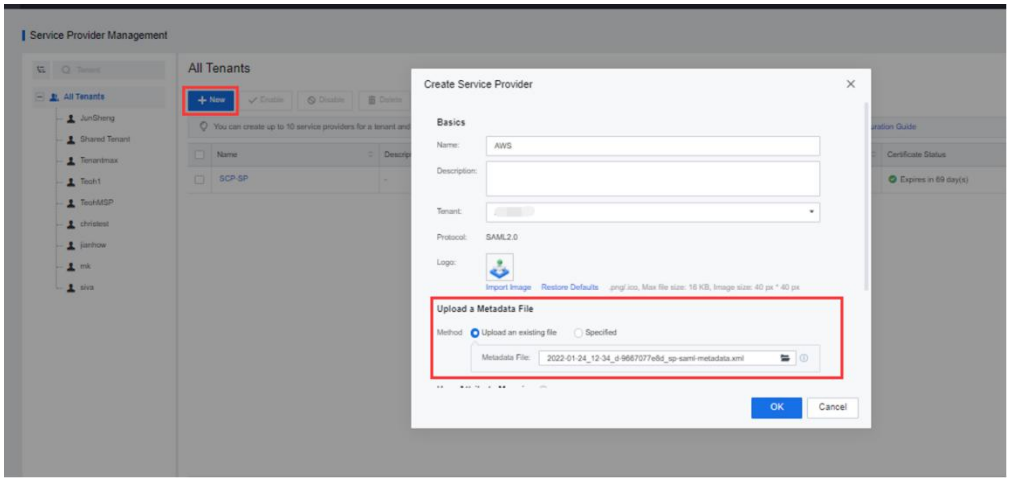
Step 3. Select **External Identity provider** and click **Download metadata file**.





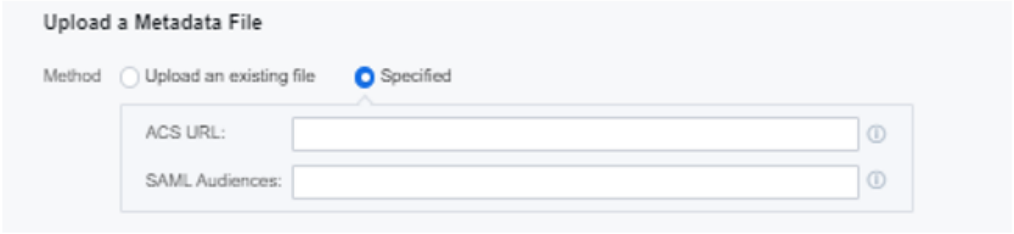
Step 4. The administrator logs in to the SCP, then navigate to the **Application Identity Service** > **Service Provider Management** page and create a service provider for AWS Cloud. Click the **New** button, and on the pop-up page, enter the name and select the tenant to which it belongs.

Step 5. Select **Upload an existing file** in **Upload a Metadata File** to upload the metadata file obtained from AWS.

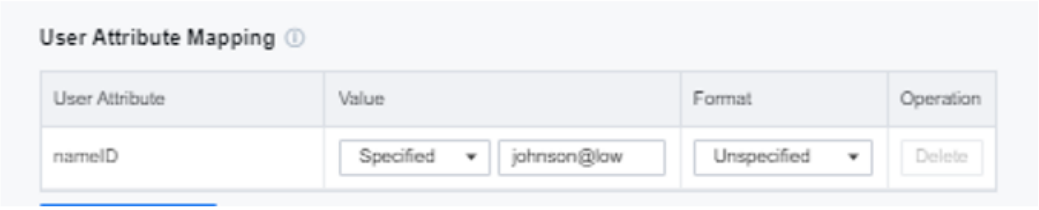


NOTE

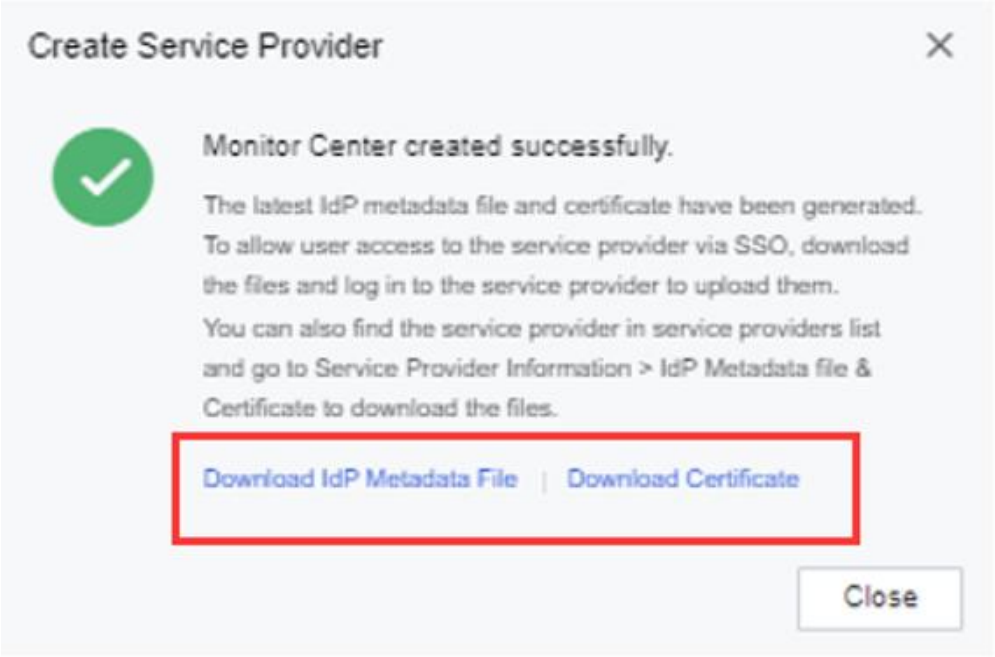
For third-party service providers, select **Upload an existing file** if a metadata file is provided. Otherwise, you need to select **Specified** and manually fill in the service provider's **SAML Audiences** and **ACS URL.**



Step 6. Configure the **User Attribute Mapping**, connect the service provider **User Attribute**, select **Specified** for **Value**, and fill in the User Login Name of AWS.



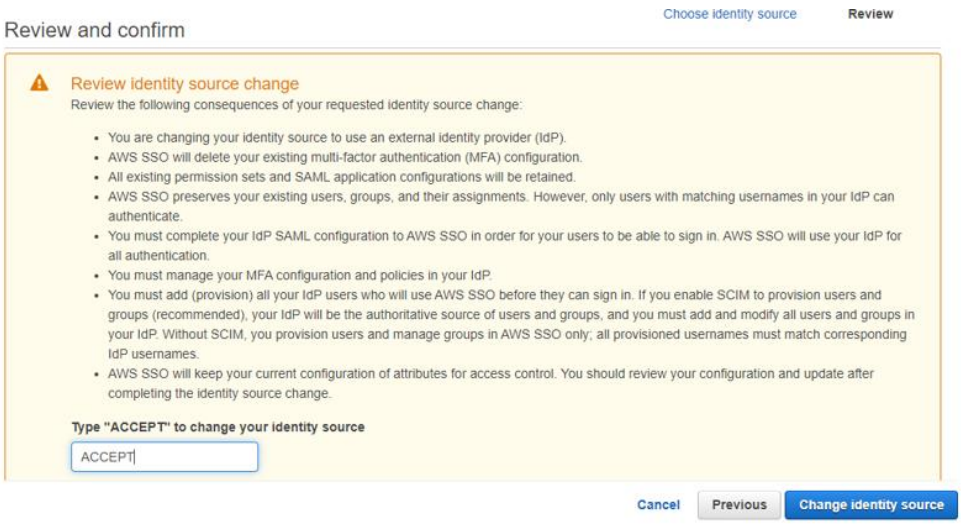
Step 7. Download Metafile from SCP and upload it to AWS.

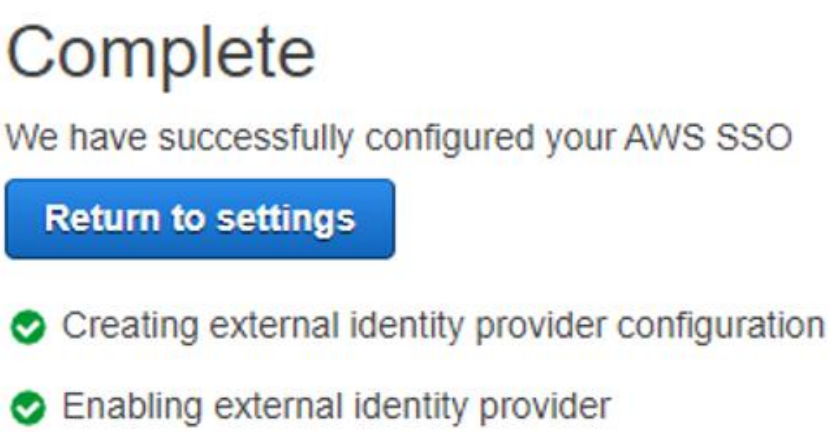


Step 8. Go back to the AWS web console, upload the Idp metadata document, and add SCP as the identity provider.



Step 9. Type **ACCEPT** to confirm to change identity source.

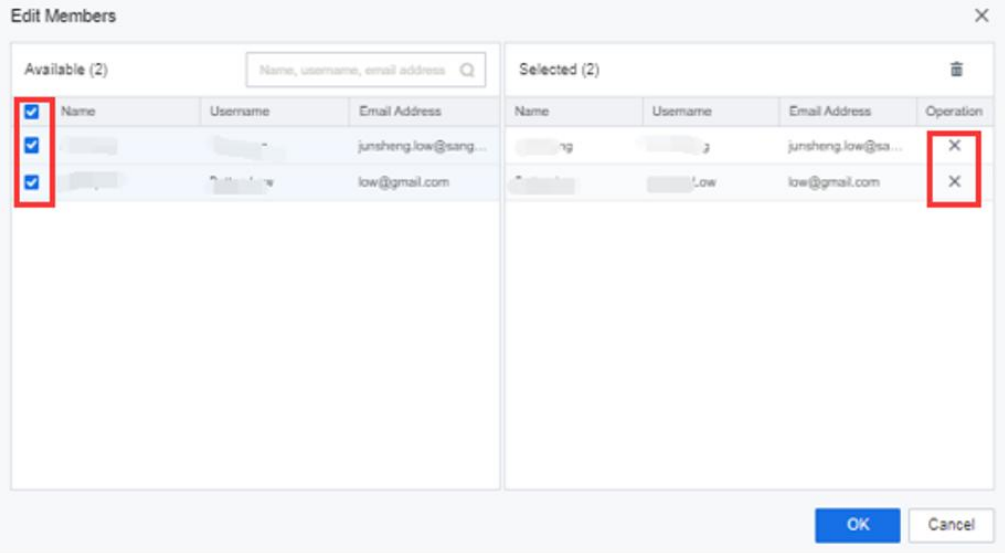




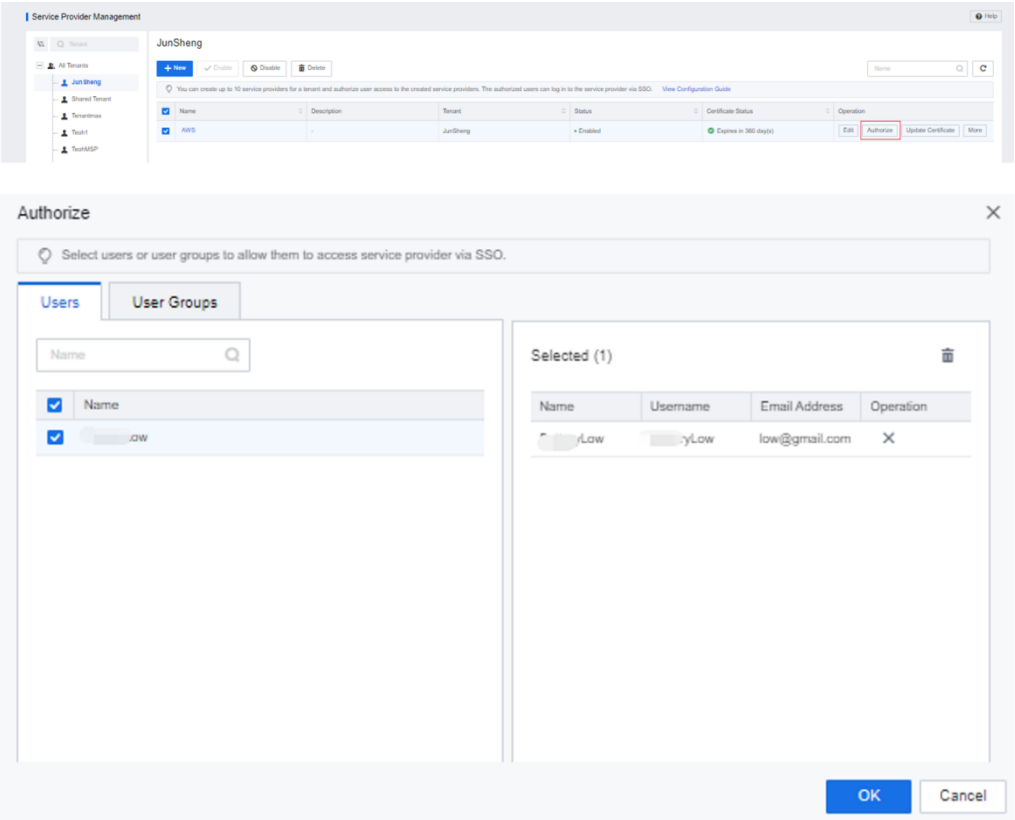
Step 10. Set up access authorization.

- The SCP administrator logs in to the **User and Access Management** > **User** interface to create tenants and tenant users that require single sign-on.
- Create a user group (optional), add multiple tenants or tenant sub-accounts to the user group, and implement batch authorization for users in the user group.

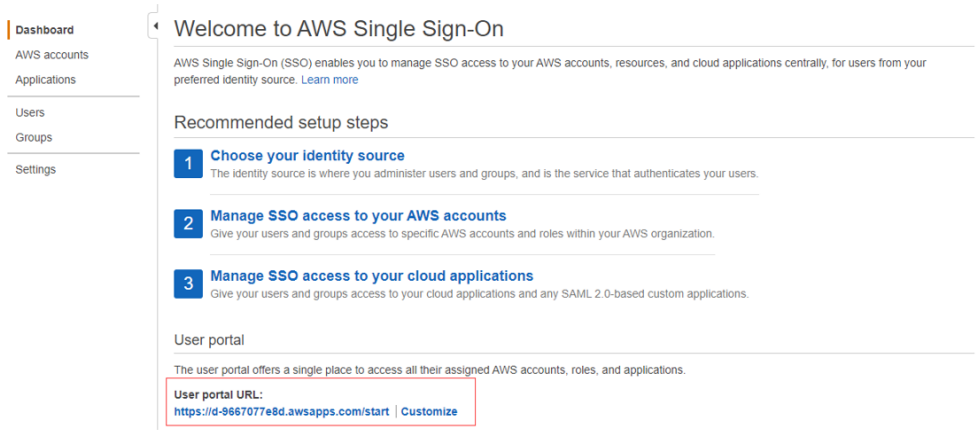
Enter **User and Access Management** > **User Group** to create a user group. After completing the creation, click **Edit group members** to add or delete user group members.



- Enter the **Service Provider** interface, find the record of AWS, click **Authorize**, and select the users and user groups to be authorized.



Step 11. After the configuration is complete, on the **Dashboard** page of the AWS Web Console, obtain the user login address, copy it to the browser, and redirect to the SCP to implement single sign-on.



4.10.5.2 SCP As Service Provider

Function Description:

The SCP platform supports the creation of identity providers of the SAML2 protocol, where SCP acts as a service provider. Due to the nature of the SAML2 protocol, no network connection is required between the SCP and the target identity provider.



Be sure to confirm the legitimacy of the identity provider. SCP will recognize the legitimacy of the identity provider site user. Illegal identity providers may log in to SCP through illegal accounts, resulting in loss of platform resources! Please carefully check the contents of the identity provider metadata document before proceeding.

Precautions:

1. As a service provider, SCP only provides HTTP-POST type SAML assertion consumption entry. Please confirm that the target identity provider supports this type.
2. Currently, up to 10 identity providers can be created.
3. If there are active and standby SCPs, the identity provider needs to be reconfigured after the active and standby switchover.

Prerequisite

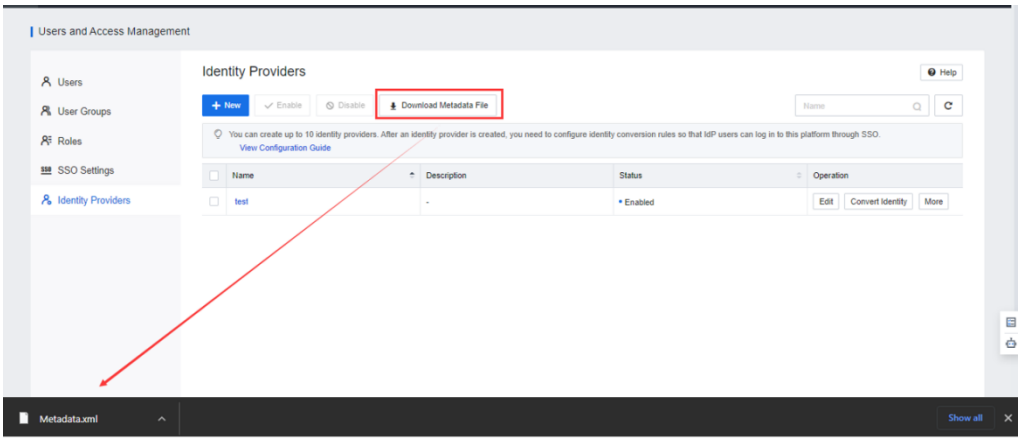
1. 1. The metadata document of the target identity provider can be obtained.
8. 2. The client can access the SCP and the target identity provider

simultaneously.

9.

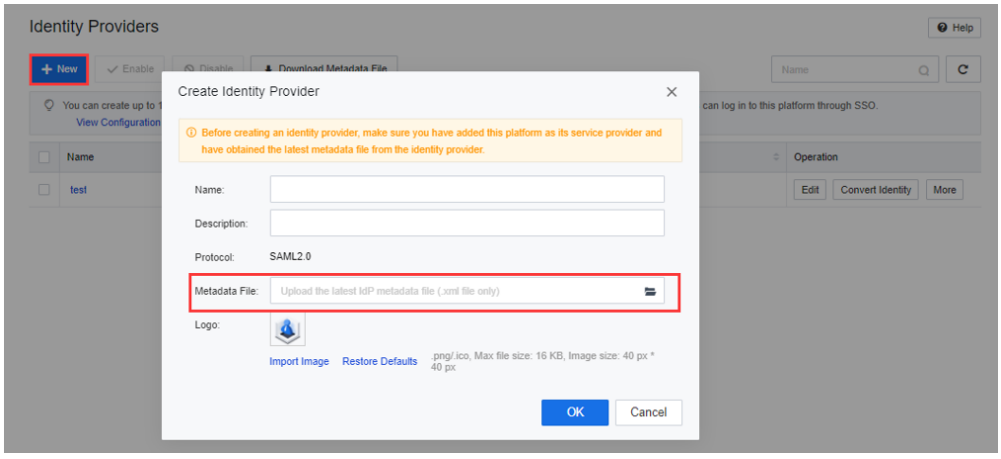
Steps:

Step 1. The administrator logs in to the SCP platform and selects **User and Access Management** from the drop-down box in the upper right corner. Select **External Identity provider** and click **Download metadata file**.



Step 2. Log in to the target identity provider site, upload the metadata document, and add SCP as its service provider. Once done, get the metadata document provided by the identity provider for the SCP.

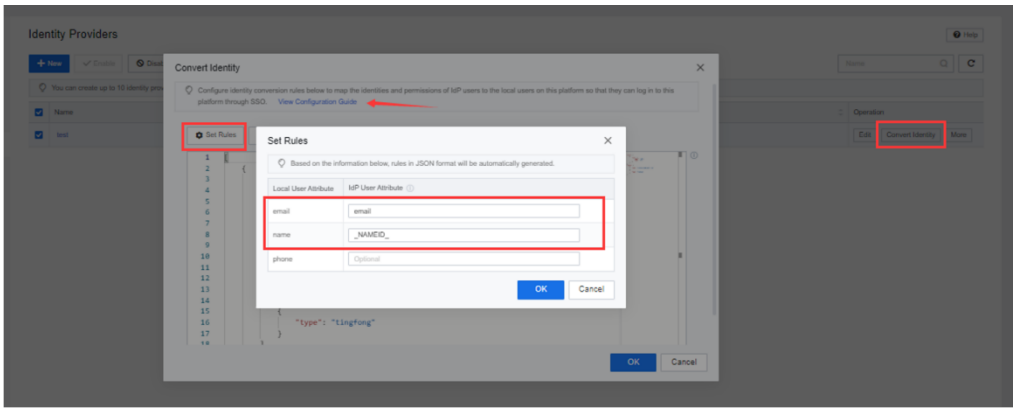
Step 3. Go back to the **Identity Provider** page of SCP, click **New**, fill in the basic information of the target identity provider, upload the metadata document obtained in the previous step, and click **OK**.



Step 4. Configure the identity conversion policy and fill in the user attributes of the identity provider corresponding to the local user attributes.

NOTE

Name is the default attribute value, and the fixed format is **__NAMEID__** (two underscores before and after). Otherwise, it will not be recognized. Otherwise, it will not be recognized. For details, see the interface configuration document.



Step 5. After completing the configuration, enter the SCP login interface. You can see **Other Login Methods** at the bottom. Click it to enter the identity provider page for single sign-on.



4.11 Storage

4.11.1 OSS

Scenario Description

Sangfor Object Storage Service (OSS) is a secure, highly reliable, and low-cost object-based storage service that allows you to store large amounts of data. OSS integrates Sangfor Enterprise Distributed Storage (EDS) to provide users with object storage and cloud data storage and processing capabilities.

Precautions

1. OSS needs to work with EDS 3.0.6 with the EDS 3.0.6.263-20210819204439.zip service pack or EDS 3.0.8 or later.
2. OSS requires the Enterprise Edition or Enterprise Plus Edition license.

4.11.1.1 OSS Network Settings

This function connects to the object storage service of EDS via SCP to provide object storage access capabilities for VMs. Specifically, EDS object storage buckets and accounts are created and managed on SCP over the management network. In this case, VMs can access object storage over the storage WAN of EDS through the business interface of HCI.

4.11.1.2 Physical Network Topology Settings

1. Connect the storage WAN of EDS used for providing object storage services to the business switch group of an HCI cluster.
2. Share or connect the management switches for HCI and EDS.

Virtual Network Settings

1. Ensure that the EDS management network is connected to the SCP management network.
2. Ensure that the business network is connected to the shared service network of SCP in a tenant VPC.

3. If the business traffic is heavy, you are advised to add a physical NIC separately as the shared service gateway and avoid reusing the outbound business interface as the shared service gateway.

4.11.1.3 Activate OSS

Function Description

This section instructs how to activate OSS.

Precautions

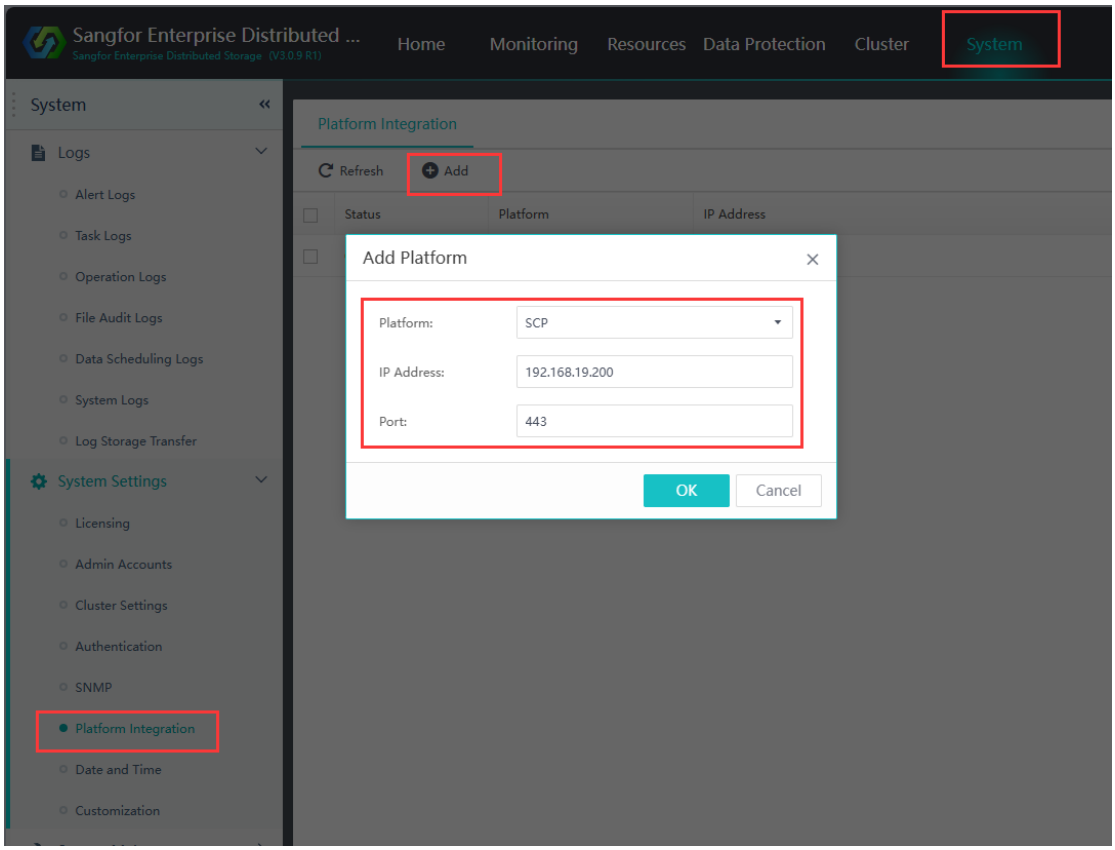
None

Prerequisites

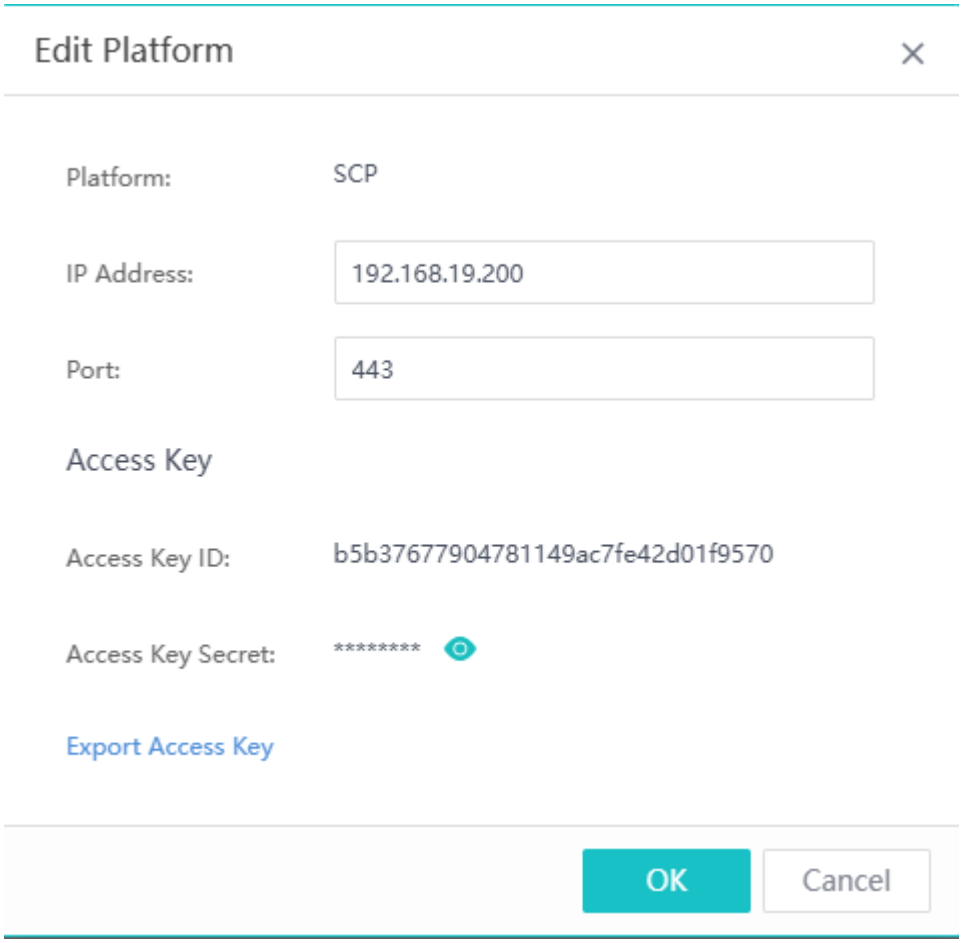
EDS has been deployed.

Procedure

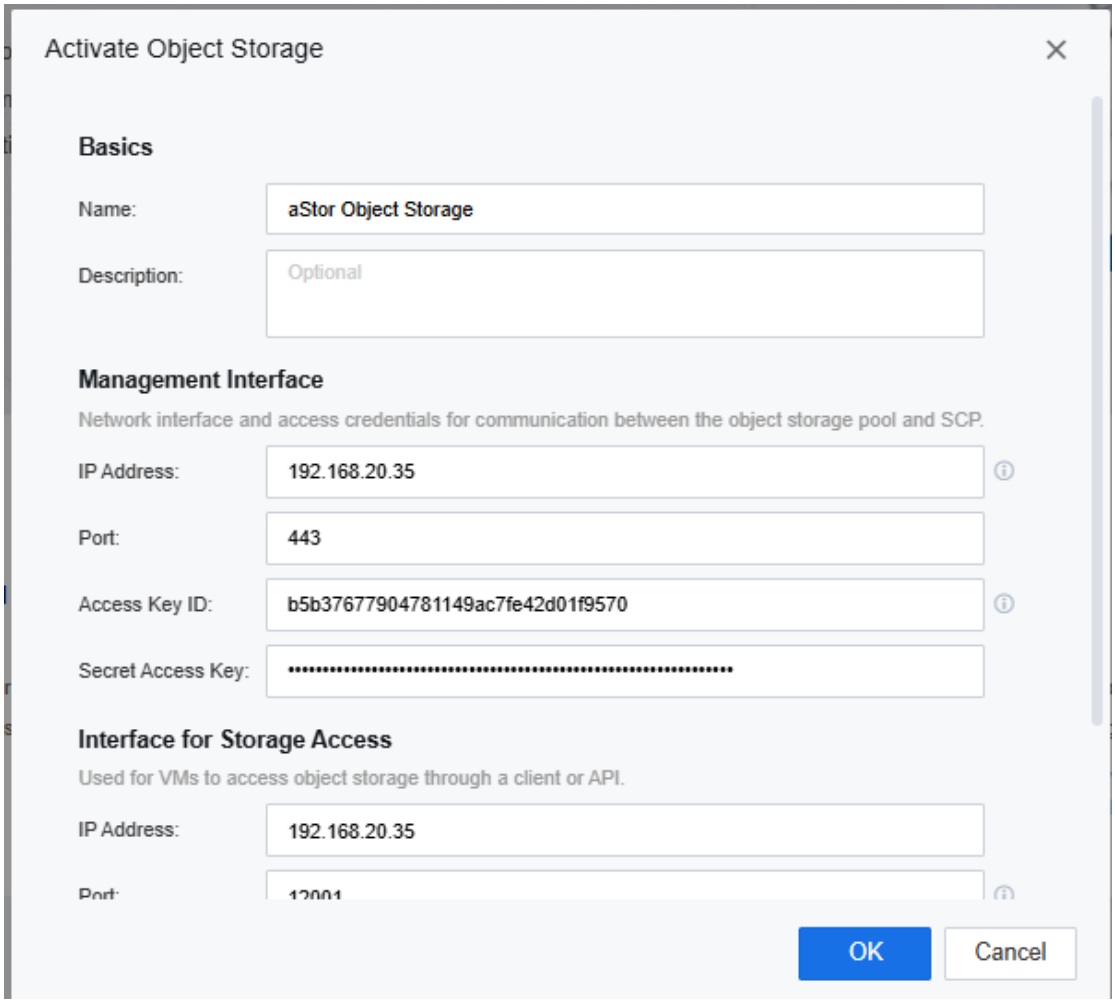
1. Log in to the EDS console, go to **System Management** > **System Settings** > **Platform Connection**, and click **Add** to connect to SCP.



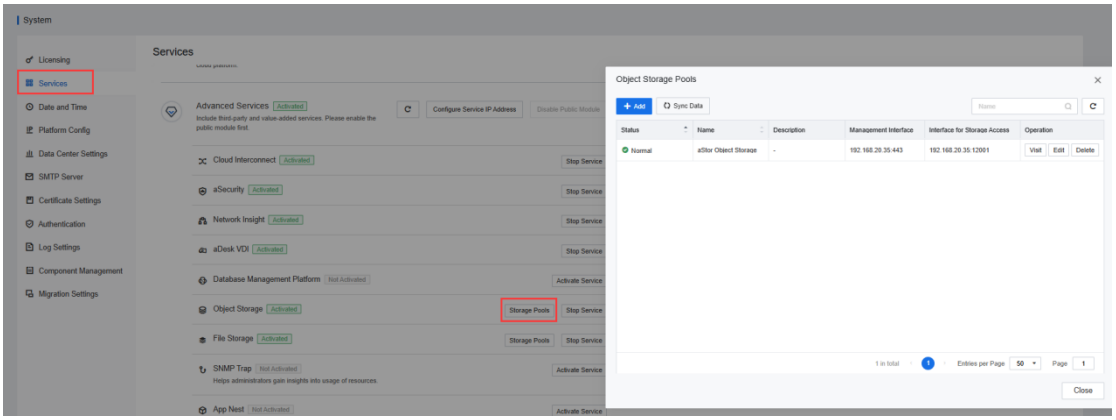
2. After the connection is successful, click **Edit** in the **Operation** column and obtain the access key ID and secret access key.



3. Go back to SCP and go to **Resources** > **Management** > **System** > **Services**. Select **Enable Public Module** for **Advanced Services** and select **Activate Service** for **Object Storage**. In the **Activate Object Storage** pop-up window, configure the IP addresses and port numbers for the management interface and interface for storage access (the port for which is 12001), and paste the access key pair obtained in the previous step.



4. After Object Storage is activated, click **Storage Pool Management** to add, edit, or delete an object storage pool.



4.11.1.4 OSS Account Management

Function Description

This section instructs how to manage OSS accounts.

Precautions

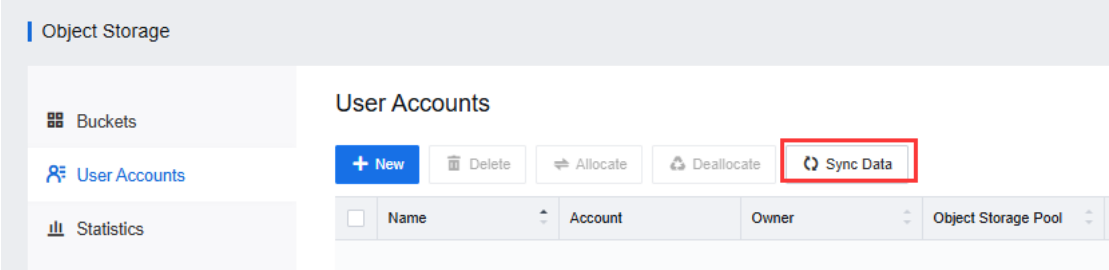
1. You can download the secret access key of your OSS account only once when creating the account. If it is lost, you need to generate it again and reconnect all clients to EDS.
2. An SCP user can have multiple OSS accounts.
3. Up to five secret access keys can be generated for each account, and each of them can be downloaded only once. For account security, you are advised to change the secret access key regularly.

Prerequisites

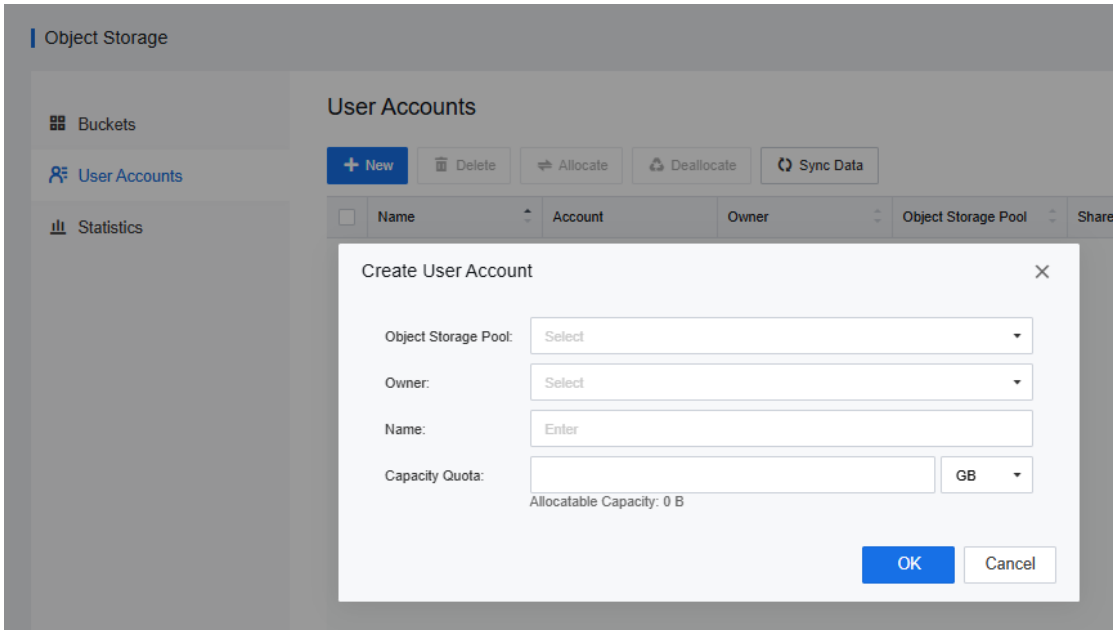
None

Procedure

1. Go to **Resources** > **Storage** > **Object Storage** > **Accounts**. EDS object storage accounts are automatically synchronized to SCP once every 10 minutes. You can also click **Sync** to start a synchronization.



2. Click **Create**. In the **Create OSS Account** pop-up window, select the resource pool, user (which can be an administrator or a tenant account), and quota.



3. After the account is created, click **Generate Secret Access Key**, and then the system will automatically download the key file. Keep the key file properly, as it can be downloaded only once. Up to five key files can be generated for each account. If the number of downloaded key files exceeds this limit, you need to delete outdated keys and generate them again.
4. Administrators or MSP users can click **More** > **Allocate** or **More** > **Revoke** in the **Operation** column to allocate an account to a tenant or revoke the account from the tenant. Clicking **Revoke** or **Allocate** can implement bulk operations.

4.11.1.5 OSS Bucket Management

Function Description

This section instructs how to manage buckets.

Precautions

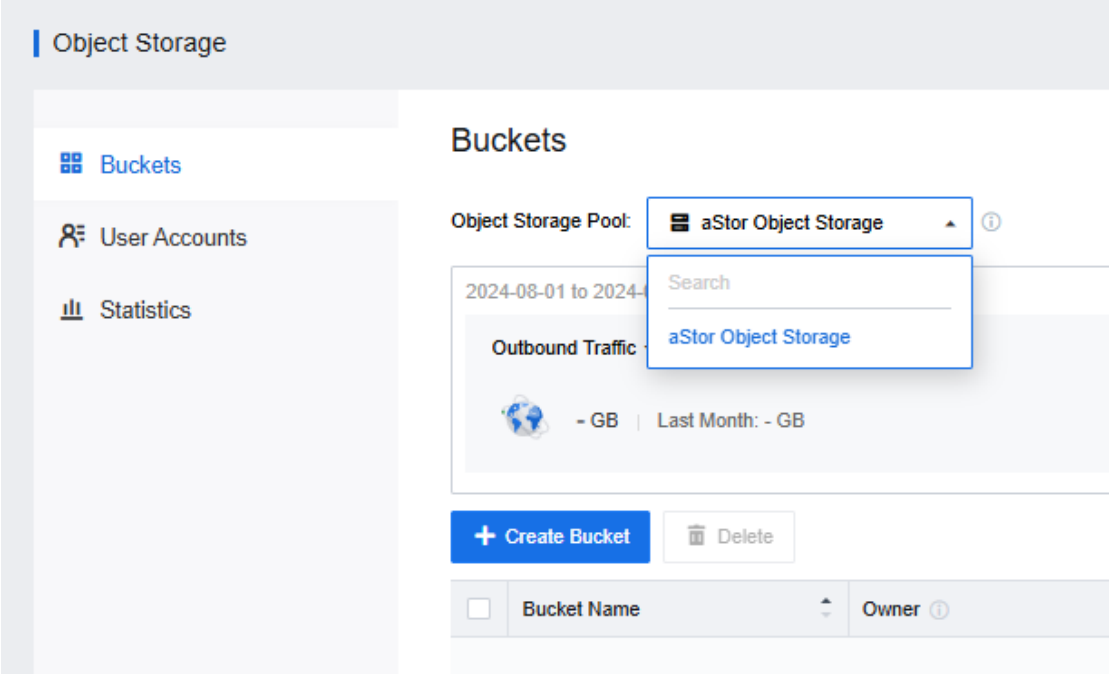
1. An OSS account needs at least one access key pair to create and associate with buckets.
2. An OSS account can have multiple buckets. A bucket can be associated with only one OSS account.

Prerequisites

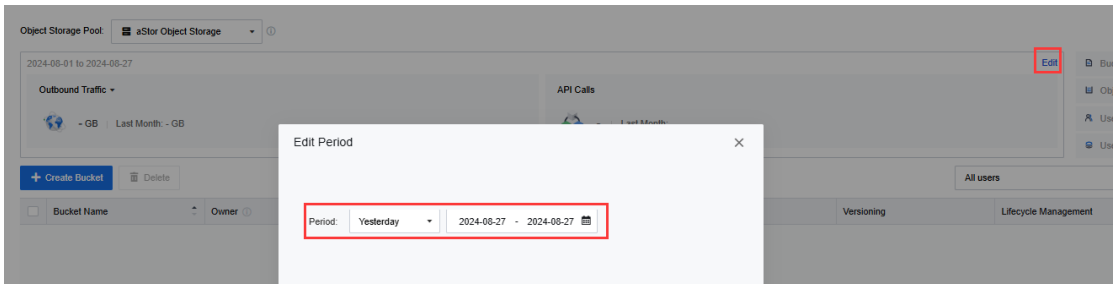
None

Procedure

1. Go to **Resources** > **Storage** > **Object Storage** > **Buckets** and select an object storage pool from the **Object Storage Pool** drop-down list.



2. Then, you can view the WAN outbound traffic and the number of API calls of the object storage pool. You can click **Specify Time** to specify a time range. Data is synchronized between 00:00 AM and 06:00 AM every day.



3. Click **Create Bucket** to create a new bucket.

- **Basic Settings**

Owner: Select an OSS account for bucket association. An account can be associated with multiple buckets.

Permission Settings: You can grant permissions to **Owner** (the account you select), **Platform Accounts** (all OSS accounts in the list), and **All Accessing Users** (all users accessing the storage pool of the bucket).

- **QoS Settings**

Bandwidth: No limit is selected by default. You can also specify the bandwidth as needed.

QoS: No limit is selected by default. You can also specify the QoS as needed.

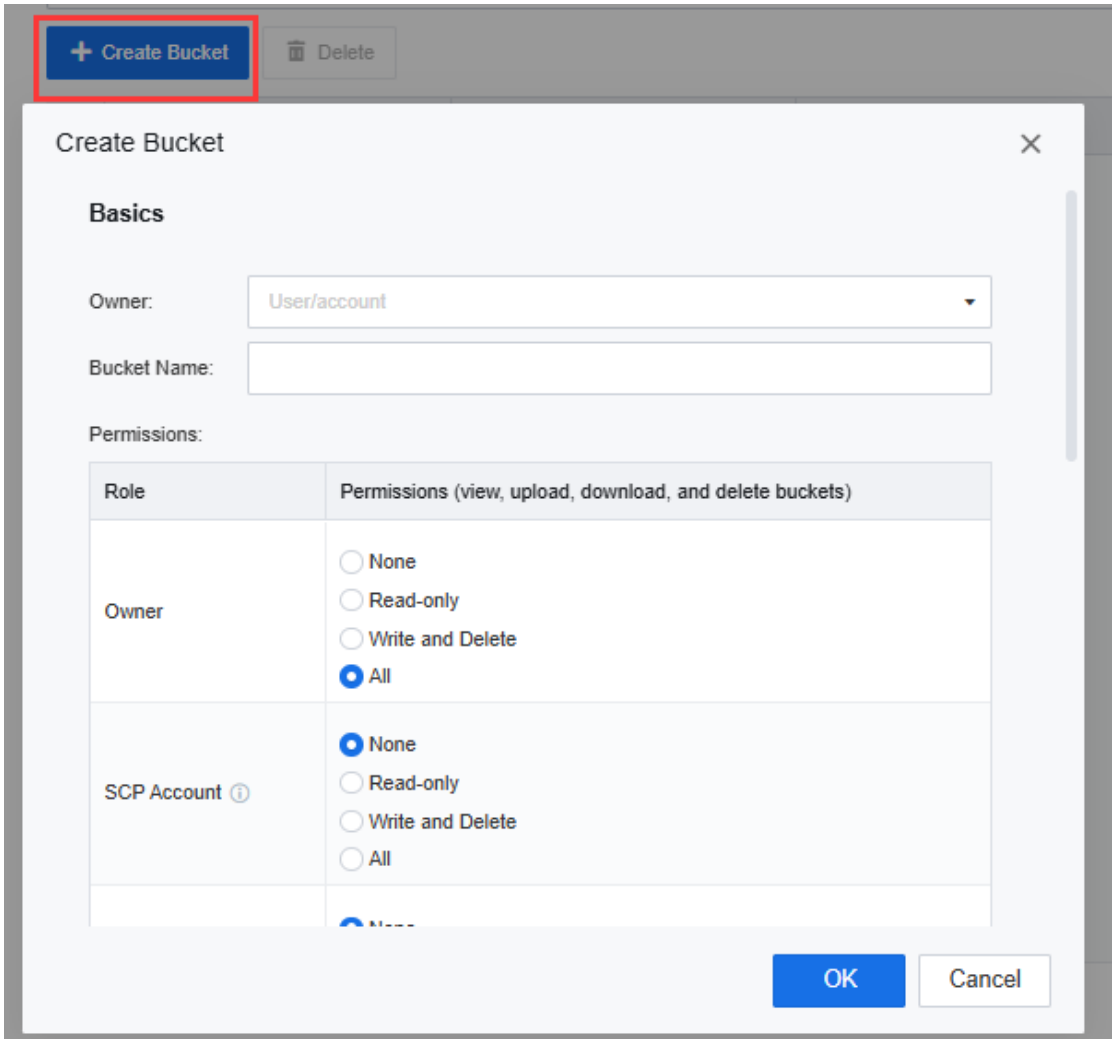
Settings for Specific Accounts: You can specify the bandwidth and QoS for specific accounts, and the settings for these accounts have a higher priority than general settings.

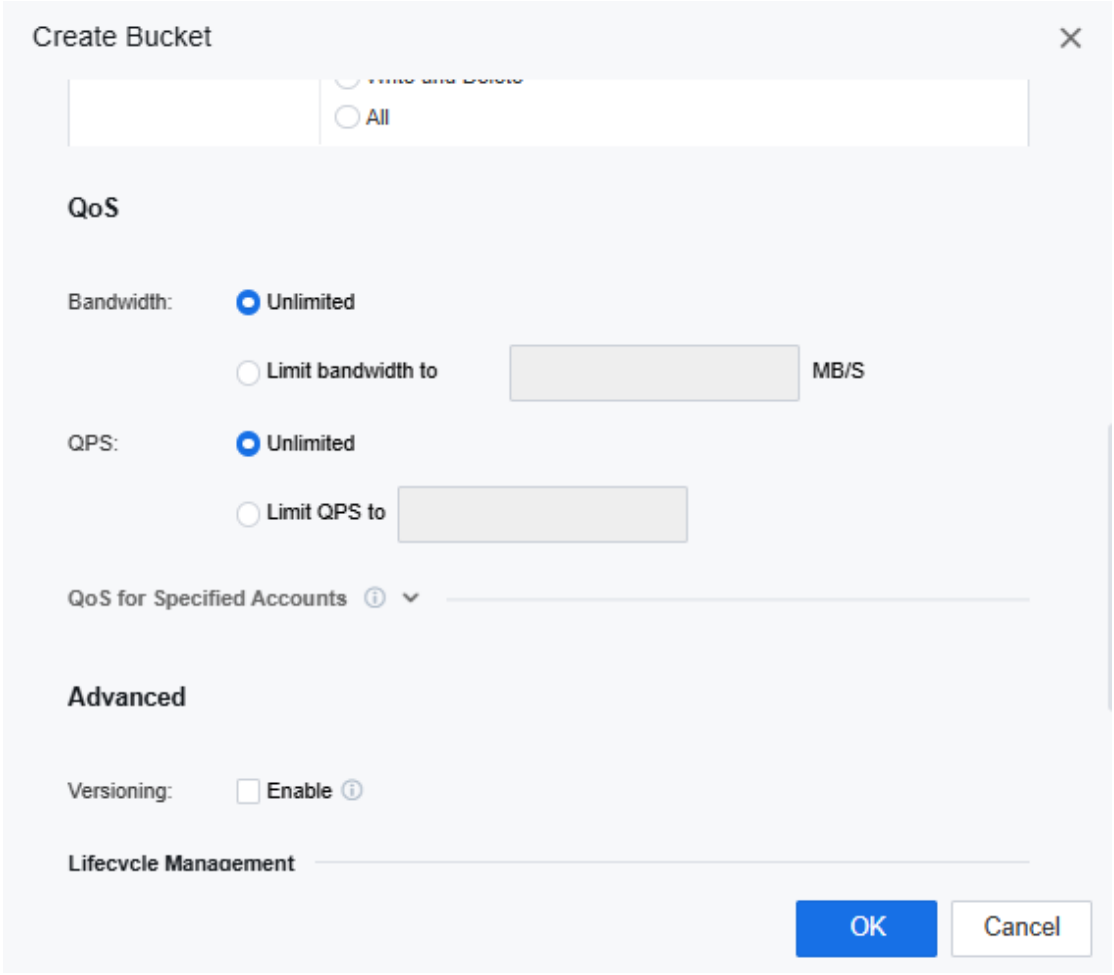
- **Advanced Settings**

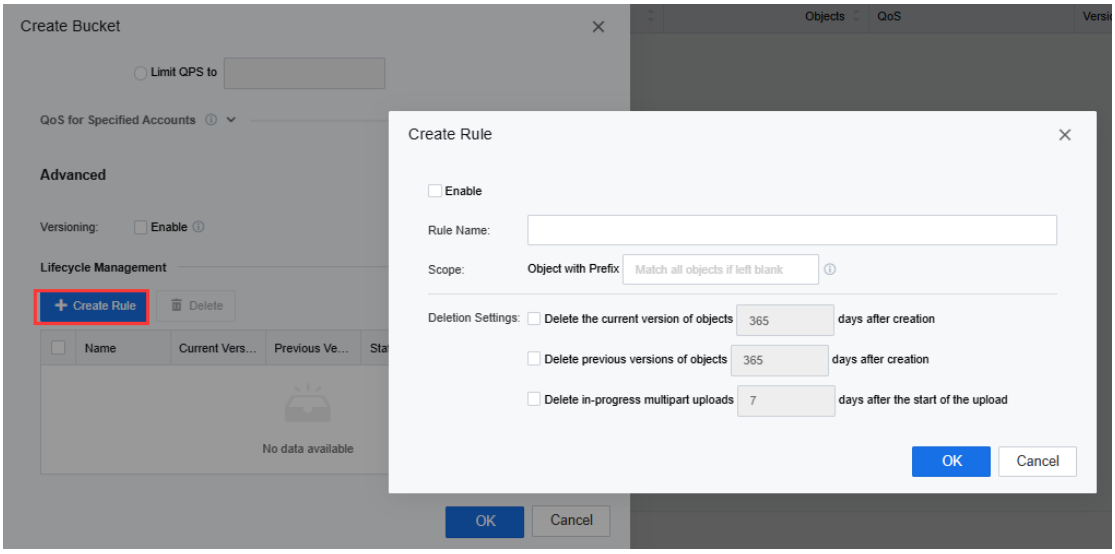
Version Control: It is disabled by default. If it is enabled, all versions of objects with the same name will be retained in the bucket.

- **Lifecycle Management**

Click **New** to create a lifecycle management rule for objects in the bucket.







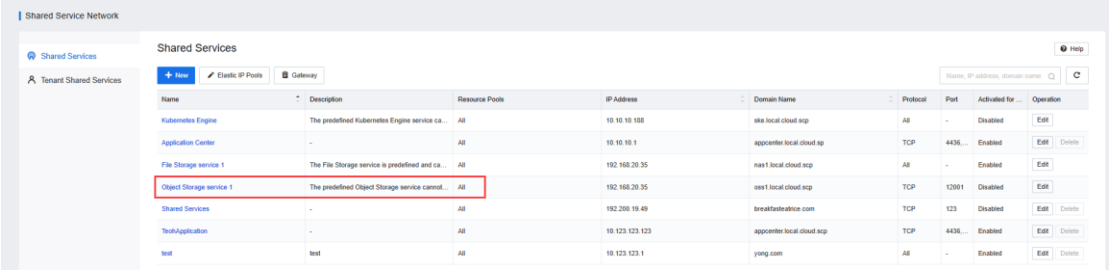
4.11.1.6 Access OSS

Classic Network

After the OSS service is activated, you can access and use it by using the IP address and port number of the interface for storage access configured in section Activate OSS and the access key pair generated in section OSS Account Management.

VPC

1. After the OSS service is activated, you can find a record in the list of shared services automatically generated for the managed object storage pool from **Resources** > **Networking** > **Shared Service Network**.



2. Enable **Object Storage** in the **Shared Services** section for the tenant. For more information, see section 4.3.5 "Shared Service Network."
3. Access and use the OSS service by using the domain name of the shared service and the access key pair generated in section OSS Account Management.

4.11.1.7 Metrics Statistics

Function Description

This section instructs how to collect information such as WAN outbound traffic, WAN inbound traffic, and the number of API calls.

Precautions

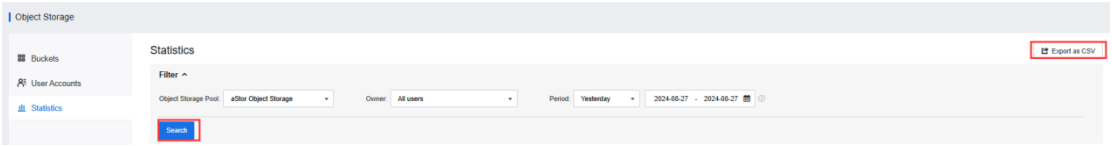
None

Prerequisites

None

Procedure

Go to **Resources** > **Storage** > **Object Storage** > **Metrics Statistics**. Select the object storage pool, user, and time range (data is synchronized between 00:00 AM and 06:00 AM every day) and click **Query**. Click **Export CSV** to export the queried list.



4.11.2 File Storage

SCP integrates Sangfor Enterprise Distributed Storage (aStor) to provide users with a highly reliable, low-cost, self-fixing, multi-tenancy, and PB-level elastic cloud storage platform. This feature is applicable to application scenarios such as unstructured data storage and massive small file storage.

For more information, contact TAC for more information.

4.12 Monitoring Center

Sangfor SCP has a complete monitoring function and alarm mechanism: the monitoring overview can comprehensively monitor three types of objects: virtual machine, physical machine, and elastic IP. Sangfor monitoring center aMC can monitor virtual machines, businesses, databases, etc. Comprehensive monitoring. While monitoring, you can view the platform alarm information through the alarm log and customize the alarm settings.

4.12.1 Monitoring Dashboard

Feature Description:

Sangfor SCP platform can monitor virtual machines, physical nodes, and elastic IPs. By adding monitoring charts, the monitoring information can be displayed as charts.

Precautions:

None.

Prerequisite

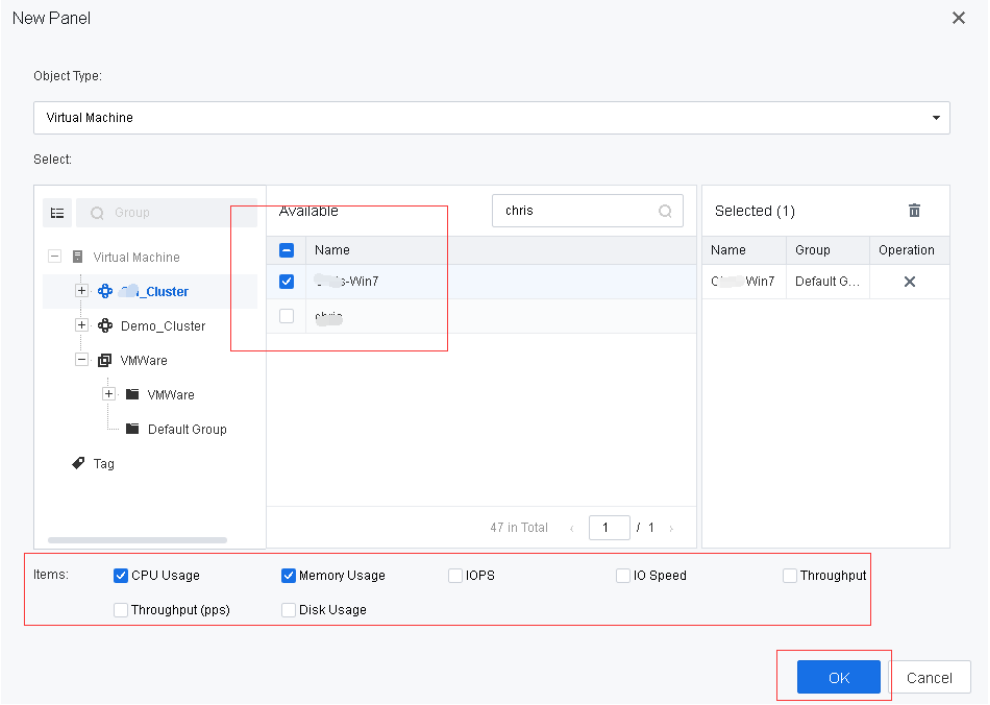
None.

Steps:

Step 1. Login to the SCP and navigate to **Resources** > **Monitor Center** > **Monitoring Dashboard.** There will be no monitoring panel by default. You need to add it manually by clicking **New Panel.**



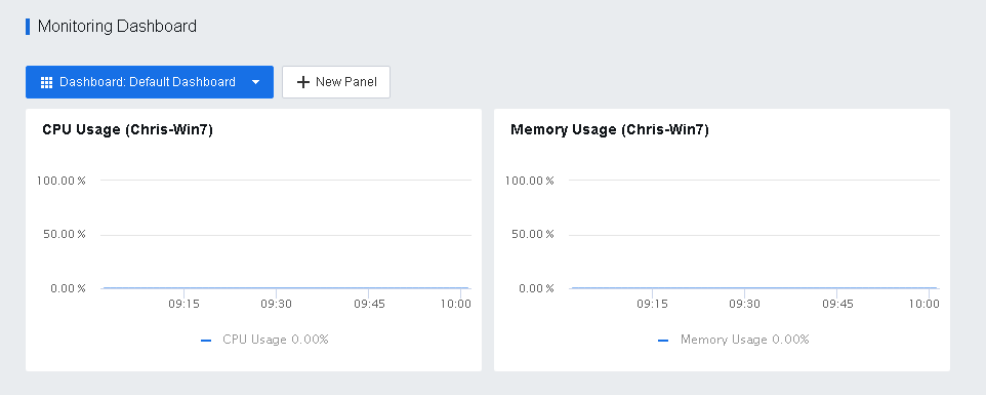
Step 2. Select the virtual machines and **Items** that need to be monitored, then click **OK** to add.



NOTE

There is currently 50 monitoring panel that can be created on the monitoring dashboard page.

Step 3. You may see the virtual machine dashboard after adding the panel.



4.12.2 Reports

Feature Description:

SCP collects statistics of real-time resource usage and monitored items to generate and export an operation and maintenance report, which can include the following metrics: **Status**, **Description**, **Run Location**, **User**, **Tags**, **Guest OS**, **hostname**, **AS group**, **Key Name**, **Static IP**, **Elastic IP**, **Disk Encryption**, **Scheduling Policy**, **CPU Clock Speed**, **Used Memory** of **Resources**, **Used Storage**, **Current Node**, **Datastore**, **Storage Policy**, **Used Memory of Host Resources**, **Logical Space Used**, **Physical Space Used**, **Downtime**, **Uptime**, **Scheduled Backup**, and **department** and **Responsible** of **Custom Attributes**.

Precautions:

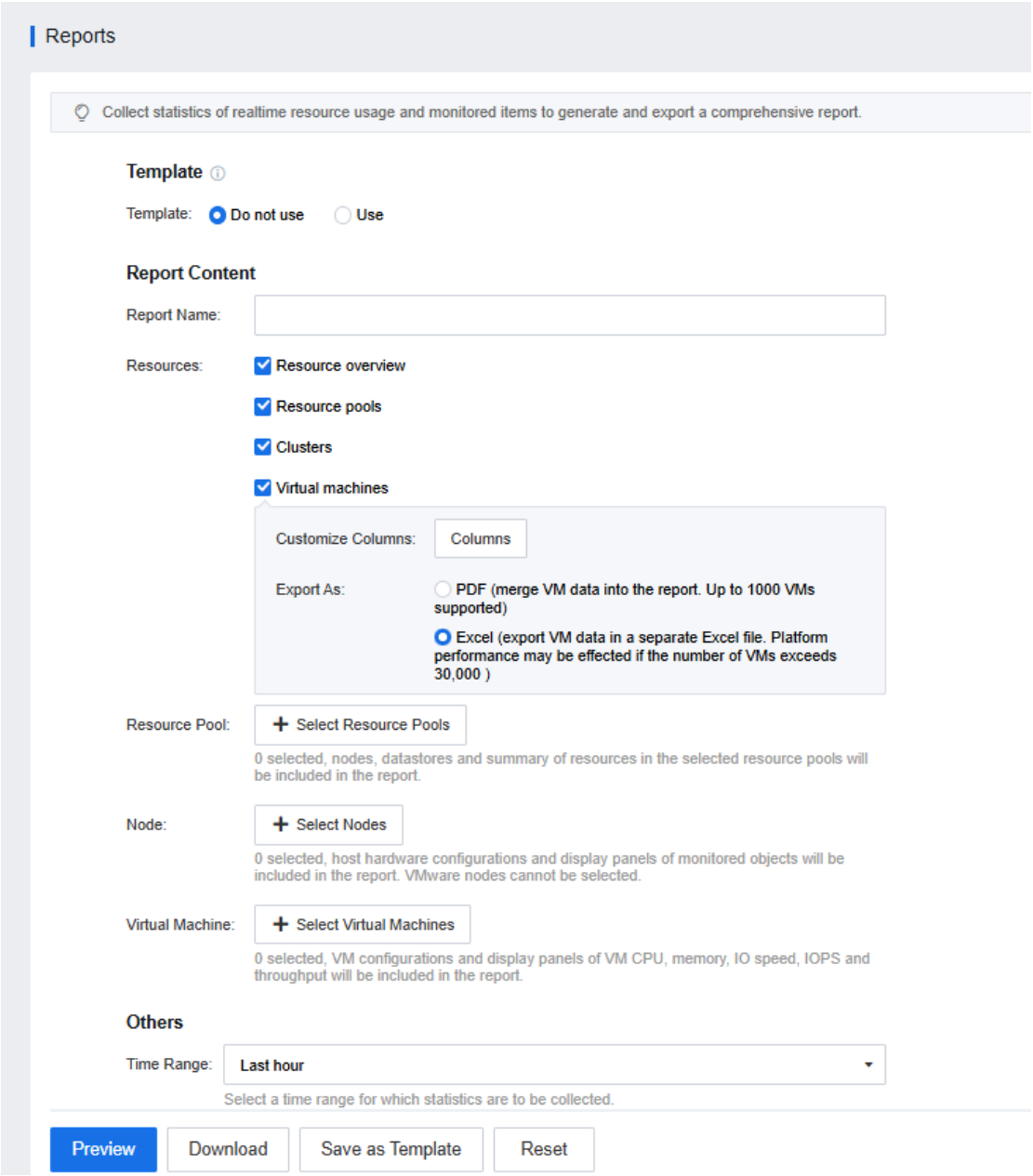
N/A.

Prerequisite

N/A.

Steps:

Step 1. Log in to SCP, go to **Resources** > **Monitor Center** > **Reports** to decide what contents to display in the report, or choose a template to export reports.



4.12.3 Monitor Center

4.12.3.1 Alerts

Features:

Sangfor SCP platform will monitor the platform and virtual machine in real-time according to the alarm setting, and all generated alerts will be recorded. Administrators can view the latest alerts or old alerts according to actual need.

Precautions:

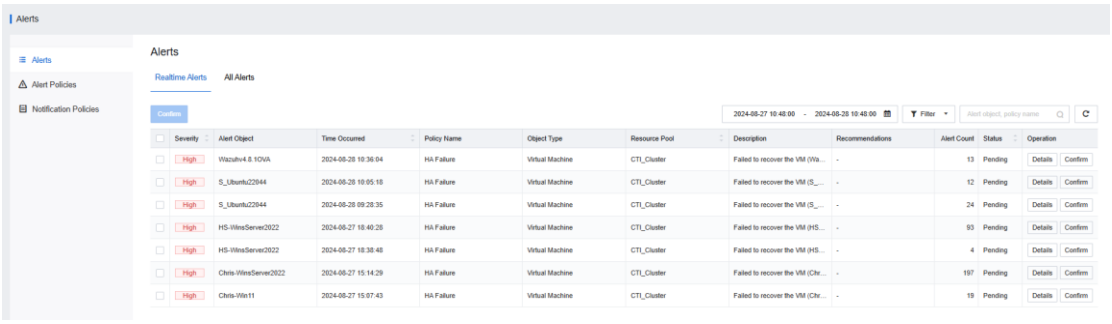
None.

Prerequisite

None.

Steps

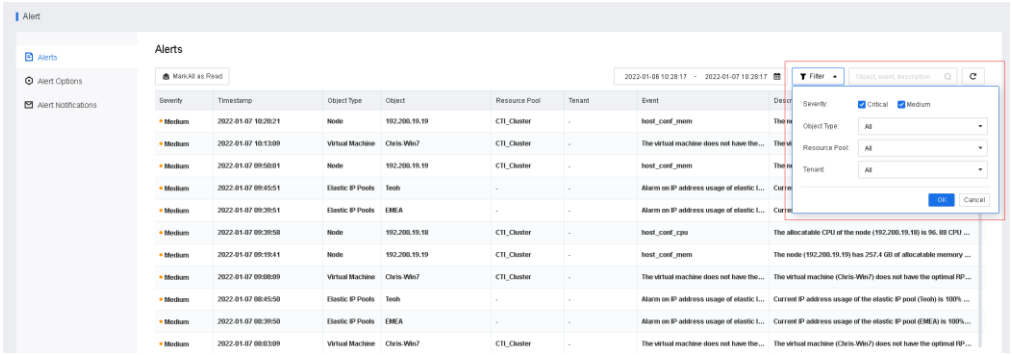
Step 1. Login to the SCP and navigate to **Resources > Monitor Center > Alerts** to view the alerts.



Step 2. You can view all the alert history on this page. The **Severity** on the left shows the severity level of the alert. You can filter the alerts log by clicking the **Filter** button.

NOTE

Unread alerts will be shown in bold text format.



4.12.3.2 Alert Options

Function Description:

Sangfor SCP platform can detect and prompt alerts on virtual machines, physical hardware, network, and License Key information. It supports email notification and customization of alert conditions.

Precautions:

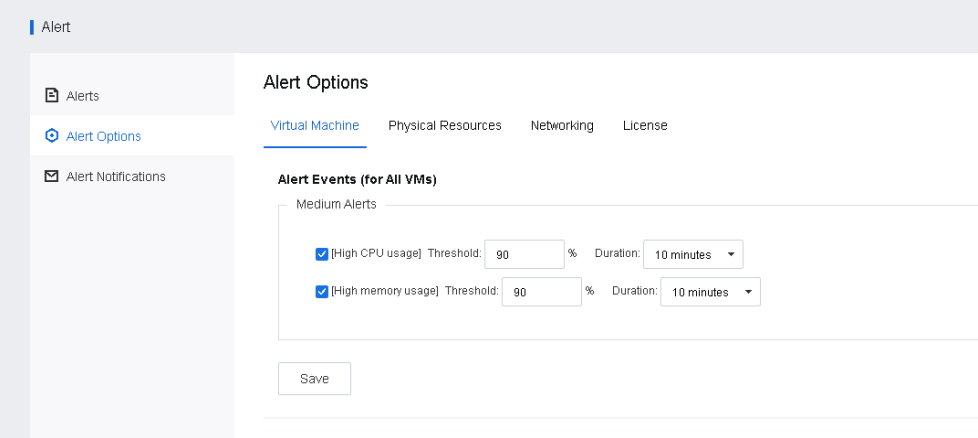
If the SMTP server is configured as a domain name, the DNS of the SCP platform must be able to resolve the domain name. Otherwise, the SMTP server can only be configured with an IP address.

Prerequisite

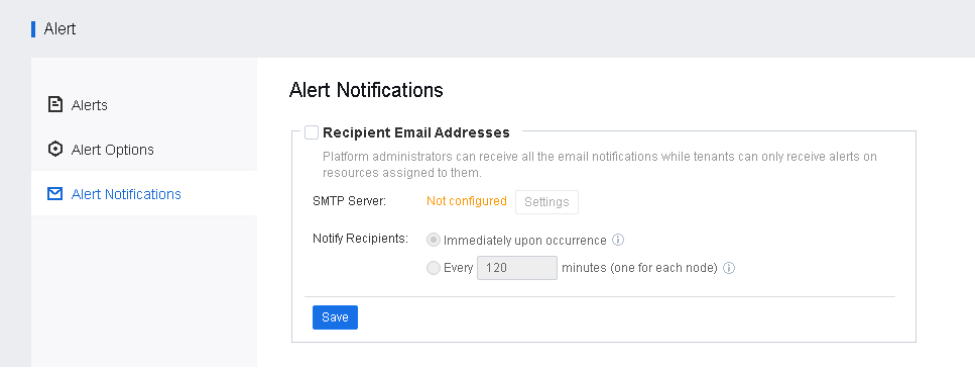
None.

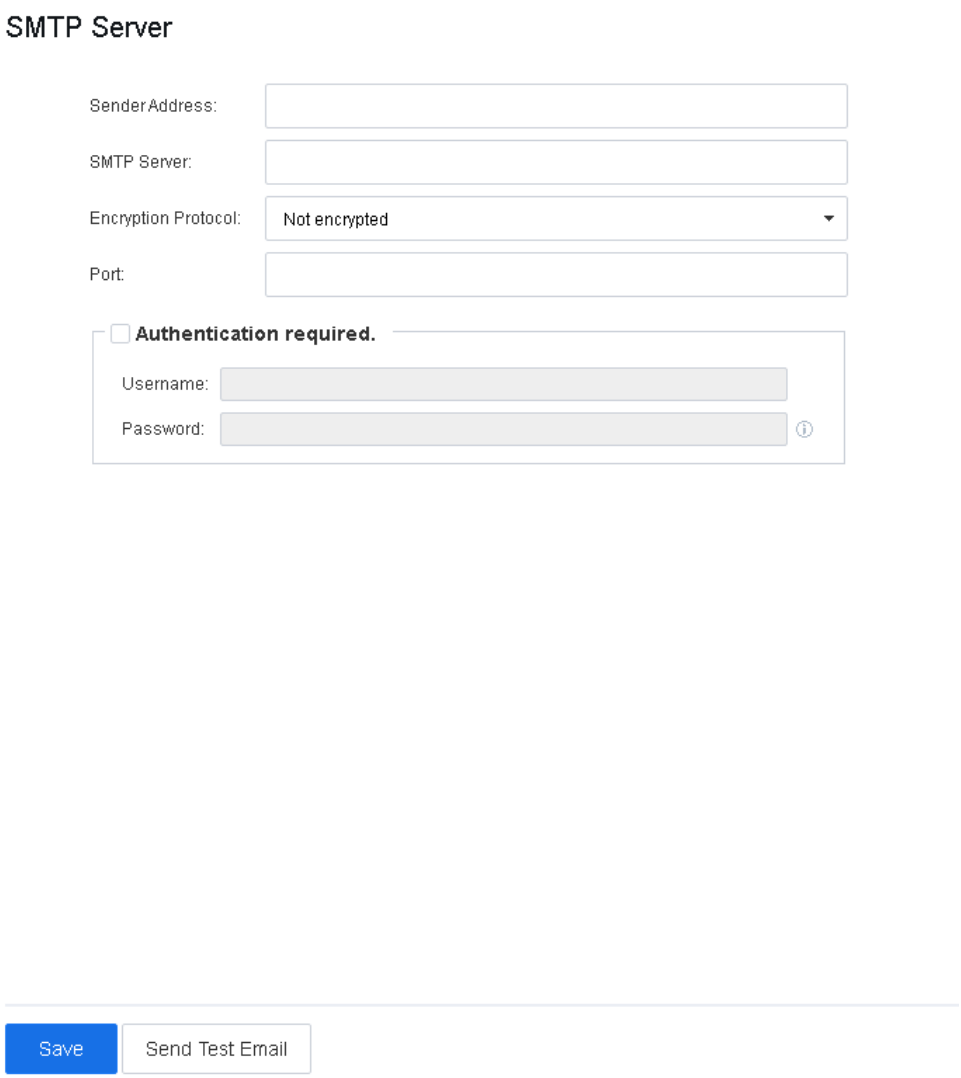
Steps:

Step 1. Login to the SCP admin portal, navigate to **Resources > Monitor Center** > **Alerts, and** click **Alert Options** to customize the condition for the virtual machine, physical resources, and networking or license-related alert.

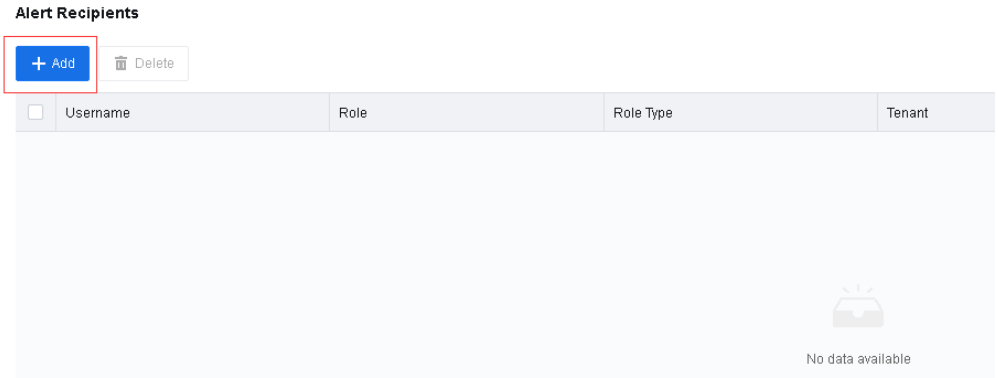


Step 2. Alert supports configuring alert notifications through email, **Recipient Email Address** can be enabled in **Alert Notifications** and configured on the SMTP server. When verifying the username and password of the outgoing server, if the email password verification fails, may try to use the email client authorization code for verification.





Step 3. It supports sending alert notifications to designated alert recipients. Click **Add** to add designated alert recipients to receive alert notifications.



NOTE

Email notification requires SCP to be able to connect to the Internet.

4.13 Management

4.13.1 Operational Audit

Function Description:

Sangfor SCP will record all operation logs and record the operation results synchronously. For example, when administrators need to view historical operation records to locate the cause of the fault, they can go to this page to view them.

Precautions:

None.

Prerequisite

None.

Steps:

Log in to the SCP platform and select **Management > Tasks.**

4.13.2 Recycle Bin

Feature Description:

After the tenant deletes the virtual machine, NFV equipment, and backup files, the deleted information will be moved to the recycle bin. The tenant can permanently delete or recover the deleted information.

Precautions:

The data in the recycle bin will be stored for 30 days by default. After 30 days, the platform will automatically delete it.

Prerequisite

N/A.

Steps:

Step 1. Navigate to **Management** > **Recycle Bin.** Tenants can view deleted virtual machines, network components, NFV devices, and backup files.

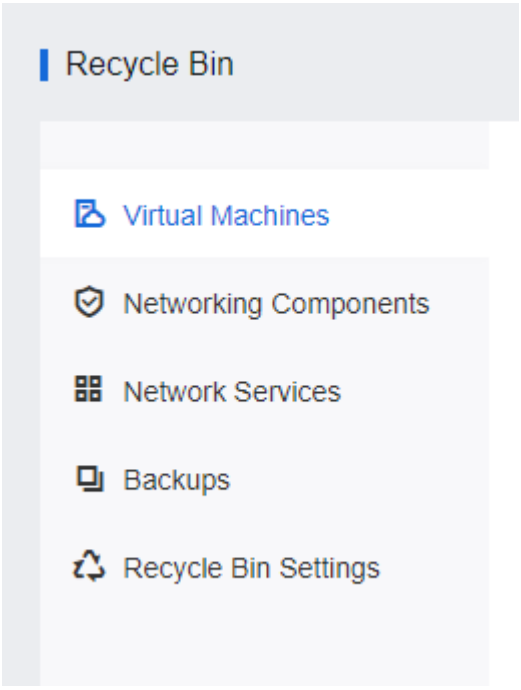
Virtual Machines: The deleted virtual machines.

Networking Components: List of network devices that have been removed,

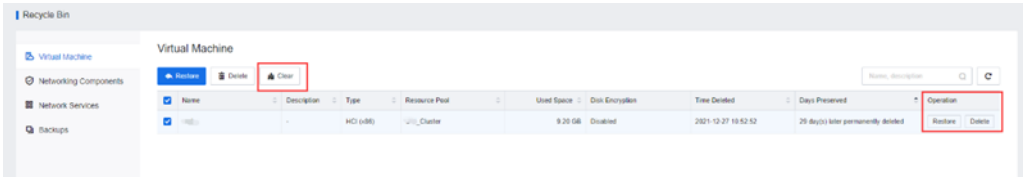
such as switches and routers.

Network Services: The deleted NFV devices.

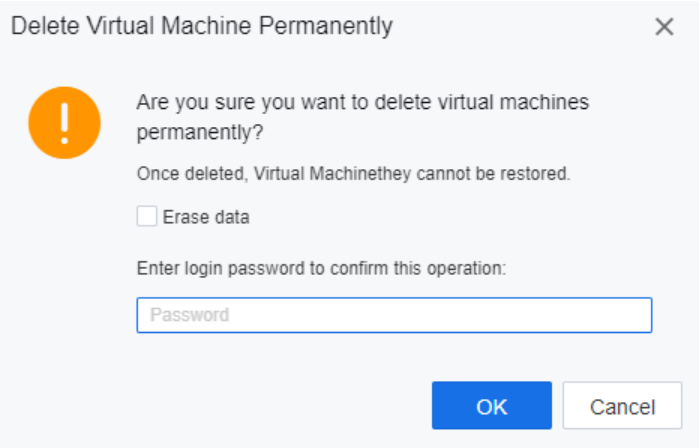
Backup: List of deleted virtual machines backup files.



Step 2. Select the corresponding virtual machine, network element, NFV device, or backup file and click **Restore** to restore the deleted virtual machine, NFV device, or backup file. Click **Delete** to permanently delete the deleted virtual machine, network element, NFV device, or backup file. Click **Delete** to delete all files, network components, NFV devices, and virtual machines currently in the recycle bin.



Step 3. Click **Delete** to delete all virtual machines or network devices in the corresponding list in the recycle bin. The operation of completely deleting and emptying the recycle bin needs to be confirmed by entering the admin user's password.



WARNING

This deletes operation will completely delete the virtual machine or network device data. Please operate with caution.

4.13.3 Custom Attributes

Function Description

In scenarios where too many business VMs and departments exist, you can use custom attributes to categorize and tag assets for unified O&M. You can create custom attributes by HCI resource (including VM, physical host, storage, and network component) and associate them with resources.

Precautions

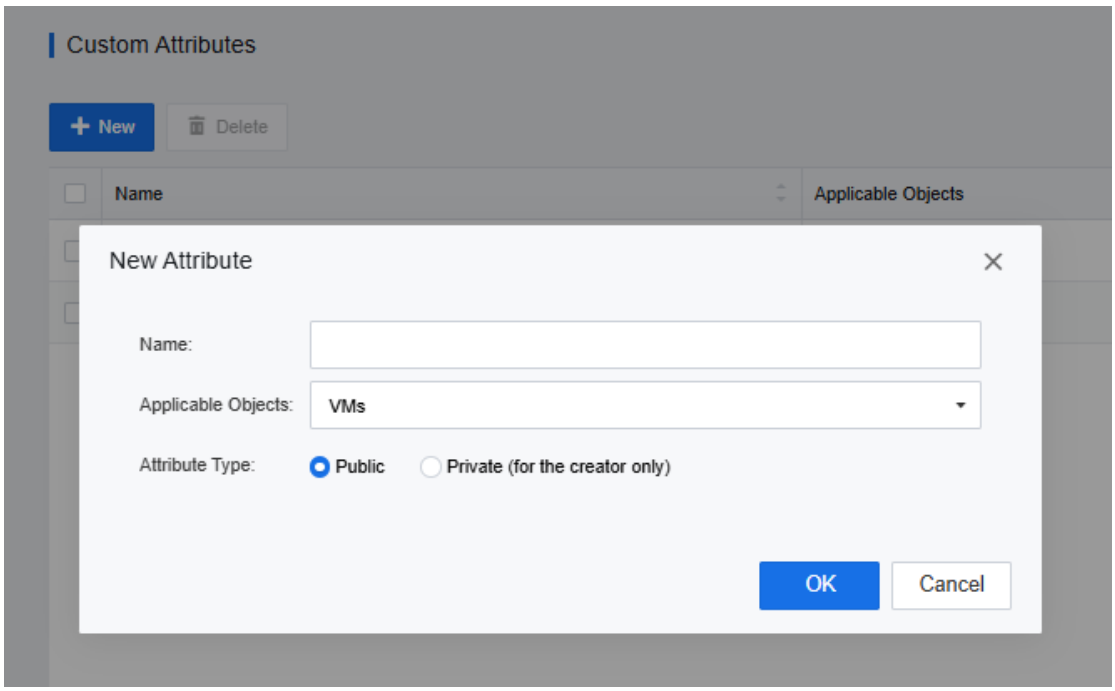
Custom attributes cannot be associated with VM images.

Prerequisites

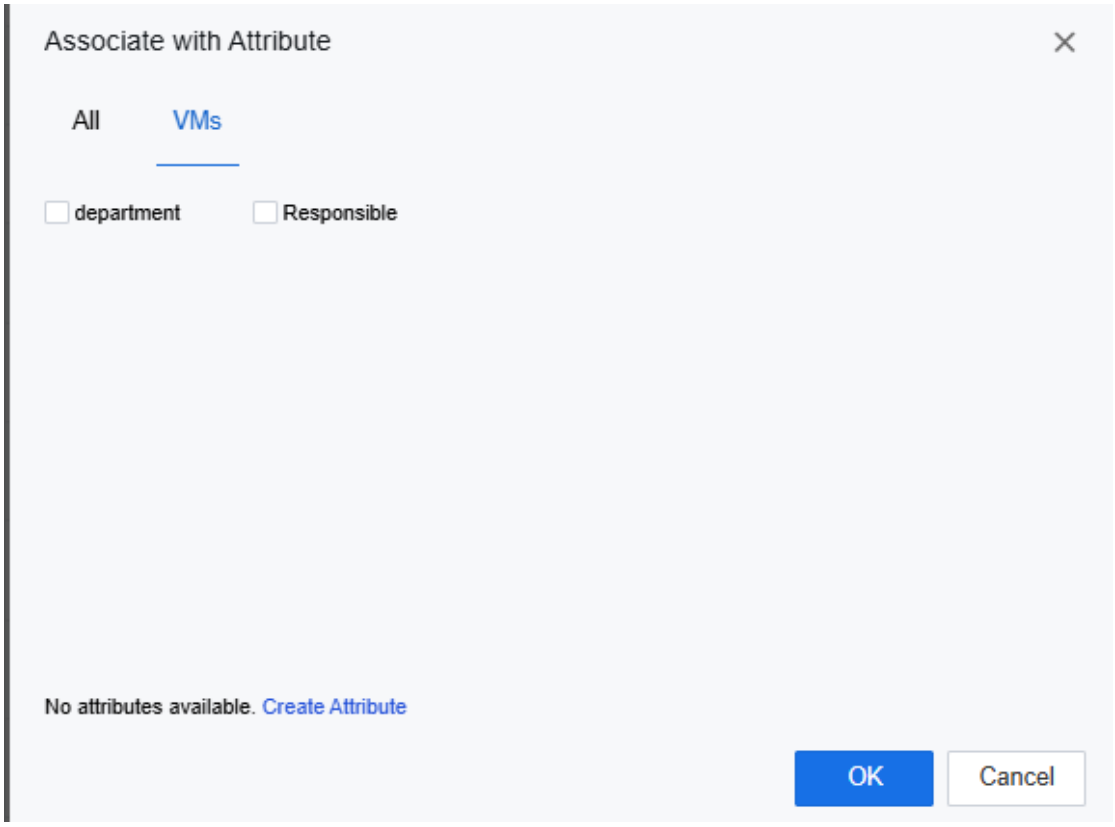
N/A

Steps

1. Go to **Management** > **Custom Attributes**, click **New**, specify the attribute name and applicable object (which can be **VMs**, **Nodes**, **Storage**, **Virtual Network Devices**, or **All**), and select an option for the attribute type (which can be **Public** or **Private**).



2. For example, if you create a custom attribute for a VM, select the target VM from the VM list, go to **More** > **Edit Attribute**, and select the defined attribute for association with the resource.



4.13.4 Platform Customization

Function Description

SCP supports login page customization to meet the requirements of customers. Customizable items include platform name, platform overview, image, and link.

Precautions

1. Requirements for the platform name:

- Must contain 1–48 characters.
- Can contain Chinese characters, letters, and digits.
- Can contain the following special characters: ()[]{}（） 【】 {} @|._-+ and spaces.

2. Requirements for the platform image:

- Company logo: An image in PNG or ICO format, up to 1 MB in size, and with a resolution of 205 x 60 pixels.
- Product logo: An image in PNG or ICO format, up to 1 MB in size, and with a resolution of 80 x 80 pixels.
- Website icon: An image in PNG or ICO format, up to 1 MB in size, and with a resolution of 32 x 32 pixels.
- Advertising image: An image in JPG format, up to 1 MB in size, and with a resolution of 1920 x 1080 pixels.

Prerequisites

Images for replacement are prepared.

Steps

1. Log in to the SCP console as the administrator and go to **Management** > **Portal Customization** to customize the login page, navigation bar, browser, and other content.
2. Click **Save**.
3. Click **Restore Defaults** to clear the customized content and restore to the default configurations.

4.13.5 Security Management

4.13.5.1 Login Policy

Features:

Sangfor SCP platform supports account login rules, including account and password, session timeout options, SMS authentication, and other functions.

Precautions:

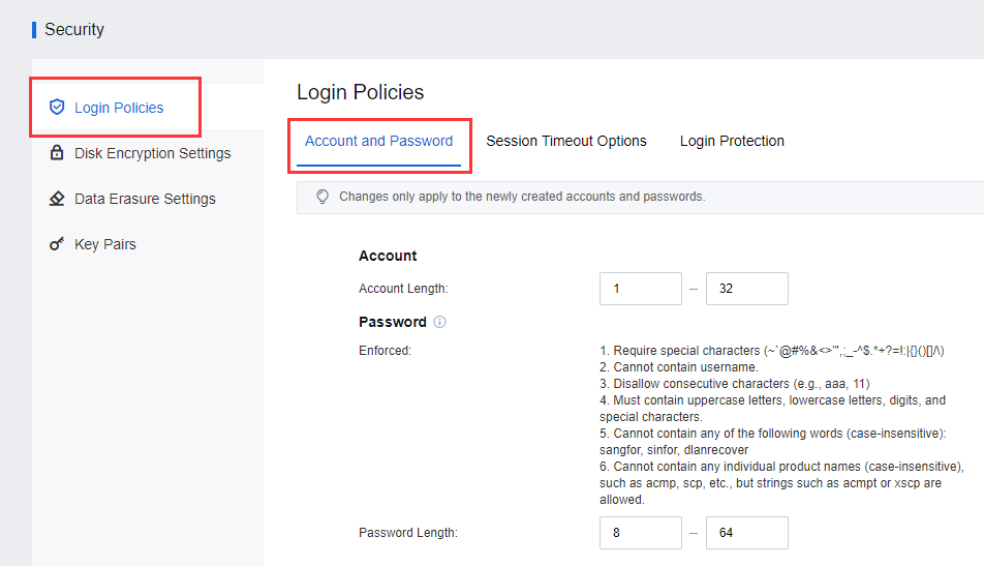
1. The login configuration applies to all accounts on the platform, including roles such as admin, tenant, and tenant users.
2. After updating the login policy, creating a new account must match the policy, and the existing account that does not meet the policy will be forced to change the password at the next login.
3. If the SMS gateway fails, the user using SMS authentication cannot use the password to log in to the SCP.

Prerequisite

An SMS gateway configuration is required if the SMS authentication function is enabled.

Steps:

Step 1. Login to the SCP platform, navigate to **Resources** > **Management** > **Security,** and select **Login Policies** for the account and password configuration.

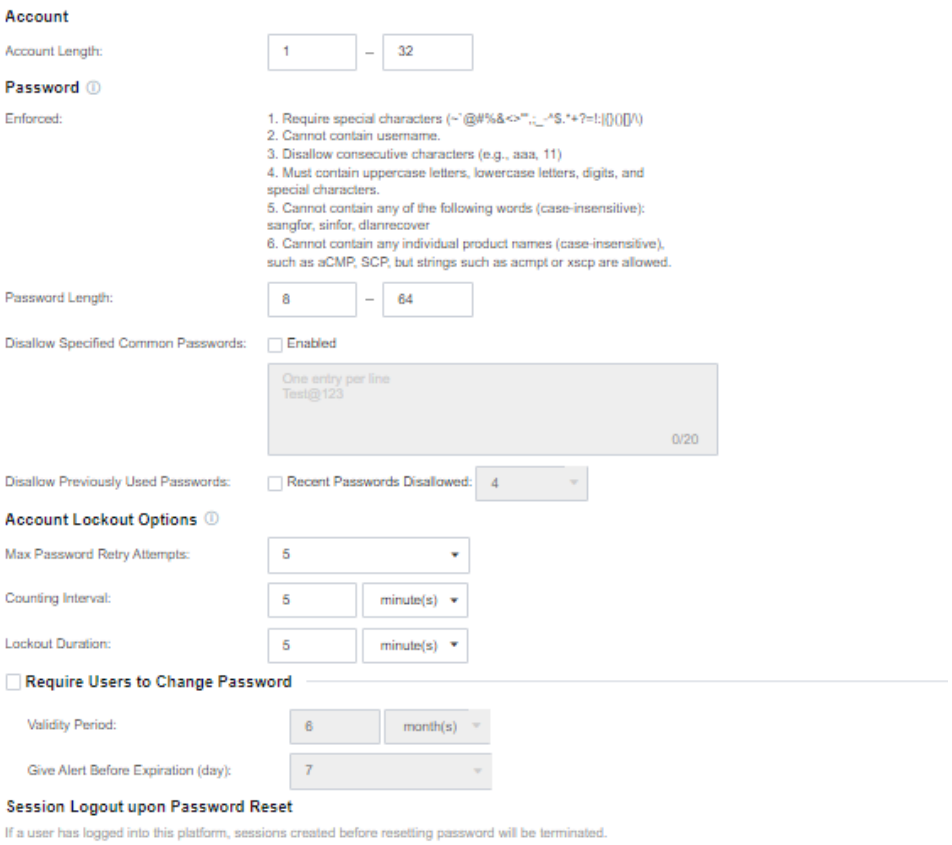


Step 2. Supports configuring **Account, Password, Account Lockout Options,** and **Require Users to Change Password**.

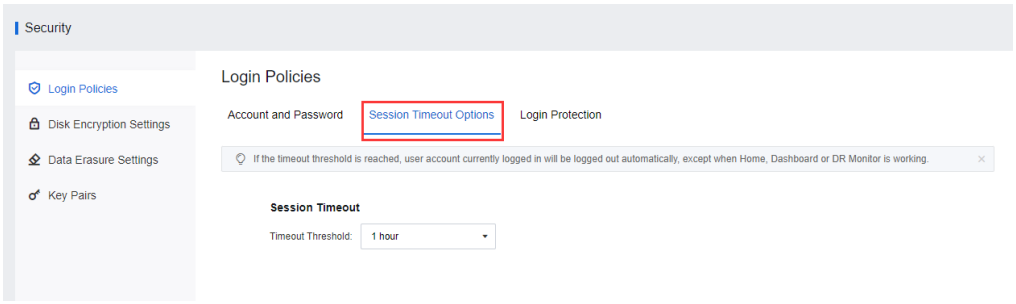
1. **Account**: To set the account length.
2. **Password policy:**

- **Enforced policy**: Require special characters, cannot contain username and disallow consecutive characters, etc. Login policies are only effective for local users, not SSO and LDAP authentication.

3. **Account Lockout Options**: The account will be locked if the number of the maximum password retry attempts within the specified interval is reached and will be unlocked after the lockout period has expired.
4. **Require Users to Change Password**: Require customers to change their passwords within a specified period.



Step 3. If the session timeout options are configured, if the timeout threshold is reached, the user account currently logged in will be logged out automatically, except when Home, Dashboard, or DR Monitor is working.



4.13.5.2 Login Protection

Features:

Sangfor SCP platform supports the two-factor authentication of user/password + SMS authentication or OTP authentication to improve user security.

Precautions:

1. If the SMS gateway fails, the user using SMS authentication cannot use the password to log in to the SCP.
2. Only the admin can configure the OTP authentication for the admin or the tenant. The tenant cannot configure it by himself.
3. The OTP authentication of the tenant requires the admin to enable login protection for the tenant, and then the tenant registers themselves on the login interface.
4. RADIUS authentication servers can be configured on SCP 6.9.0 and later versions.

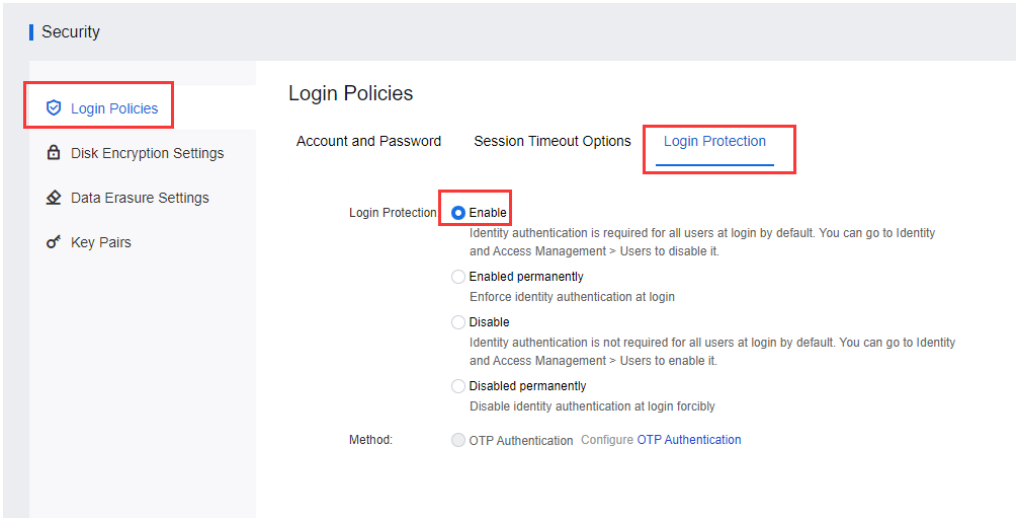
Prerequisite

1. An SMS gateway configuration is required if the SMS authentication function is enabled.
2. The platform SMTP server configuration must be completed if the user uses the email for OTP function recovery.

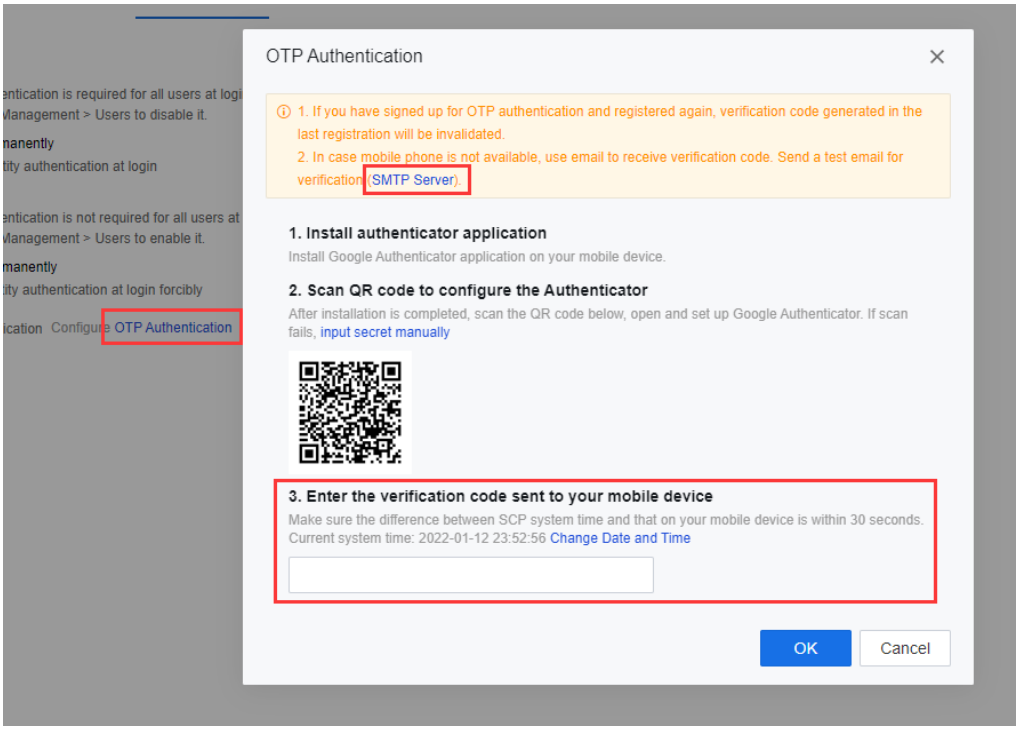
Steps:

Google OTP

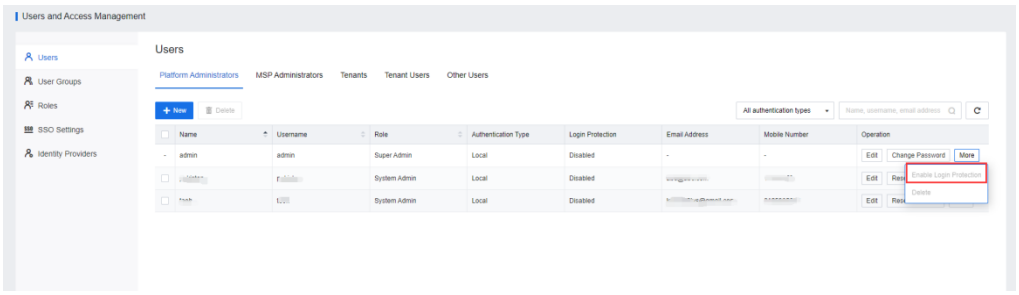
Step 1. Login to the SCP platform, and navigate to **Resources > Management > Security**. Under **Login Policies**, select **Login Protection** for the configuration.



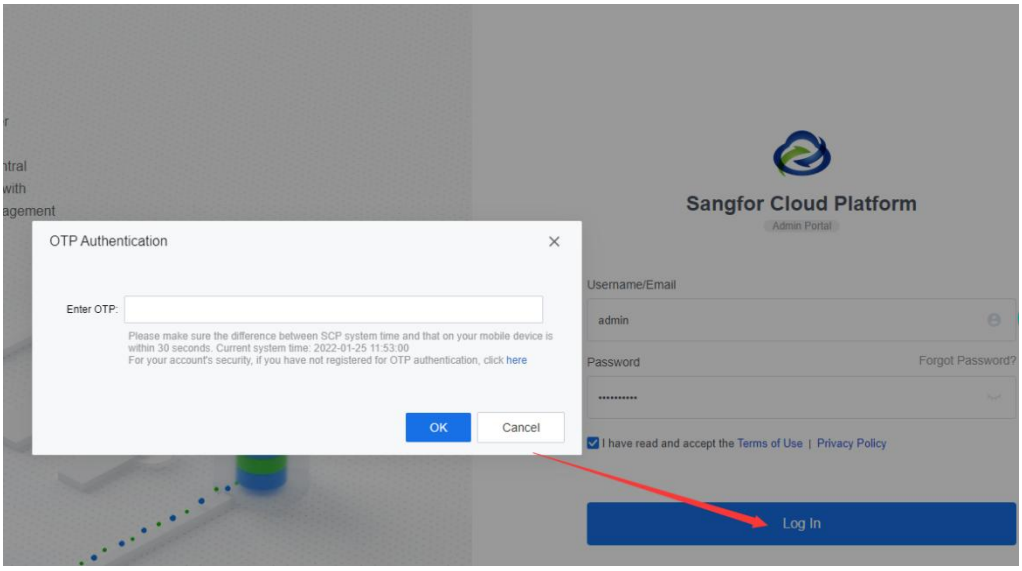
Step 2. Select **OTP Authentication** to set up the OTP authentication docking. Configure the SMTP server as an alternative in case the mobile phone is unavailable and may obtain the OTP via email.



Step 3. In **Users and Access Management**, click **More** to enable login protection.



Step 4. After the configuration is complete, OTP authentication or registration can be performed when the admin or tenant login to the SCP platform.



RADIUS OTP

For more information, see Third-party OTP authentication in section 4.13.6.9 "Authentication Settings."

4.13.5.3 Disk Encryption Settings

Function Description:

Sangfor SCP platform can enable disk encryption settings. After enabling, it supports the encryption of storage data of virtual machines, networks, and security resources to guarantee data security and avoid information theft.

Precautions:

1. Currently, SCP only supports using the AES-256 encryption algorithm to encrypt data.
2. Once the disk encryption settings are enabled, it will not automatically adopt disk encryption to the virtual machines until the enable disk encryption has

been enabled manually on the virtual machine setting.

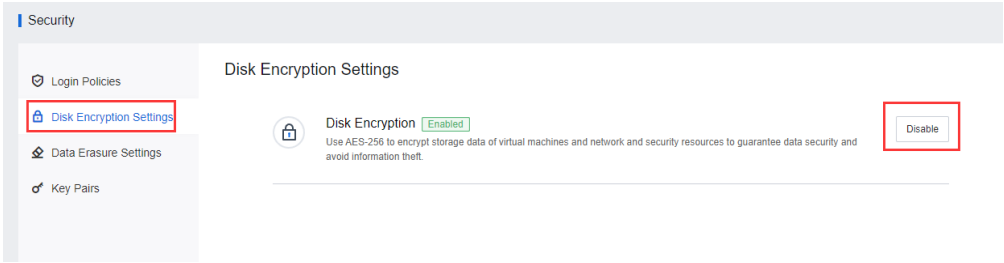
3. Enabling or disabling disk encryption for a single resource pool is not supported.
4. The virtual machine must be powered off to enable disk encryption on the virtual machines.
5. After the disk has been encrypted, it doesn't support disk decryption.
6. The disk encryption process takes a while to complete, and operations such as powering on are not supported. It is recommended to perform during non-business hours.
7. After the disk encryption is enabled on the virtual machine, the virtual machine will no longer support cloning, creating images, exporting operations, CDP backup, and disaster recovery functions and cannot be recovered.

Prerequisite

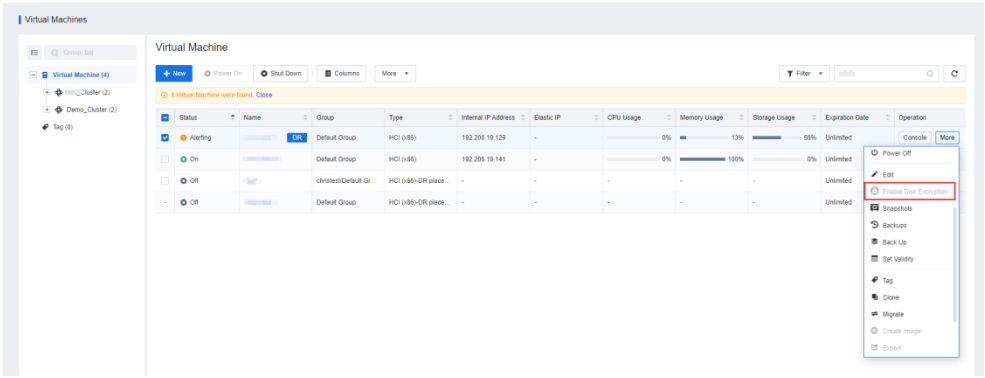
Disk encryption setting must be enabled for the virtual machine.

Steps:

Step 1. Login to the SCP platform, and navigate to **Resources** > **Management** > **Security**. Select **Disk Encryption Settings** to enable the feature.



Step 3. After enabling the disk encryption settings, navigate to **Compute** > **Virtual Machines**, locate the appropriate virtual machine, click **More,** and select **Disk Encryption**.



4.13.5.4 Data Erasure Settings

Function Description

When VMs and backups in the Recycle Bin are permanently deleted, their data will be erased to guarantee data security.

Precautions:

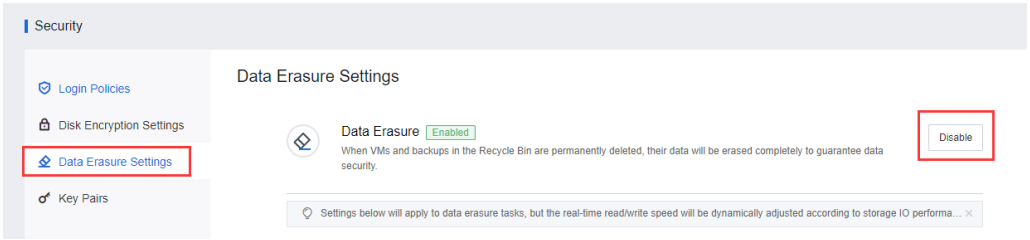
None.

Prerequisite

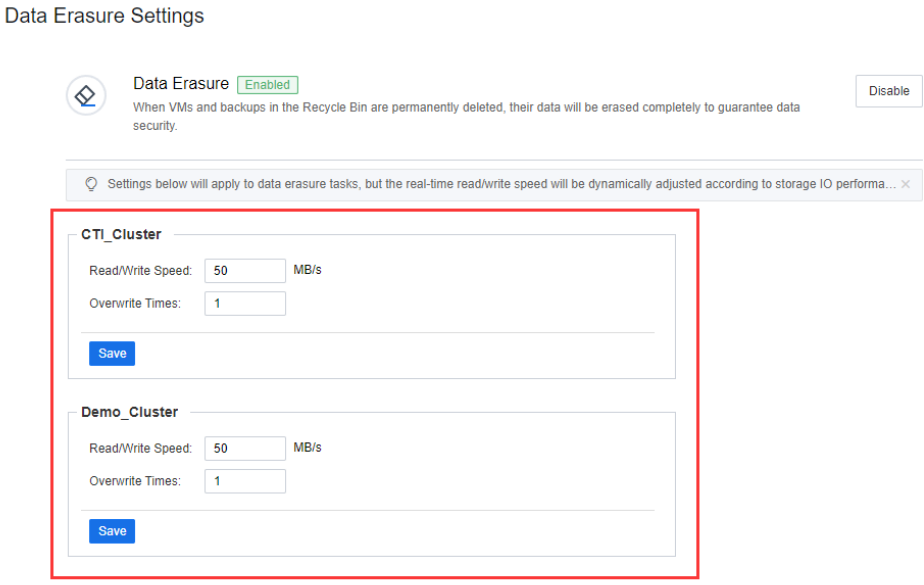
None.

Steps:

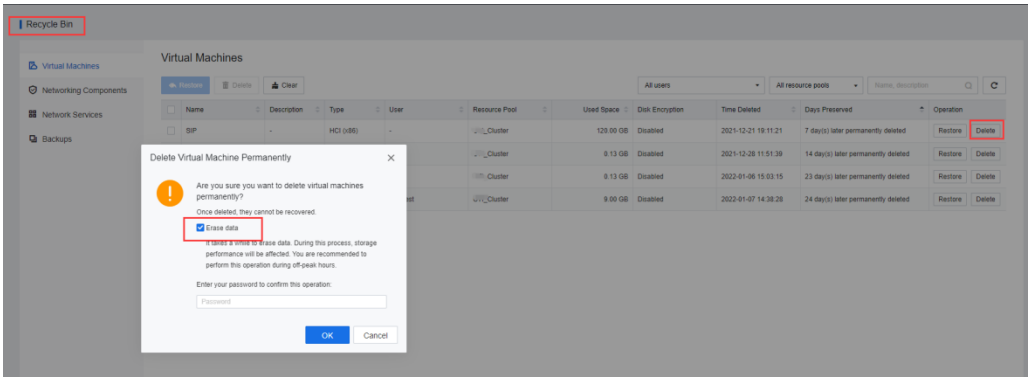
Step 5. Login to the SCP platform, navigate to **Resources** > **Management** > **Security,** and click **Data Erasure Settings** to enable the data erasure feature.



Step 6. It supports configuring the real-time **Read/Write Speed** and the **Overwrite Times** separately for resource pools.



Step 7. After configuring the data erasure settings, navigate to **Management** and go to **Recycle Bin**, select the deleted virtual machine, click **Delete,** and check the **Erase Data** checkbox to delete all the residual data permanently.



4.13.5.5 Key Pairs

Function Description:

Using the account password to log in to the virtual machine is a relatively weak authentication method. There is a risk of brute force attack, and security cannot be guaranteed. The key pair is a safe and convenient login authentication method. The SCP platform provides the virtual machine key pair management. Users can log in to the virtual machine remotely through the private key.

After the SCP platform creates a key pair, it will generate a public key and a private key. When binding the key pair to the virtual machine, the public key

will be pushed down to the virtual machine. Users can securely log in to the virtual machine via SSH using the private key.

Precautions:

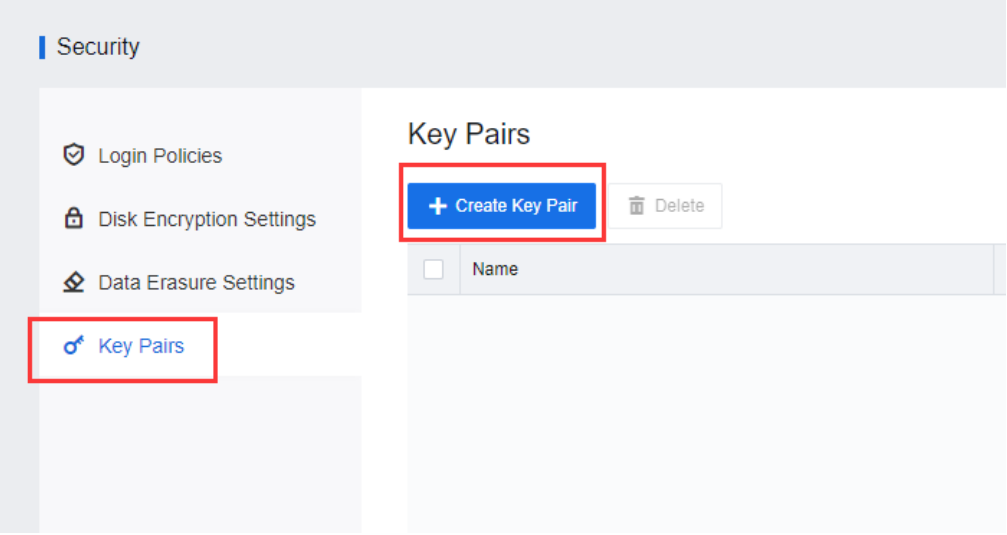
1. The key pair management only supports the SSH protocol of the Linux operating system and is only valid for the root user.
2. The key pair is downloaded to the local PC through the browser only when it is created. The key pair will not be saved on the SCP platform and cannot be downloaded later. Be sure to download the private key after creation and save it properly.
3. The key pair can be unbound on the virtual machine management interface if the private key is lost.
4. After binding the key pair to the virtual machine, it can no longer log in to the virtual machine with the username/password using SSH.

Prerequisite

None.

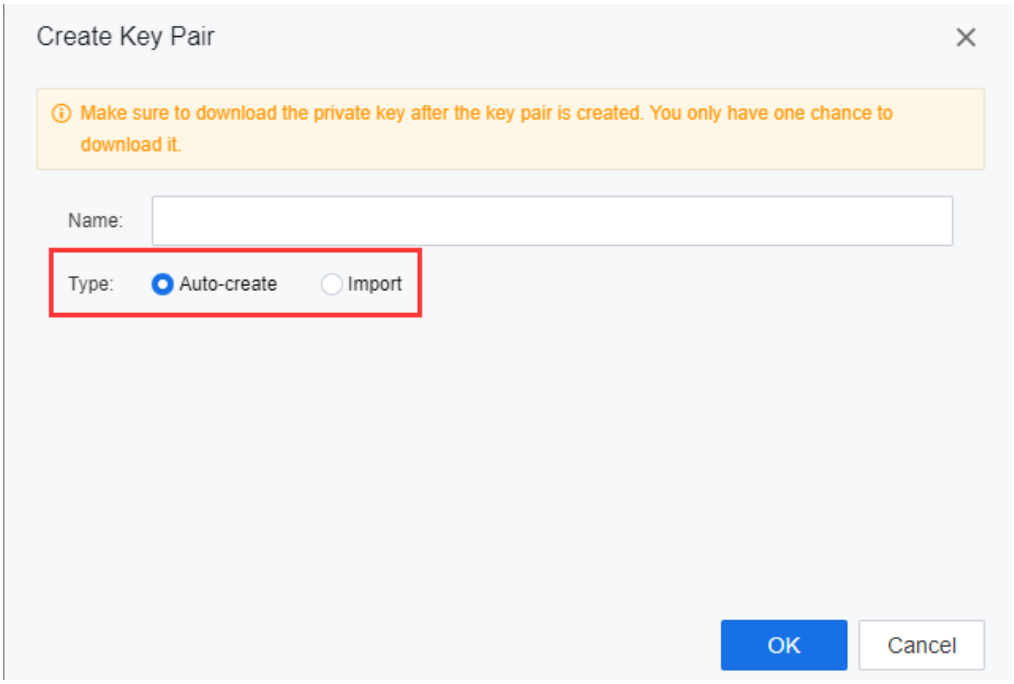
Steps

Step 1. Login to the SCP platform, and navigate to **Resources > Management > Security**. On the **Security** page, click **Key Pairs** and click **Create Key Pair** to create key pair.

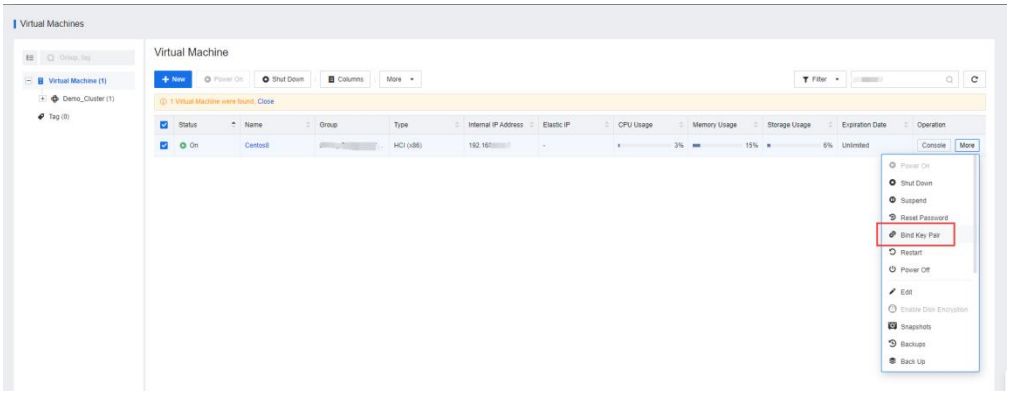


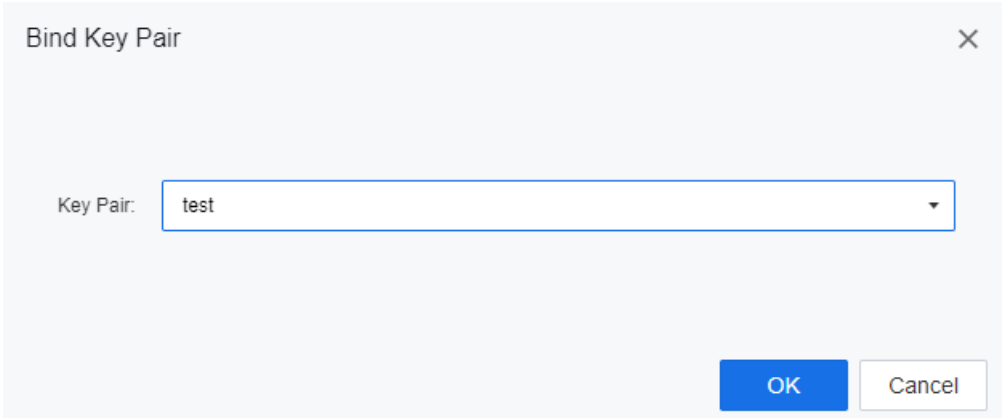
Step 2. Select **Auto-Create.** Select Auto-Create. Please note that after the key pair creation is complete, download the private key and save it. Unfortunately, the SCP platform does not save the private key, and you cannot download the

private key again. Or select **Import** to import the existing public key to the SCP platform for use.



Step 3. After creating a new key pair, locate the specific virtual machine that needs to be bound, clicks **More,** and select **Bind Key Pair** to bind the key pair.





Step 4. Click **OK** to bind the key pair.

4.13.5.6 Key Management Service

Feature Description:

Instruct the administrator to encrypt the virtual machine's disk in the shutdown state, which is often used in improving the security protection of the important virtual machine.

Precautions:

1. The virtual machine encryption needs to be operated on the SCP side. The user master key is stored on the SCP side, and the data key is stored on the HCI side. When the SCP and HCI communication is abnormal, the encrypted virtual machine cannot be powered on. It needs to solve the communication abnormality before it can be powered on.

2. The encrypted virtual machine does not support export, clone, template deployment, cross-cluster migration, migration to VMware, backup, new, and restore operations.

3. The encrypted virtual machine supports decryption on the SCP platform.

4. During encryption of the virtual machine that uses KMS encryption, if the connection between SCP and KMS is disconnected, the connection between SCP and HCI cluster is disconnected, and the HCI node at the running location is out of SCP management, the virtual machine will be shut down after being shut down. Unable to use because there is no key to decrypt.

5. The virtual machine's performance with encryption enabled will drop by 30%-50% compared to when it is not encrypted.

6. Virtual machines with encryption enabled will not be able to use CDP, disaster recovery, cloning, exporting, and mirroring.

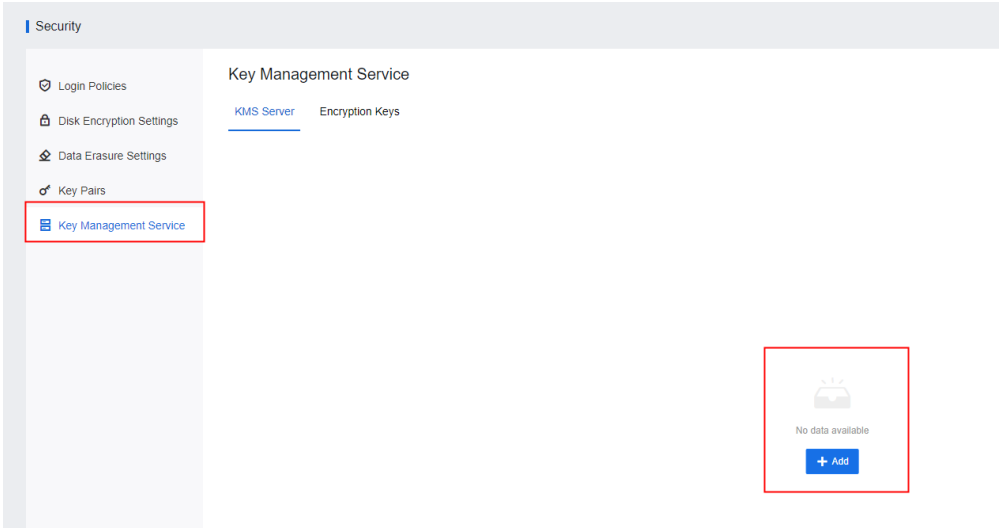
7. The encryption process takes a period, and operations such as booting are not supported. It is recommended that you handle it when your business is idle.

Prerequisite

The SCP must activate the KMS service, which can be activated on the SCP platform.

Steps:

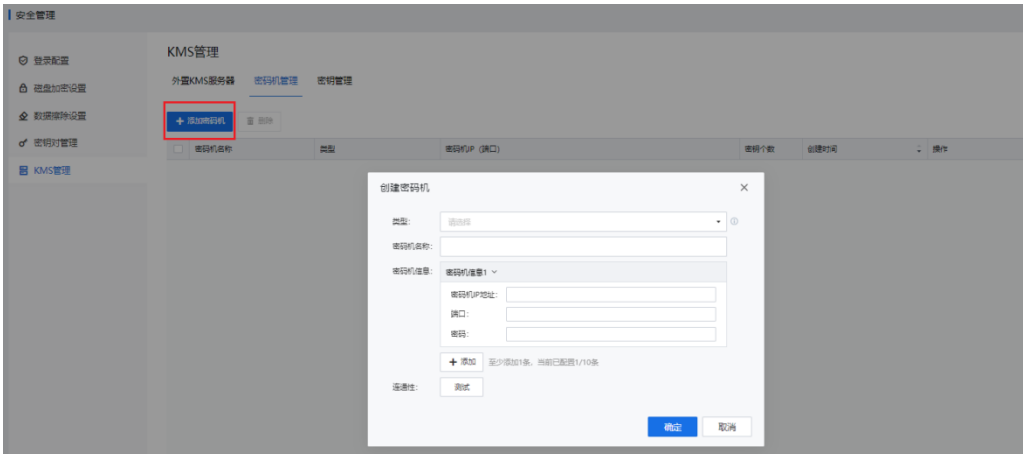
Step 1. Login to the SCP platform and navigate to **Resources** > **Management** > **Security**. Click **Add** to add a KMS server to the SCP platform.



HSM Management

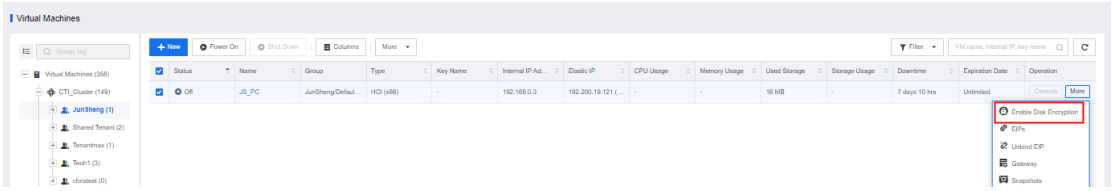
On the **HSMs** tab, click **Add**.

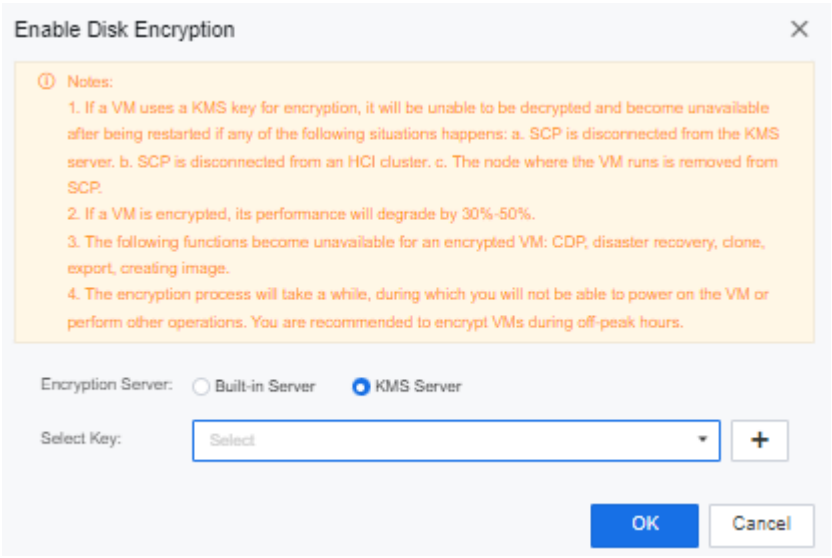
- Type: You can select type A (for Sansec) or B (for JIT).
- Information: Configure the IP address, port number, and password for the HSM. You can add up to 10 HSMs.



1. Virtual Machine Encryption

Step 1. Enter the **Compute > Virtual Machines** interface, select the virtual machine that needs to be encrypted, and click **More > Enable Disk Encryption** to convert the ordinary virtual machine into an encrypted virtual machine.





3. Virtual Machine Decryption

Step 1. Enter the **Compute > Virtual Machines** interface, select the virtual machine that needs to be decrypted, and click **More > Disable Disk Encryption** to convert the encrypted virtual machine into an ordinary virtual machine.

4.13.6 System Configuration

4.13.6.1 License Key

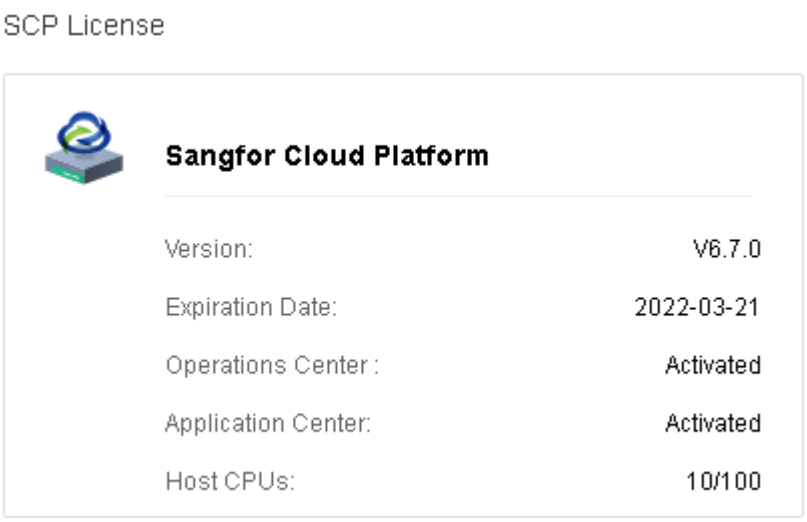
Feature Description:

SCP controls the authorization of each module through the license key. Currently, there are three licensing modes: **Advanced Edition, Enterprise Edition,** and **Enterprise Plus Edition**. The differences between the three are shown in the figure below.

Resource	Features	Advanced Edition	Enterprise Edition	Enterprise Plus Edition
Resource Overview	Supports creating HCI or Vmware resource pools of different versions	✔	✔	✔
	Supports adding and management of HCI or Vmware clusters	✔	✔	✔
	Physical Machine	-	Standalone mode	Standalone mode
	Vmware VM & Backups	Standalone mode	Standalone mode	Standalone mode
Compute	Virtual Machines	✔	✔	✔
	aGPU	Standalone mode	Standalone mode	Standalone mode
	Containers	Standalone mode	Standalone mode	Standalone mode
Images	Images	✔	✔	✔
Network	Visualized Network Topology	✔	✔	✔
	Distributed Firewall	✔	✔	✔
	Tenant VPC	-	✔	✔
	Tenant EIP	-	✔	✔
	Tenant Direct Connection	-	✔	✔
	Tenant Shared Bandwidth	-	✔	✔
	Shared Service Network	-	✔	✔
Security Services	aSEC Components (ADC, NGAF, SSL VPN)	Standalone mode	Standalone mode	Standalone mode
	Security Integration with Cyber Command	Standalone mode	Standalone mode	Standalone mode
	WAF Protection	✔	✔	✔
	Security Enhancement	✔	✔	✔
Hybrid Cloud	Third-Party Public Cloud	-	-	✔
Reliability	Scheduled Backup	✔	✔	✔
	CDP	Standalone mode	Standalone mode	Standalone mode
	Disaster Recovery	Standalone mode	Standalone mode	Standalone mode
	VM Failover	✔	✔	✔
	DRS (Dynamic Resource Scheduling)	✔	✔	✔
	Resource Reservation	✔	✔	✔
	Reliability Monitor	✔	✔	✔
	Auto Scaling	-	✔	✔
Operations Center	Multi-Tenant	-	✔	✔
	Work Orders	-	✔	✔
	Bills	-	✔	✔
	Edit Resource Quota	-	✔	✔
	Billing Center	-	✔	✔
Monitoring	Monitoring Dashboard	✔	✔	✔
	Reports	✔	✔	✔
Management	Open Interfaces	✔	✔	✔
	Portal Customization	✔	✔	✔
	LDAP	-	✔	✔
	SSO (CAS authentication)	-	✔	✔
	Tasks	✔	✔	✔
Application Center	Application Center (app deployment and management)	-	-	✔
	Redis (open source)	Standalone mode	Standalone mode	✔
	MongoDB (open source)	Standalone mode	Standalone mode	✔
	Kafka (open source)	Standalone mode	Standalone mode	✔
	RabbitMQ (open source)	Standalone mode	Standalone mode	✔
	CDH (open source)	-	-	✔
aOPS	CMDB	Standalone mode	Standalone mode	Standalone mode
	Monitoring and Alerts	Standalone mode	Standalone mode	Standalone mode

Precautions:

The **Number of CPUs on Physical Hosts** of the SCP must not be lower than the number of CPUs in all managed clusters. Regardless the HCI is using standalone mode or centralized mode.

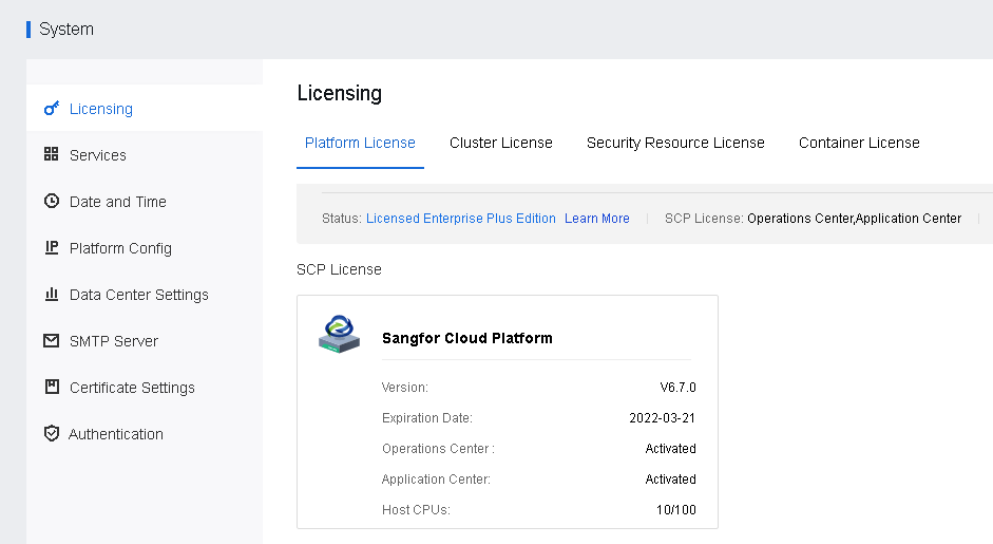


Prerequisite

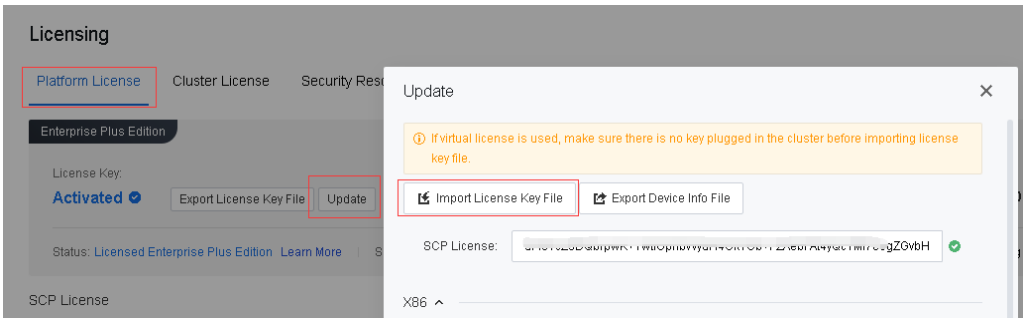
Has the license key ready.

Steps:

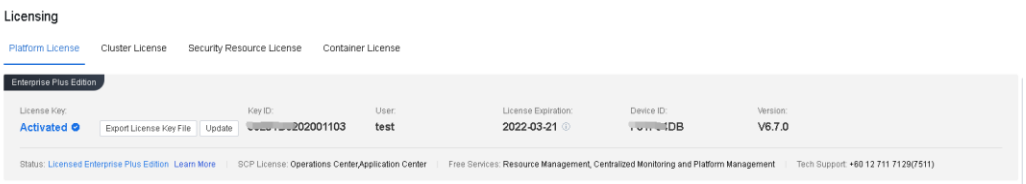
Step 1. Login to the SCP platform, navigate to **Resources** > **Management** > **System,** and then select **Licensing** to enter the license page.

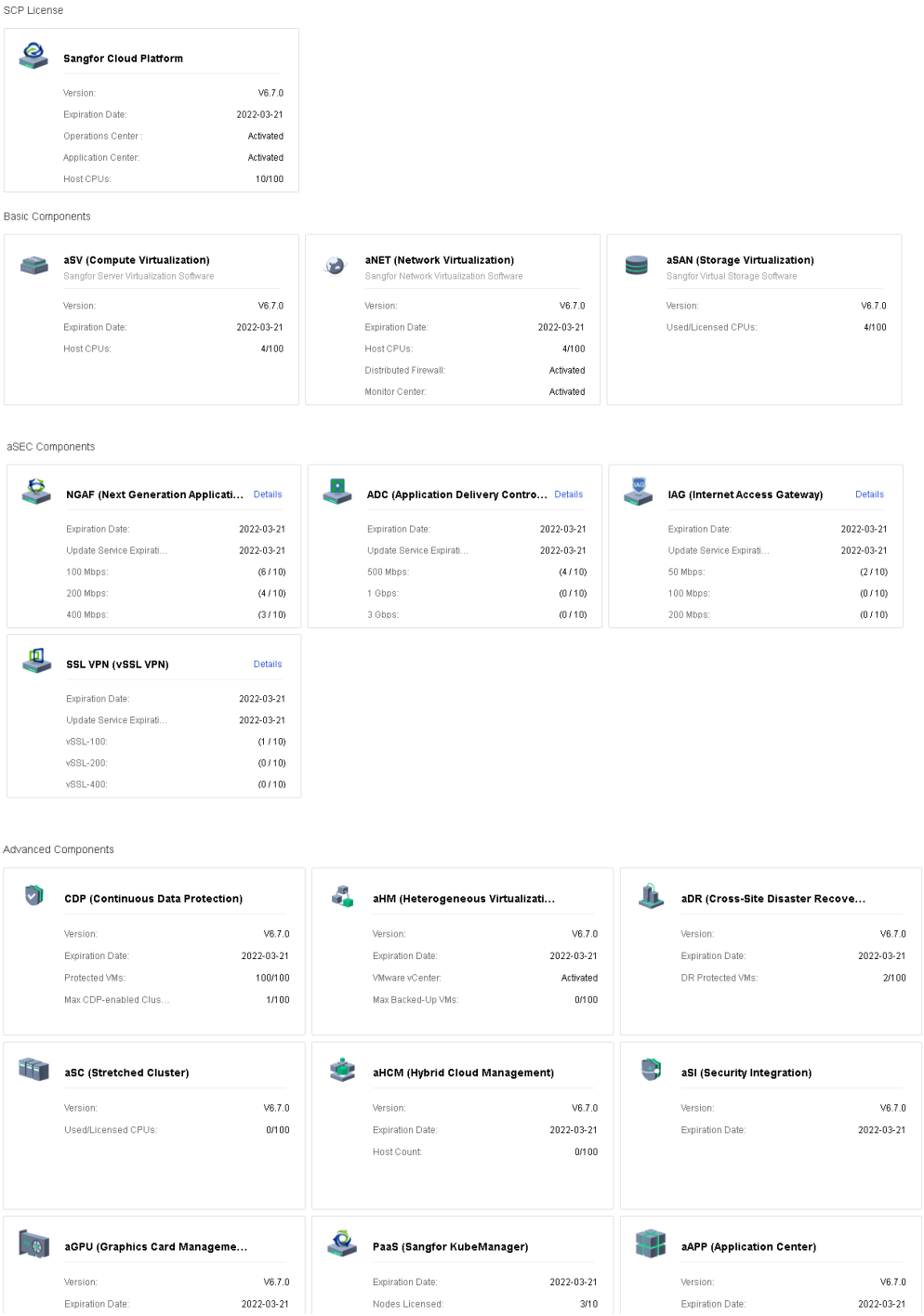


Step 2. In **Platform License,** click **Update** and then click **Import License Key File** to import the license key or renew the license.



Step 3. After the license key file has been imported successfully, you can view all the licensing-related information.





4.13.6.2 Services Management

Feature Description:

The SCP platform supports custom starting and stopping **API service**, **Billing Center**, and **Application Center**.

API: SCP external interface service can be used for secondary development and docking with third-party cloud computing platforms.

Billing Center: User resource billing and metering service, support expenses overview, tenant expenses details query, and pricing.

Application Center: Traditional and cloud-native application services, providing full lifecycle management such as rapid deployment, configuration, monitoring, and backup.

Precautions:

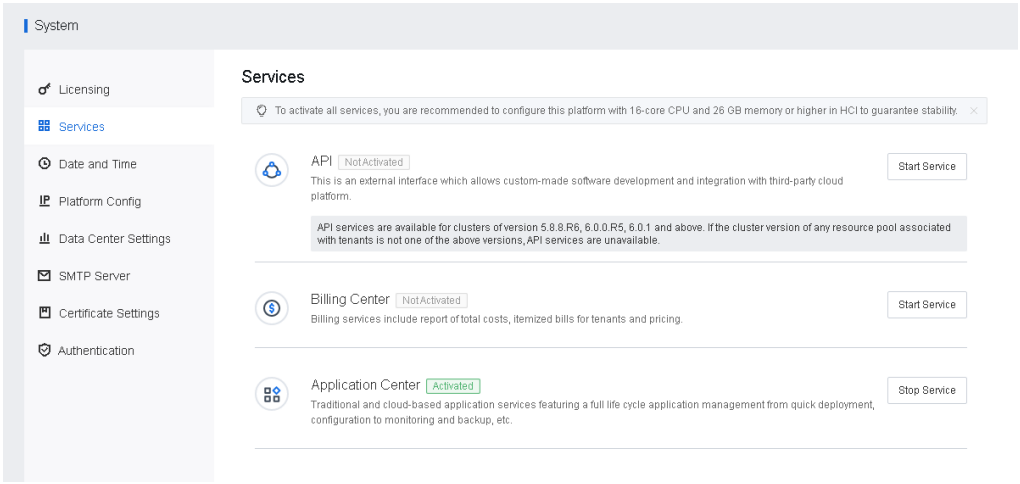
If required to enable the API service and the billing center simultaneously, it is recommended to configure the platform with a 16-core CPU, 24G memory, or higher in HCI to ensure stable operation.

Prerequisite

None.

Steps:

Step 1. Login to the SCP platform, navigate to **Resources** and look for **Management**, click into **System** and select **Services**.



Step 2. Click **Start Service** or **Stop Service** to start or stop service.

4.13.6.3 Date And Time

Features:

Sangfor SCP supports time customization and the automatic acquisition of NTP time.

Precautions:

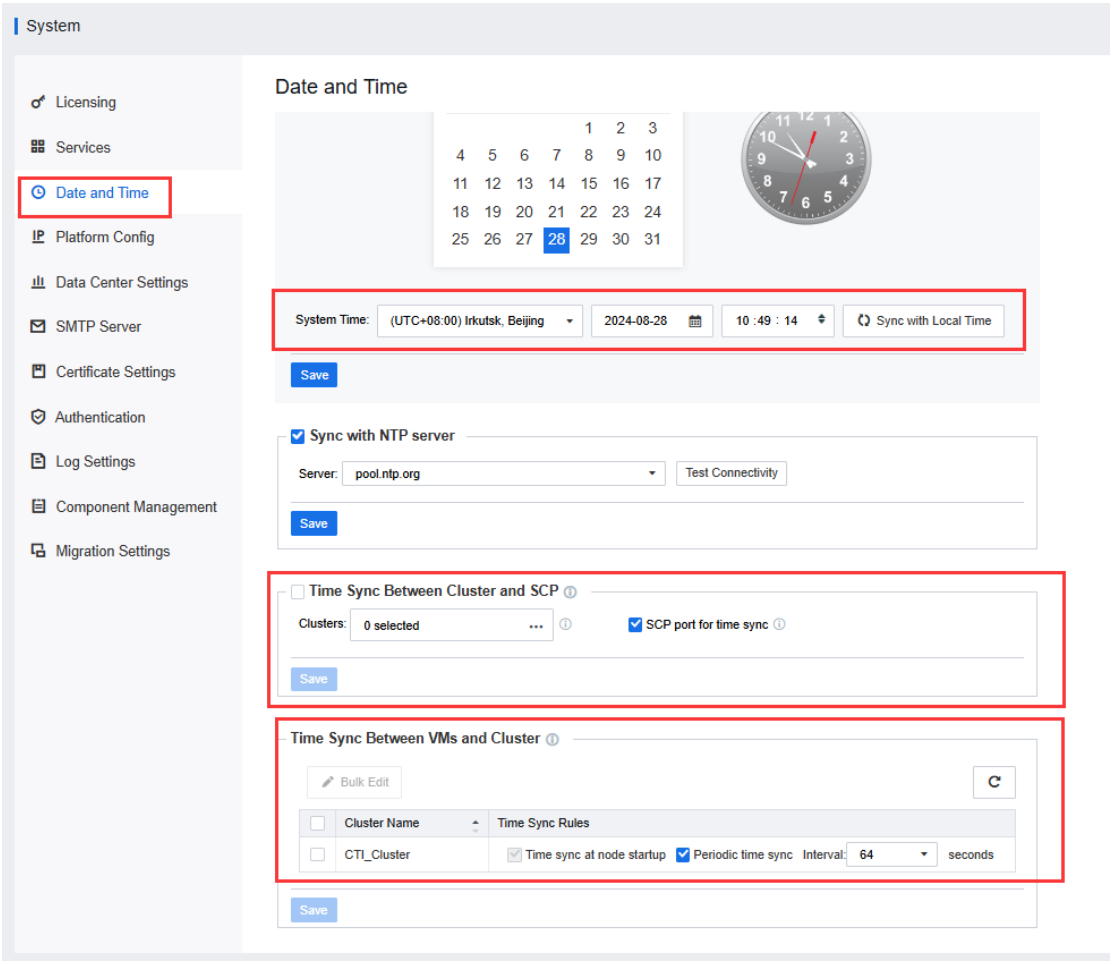
N/A.

Prerequisite

N/A:

Steps

Step 1. Login to the SCP platform, navigate to **Resources** > **Management** > **System,** and select **Date and Time** to enter the date and time page for modification. Supports enabling **Time Sync Between Cluster and SCP** and **Time Sync Between VMs and Cluster**.



4.13.6.4 Platform IP Configuration

Features:

SCP supports changing IP on demand and can configure DNS and routing for SCP to meet the network requirements of different scenarios.

Precaution:

N/A.

Prerequisites

The IP information, routing configuration, and DNS configuration of the platform have been properly planned.

Steps:

Step 1. Login to the SCP platform, navigate to **Resources > Management > System,** and click **Platform Config**.

Step 2. Configure the IP information, routing configuration, and DNS according to actual requirements.

4.13.6.5 Data Center Settings

Function Description:

Sangfor SCP supports docking with managed cloud accounts, and the local data center information needs to be configured before docking.

Precautions:

Port 443 of the local data center must be able to communicate with the Sangfor SCP. In NAT scenarios, kindly ensure that port 443 has been allowed.

Prerequisite

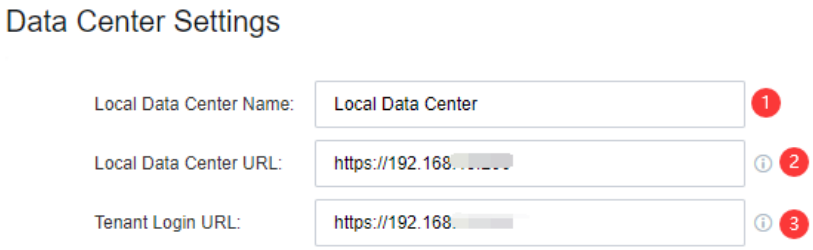
None.

Steps:

Step 1. Login to the SCP platform, navigate to **Resources** > **Management** > **System,** and click **Data Center Settings** to enter the configuration page.

Step 2. Fill up the **Data Center Settings**:

- Fill up the Local Data Center Name.
- Fill up the HTTPS address of the local data center for communication between the local data center and the SCP, and it must be using port 443.
- Fill up the **Tenant Login URL**.



Step 3. Click **Save** to save the configuration.

4.13.6.6 SMTP Server

Features:

Sangfor SCP supports configuring the SMTP server. Alerts can be sent by email and allow customers to keep track of the cluster's running status at any time.

Precautions:

1. If the verification using the email password fails, you may try to use the email client authorization code for verification.
2. If the SCP platform IP setting does not have DNS configured, the SMTP server address can only fill in the IP.

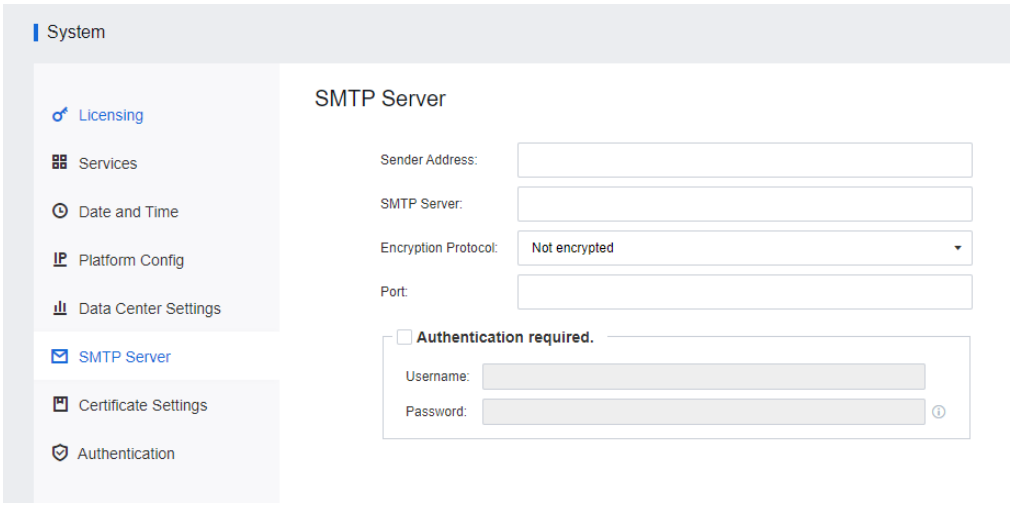
Prerequisite

N/A.

Steps:

Step 1. Login to the SCP platform, navigate to **Resources** > **Management > System,** and click the **SMTP Server** to enter the configuration page.

Step 2. Fill in the **Sender Address** and **SMTP Server** information according to the actual requirement. If the sending server needs to verify the username and password, enable the **Authentication required, fill** in the corresponding username and password, and click **Send Test Email** for testing.



NOTE

If the verification using the email password fails, you may try to use the email client authorization code for verification.

4.13.6.7 Certificate Settings

Features:

The SSL certificate establishes an SSL secure layer between the client and the SCP platform. When the client's browser marks an insecure warning on the HTTPS website, installing the SSL certificate can make the client trusted by the browser and remove the insecure warning. Sangfor SCP supports the manual import of trusted certificates.

Precautions:

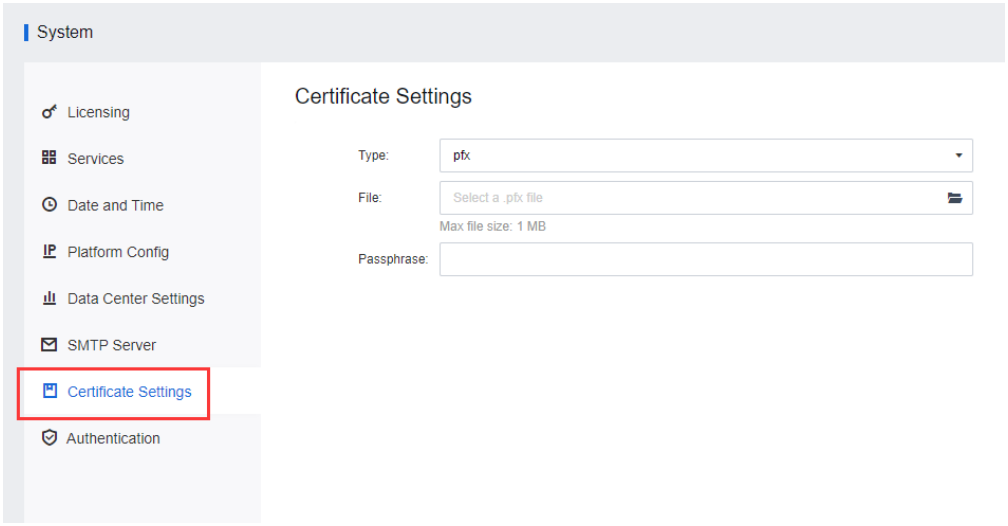
N/A.

Prerequisite

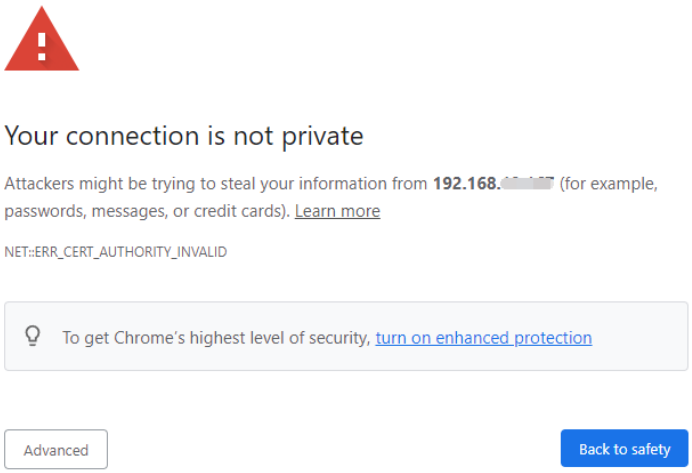
N/A.

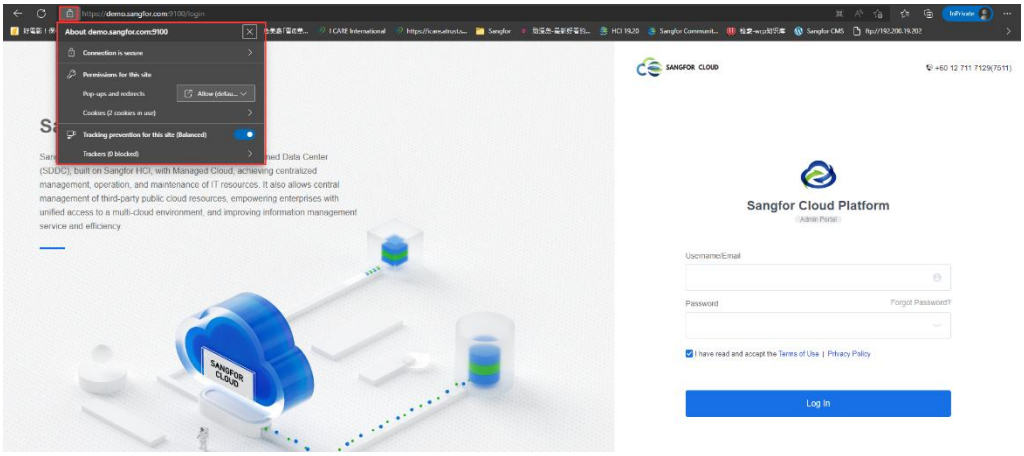
Steps:

Step 1. Login to the SCP platform, navigate to **Resources > Management > System,** and click **Certificate Settings** to enter the configuration page. Currently, four certificate types are supported: **pfx**, **p12**, **crt+key,** and **pem**.



Step 2. After a trusted certificate has been imported, the client's web browser is trusted now, and the connection alert has been resolved.





4.13.6.8 Authentication

Feature Description:

1. Sangfor SCP supports correlating with LDAP authentication and can import LDAP users into this platform to manage user authentication. LDAP is a lightweight directory access protocol generally used as an authentication server. SCP supports importing users from the LDAP server into SCP and assigning corresponding roles.
2. SCP 6.9.0 and later versions can connect to third-party OTP servers via standard RADIUS protocols. Both username/password and OTP verification code are required for login, which enhances account security. Remote Authentication Dial-In User Service (RADIUS) is a protocol for network access control. If a user attempts to access the network, the network device sends the user identity information to the RADIUS server for authentication.

Precautions:

1. If the LDAP server is disconnected from the SCP or the LDAP server is down, users will not be able to log in on the SCP.
2. When modifying user information on the LDAP side, it is not recommended to change the login username and email address at the same time. A new user would be created in SCP during the import if both were changed simultaneously.
3. The import username cannot be **admin** or **SCP**.
4. Users who do not have email addresses and mobile phone numbers on the LDAP server will have their mobile phone numbers, and email addresses randomly generated on the SCP after being imported into the SCP.

Prerequisite

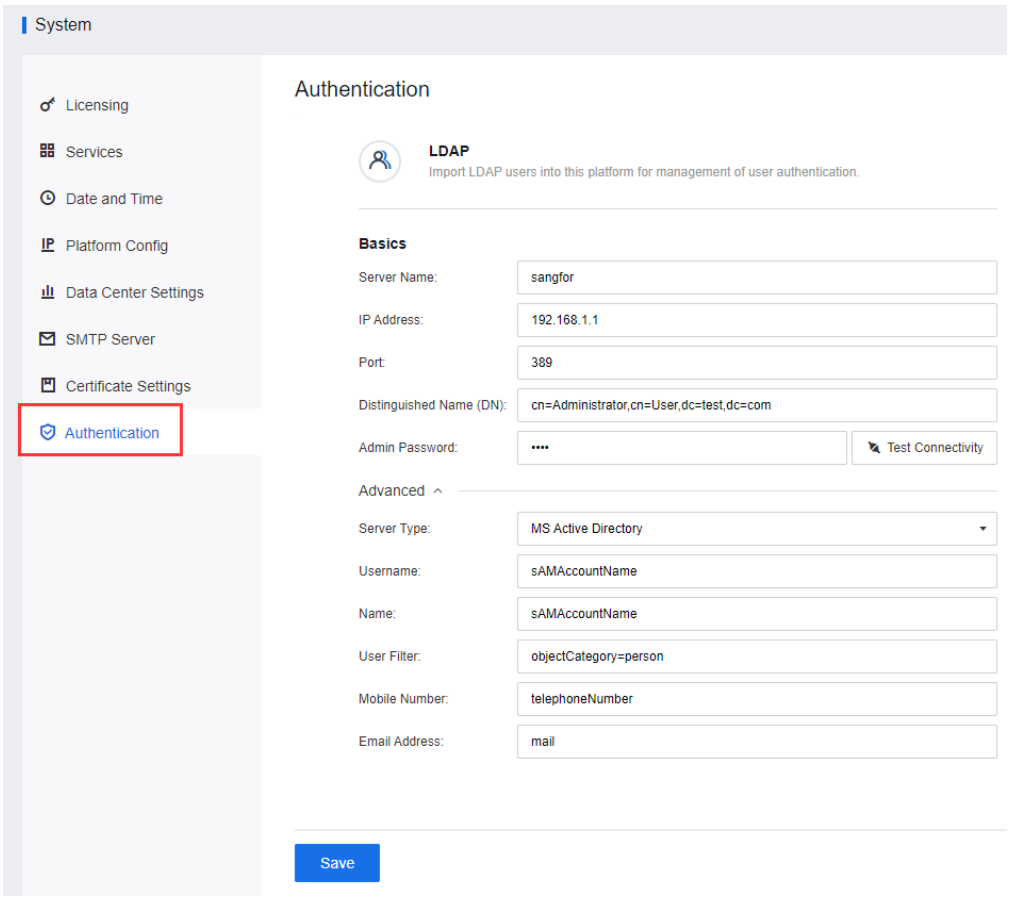
1. If the operating system of the LDAP server is Windows, the Windows server 2012 version is supported.
2. If the operating system of the LDAP server is Linux, it must support OpenLDAP.
2.

Steps:

LDAP Authentication

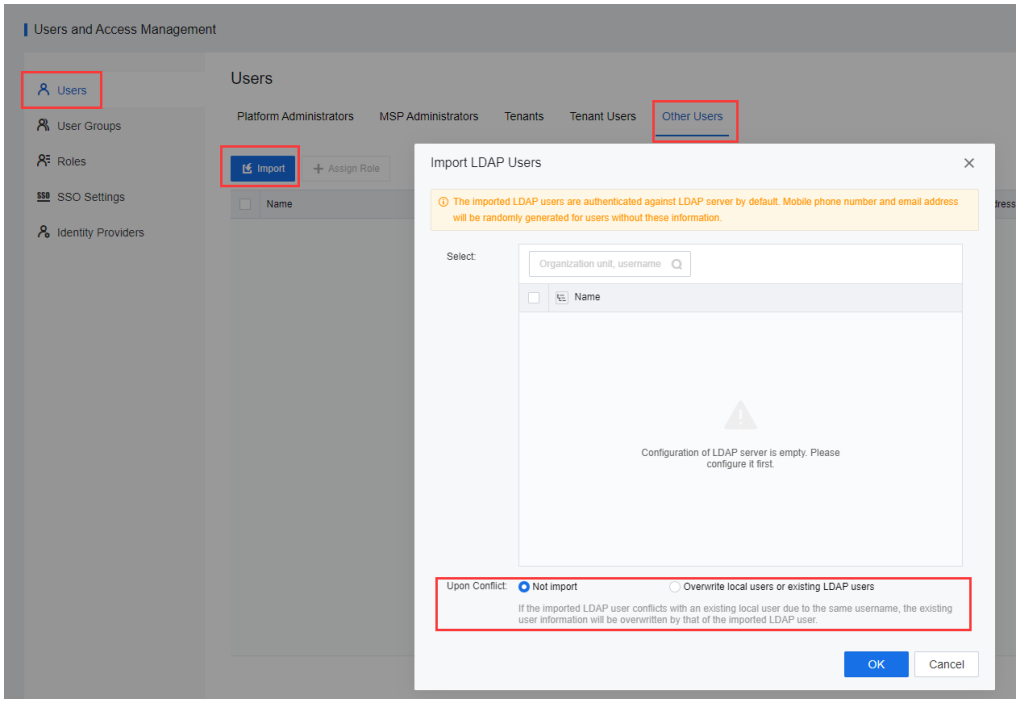
Step 1. Login to the SCP platform, navigate to **Resources > Management** > **System,** and click **Authentication** to enter the configuration page.

Step 2. Configure the **Server Name, IP Address, Port, Distinguished Name (DN)**, and **Admin Password,** as shown in the below figure.



Step 3. After the configuration is complete, click **Test Connectivity** to verify the configuration. Finally, click **Save** to save the configuration.

Step 4. Navigate to **Users and Access Management > Users** > **Other Users**, click **Import,** select **Import LDAP Users,** and configure the **Upon Conflict**. Click **OK** to import users.



Step 5. After completing the import, click **Assign Role** to the corresponding users and configure the corresponding role. The imported user can be configured as a tenant or tenant user role.

4.13.6.9 SSO Settings

Features:

Single sign-on (SSO) is a one-time authentication login through the user. After the user logs in once on the authentication server, the user has the right to access other related systems and application software in the single sign-on system.

Sangfor SCP supports docking with the customer's existing CAS system. When logging in to the SCP, the customer's existing account information is used for logging in. After assigning roles, single sign-on can be realized, reducing the customer's burden of operation and maintenance.

Prerequisite

1. The customer's existing CAS authentication system is operating normally, and the communication between the CAS server and the SCP platform is normal.
2. The supported CAS version includes CAS_V2 and CAS_V3.
3. Platform administrators do not support single sign-on using CAS. Only

tenants and tenant users can log in through CAS.

Precautions:

After the user is single sign-on, if it conflicts with the existing user of the SCP platform (the login username is the same), the new user information will be imported, and the existing information will be overwritten. Otherwise, the user will be registered and displayed in the **Other Users** list. Available after assigning role.

Steps:

Step 1. Login to the SCP platform using the admin account, navigate to **Users and Access Management,** and then click **SSO Settings**.

Step 2. Configuring the basic settings:

- SSO: check the **Enable CAS SSO** checkbox.
- Entry & Text: Can customize, for example, CAS login.
- Version: Select the appropriate version.
- Login URL: https://cas.example.com/cas/login?service=https://SCP.com/sso/cas/callback.

  For example, if the CAS server IP address is 192.168.1.1 SCP platform IP address is 192.168.10.1, the login URL will be https://192.168.1.1/cas/login?service=https://192.168.10.1/sso/cas/callback.
- Ticket Verification URL: https://CAS server IP/cas/p3/serviceValidate?ticket={ticket}&service=https://SCP IP/sso/cas/callback

  Take the above IP addresses as example:

  https://192.168.1.1/cas/p3/serviceValidate?ticket={ticket}&service=https://192.168.10.1/sso/cas/callback

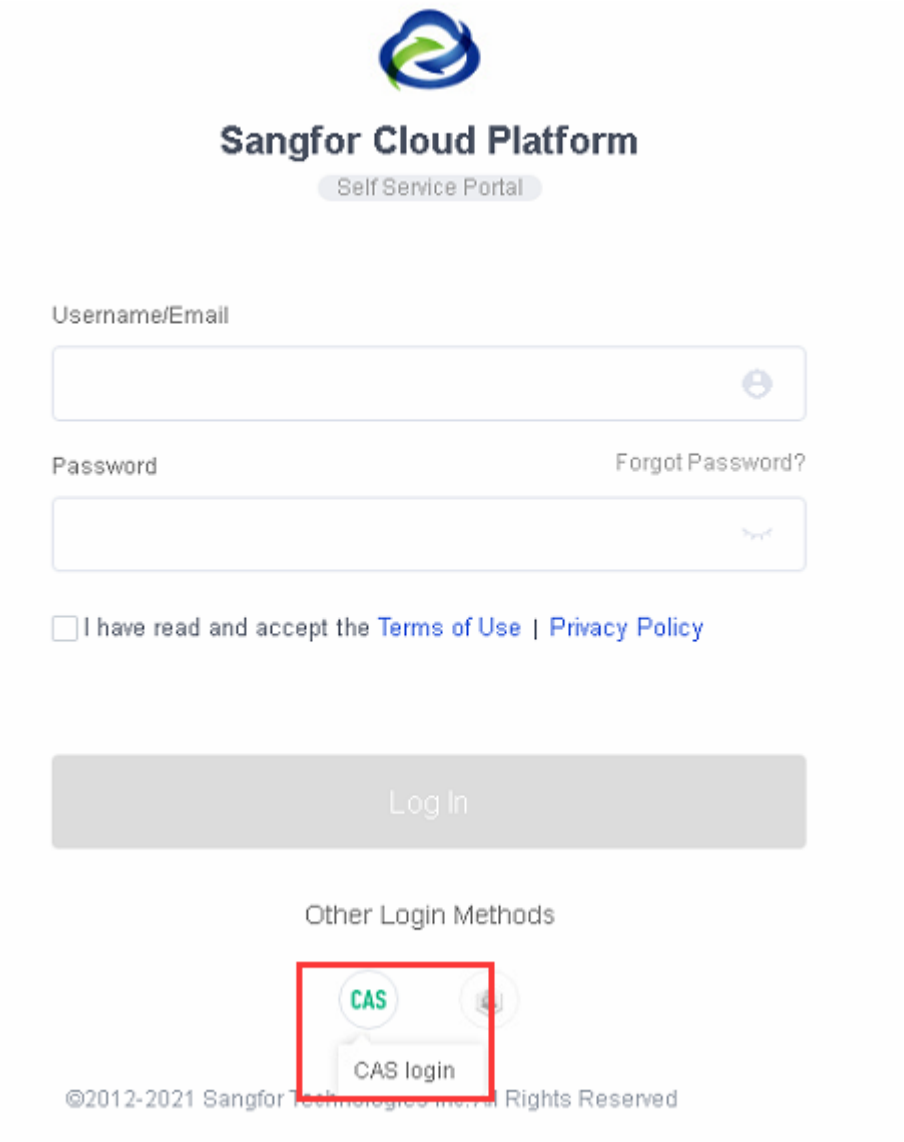
Step 3. Advanced Settings

- Username: Obtain from the client.
- Name: Obtain from the client.
- Email Address: Obtain from the client.

- Mobile Number: Obtain from the client.
- Auto Registration: check the **Enable** checkbox to enable auto registration. Auto Registration: check the Enable checkbox to enable the auto registration. It will convert the uppercase letters in a username returned from the CAS server into lowercase letters to create an associated user account on the platform with data synchronized.

Step 3. Click **Save** to save the configuration.

Step 4. Through the IP address of SCP with https://SCP IP, visit the self-service portal and log in.



Step 5. At this time, it will prompt **the account has no access rights. Please contact the administrator**. Use admin to login to the SCP platform, navigate to **Users and Access Management** under **Users,** select **Other Users**, and add

the role of the **tenant** to the imported CAS User.

Step 6. Login through the **CAS login portal** of the self-service portal again, enter the username and password, and log in to the tenant interface.

Step 7. When the client CAS server has multiple users, it is also possible to manually import users in batches.

4.13.6.10 Component Management

Function Description

You can configure the display status of a component on SCP.

Prerequisites

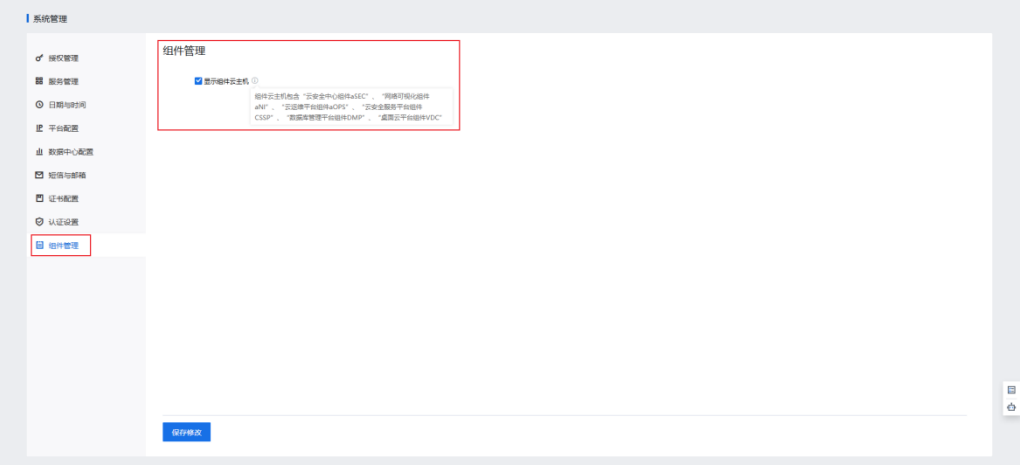
N/A

Precautions

VMs whose components can be managed are VDC, aSecurity, aNI, and more.

Steps

Go to **Management** > **System** > **Component Management** and select or deselect **Display component VMs**.



4.14 Application Service

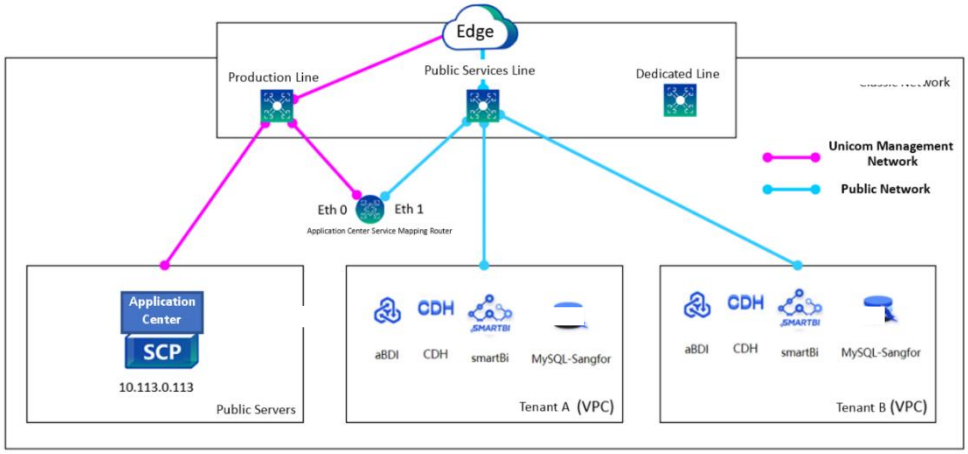
4.14.1 SCP Application Center

4.14.1.1 Application Center Network Planning

Scenario:

Sangfor SCP introduces an application center module to support rapid application deployment, testing, and operation and maintenance, deliver rapid application development and online and ensure future full life cycle operation and maintenance management.

Topology Planning



Precautions:

1. The application center is embedded in SCP and uses its address, but it needs to communicate with the tenant through the shared service network, so a new router for service address mapping is required. In this manual, the router will be named **Application Center Service Mapping**.
2. One of the interfaces in the **Application Center Service Mapping** router will be connected to the production edge to communicate with the SCP, while another interface will be connected to the public service edge to communicate with the tenant VPC.
3. Map the ports 4436 and 5671 of the SCP to the public service network in the **Application Center Service Mapping** router to forward the request from the tenant to the **Application Center**.
4. Convert the source address of the packets after port mapping to the address of the connected SCP on the router so that the destination address of the SCP when it returns packages is the address of the connected SCP on the router.

Device	Interface	IP Address	Remark
Application Center	-	192.168.1.100/24	SCP as Application Center

Elastic IP Pool	-	10.10.10.20 – 10.10.10.50/24	-
Application Center Service Mapping Router	Eth0	192.168.1.101/24	Connect to the edge outgoing interface and SCP management interface.
	Eth1	10.10.10.1/24	1. Connect to the shared network, and it is excluded from the public service elastic IP pool. 2. Bind and map this IP address to domain name **appcenter.local.cloud.scp** from shared service.

Table 7: IP Details

4.14.1.2 Application Center Deployment

Features:

Sangfor SCP introduces an application center module to support rapid application deployment, testing, and operation and maintenance, deliver rapid application development and online and ensure future full life cycle operation and maintenance management.

Precautions:

The domain name of the application center in the shared service network must be **appcenter.local.cloud.scp**, and the IP address is the public service address of the application center service mapping router, and this address must be in the same segment with the elastic.

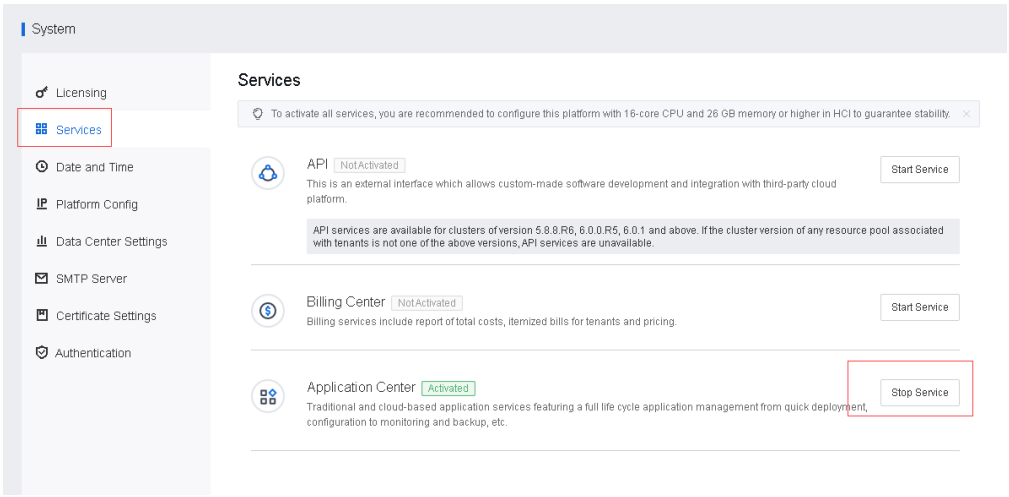
IP of the shared service network and excluded from the elastic IP pool.

Prerequisite

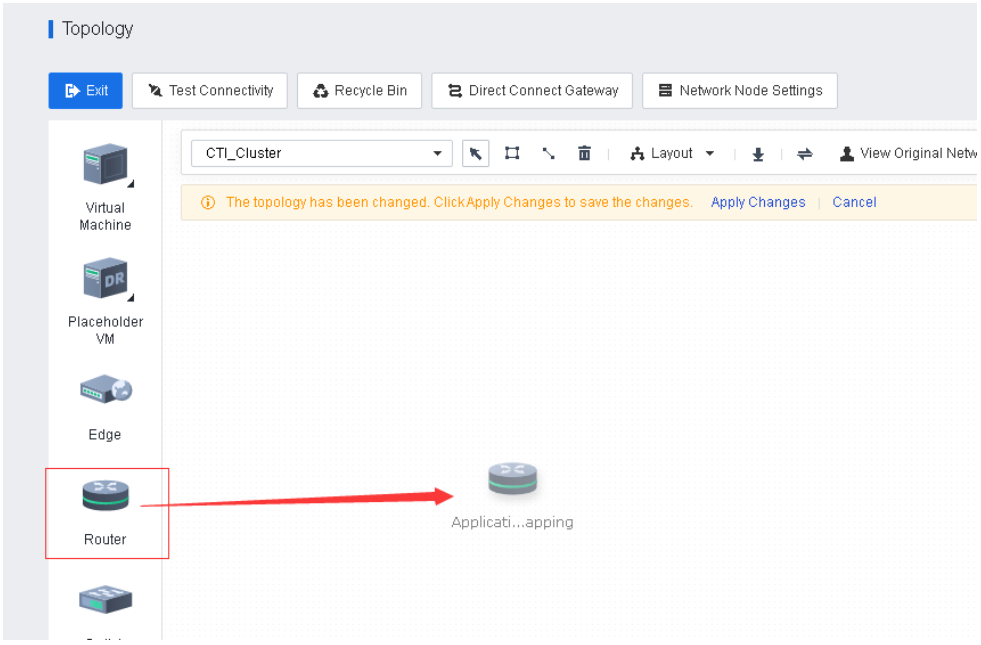
1. The SCP has the **Application Center** license, and this module is enabled.
2. The shared service network gateway planning has been completed.
3.

Steps

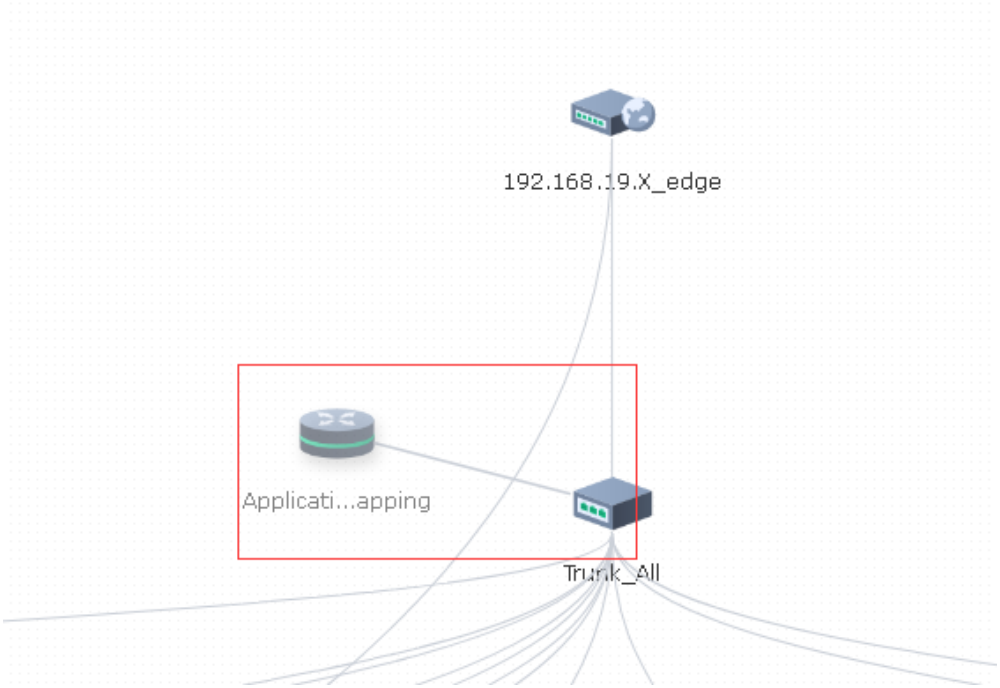
Step 1. Navigate to **System** > **Services > Application Center** and click **Start Service**.



Step 2. Navigate to **Networking** > **Topology** to edit the virtual topology and add a **Router** with the name **Application Center Service Mapping**.

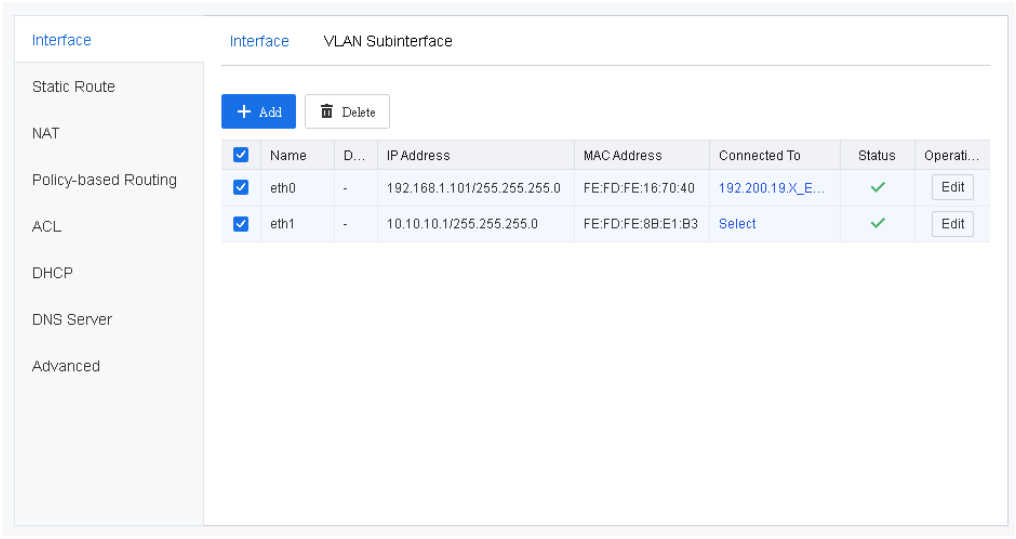


Step 3. Connect one router's interface to the physical network for communication with the shared service network and another interface to the management network for communication with the SCP.



Step 4. Configure the interface address according to the plan in the **Application Center.**

Network Planning section.



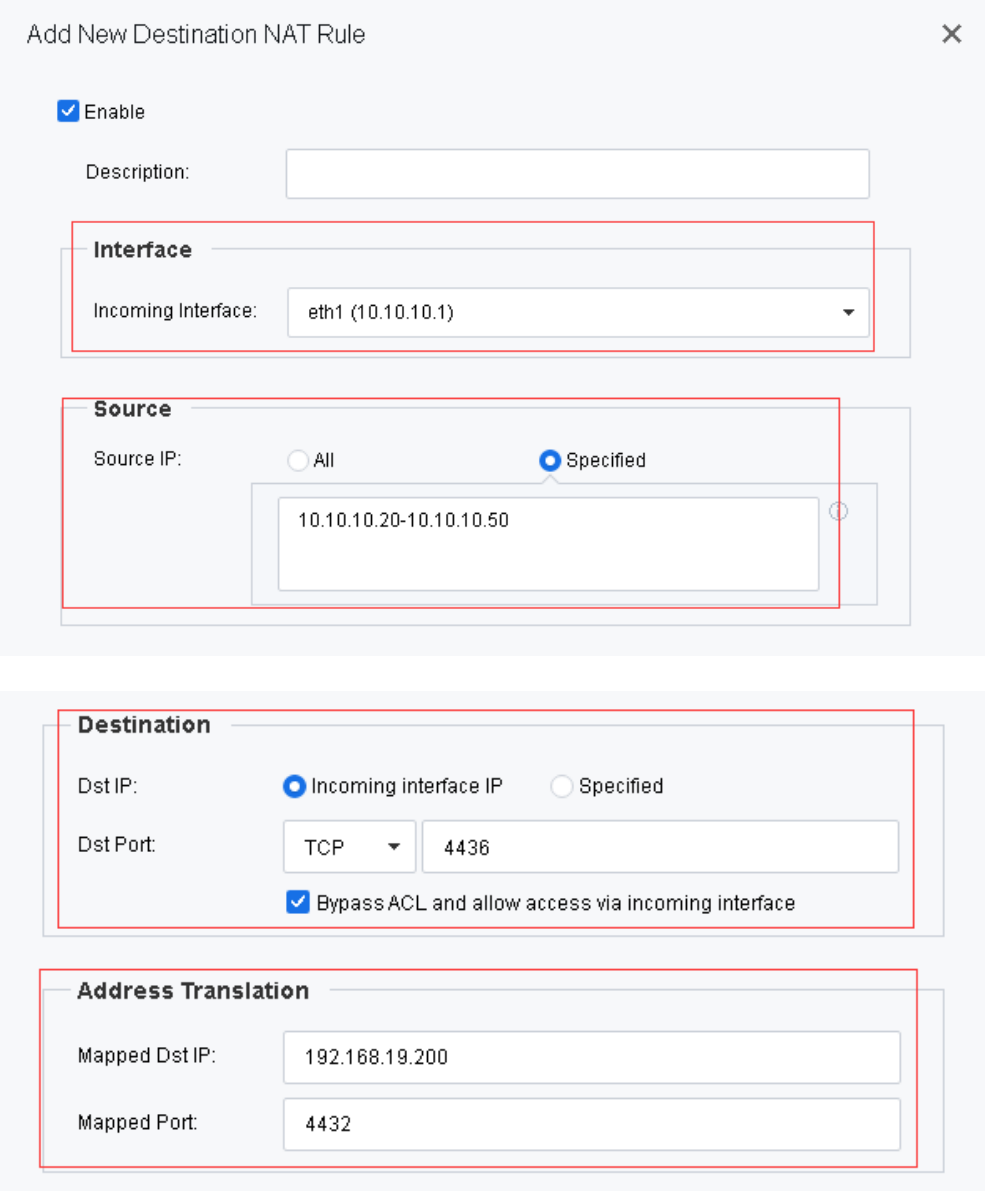
Step 5. Configure the DNAT policy to map ports 4436 and 5671 of the Application Center SCP on the Application Center Service Mapping Router to forward requests from the tenant to the Application Center after configuration.

Incoming Interface: The interface of the Application Center Service Mapping route to the shared service network.

Source IP: The IP in the resilient IP pool of the shared service network.

Destination IP: The IP of the inbound network interface.

Mapped Destination IP: The IP of the SCP.



Step 6. Configure the SNAT policy to convert the source address of the packet after DNAT to the address on the router connecting to the service gateway so that the destination address of the SCP when it returns the packet is the address on the router.

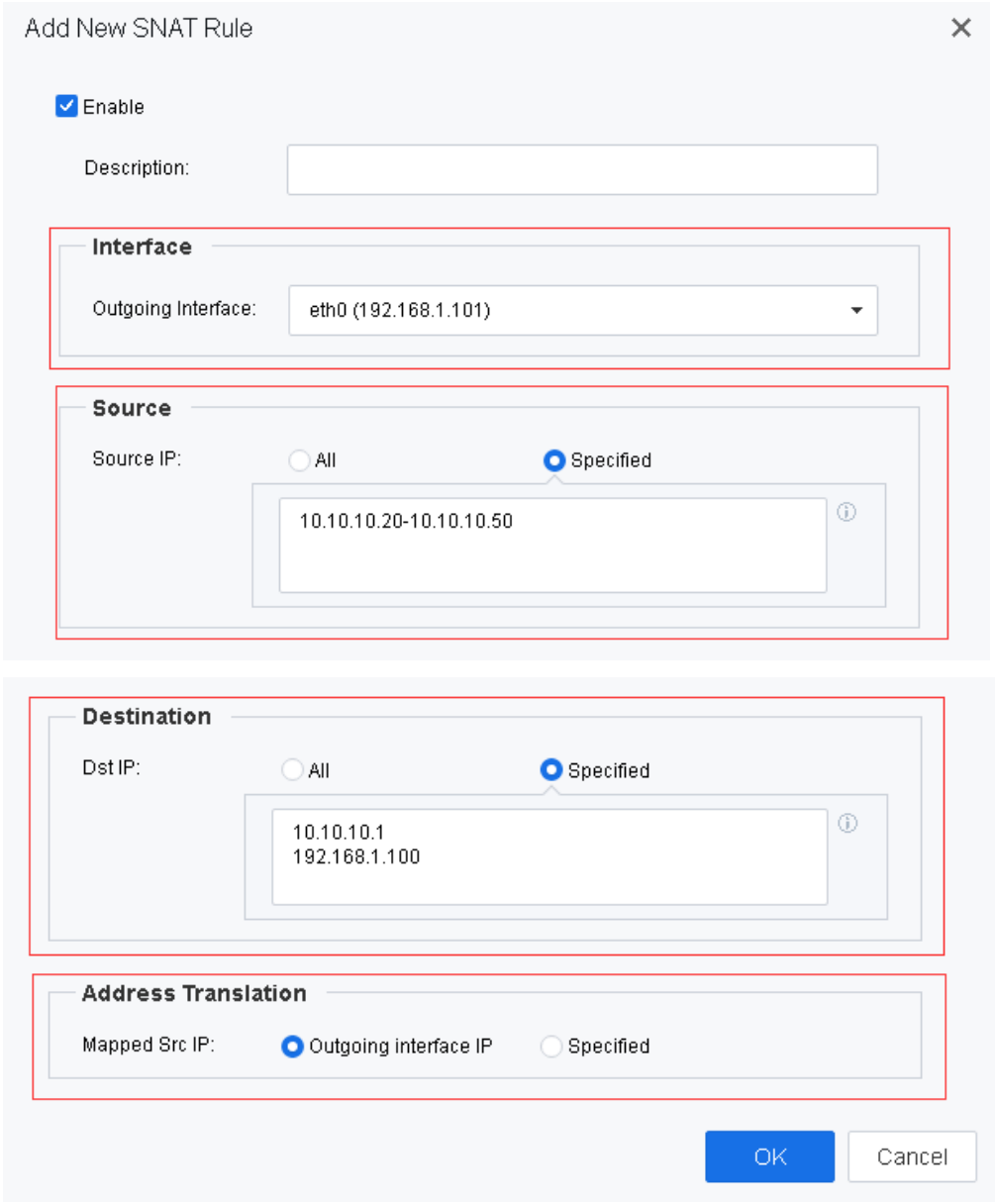
Outgoing Interface: The interface of the Application Center Service Mapping route connects to the management network.

Source IP: The IP in the resilient IP pool of the shared service network.

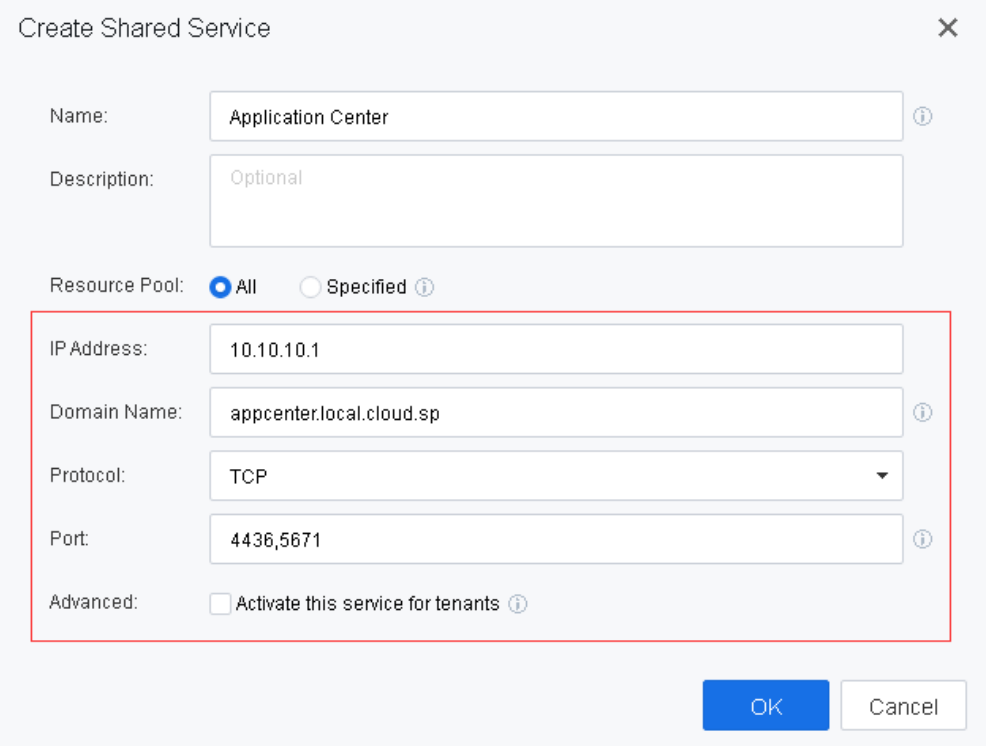
Destination IP: The interface address to which the Application Center Service Mapping router connects to the shared service network and the SCP.

Mapped Source IP: The interface of the Application Center Service Mapping

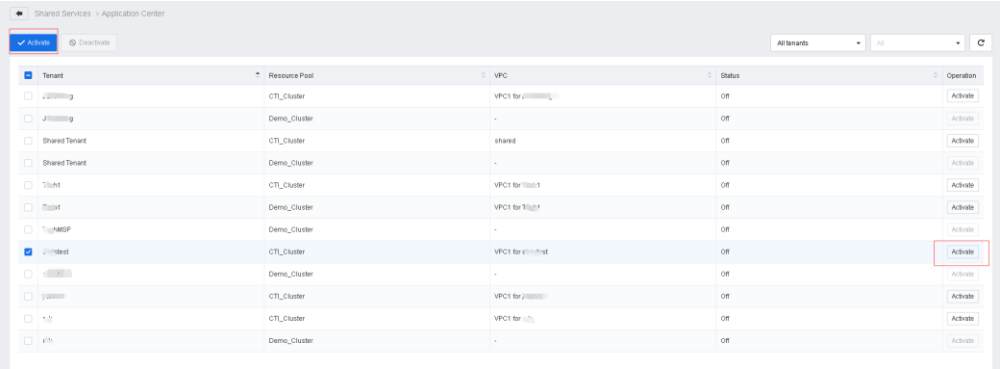
router to the management network.



Step 7. Refer to chapter **3.7 Configure Shared Services Gateway.** Refer to chapter 3.7 Configure Shared Service Network. Create a new application center shared service with the IP address of the application center service mapping router to connect to the shared service. The domain name must be **appcenter.local.cloud.scp** and the ports are TCP 4436 and 5671.



Step 8. Navigate to **Resources > Networking** > **Shared Service Network.** In **Shared Services,** click the created shared services named **Application Center** to enter the overview of tenant shared services to activate the shared services for tenants.



Step 9. **Configuration Verification**: Using a Linux VM on a tenant VPC, verify the domain name resolution using the command **nslookup appcenter.local.cloud.scp**. Besides, verify the application center network using the command **curl https://appcenter.local.cloud.scp:4436/latest/user data kfsSL**. (as shown in the result of verification success).

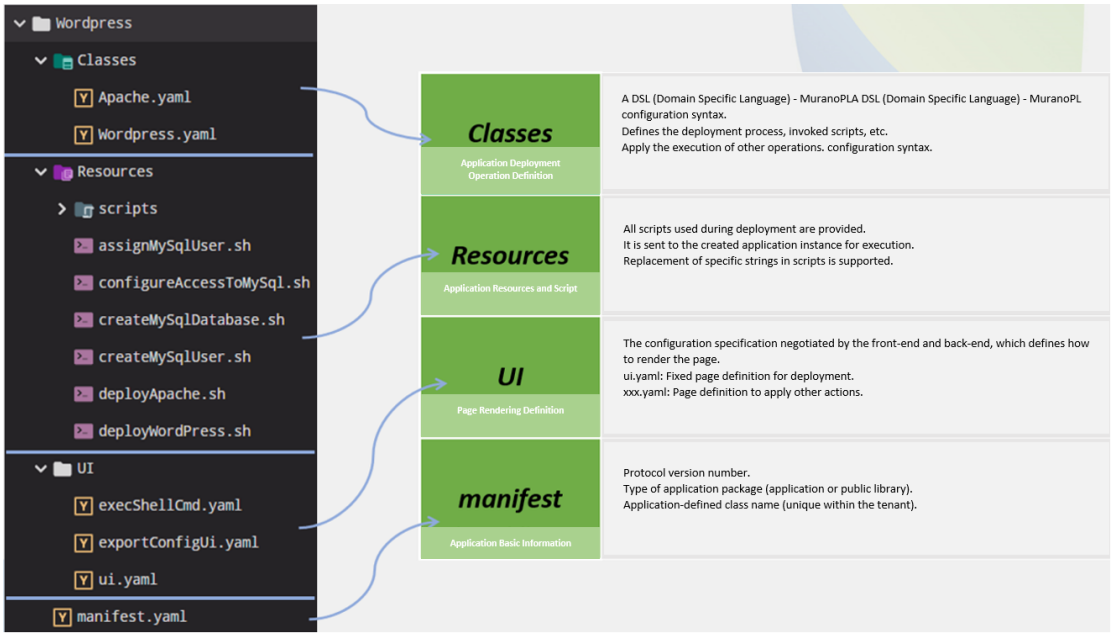
```
[root@localhost ~]# nslookup appcenter.local.cloud.scp
Server:    8.8.8.8
Address 1: 8.8.8.8 dns.google

Name:      appcenter.local.cloud.scp
Address 1:  appcenter.local.cloud.scp
[root@localhost ~]# curl https://appcenter.local.cloud.scp:4436/latest/user-data
 -kfsSL
curl: (22) The requested URL returned error: 404 Not Found
[root@localhost ~]#
```

4.14.1.3 Application Package Import

Features:

The overall structure of the application package is composed of **yaml** definition file and **sh** script file, which is allowed to be self-written and self-define. It is mainly used for configuration guidance when deploying applications.



Precautions:

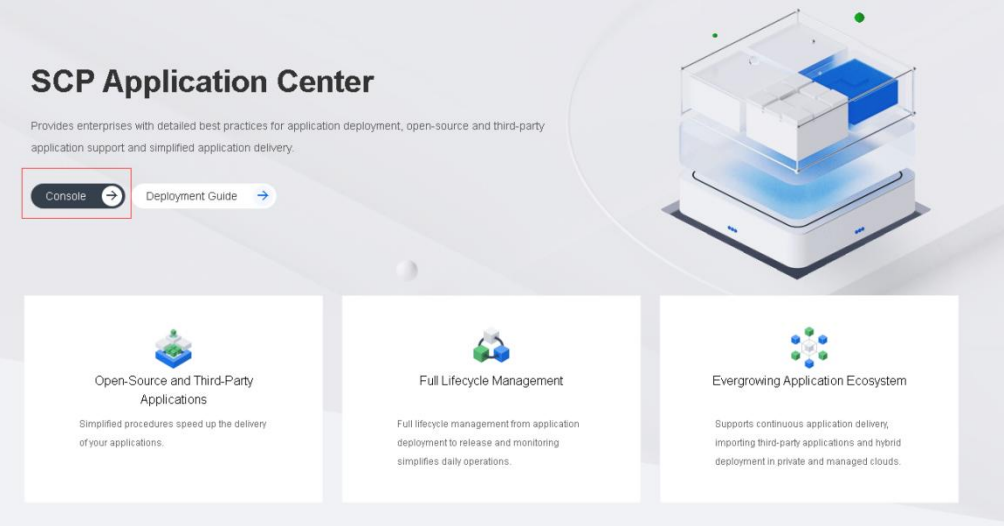
1. Currently doesn't support MSP. Tenants apply for application middleware quota through work orders. (Redis, Kafka, MongoDB, RabbitMQ)
2. The default quota of the middleware is 9999 and is unable to change.
3. After the admin and tenant deploy the application, a virtual machine group prefixed with APP will be automatically generated to distinguish between ordinary virtual machines and application virtual machines.

Prerequisite

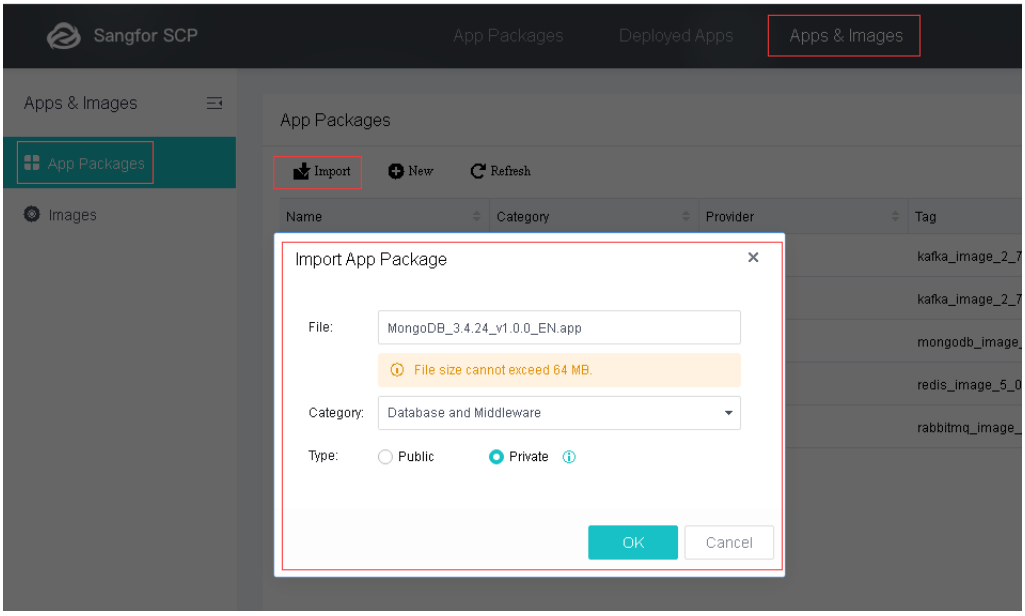
1. The application center has been successfully deployed.
2. The required APP packages have been ready.

Steps

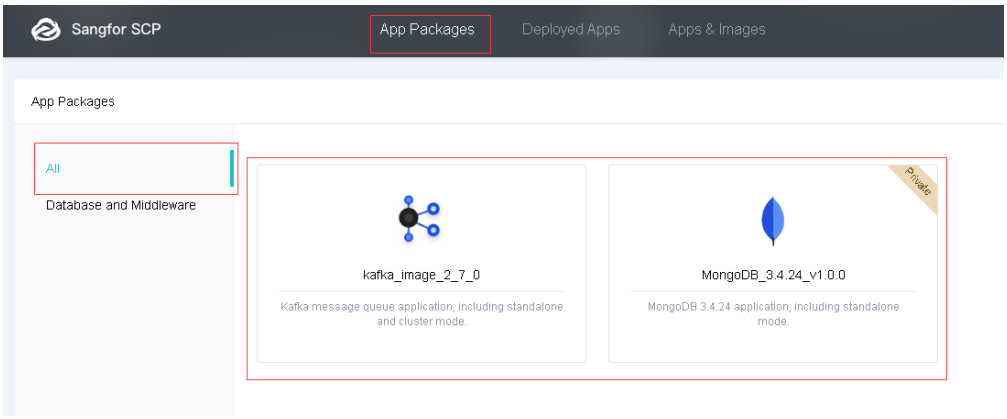
Step 1. Navigate to **Resources > Application Service > Application Center, and** click **Console** to enter the SCP Application Center portal.



Step 2. On the SCP Application Center main page, go to **Apps & Images** and select **App Packages. Then, click Import** to upload the APP package.



Step 3. After uploading the image, go to **App Packages** and look for **All** to view the uploaded components and application tag.



4.14.1.4 Application Image Import

Feature description:

The Sangfor SCP platform requires the corresponding application image to create the application.

Precautions:

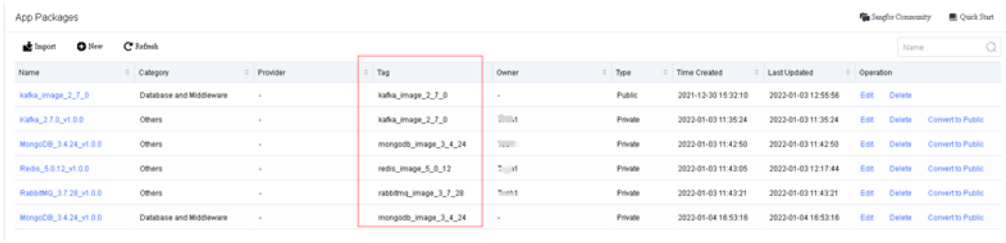
The application tag of the uploaded image must be the same as the tag of the application package. Otherwise, the application cannot be created.

Prerequisite

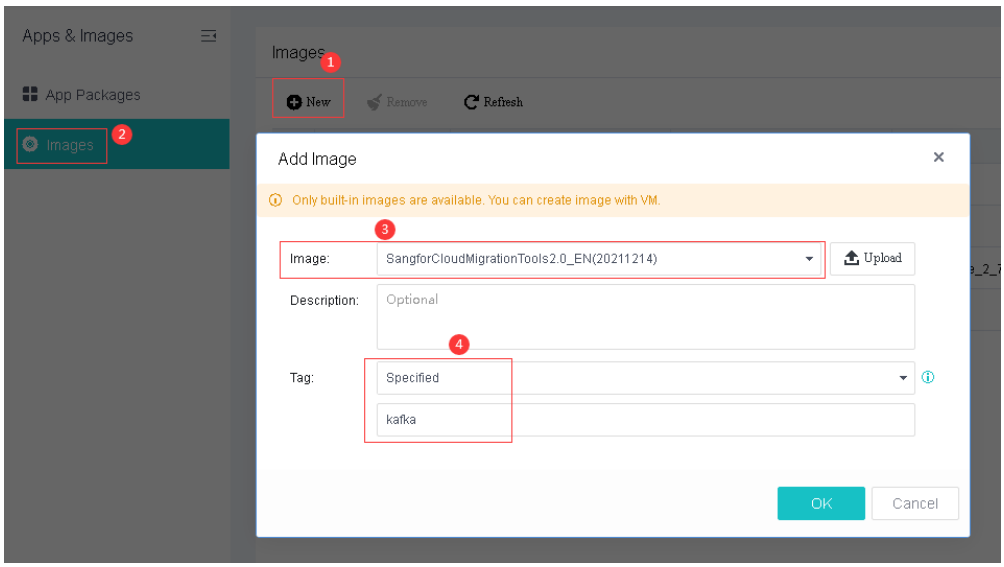
1. The application center has been successfully deployed.
2. The required APP packages have been ready.
3. The application image has been uploaded according to **Chapter 4.2.2 Image Management**.

Steps

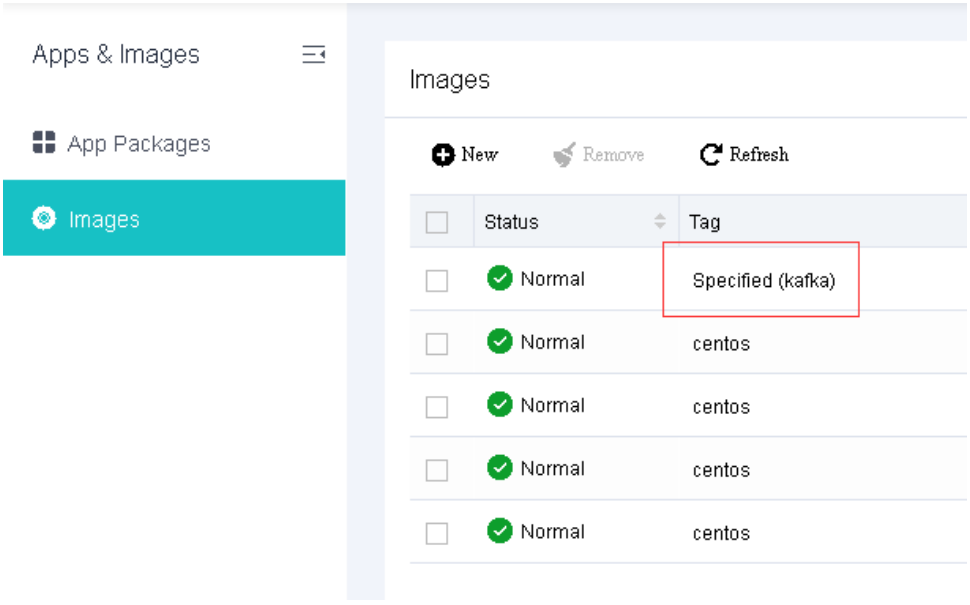
Step 1. Locate the appropriate application tag on the **App Packages** page.



Step 2. In SCP Application Center, go to **App & Images** and select **Images**, click **New** to select the uploaded image, and then manually specify the application tag.



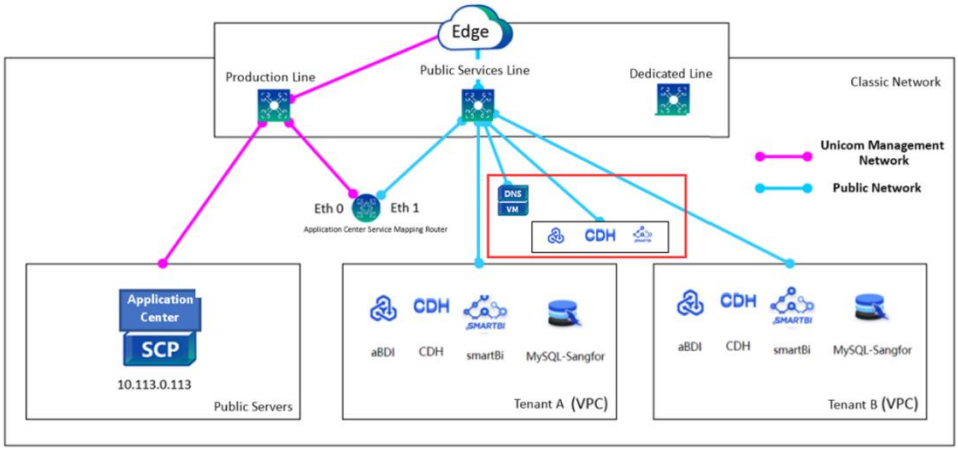
Step 3. Verify that the application tag of the image must be included in the application package's application tag.



4.14.1.5 Classic Web Application Deployment

Feature Description:

When the SCP platform uses the application center to deploy applications in the classic network, a separate DNS server needs to be deployed to resolve the application center address appcenter.local.cloud.scp.



Precautions:

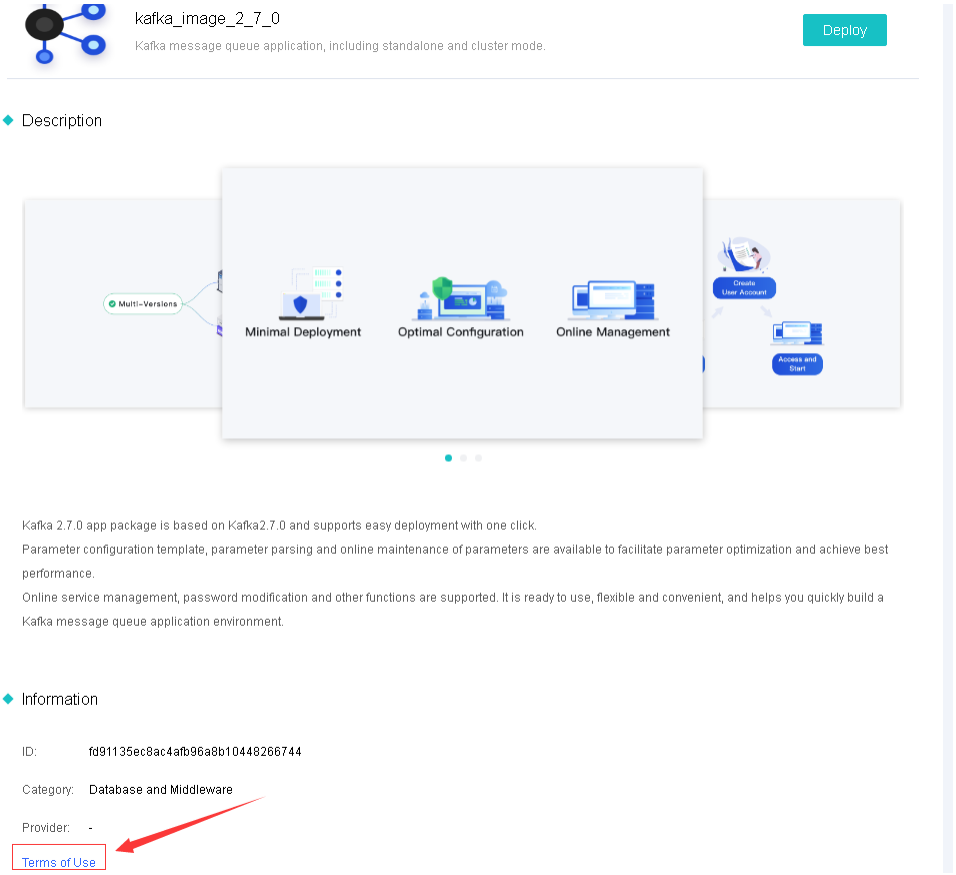
N/A.

Prerequisite

1. The SCP platform has the authorization of the Application Center, and the services have been enabled.
2. The deployment of the shared service network is completed.
3. The corresponding application package and image have been uploaded.
4.

Steps:

Step 2. Click the application's name to be deployed, click **Deploy** to configure the deployment information for the application, or click **View Details,** then click the **Terms Of Use** located at the bottom left to view the corresponding deployment document.



4.14.1.6 VPC Application Deployment

Features:

The application center supports rapid deployment in the application development, testing, operation and maintenance scenarios, and future routine operation and maintenance management.

Precautions:

None.

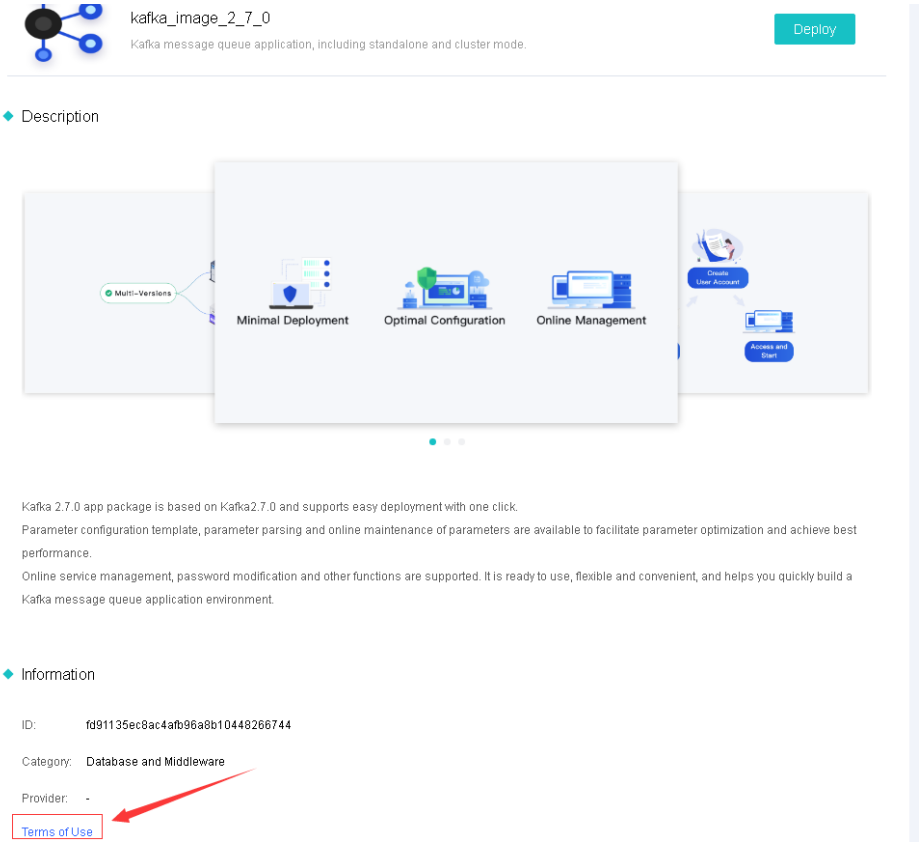
Prerequisite

1. SCP platform has the authorization of the **Application Center,** and the service has been enabled.
2. The deployment of the shared service network is completed.
3. The corresponding application packages and images have been uploaded.
5.

Steps

Step 1. Click the application's name to be deployed, click **Deploy** to configure

the deployment information for the application, or click **View Details**, then click the **Terms Of Use** located at the bottom left to view the corresponding deployment document.



4.14.1.7 Application Package Upgrade

Function Description:

Sangfor SCP can upgrade the application package so that the application instance can obtain the latest functions.

Precautions:

None.

Prerequisite

The latest version of the application package has been obtained.

Steps:

Step 1. Refer to the **Chapter 4.12.1.4 Application Image Import** to import the new version of the application package.

Step 2. After importing the new version of the application package, the

version column of the existing application instance of the platform will display the word **upgradeable**, and the **Details** button can view the details of the new features of the version. Click the **Upgrade** button above to upgrade the existing application instance.

4.15 Chinese/English language switch

Function Description:

Sangfor SCP supports Chinese/English language switching to meet the scenarios of operation and maintenance personnel using different languages to manage the platform.

Precautions:

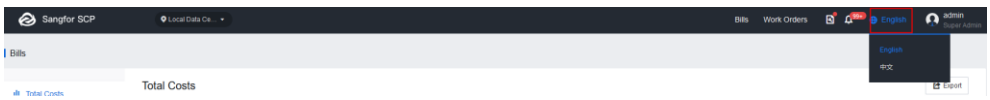
1. SCP 6.8.0 and above support Chinese/English switching but do not support region switching for the time being.
2. NFV, aSEC, and VDC do not support language switching. Please use the corresponding component package of the overseas version.
3. User-defined content, such as virtual machine name/description, network device name/description, etc., does not support switching.
4. Support single-user-level language switching. In the Multi-users scenario, users have to switch the language by themselves.

Prerequisite

None.

Steps:

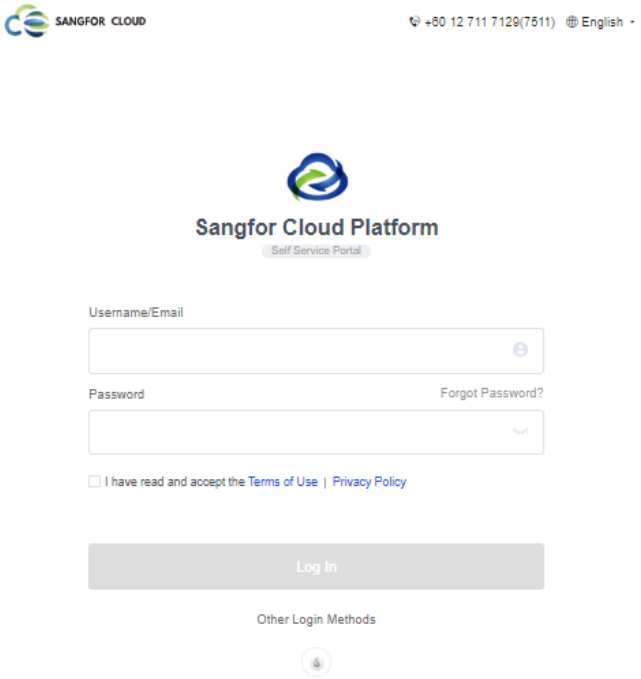
In the upper right corner of the interface, click the language button to switch between Chinese and English.



5 Tenant User Guide

5.1 Login Method

The login IP address of the tenant portal is https://SCP IP (no 4430 port number



is required), and you can log in to the tenant portal by entering the tenant account username and password.

If you forget your tenant password, click **Forgot Password** for password recovery. Password recovery will go through the email address associated with the tenant account.

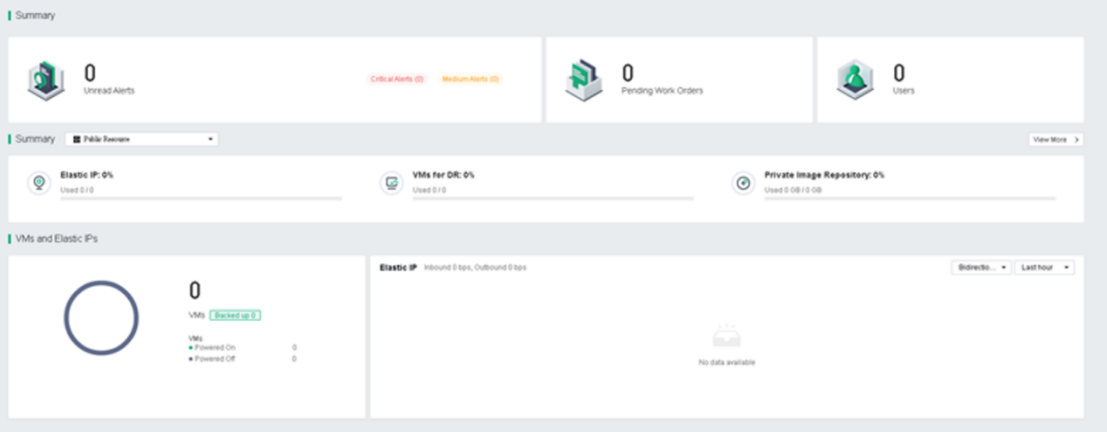
5.2 Overview

Features Description:

The newly designed tenant homepage provides an overview, tenant resource overview, virtual machine, and elastic IP. It supports tenants' shortcut alerts viewing, pending orders, sub-accounts, virtual machine operating status, elastic IP, and other information and provides tenants with access to various services.

This interface is the home page of the tenant after logging into the console. It is

mainly used to display the current alert information, work order information, sub-account information, resource usage, virtual machine status, and the current account's elastic IP flow rate chart. Complete user interface as below image shown.



5.3 Compute

5.3.1 Virtual Machine

The virtual machine is one of the essential modules of Sangfor SCP to deliver services. Tenants can manage the validity of the virtual machine.

5.3.1.1 Create / Delete Virtual Machine

Features:

Guide tenants to create and delete virtual machines.

Precautions:

N/A.

Prerequisite

1. The tenant has uploaded or made the required image to create the virtual machine.
2. The tenant has a sufficient resource quota to create a virtual machine.

Steps:

Step 1. In the tenant portal, navigate to **Compute > Virtual Machine. Click New** to create virtual machine.

Step 2. Select the **Resource Pool** and **Image** for the virtual machine.

Step 3. Configure the **Number of Virtual Machines**, **Compute**, **Storage**, **Networking,** and other parameters according to actual requirements, then click **Next**. Parameters configuration can refer to chapter **4.1.5.1 Create Virtual Machine**.

Step 4. Fill up the **Virtual Machine's name**, **Description**, **Group**, **administrator's password**, **Hostname,** and **Expiration Date** according to actual requirements, then click **Next**.

Step 5. After confirming the information, click **OK** to start creating the virtual machine.

Step 6. After creating the virtual machine, you can click the **Console** to enter the virtual machine, or click **More** to **Shut Down**, **Suspend**, **Restart**, **Power Off**, and **Bind Key Pair**, **Snapshots/Backups Management**, **Clone**, **Create Image**, **Export**, **Delete,** and other operations.

5.3.1.2 Virtual Machine Validity

Features:

The SCP platform supports setting an expiration date for the virtual machines, and virtual machines that exceed the service validity will generate alert messages.

Precautions:

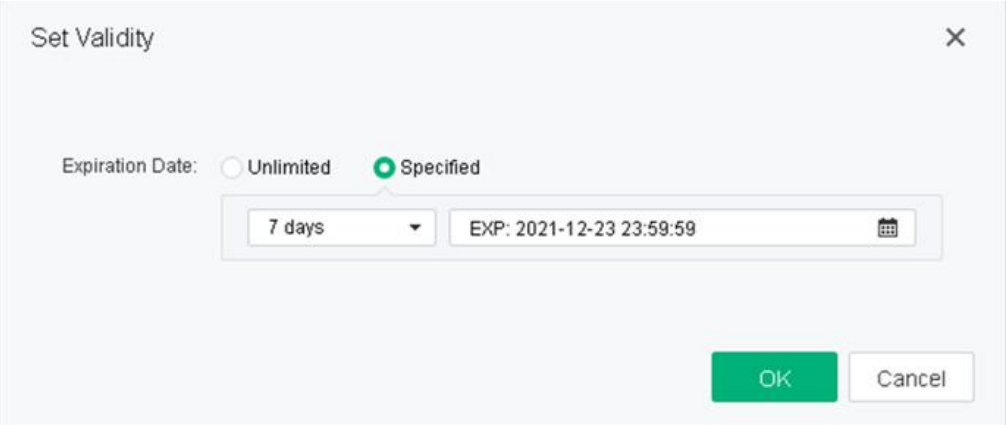
1. The expiration date of the virtual machine is in days units, and the minimum granularity of the expiration date is set to days.
2. A cloned virtual machine from the virtual machine with an expiration date the validity of the cloned virtual machine is unlimited.
3. It only supports the setting of the expiration date for the HCI virtual machine and does not support the setting of the expiration date for the VMware virtual machine.
4. The virtual machine is about to expire or has expired. It will not affect any operation of the virtual machine. Only a new alert log about to expire/expired will be added, and the virtual machine's status will be stated as a warning.

Prerequisite

N/A.

Steps:

Login to the SCP, navigate to **Compute** > **Virtual Machine, select** the particular virtual machine, click **More,** look for **Set Validity, change** the **Expiration Date** from **Unlimited** to **Specified,** and set the expiration date of the virtual machine.

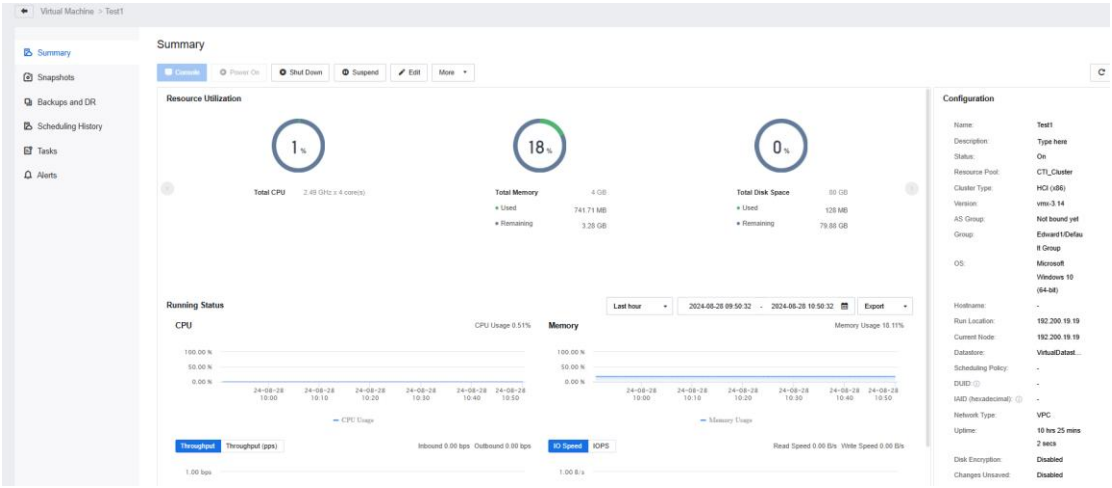


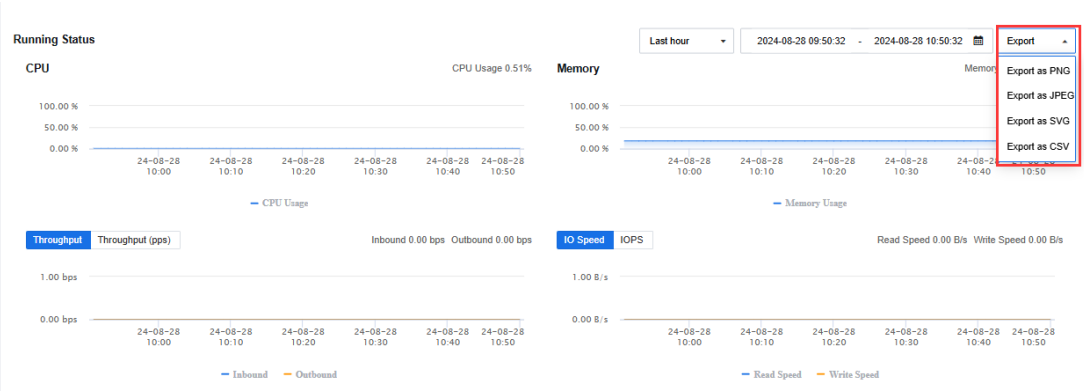
5.3.1.3 View Virtual Machine Summary

Features:

Click the corresponding virtual machine name redirecting to the virtual machine summary interface. This interface provides multiple functions such as reviewing virtual machine information, snapshots, backups, operation audits, Alerts, consoles, etc.

SCP displays all VMs in the VM list and supports displaying their tenants, **Guest OS**, **resource usage**, **Run Location**, **hostname**, **Scheduling Policy**, **Tags**, **CPU Clock Speed**, **Datastore**, **Storage Policy**, **Logical Space Used**, **Used Memory**, and **Uptime**.





5.3.1.4 Export Virtual Machine

Features:

This feature supports exporting VMs as OVA, VMA, OVF, MF, or VMDK files. When exporting the list, you can choose to include **Run Location**, **hostname**, **Scheduling Policy**, **Tags**, **CPU Clock Speed**, **Datastore**, **Storage Policy**, **Logical Space Used**, **Used Memory**, **Uptime**, and **Scheduled Policy**.

Precautions:

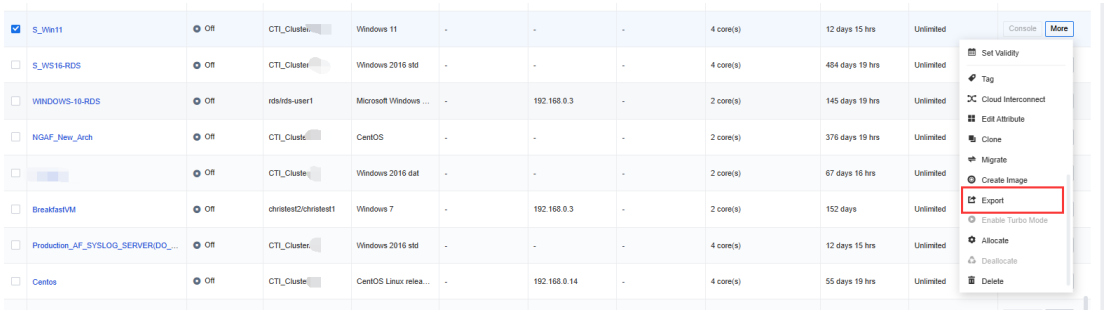
None.

Prerequisite:

The VM has been shut down.

Steps:

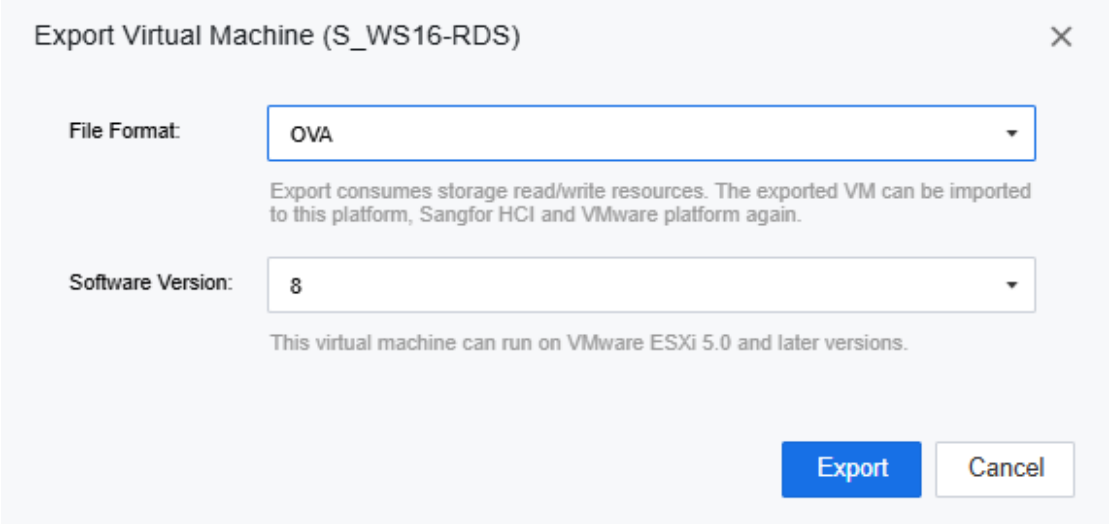
Step 1. Log in to SCP, go to **Resources** > **Compute** > **Virtual Machines**, click **More** of the VM to be exported, and then click **Export**.



Step 2. Select **OVA**, **VMA**, or **OVF, MF, VMDK** for **File Format**, and click **Export**.

NOTICE

If you select **VMA** for **File Format**, you can export the VM directly by clicking **Export**. if you select **OVA**, you need to select a VMware Workstation version for **Software Version** before exporting the VM.



Step 3. Wait for the VM to generate the export file and download it.

5.3.1.5 Virtual Machine Snapshots

Features:

This section instructs tenants to create VM snapshots, with the snapshot types of disk based snapshots and storage based snapshots.

In SCP 6.10.0 and higher, **Disk Based Snapshot** of **Snapshot Type** is changed to **External Disk Based Snapshot** with support for configuring **Merging Speed for External Snapshot Deletion**. As compared to internal disk based snapshots, external disk based snapshots release space after being deleted,

which eliminates the impact of snapshots on the VM performance.

Precautions:

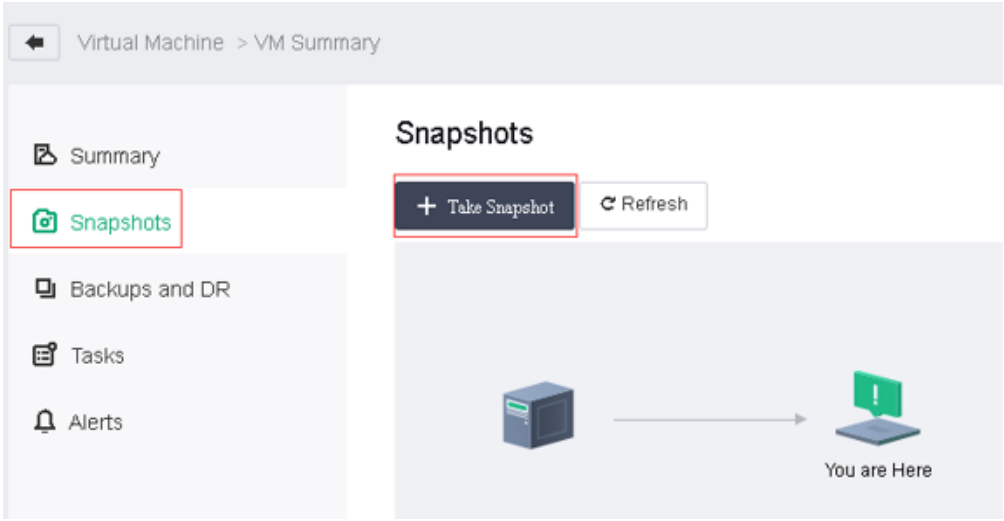
1. Snapshots are often used in scenarios where original data needs to be protected before virtual machine patches or upgrades, software updates, and other high-risk operations. If data backup is required, it is recommended to use the backup function.
2. Supports tenant users to create VM snapshots and recover VMs from snapshots.
3. A VM cannot have an external snapshot and an internal snapshot at the same time, nor a storage based snapshot and a disk based snapshot at the same time.
4. Snapshots created for VMs with internal snapshots on SCP 6.10.0 upgraded from a lower version are internal snapshots by default.
5. Disk based snapshots created for newly created VMs or VMs without snapshots are external snapshots by default.
6. It is not supported to delete snapshots outside fork points. Each snapshot contains incremental changes to the basic disk, and if snapshots outside the fork points are deleted, multiple snapshot chains and a large amount of data will be merged, which has a negative impact on system performance.
7. External snapshot deletion takes more time than internal snapshot deletion. External snapshots contain incremental changes to basic disks as well as related index information, and when deleting an external snapshot, these incremental changes are merged into the basic disks to recover the VM to the state when the snapshot was deleted, which can be very time-consuming.

Prerequisite

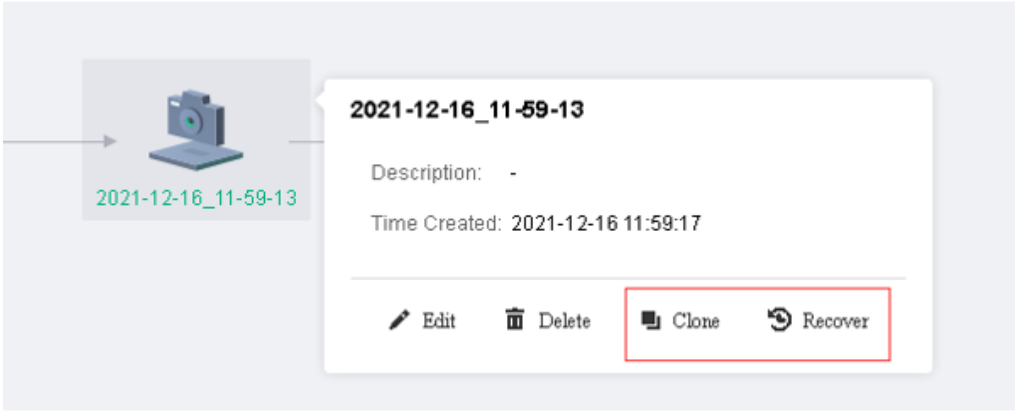
N/A.

Steps:

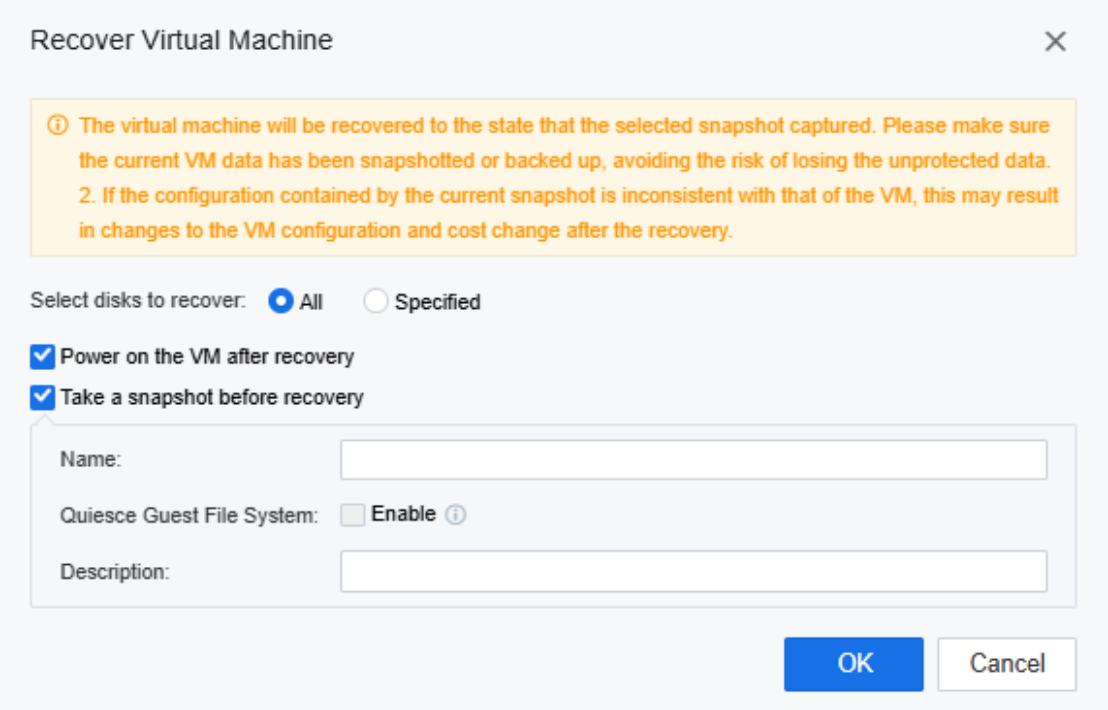
Step 1. In the virtual machine summary, select **Snapshots**, and click the **Take Snapshot** button to create a snapshot of the current virtual machine.



Step 2. After creating a snapshot, you can use the snapshot to recover the virtual machine or clone a new virtual machine.



Step 4. Select **All disks** or **Some disks** to recover the VM from the snapshot.



5.3.1.6 Virtual Machine Backup

Features:

Tenants can perform backup operations on the virtual machine to protect data.

Precautions:

N/A.

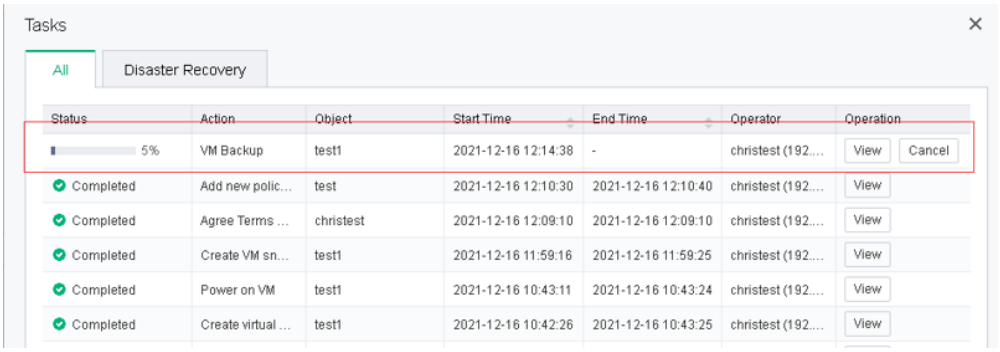
Prerequisite

The tenant has a sufficient backup repository quota.

Steps:

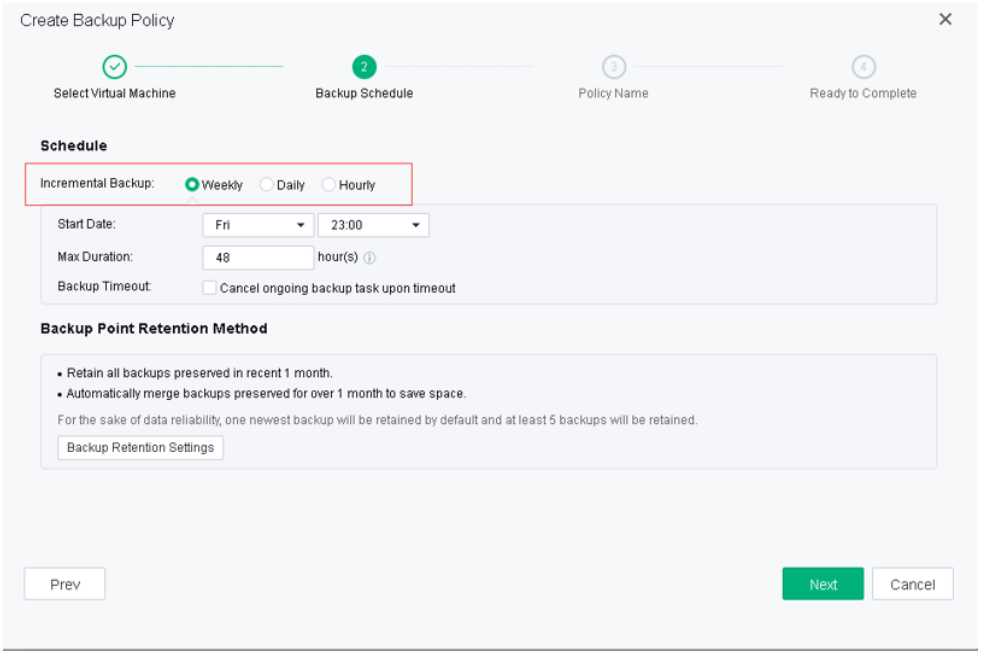
Step 1.

Manual Backup: In the virtual machine summary, select **Backups and DR**, and click the **Backup** button to back up the current virtual machine. A tenant can monitor the backup progress in the task list.



Step 2.

Auto Backup: In the virtual machine summary, select **Backup and DR**, click the **Setting** button, add a **Scheduled Backup** policy, and click **Create Backup Policy.** You can adjust the backup schedule according to the requirements and follow the steps to associate the virtual machine with policy.



5.3.1.7 Browse Files

Feature Description:

When files in the virtual machine are deleted or damaged by mistake, the tenants can recover important files of the virtual machine through the backed-up files, and file recovery is supported for Windows and Linux operating systems.

Precautions:

1. The HCI cluster managed by SCP supports a limited number of file recovery

sessions, and each node supports a maximum of 3 sessions. For example, a 3-node HCI cluster supports up to 9 sessions at the same time.

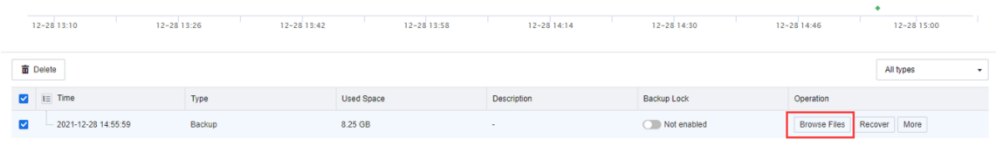
2. Currently, file recovery only supports Windows NTFS, FAT32 file system format, and Linux system ext2, ext3, ext4, xfs file format.
3. The browse of files containing special characters, such as (!@#$%^&*), is not supported.
4. It doesn't support the browsing of file sizes bigger than 5GB.
5. When the backup of the virtual machine is stored in sffs, the soft connection file of the virtual machine is linked to /proc, and file download is not supported in the /run directory.

Prerequisite

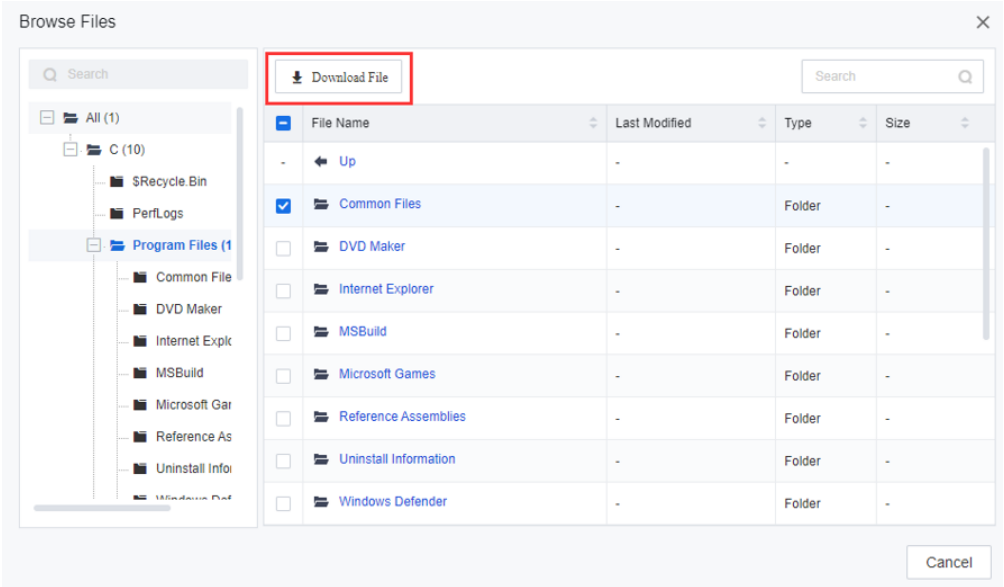
The virtual machine has backup files that exist already.

Steps:

Step 1. Go to the virtual machine summary, select **Backup and DR,** then click **Browse Files**.



Step 2. Select the files to be recovered, then click **Download File** for file recovery.



5.3.2 Image

Features:

Guide tenants to upload or create private VM images.

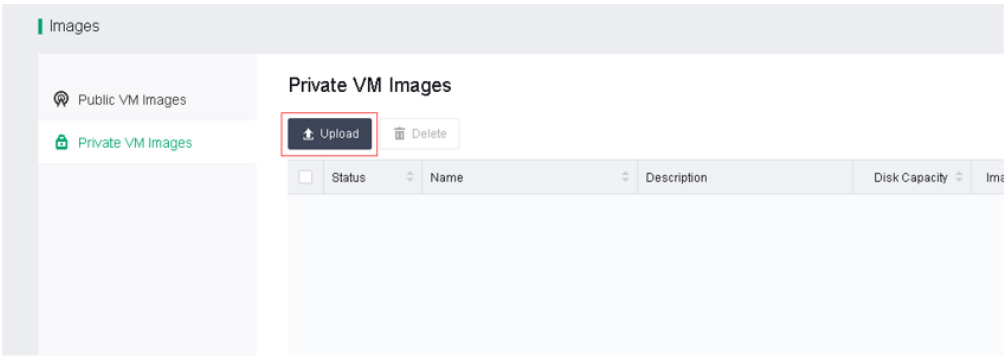
Precautions:

Tenants have sufficient private VM image repository quota.

Steps

Step 1. Upload an ISO image.

- Go to https://SCP IP, log in tenant account, select **Image,** select **Private VM Images,** then click **Upload**.



- Select the local image file (ISO), Operating System, Resource Pool, and then click **Upload**.
- After the upload is complete, click the **Finish** button to continue uploading or click the **Close** button.

Step 2. Make Built-in Image

- Go to https://SCP IP, log in to the tenant account, navigate to **Compute,** and then select **Virtual Machine. Next, select** the virtual machine that has vmTools installed.
- Click **More**, select **Edit**. It is recommended to enable CPU hot add and memory hot add in **Advanced**.
- Click **More**, select **Create Image,** then fill up the name of the image and description. Then, select the type of operating system and the resource pool, and click **OK** to begin the image creation.

5.4 Networking

5.4.1 Network Topology

Features:

The brand-new designed tenant network topology interface displays the virtual machine, subnet information, virtual network equipment, and other information the tenant uses in a graphical form. What you draw is what you get. What you draw is what you get.

Tenants can use the Virtual Private Cloud (VPC) network. Within the network topology, the environment can be constructed according to the actual needs. Including binding elastic IP, adding subnets, the basic configuration of VPC, and deployment of NFV equipment.

Tenants can use the classic network. The deployed virtual machine can directly communicate with the local data center in the classic network.

Precautions:

1. In the VPC, the vNGAF remains inactivated by default. The quota is required for activation.
2. In the VPC, the router is enabled by default, and all virtual machines of the tenant will communicate with outside through the router.
3. In the VPC, all devices are not bound to an elastic IP by default.
4. Tenant classic network does not support tenants to create NFV devices by themselves. If necessary, please contact admin to create and deploy.

5.4.1.1 Virtual Machine Operation

Features:

The supported virtual machine shortcut operations in the network topology, as below:

1. Create a virtual machine.
2. Check the virtual machine console.
3. Perform operations such as powering off, restarting, binding/unbinding elastic IP, and cloning towards the virtual machines in the powered-on state.

4. Perform operations such as subnet configuration, multiple network card configuration, hard disk mounting and deletion, virtual machine editing, deleting, mirroring, exporting, etc., for the virtual machines in the shutdown state.

5.4.1.2 Subnet Management

Features:

Tenants can create a subnet for virtual machine. The subnet in HCI corresponds to a network divided by an allocated switch under the VPC internal router. Tenant users can deploy virtual machines and NFV devices under the subnet.

Precautions:

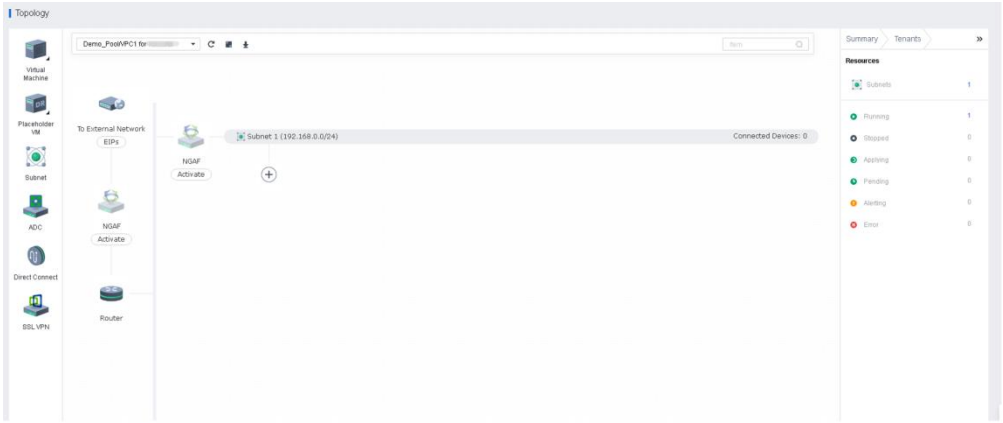
N/A.

Prerequisite

N/A.

Steps:

Step 1. Login tenant account from https://SCP IP, and navigate to **Network > Topology** to enter the tenant's network topology.



Step 2. Click the **Virtual Machine** on the leftmost to add the virtual machine that has not been added to the network to a particular subnet by drag and drop.

Step 3. Drag the **Subnet** icon on the left to create a subnet. The current version supports the creation of subnet 192.168.xx, 10.0-253.xx, and 172.16-

28.xx network segments. If you need to create other network segment subnets, please contact Sangfor Technical Support.

5.4.1.3 Port Mapping Configuration

Features:

After the router is bound to the public IP, it can be used for port mapping. (port mapping refers to mapping a port of the IP address of the external network to a machine in the internal network to provide corresponding services.)

Let's take a case as an example to explain how to configure the port mapping function: map the router's elastic IP address TCP 80 port to the virtual machine port 80.

Precautions:

N/A.

Prerequisite

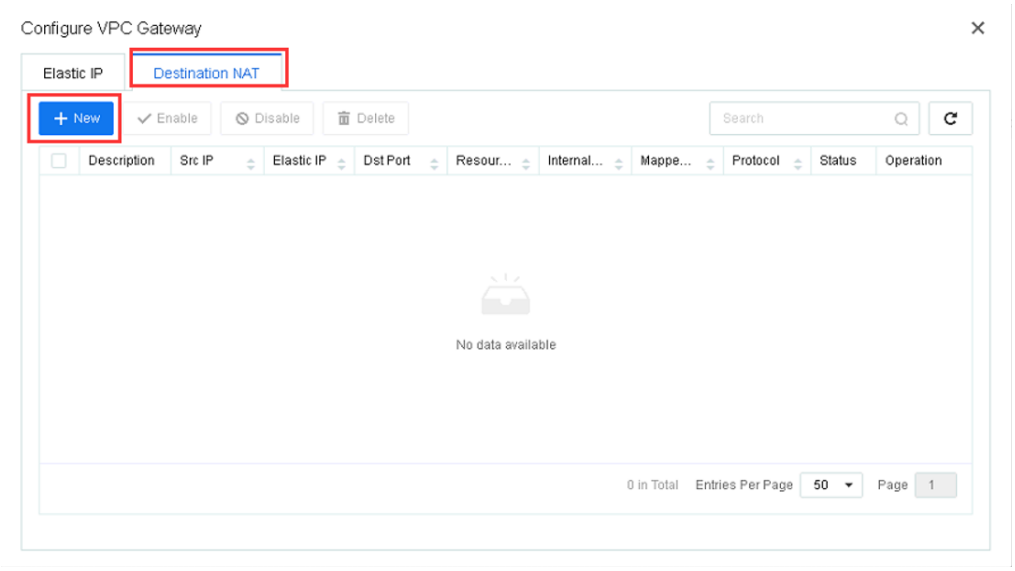
N/A.

Steps:

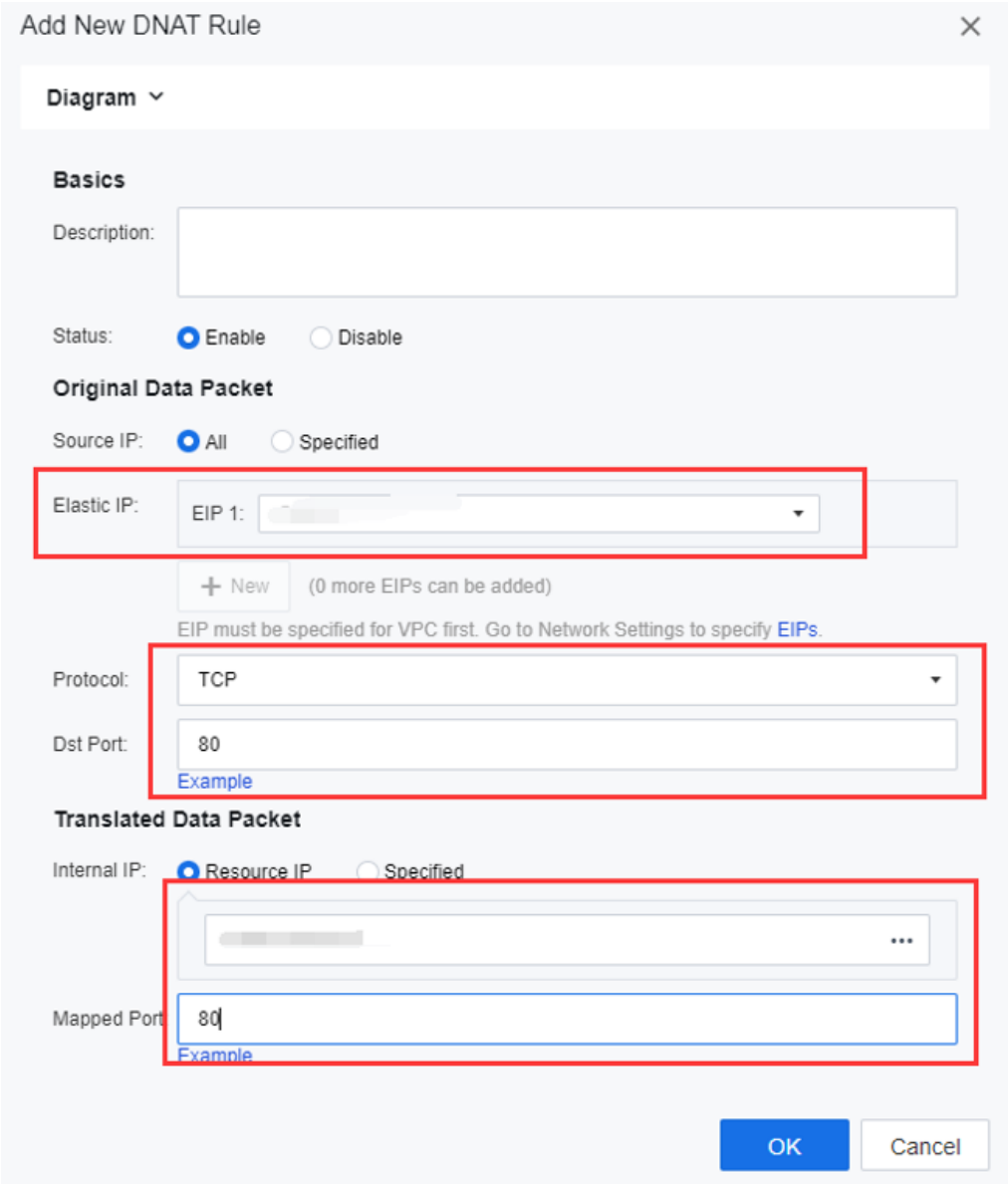
Step 1. Point and click the cursor on the **To External Network** and click on the **Settings** located in the lower right corner.



Step 2. Select the **Destination NAT** feature and click the **New** button.



Step 3. According to the actual situation, configure the **Original Data Package** information and the **Translated Data Package** information as follows.



5.4.2 IP And Bandwidth

5.4.2.1 Elastic IP

Features

Elastic IP is an independent Public IP resource, which can be bound to the virtual machine, routers, ADC, SSL VPN, and other devices of the VPC. It can be dynamically unbound to achieve the decoupling of public IP and these devices, meeting the requirements of flexible management and dynamic provisioning.

Precautions:

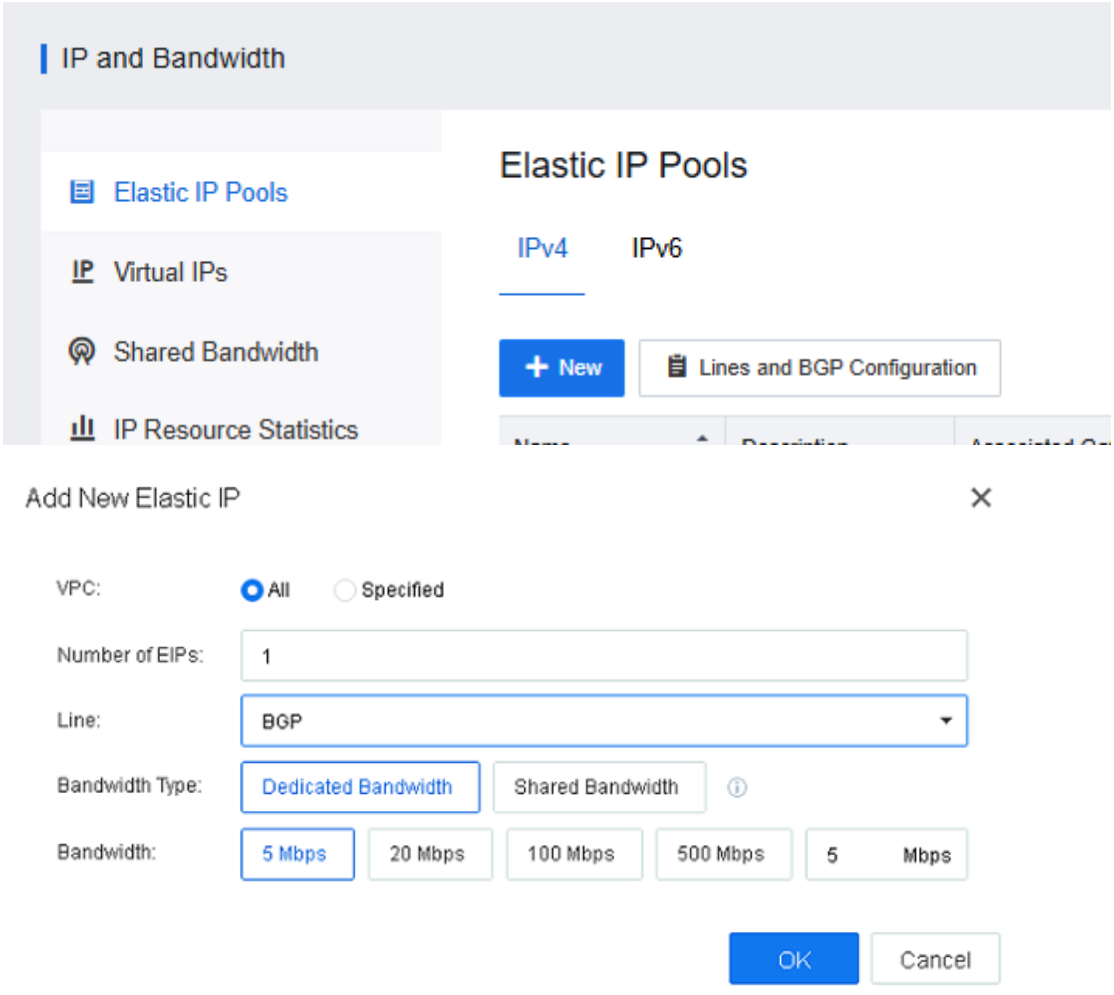
SCP Version 6.7.0 and below, the elastic IP is associated with the resource pool. SCP version 6.7.0 and above, the elastic IP is associated with VPC.

Prerequisite

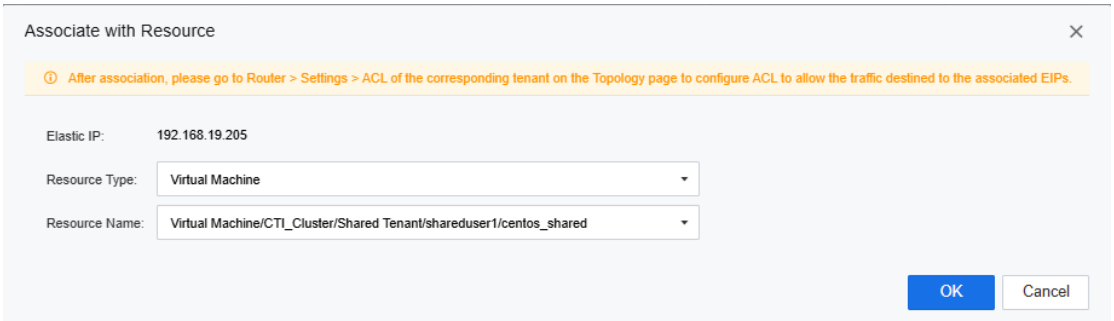
Tenants have sufficient elastic IP resources.

Steps:

Step 1. Navigate to Networking > IP and Bandwidth, click the New button, select All or Specified the VPC, fill in the Number of IPs, select the type of Line, and the Bandwidth Type can select either Dedicated Bandwidth or Shared Bandwidth. When selecting Shared Bandwidth, you can use the existing shared bandwidth or create a new shared bandwidth. Note: SCP 6.10.0 supports IPv6 elastic IP pools.



Step 2. Click **Associate** or **Disassociate** of elastic IP addresses to associate them with or disassociate them from virtual IP addresses in the same resource pools for tenants.



5.4.2.2 Shared Bandwidth

Features:

Dedicated bandwidth means that a single elastic IP uses the allocated bandwidth and does not affect other elastic IPs. Shared bandwidth can be shared by multiple elastic IPs. For instance, three elastic IPs can share a total bandwidth of 10 Mbps. Therefore, the total bandwidth available for these three elastic IPs is 10Mbps.

Tenants can create a shared bandwidth and associate it with an elastic IP. After the association, the elastic IP can use the same bandwidth together.

Precautions:

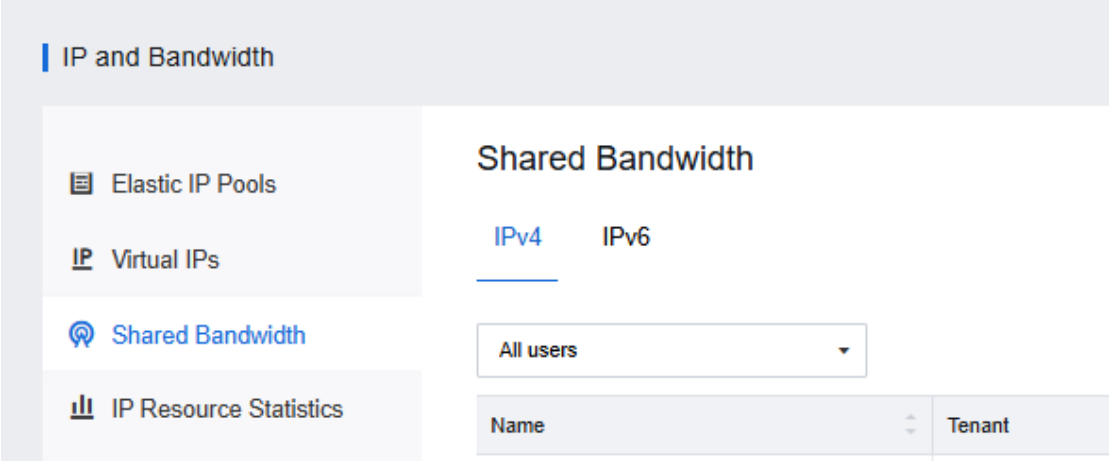
1. After the shared bandwidth is associated with an elastic IP, the elastic IP must be deleted before the shared bandwidth can be deleted.
2. SCP version 6.7.0 and above, since the elastic IP is associated with the VPC. Therefore, only the dedicated bandwidth elastic IP associated with the corresponding VPC can be converted to shared bandwidth.

Precautions:

N/A.

Steps:

Navigate to **Networking** > **IP and Bandwidth**, select the **Shared Bandwidth**, click the **New** button, enter the **Name** of the shared bandwidth, select the appropriate **VPC and Line**, set the **Bandwidth**, and lastly, associate with the **Existing EIPs**, **New** or **Associate Later** manually. Note: SCP 6.10.0 supports IPv6 shared bandwidth.



5.4.3 Network Deployment

5.4.3.1 VPC

Features:

Virtual Private Cloud (VPC) is a virtual private cloud to build an isolated virtual network environment that tenants can configure and manage independently, improve the security of resources in the user's enterprise cloud, and simplify the network deployment. Virtual Private Cloud provides tenants with a completely logically isolated private network. Tenants can also add subnets, access control, port mapping, deployment of NFV equipment, and other network and maintenance operations in the VPC.

1. Subnet Management

Features:

Tenants can create subnets for virtual machines. The subnet in HCI corresponds to a network divided by an allocated switch under the VPC internal router. Tenant users can deploy virtual machines and NFV devices under the subnet.

Precautions

1. Subnet supports DHCP by default. The IP address and DNS will be configured automatically.
2. Under a VPC, a maximum of 20 subnets can be configured by default. If you

need to use more subnets, please contact Sangfor Technical Support (a maximum of 128 subnets are supported).

3. DHCP is enabled by default for VPC subnets. All subnets under the same VPC are intercommunicable with Layer 3. If isolation is required, may use access control.
4. Under different VPCs, subnets are not intercommunicable.

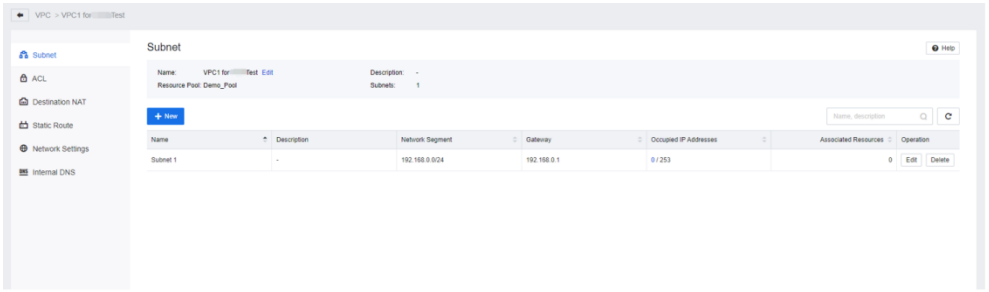
Prerequisite

N/A.

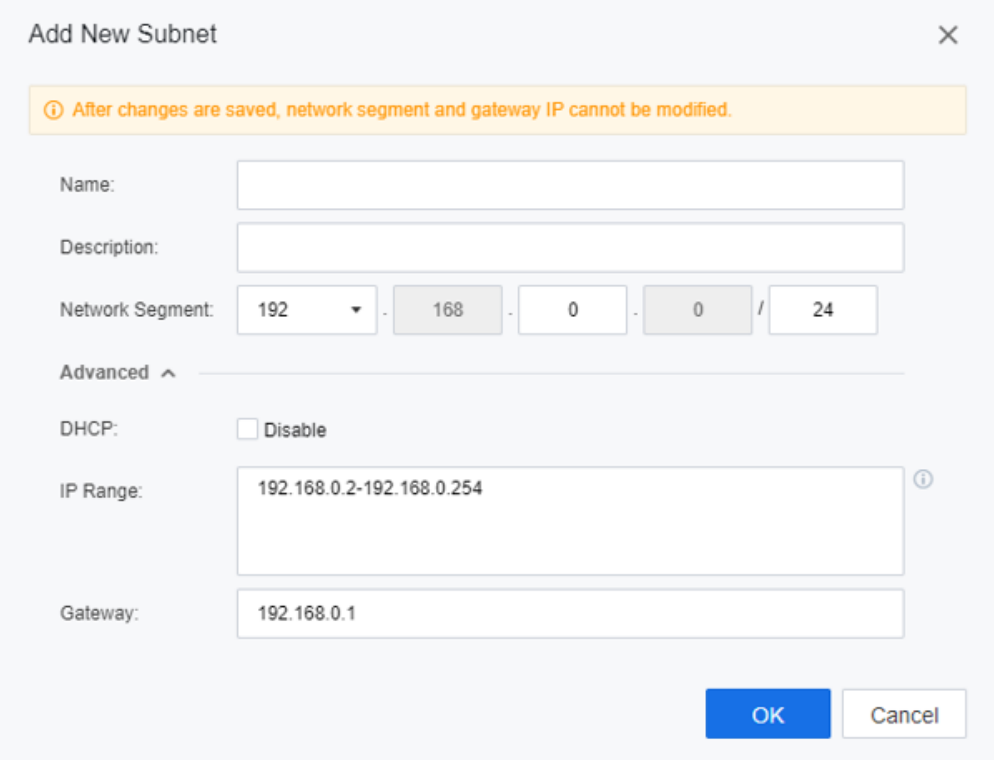
Steps

Step 1. Login tenant account from https://SCP IP, navigate to **Networking** > **Network Deployment** to enter the **VPC** management interface.

Step 2. Click the VPC name to enter the **Subnet** interface to view and manage subnet information. You can create, delete, and edit subnets.

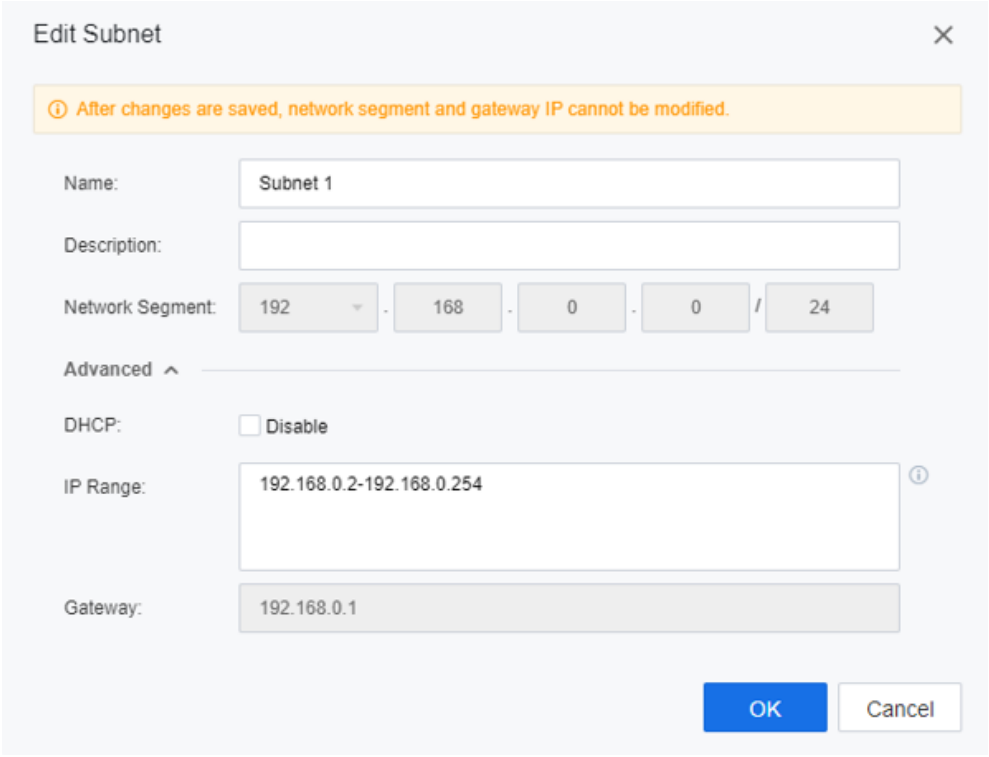


Step 3. Click **New** to create a new subnet, and insert the **Name**, **Description**, **Network Segment**, **IP Range,** and **Gateway**.



Step 4. Click **OK** to complete the subnet creation.

Step 5. When editing a subnet, you can only edit the **subnet's Name and IP Range, not the subnet's Gateway and Network Segmen**t.



2. Access Control List (ACL)

Features:

Access control is the prime countermeasure for network security prevention and protection. By setting the access control list, access control between the cloud intranet and the external network can be achieved.

The access control list consists of the following parts: source/destination IP address, service type, and control action.

- Set the permissions of the cloud intranet to access the external network.
- Set the permissions for the external network to access the cloud intranet.
- Set the mutual access permissions between different network segments in the cloud network.

Precautions:

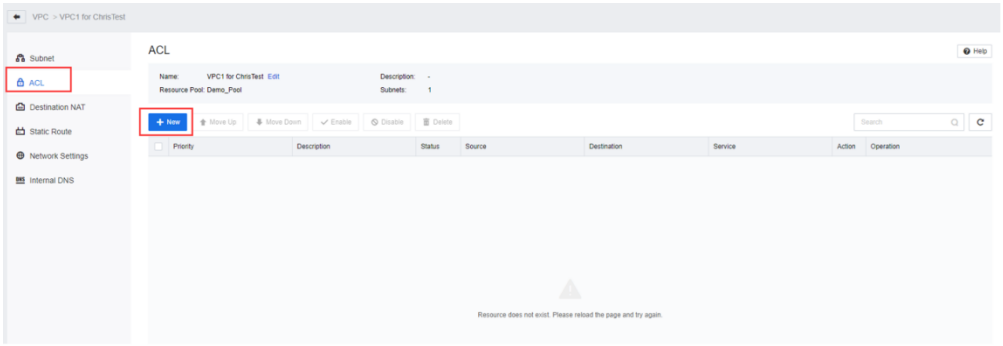
1. The service type can specify the built-in service of the system or customize the service, supporting TCP/UDP/ICMP/other protocols.
2. The action of access control includes **Allow Access** and **Deny Access**.
3. By default, an access control list is allowed for all-access, which means no restriction. Access control list matching order:
4. The access control list is matched from top to bottom. The newly added policy is matched first and placed at the top of the access control list.

Prerequisite

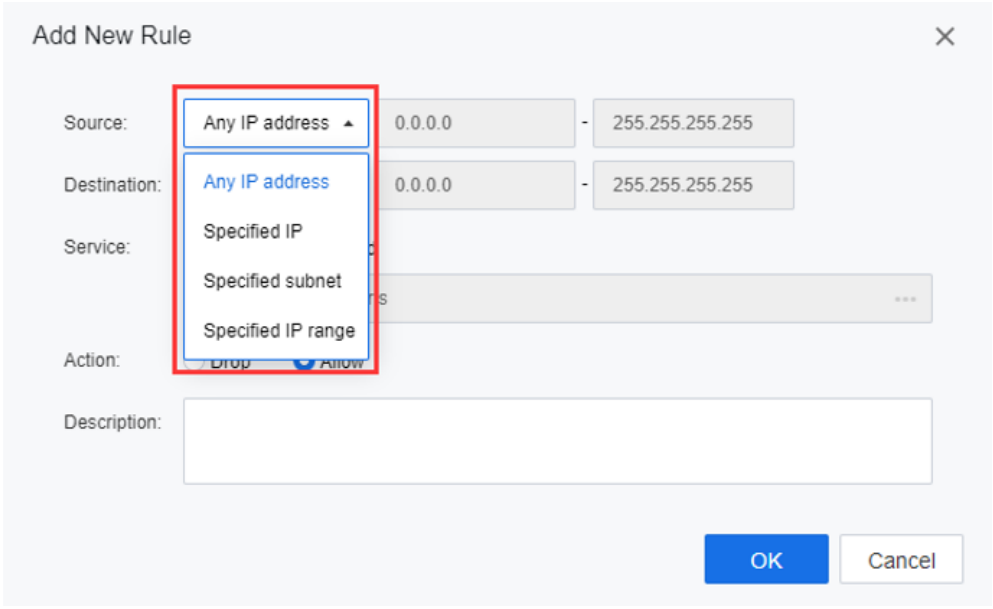
None.

Steps

Step 1. Log in to the console, navigate to **Networking > Network Deployment**, in VPC select the appropriate **VPC Name**, then look for the **ACL** and click **New**.

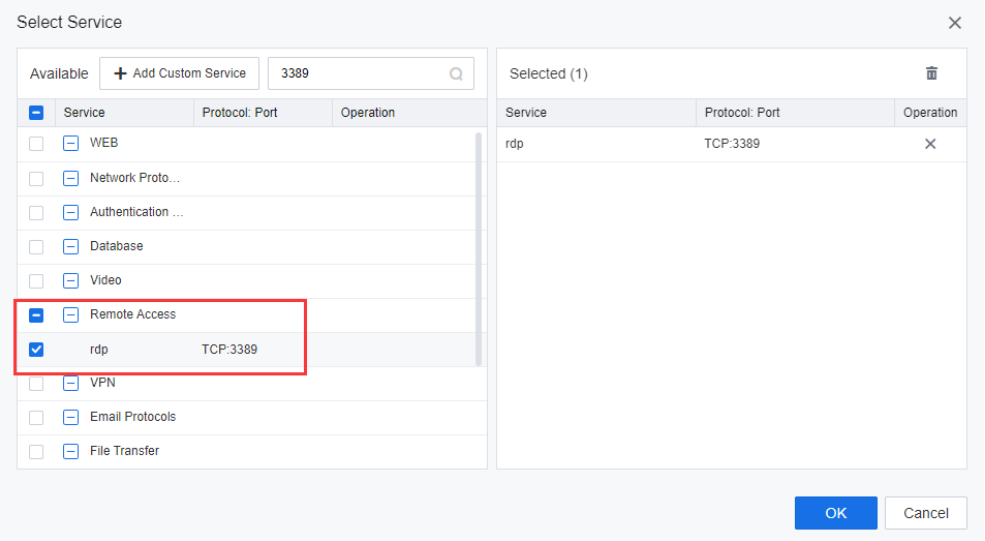


Step 2. Set the **Source** and **Destination** IP addresses, Any IP: from 0.0.0.0 to 255.255.255.255. **Specified IP**: Any IP address can be specified. **Specified Subnet**: the subnet that the platform has created. **Specified IP Range**: may define the IP range.

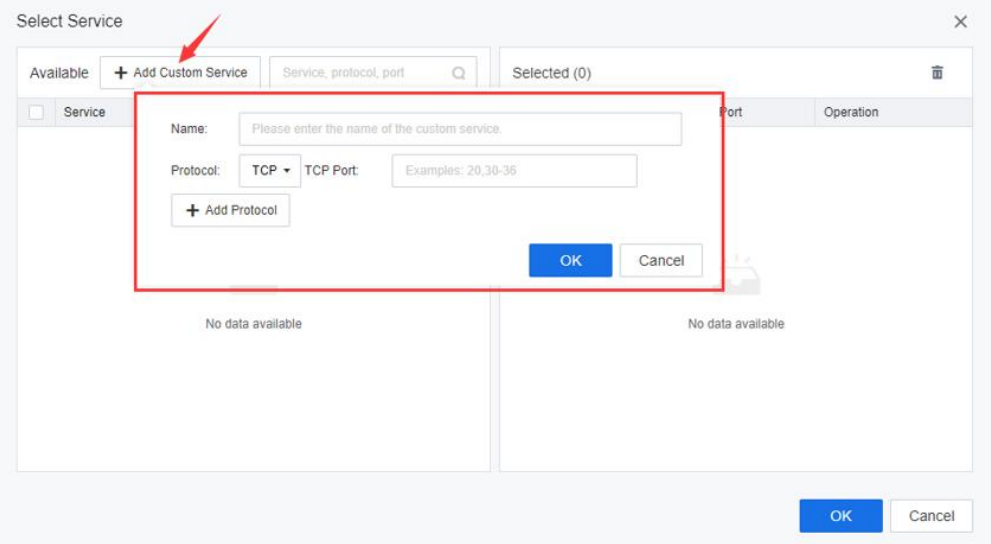


Step 3. Set the **Service** type.

- **Specified Service** setting (for example, specify the TCP 3389 remote desktop service), as shown in the figure.



- **Custom Service:** Supports customization of TCP, UDP, ICMP, and other protocols. As shown in the figure.



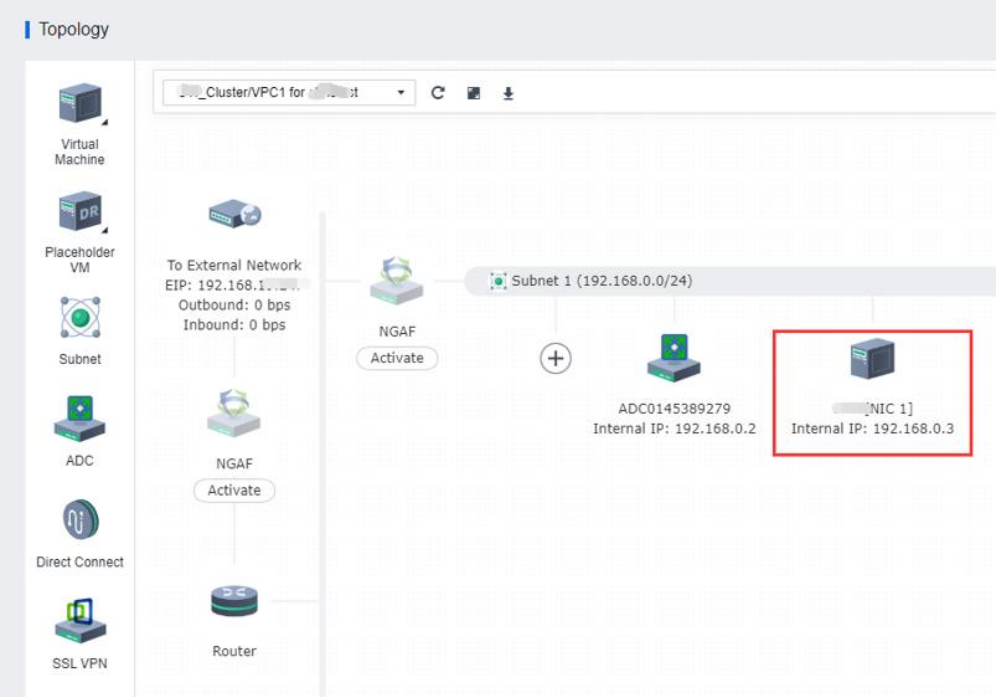
Step 4. To select the corresponding control action. After successfully adding the access control policy, you can tick the corresponding access control policy to **Disable**, **Edit,** and **Delete**. The disabled policy can be manually **Enabled**.

3. Destination Network Address Translation (NAT)

Features

After the edge network is bound with an elastic IP, it can be used for port mapping (port mapping refers to the mapping of a port of the IP address of the external network to a virtual machine in the internal network to provide corresponding services. When the user accesses this port of the IP, the server

automatically maps the request to the virtual machine inside the corresponding LAN) below. Let's take a case as an example to explain how to configure the port mapping function: map the router's elastic IP address TCP 80 port to the virtual machine port 80.



Precautions:

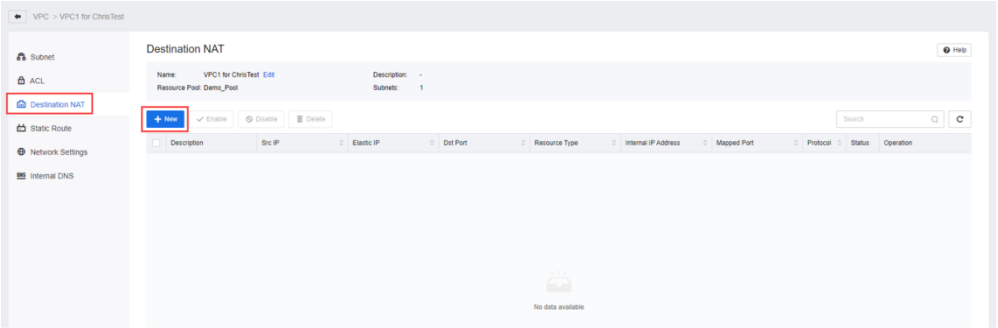
None.

Prerequisite

If the VPC is not bound or does not have an elastic IP that meets the requirements, please click **EIPs** in blue for the setting.

Steps:

Step 1. Log in to the tenant portal, and navigate to **Networking > Network Deployment** > **VPC.** Click the appropriate network Name and then choose **Destination NAT** and click **New**. As shown in the figure below.



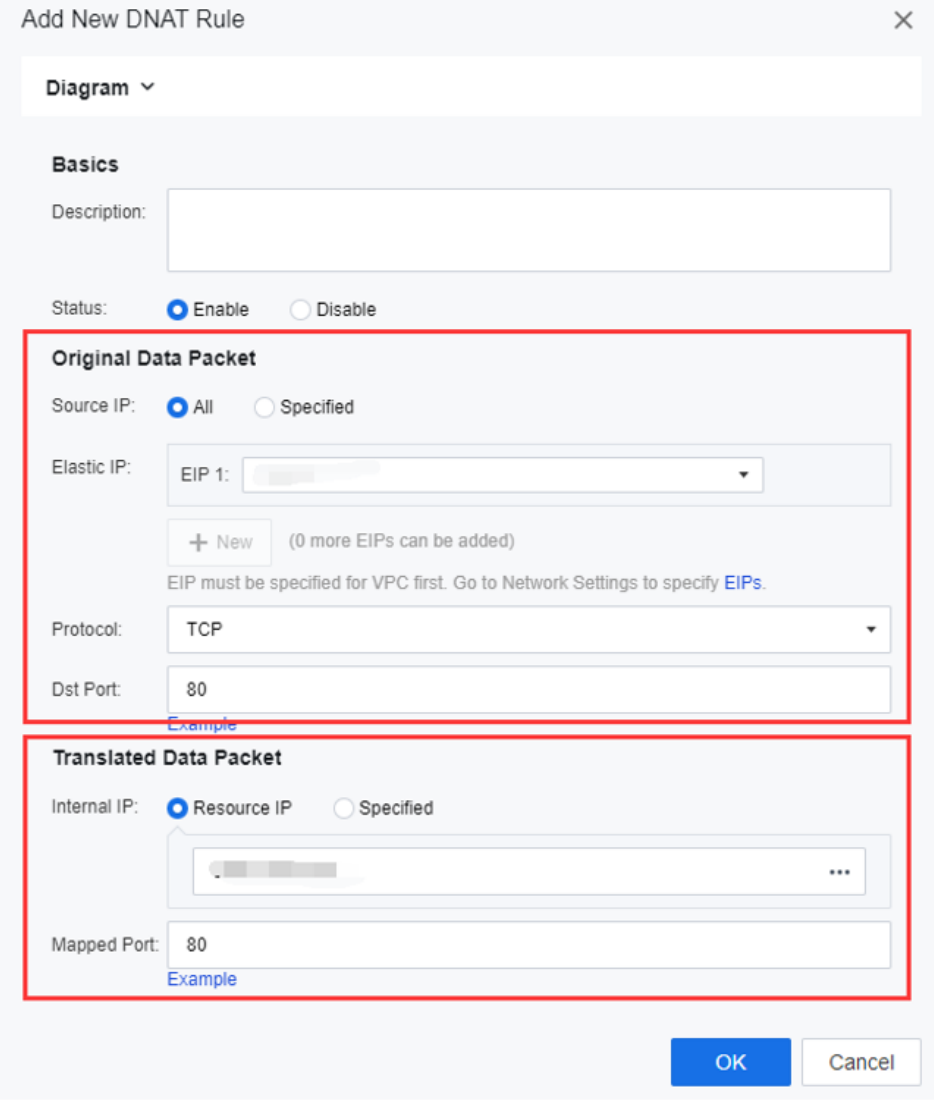
Step 2. Configure the source IP address that matches the DNAT policy.

Configure the source IP address that matches the DNAT policy. **All** is selected by default (all IP addresses in the public network can access the mapped service) and **Specified** (only allow the specified IP address in the public network to access the mapped service).

Step 3. Select the mapped **Elastic IP** and set the corresponding mapped port.

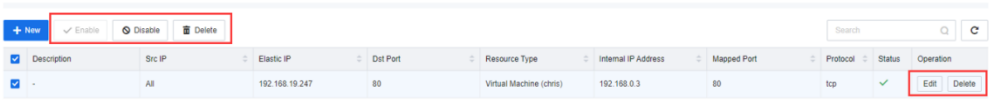
Click the sign to select the corresponding **Protocol** (support TCP, UDP, ICMP) and configure the **Elastic IP port**.

Step 4. Click ··· to select the node that needs to publish the service, configure the internal IP port, and then click the **OK** button. According to the example, the configuration is as follows.



Step 5. After the policy is added successfully, you may tick the specific destination NAT policy to **Disable**, **Edit,** and **Delete.** The disabled policy can be

manually **Enabled,** as shown below.



4. Static Route

Features:

Instruct users to add static routes, which can be created one by one or in batches.

Precautions:

None.

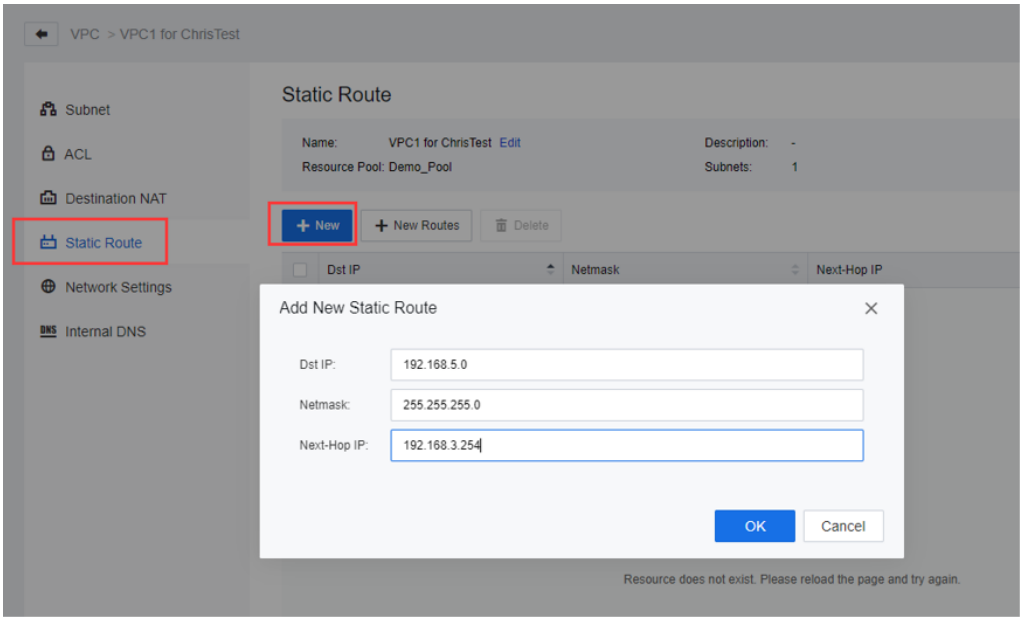
Prerequisite

None.

Steps:

Step 1. Log in to the console, and navigate to **Networking** > **Network Deployment.** Under the **VPC** interface, select the appropriate network **Name,** choose **Static Route**, and click **New** or **New Routes** to create a static route.

Step 2. Add **Destination IP**, **Netmask,** and **Next-Hop IP**. **Destination IP:** The destination network needs to be reached. **Netmask:** The corresponding destination network subnet mask. **Next-Hop IP:** The next-hop address of the target destination network.



Step 3. Click **OK** to create the static route.

5. Network Settings

Features:

Instruct users to bind the VPC edge IP and modify the DNS server.

Precautions:

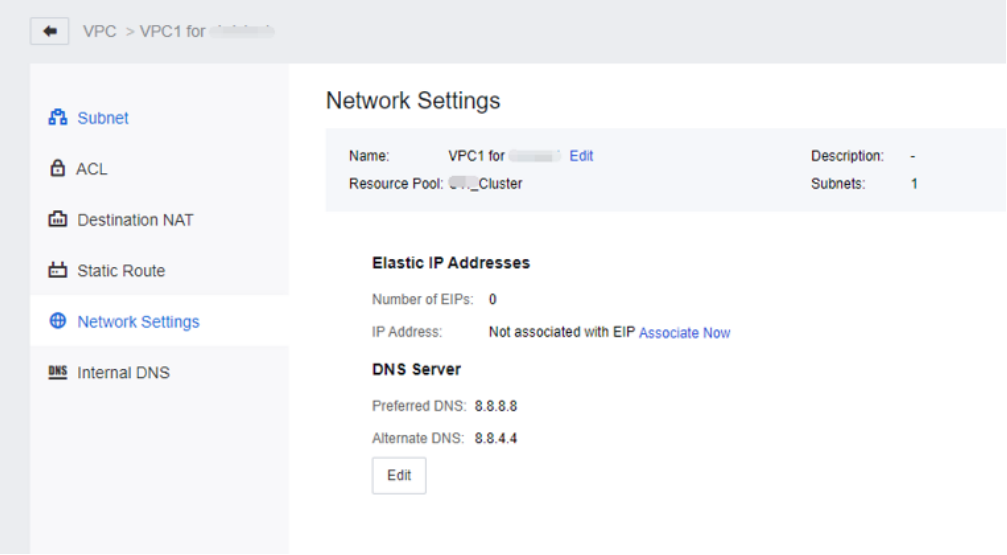
When different service provider provides the DNS server and the VPC edge IP, it may cause network disconnection or slowness. After changing the DNS server, it will be updated to all virtual machines within one day. If you need to update immediately, please change the DNS in the virtual machine.

Prerequisite

Bind an elastic IP to the VPC edge and must have sufficient elastic IP resources.

Steps:

Log in to the console, and navigate to **Networking** > **Network Deployment.** Under the **VPC** interface, select the appropriate network **Name** and then choose **Network Settings. Click Associate Now** if no elastic IP is associated, or bind an elastic IP. Click **Edit** to modify the DNS server configuration.



6. Internal DNS

Features:

After the internal DNS is configured, the virtual machine in the VPC can access intranet servers through the domain name.

Precautions:

1. It is not allowed to create duplicate internal DNS records, or a conflict alert will prompt.

- Only repeated domain names are allowed, and one domain name can correspond to up to 8 IP addresses.
- Only duplicate IPs are allowed, which applies to scenarios where multiple domain names have the same IP.

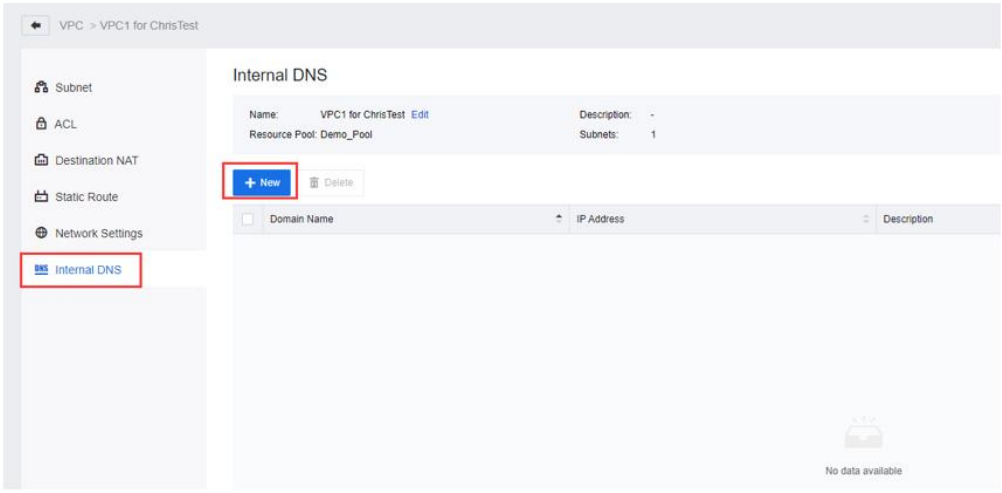
2. After configuring the internal DNS to access the domain name, the system and the browser will cache the DNS resolution results. The cache needs to be cleared after modification.

Prerequisite

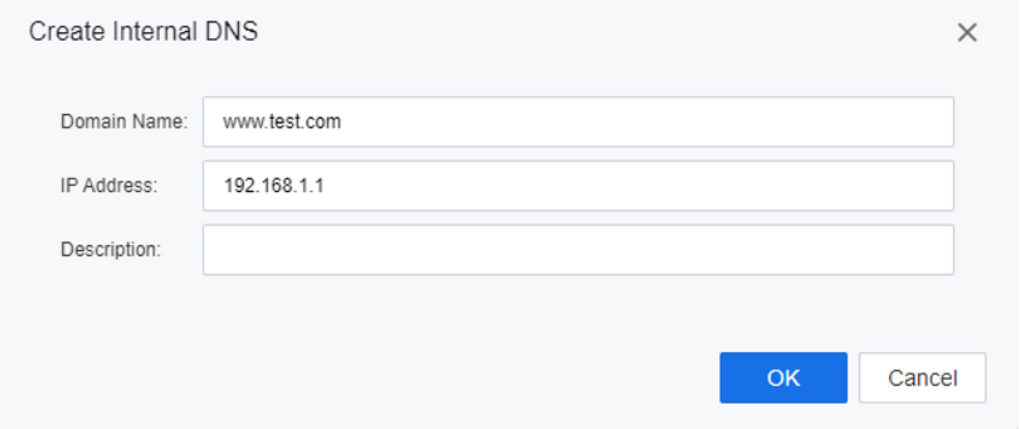
N/A.

Steps

Step 1. Log in to the console, navigate to **Networking** > **Network Deployment** under the **VPC** interface, select the appropriate network **Name** and then choose Internal DNS. Click New to create an internal DNS. Click **New** to create a tenant VPC.



Step 2. Configure the corresponding **Domain Name**, **IP Address,** and **Description,** and then click **OK**.



5.4.3.2 Classic Network

Features:

The classic network is applicable for direct communication scenarios such as tenants and other tenants or physical environments. The virtual machine, NFV devices, etc., can communicate with the outside through the tenant's classic network outgoing interface. Tenants can customize the name of the classic network outgoing interface.

Precautions:

Tenants cannot create NFV on the classic network. Please contact the platform administrator for deployment if you need to use NFV devices.

Prerequisite

The platform administrator has created a classic network outgoing interface for the tenant.

Steps

Step 1. Go to **Networking** and select **Network Deployment.** Then, in **Classic Network,** click **Edit** to modify the name of the network outgoing interface.

Step 2. Go to **Networking** and select **Topology,** then choose **Classic Network** to enter the network topology for basic topology editing.

5.4.4 Application Delivery Controller (ADC)

Feature Description:

Tenants can create Virtual Application Delivery (vAD) devices as professional application delivery devices that can provide users with a full range of

solutions, including multi-data center load balancing, multi-link load balancing, and server load balancing for users applications published.

vAD: Application delivery uses bypass mode to mount under the VPC subnet and load balance services on the same subnet. It supports functions such as one-click creation, one-click deletion, and performance tier modification under shutdown state and supports binding elastic IP.

Precautions:

1. The vAD device image used in the tenant VPC is different from the vAD device image used in the HCI.
2. In High-Available (HA) deployment, only two vADs connected to the same subnet are supported to deliver associated active and standby. After the association is complete, please log in to the ADC to configure the HA deployment in detail.

Prerequisite

1. Make sure the tenant has sufficient NFV quota.
2. Make sure the required device image is ready.

Steps:

Step 1. Go to **Networking, select ADC,** and click **New** to create a vAD device. Select the **Configuration** and **Function** parameters, the **Resource Pool** that the device belongs to, enter the **Name** of the vAD, the **Subnet**, choose whether to bind the elastic IP, and click **OK** to complete the deployment of the vAD.

Step 2. vAD supports HA deployment, In **Advanced** to associate the HA Peer.

5.5 Security

5.5.1 NFV Features

Features:

Tenants can create vNGAF and SSL VPN security devices.

vNGAF: Sangfor's NGAF provides full life cycle protection for user services by proposing the value proposition of **integrated security**, **simple and effective**, and truly achieving full visibility and full protection. It adopts routing mode

deployment and supports one-click creation, editing, deletion, enabling protection, and disabling protection.

vAD: Sangfor vAD is a professional product that offers a comprehensive solution for application delivery. It provides solutions such as multi-data center load balancing, multi-link load balancing, and server load balancing.

SSL VPN: More secure and better-experienced application publishing products make the access of business systems more secure. Use single-arm deployment mode to mount under the VPC subnet, support one-click creation, one-click delete, modify the configuration and function in the shutdown state, and other functions, and support binding elastic IP.

Precautions:

1. After a tenant creates a vNGAF device, the protection is enabled by default and can manually choose whether to add to the security center.
2. SSL VPN doesn't support adding into the security center.

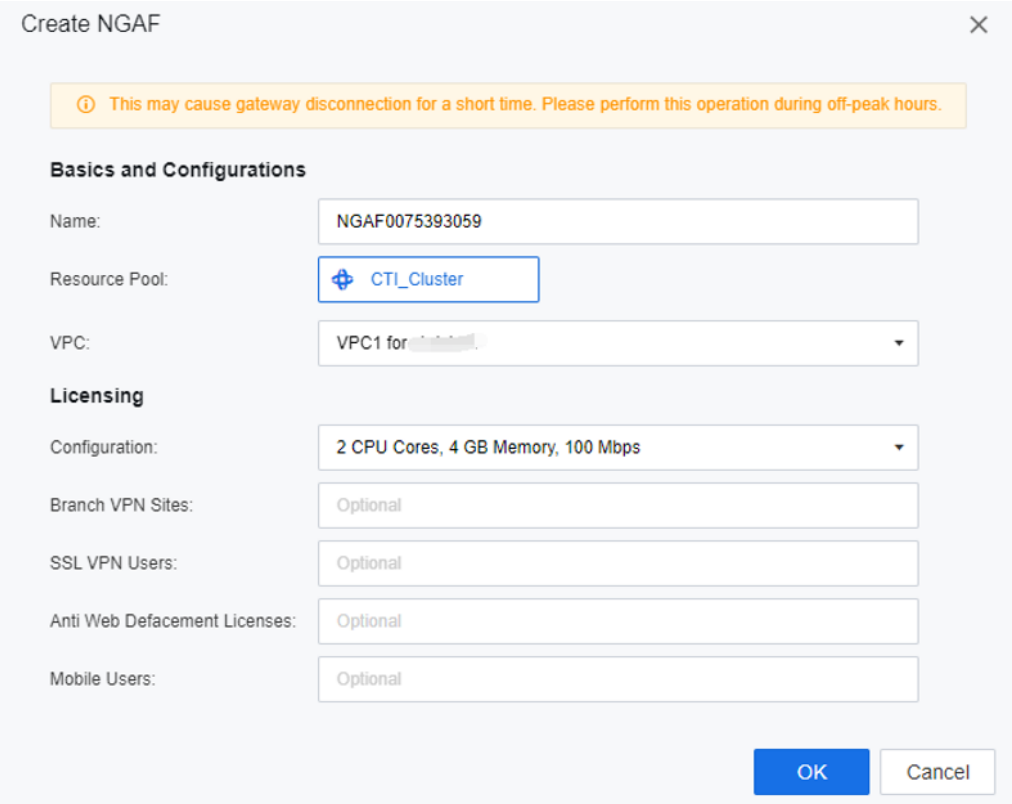
Prerequisite

1. Tenants need to have enough quota to create NFV equipment.
2. Tenants need to have device images to create NFV equipment.

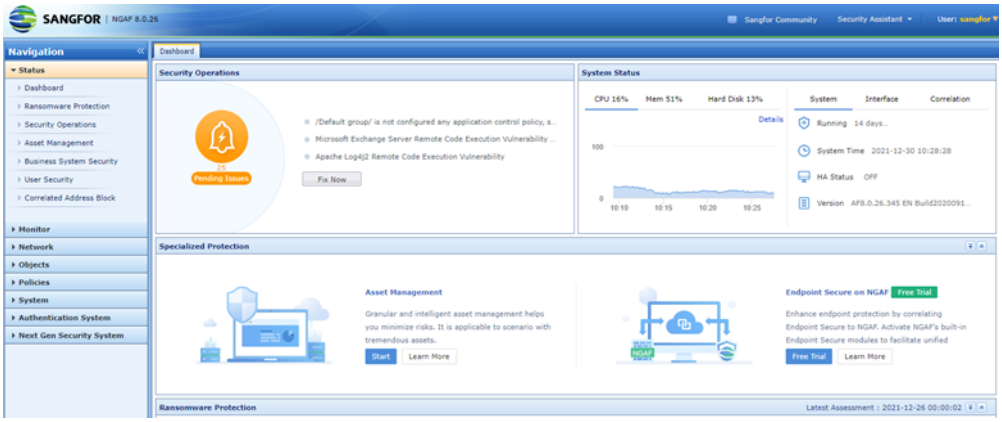
Steps:

- vNGAF

Step 3. Go to **Security Product** and then select **NGAF. Click New** to create a new AS policy. Configure the **Licensing** and **Configuration**, **Resource Pool**, **Name** of the vNGAF, and then click **OK** to create the vNGAF.

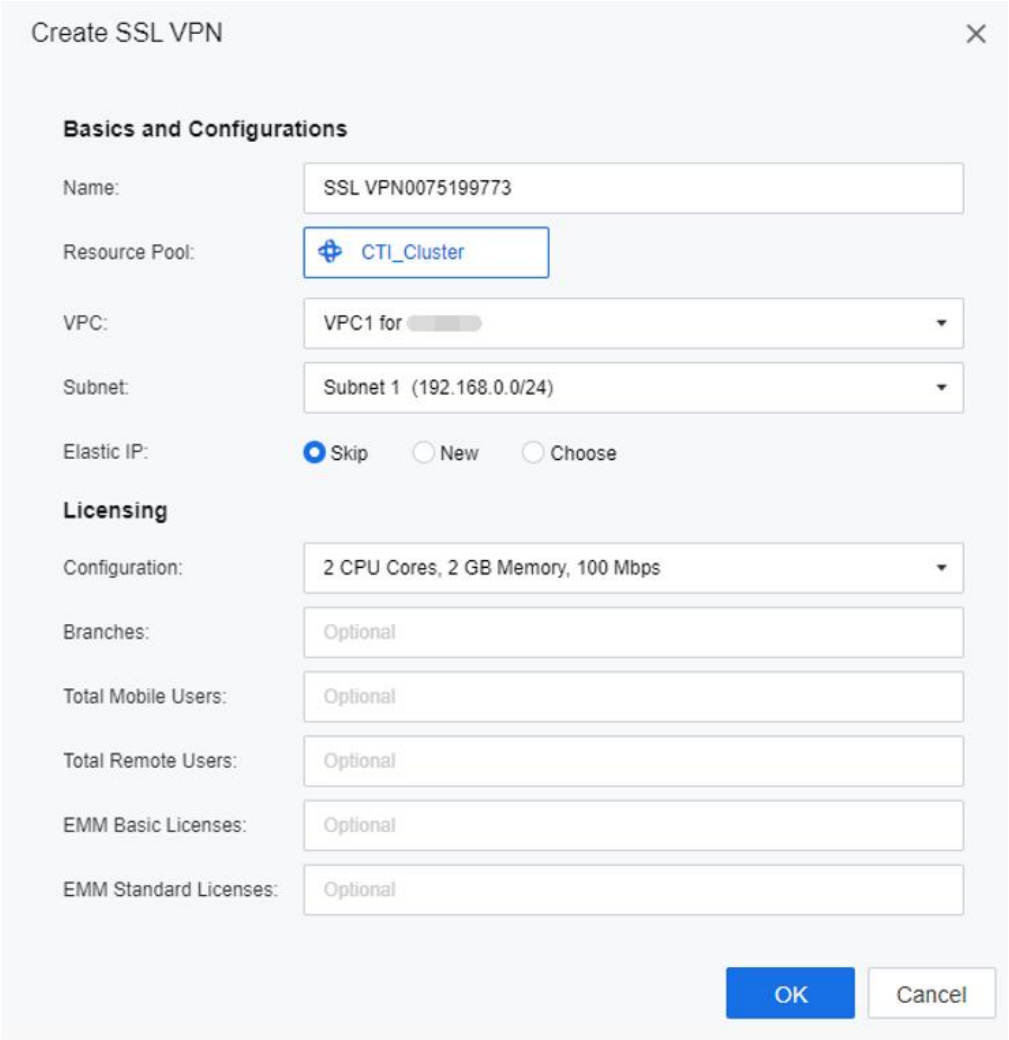


Step 4. After successfully creating, you can view the device status information from the list. Click **Edit** to edit the configuration and device name. Click **More** to redirect to the vNGAF console and enable protection. Click **Disable Protection** to stop device protection.

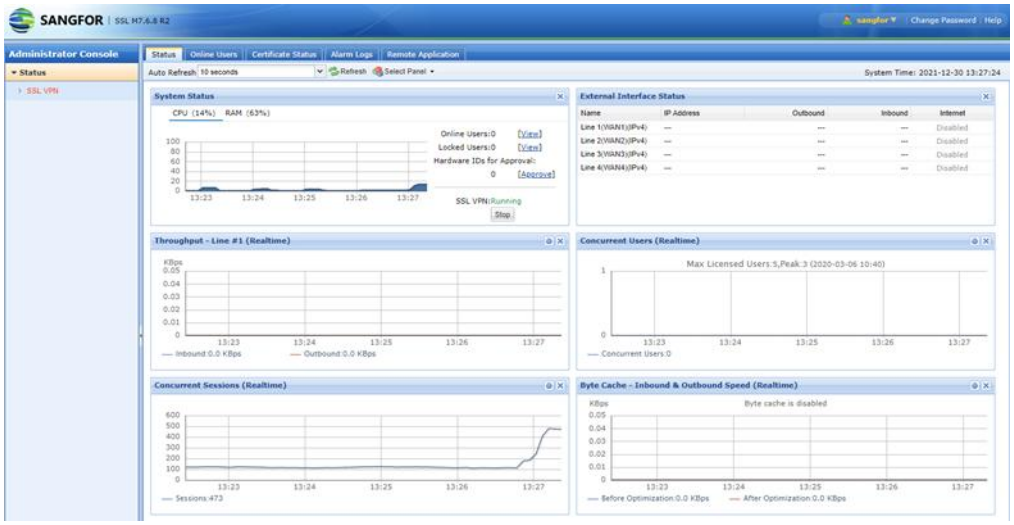


- SSL VPN

Step 5. Go to **Security Product** and then select **SSL VPN. Click New** to create a new shared service. Configure the **Licensing** and **Configuration**, **Resource Pool**, **Name** of the SSL VPN, select the **Subnet**, configure **Elastic IP** if required, and then click **OK** to create the SSL VPN.



Step 6. After successfully creating, you can view the device status information from the list. Click **Edit** to edit the device name. Click **More** to redirect to the SSL VPN console for customized settings.



5.5.2 Distributed Firewall

Feature Description:

SCP tenants can set distributed firewall policies in the network topology to which they belong to manage tenant networks.

Precautions:

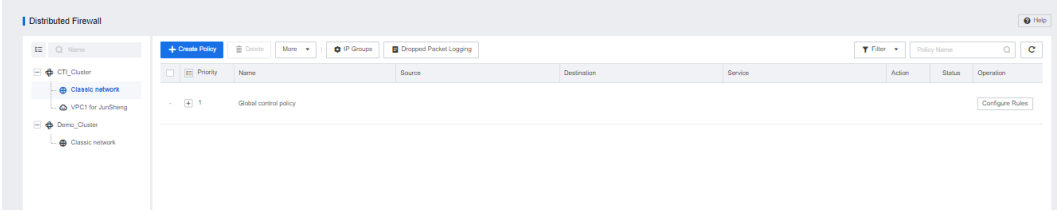
The role of the tenant distributed firewall takes effect only in the area of the tenant.

Prerequisite

None.

Steps:

Step 1. Log in to the SCP tenant interface, select **Security Services > Distributed Firewall** after successful login, enter the firewall editing page, and you can see the existing firewall policies.

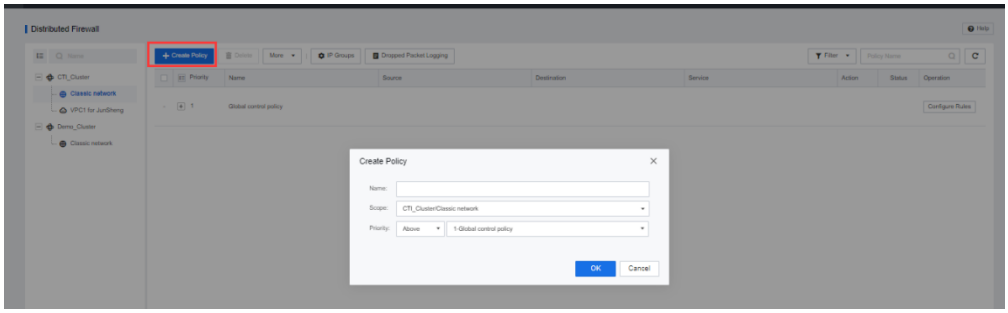


Step 2. Select the tenant network name from the list on the left, enter the corresponding page, and click the **Create Policy** button to create a firewall policy for the tenant network.

Name: The firewall policy name.

Scope: The effective domain of the firewall policy.

Priority: The policy priority created by the tenant is higher than the platform default policy, and other policy priorities can be adjusted manually.

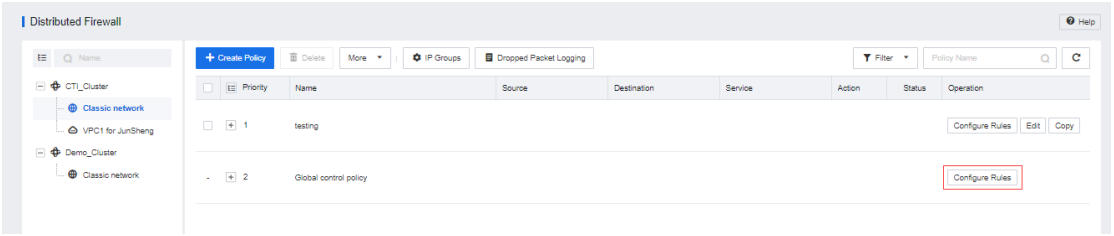


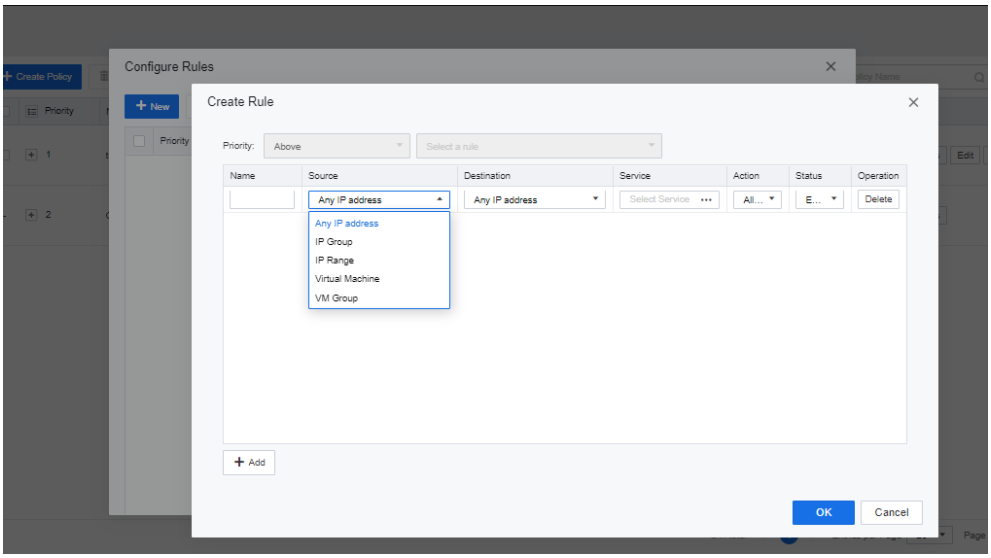
Step 3. Support group management of firewall interception rules. Add distributed firewall rules under the policy to the created policy. Click the **Configure Rules** button of the corresponding policy, and click **New.** The options here belong to the effective domain where the policy is located.

Source/destination matching conditions: Supports configuring IP Group, IP Range, Virtual Machine, and VM groups.

NOTE

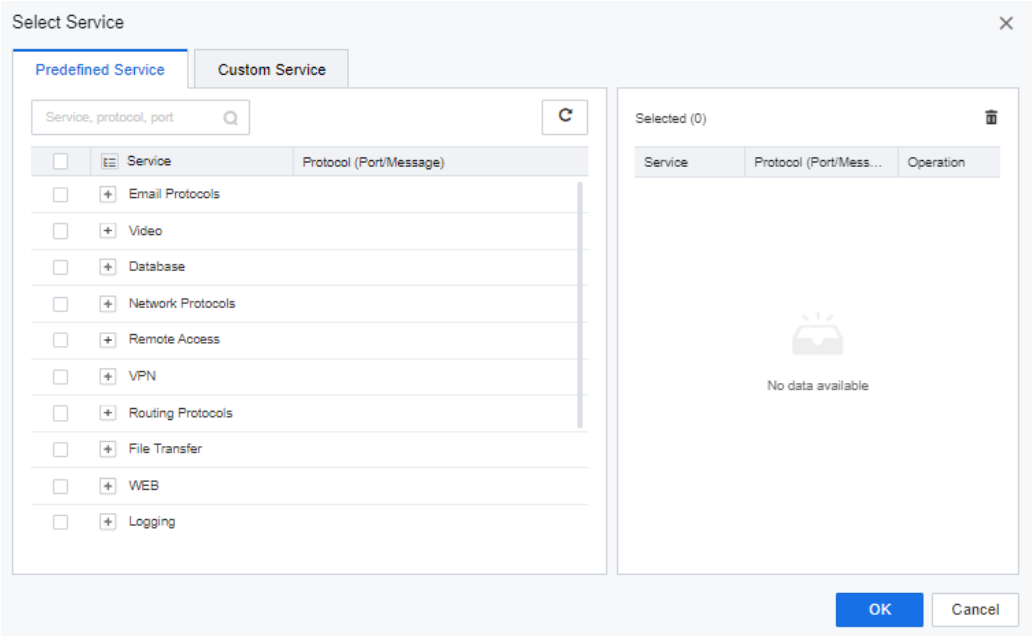
When the source/destination selects a virtual machine, if the virtual machine does not have vmTools installed, the system cannot automatically obtain the virtual machine IP, and the underlying firewall rules cannot perform effective IP conversion. The rules are actually ineffective for the virtual machine. Therefore, in this case, you need to configure an IP for the virtual machine before using it as the source/destination of firewall rules.



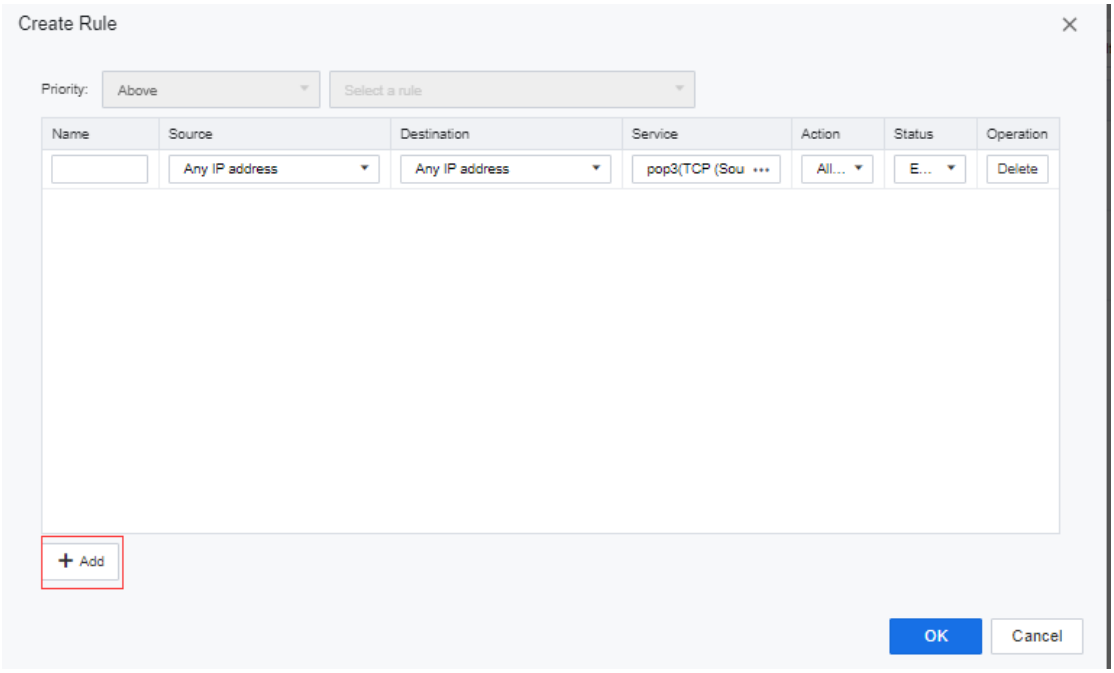


Service: Supports the selection of the platform's predefined service and supports custom service based on protocols and port numbers. Custom

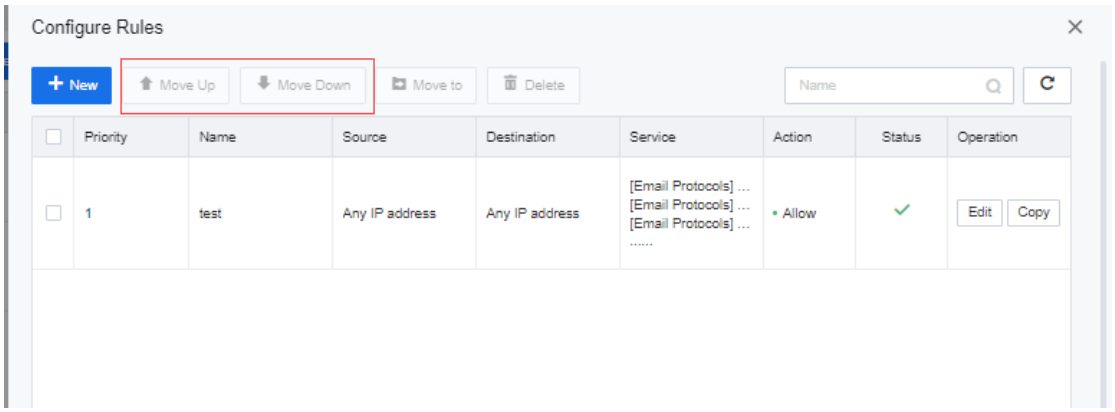
service in the same effective domain can be shared by multiple rules.

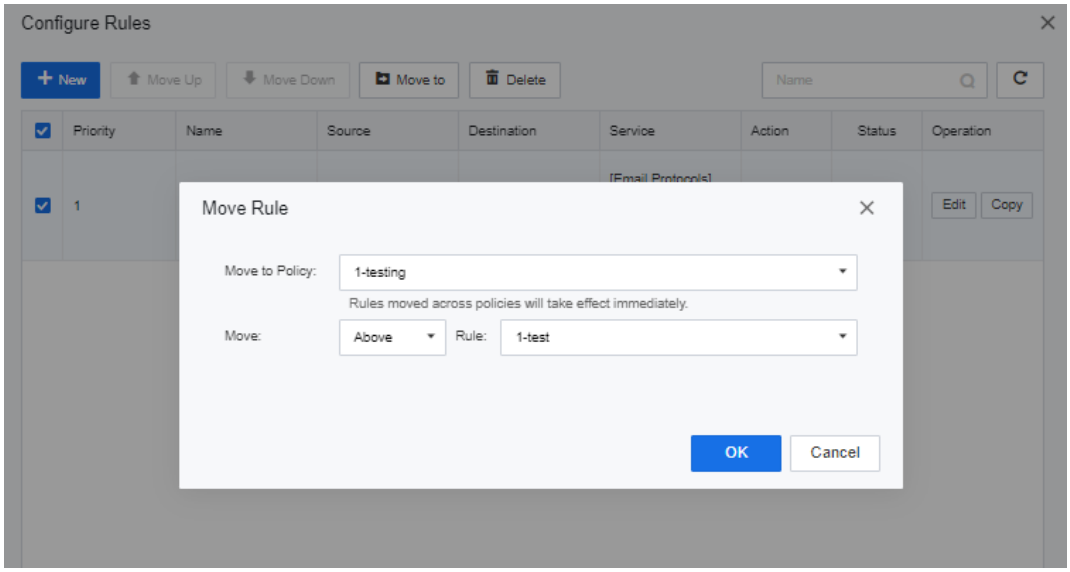


Step 4. Go back to the **Create Rule** page and click the **Add** button to continue adding other rules.

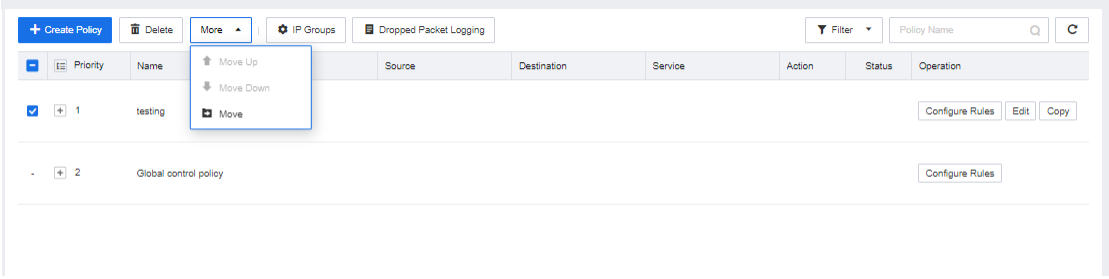


Step 5. After confirming that all rules are added correctly, click **OK**. On the Rule Configuration interface, select a rule record and click the **Move Up** or **Move Down** button to adjust the priority of the created rule. Click **Move to** to move the rule to another policy group.

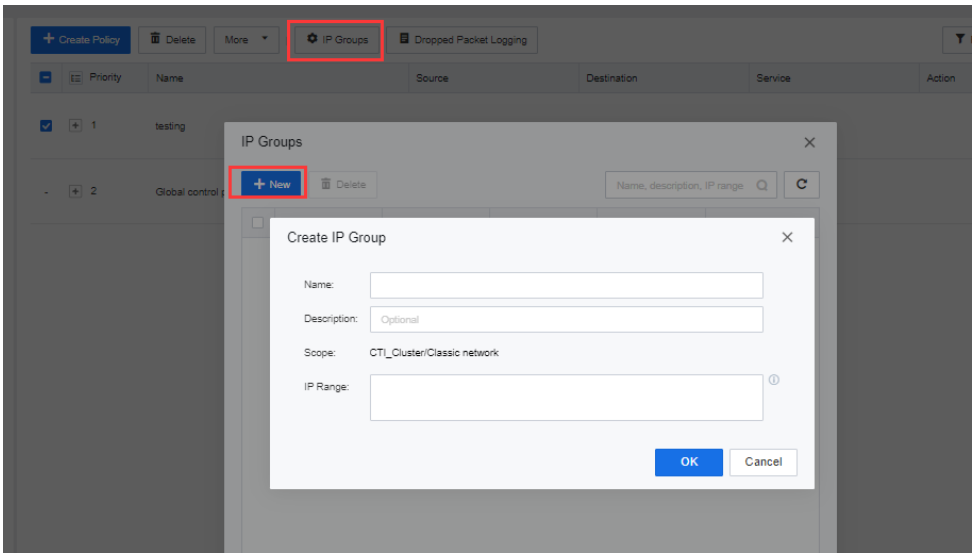




Step 6. It also supports the priority adjustment of distributed firewall policies. Select the policy whose priority needs to be adjusted in the list, and click **More** to adjust.



Step 7. **IP Groups**: Tenants can manage IP groups in the distributed firewall policy, click the **IP Group**s button, click the **New** button, enter the name and describe the IP range, and then complete the operation of adding an IP group



NOTE

Multiple rules can share a custom IP group in the same effective domain.

5.6 Reliability

5.6.1 Scheduled Backup Policy

Feature Description:

Tenants can set backup policies to customize the virtual machine's backup to protect the virtual machine's data.

Precautions:

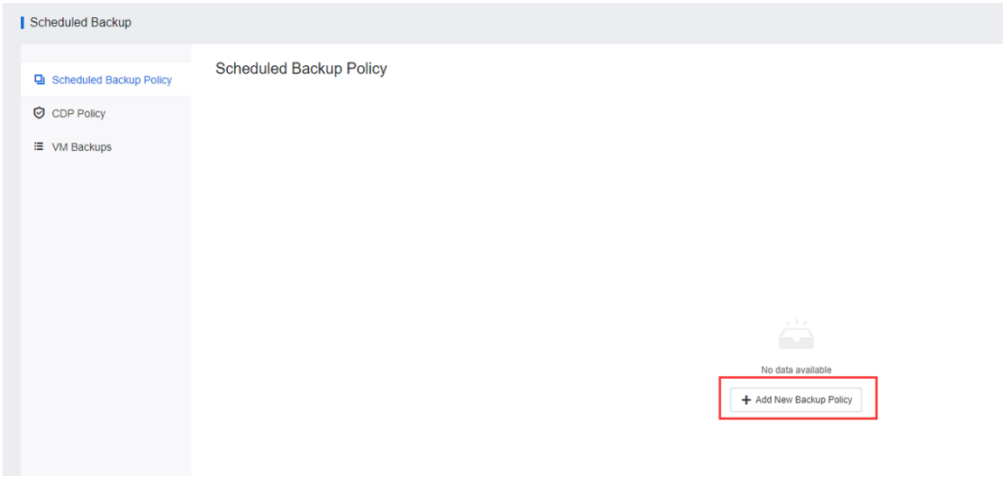
Tenants must have sufficient backup repository quota.

Prerequisite

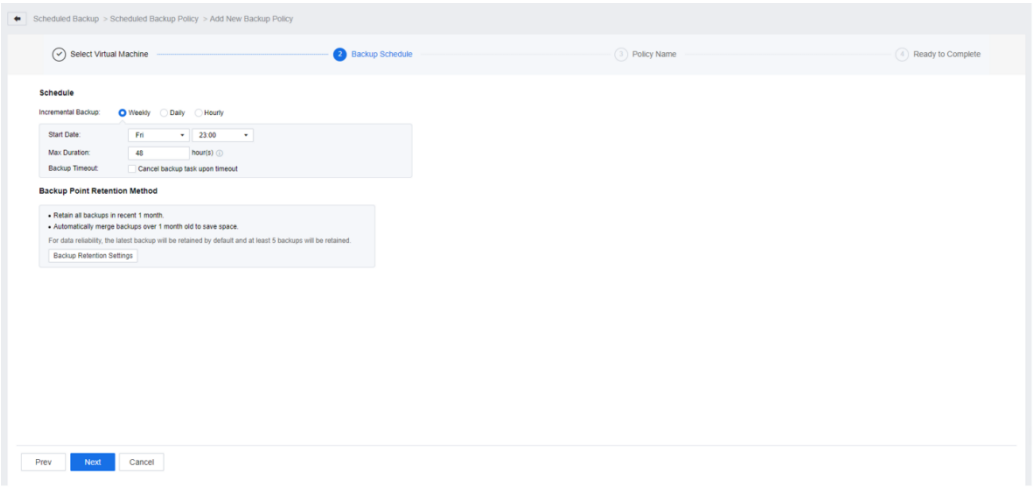
The backup repository is ready.

Steps:

Step 1. Navigate to **Disaster Recovery** and select **Scheduled Backup/CDP.** Click **Add New Backup Policy** to create a backup policy.



Step 2. Select the **Virtual Machine** that needs to be added to the backup policy. Next, set the **Schedule** and **Backup Point Retention Method**, **Name** of the backup policy, verify the information, then click **OK** to complete creating the backup policy.



5.6.2 CDP Policy

Function Description:

Sangfor SCP platform supports Continuous Data Protection (CDP) backup protection for tenant virtual machines. CDP stands for continuous data protection. It is an advanced Input/Output (IO) second-level backup technology that can back up every IO.

Precautions:

Tenants don't have permission to create CDP backup policies, and only the SCP administrator can create the CDP backup policies. After creating the backup policy, it takes effect by default, and tenants can enable and disable the CDP

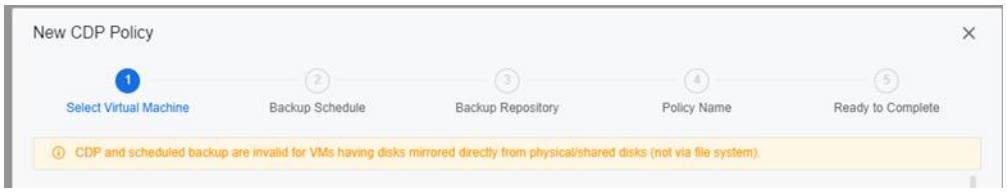
policy.

Prerequisite

None.

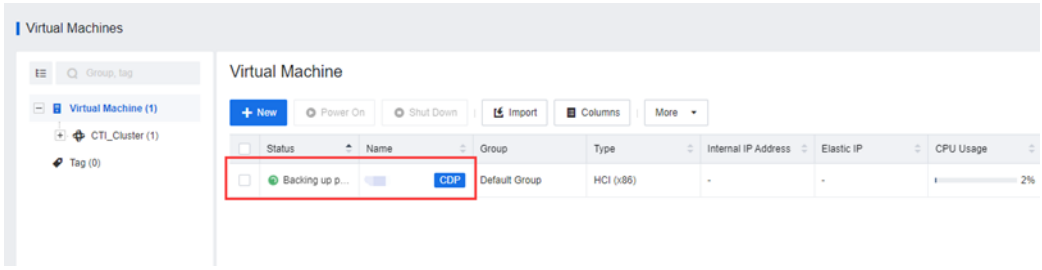
Steps:

Step 3. Login to https://SCP IP:4430 as admin, go to **Reliability** and select **Scheduled Backup/CDP**, choose **CDP Policy,** and click **Create CDP Policy** to create a new policy.

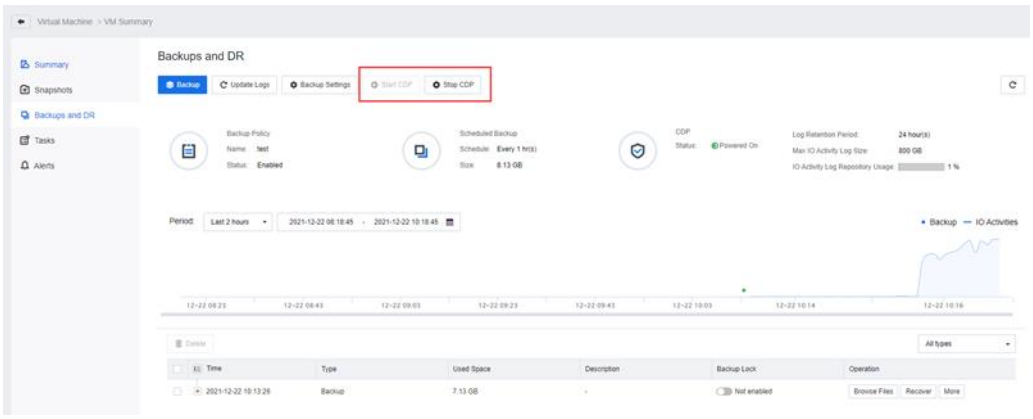


Step 4. Configure the CDP parameters: Add the virtual machine that the tenant wants to perform CDP backup into the policy, set the policy **Schedule** and **Backup Point Retention Method**, select the **Backup Repository**, fill in the **Name** of the policy, and verify the information, then click **OK** to complete the creation of the policy.

Step 5. After the platform administrator has created a CDP backup policy, tenants can view the CDP backup details on the **Virtual Machine** details page. Log in as a tenant from https://SCP IP. Go to **Compute** > **Virtual Machine** to enter the virtual machine list, and click the virtual machine name to enter the virtual machine details page.



Step 6. Click **Backup and DR** to view the status of the backup policy. Click **Stop CDP** to stop CDP backup and click **Start CDP** to enable CDP backup.



5.6.3 Disaster Recovery

Features:

When tenants use a virtual machine, they can perform aDR by themselves and add virtual machines that need disaster recovery to the disaster recovery policy for disaster recovery.

When the primary site is normal, and the virtual machine fails, the virtual machine can be recovered through local recovery. When the primary site requires planned maintenance or an unforeseen disaster occurs, the disaster recovery data of the secondary site can quickly recover the virtual machine from the secondary site to resume production.

Precautions:

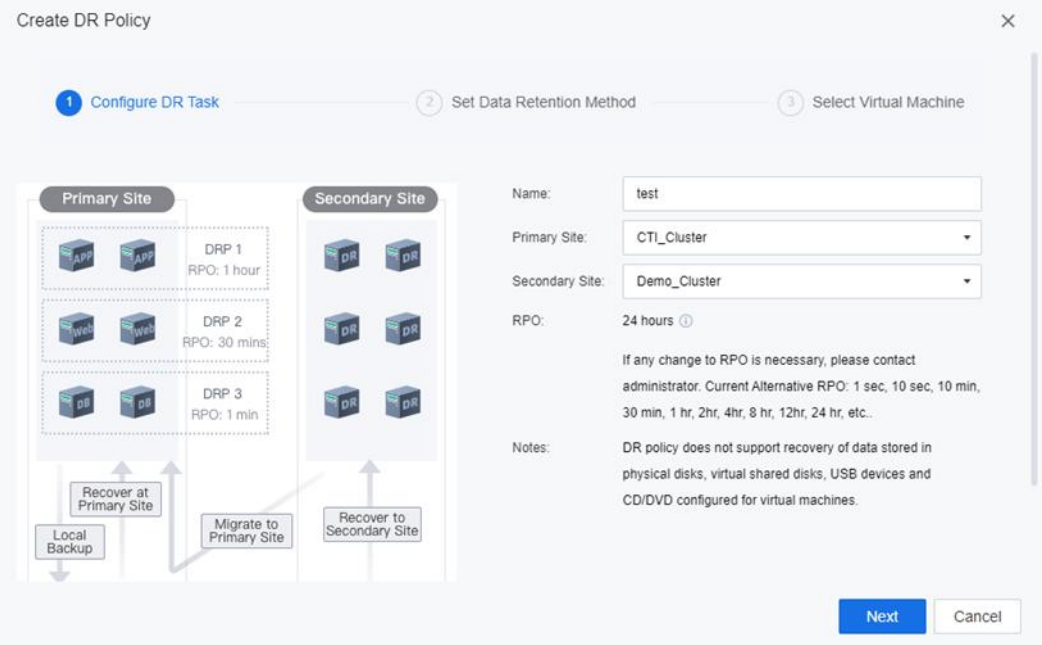
1. The default RPO for tenants to perform remote disaster recovery is 24 hours. If the tenants need to change the disaster recovery RPO, please contact the administrator. Currently supports RPO: 1 second, 10 seconds, 10 minutes, 30 minutes, 1 hour, 2 hours, 4 hours, 8 hours, 12 hours, and 24 hours.
2. The physical disks, virtual shared disks, external USB devices, and external optical drives of virtual machines do not support remote disaster recovery.

Prerequisite

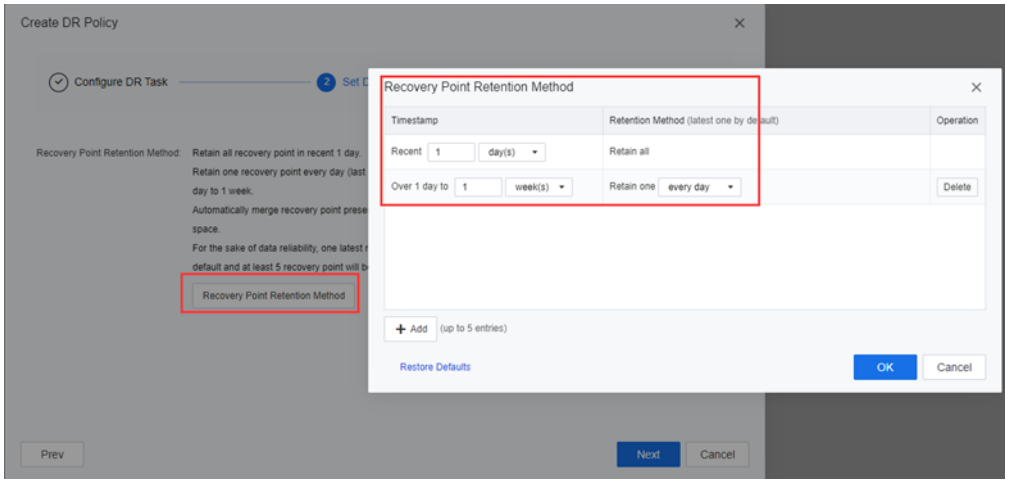
1. SCP platform admin must have configured the linkage for the primary and secondary sites and ensure stable connectivity between the cluster's management interface.
2. The tenant has sufficient backup repository quota and quota for disaster recovery virtual machines.

Steps

Step 1. Navigate to **Reliability** > **Disaster Recovery > DR Policy and click New** to create a disaster recovery policy. Fill in the **Name** of the DR policy and select the **Primary Site** and **Secondary Site**. The **Recovery Point Retention Method** can be selected from recent one week, recent one month, or recent three months.



Step 2. Configure **Recovery Point Retention Method**.

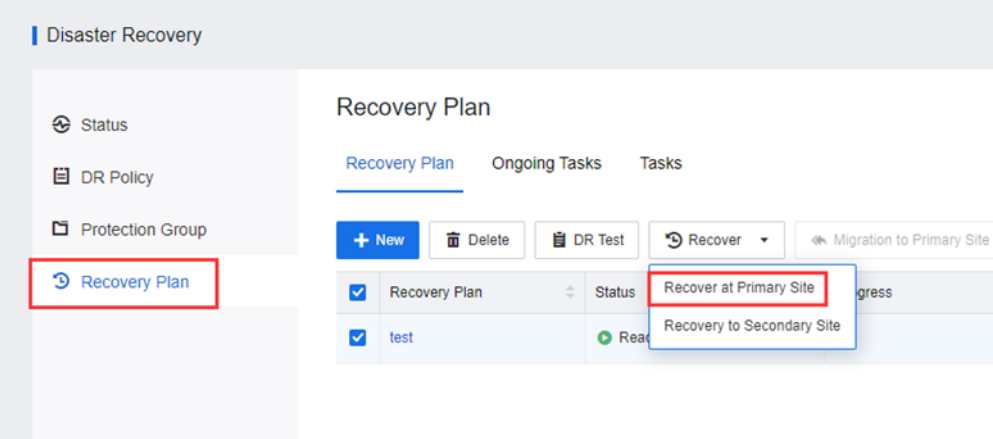


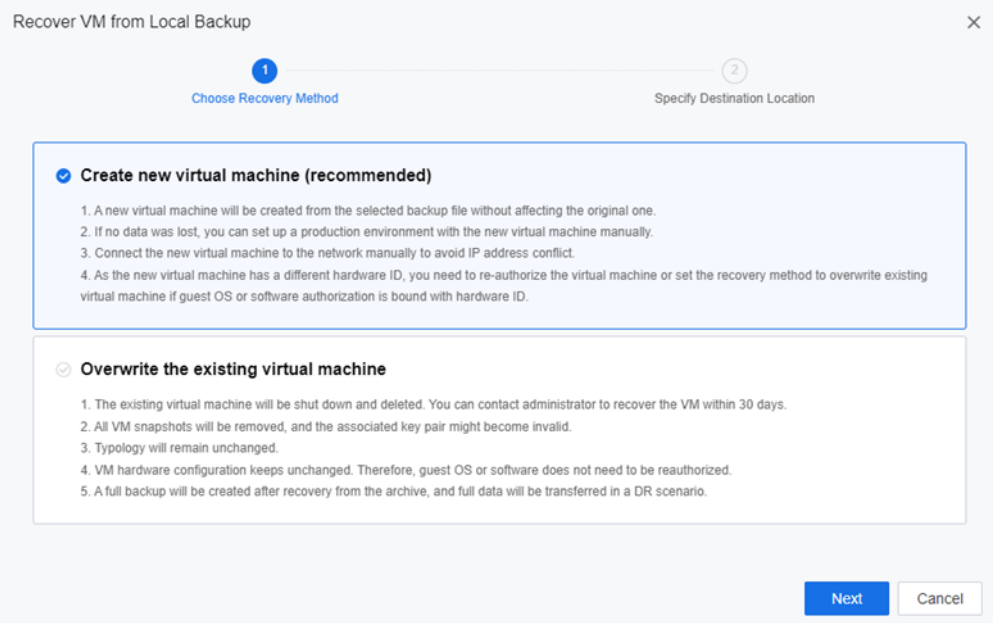
Step 3. Select the virtual machines that need protection and click **OK** to complete the DR policy creation.

Step 4. Configure the network for the disaster recovery standby virtual machine, click **Configure Network**, add the disaster recovery standby machine to the subnet, and configure the network according to actual needs (binding

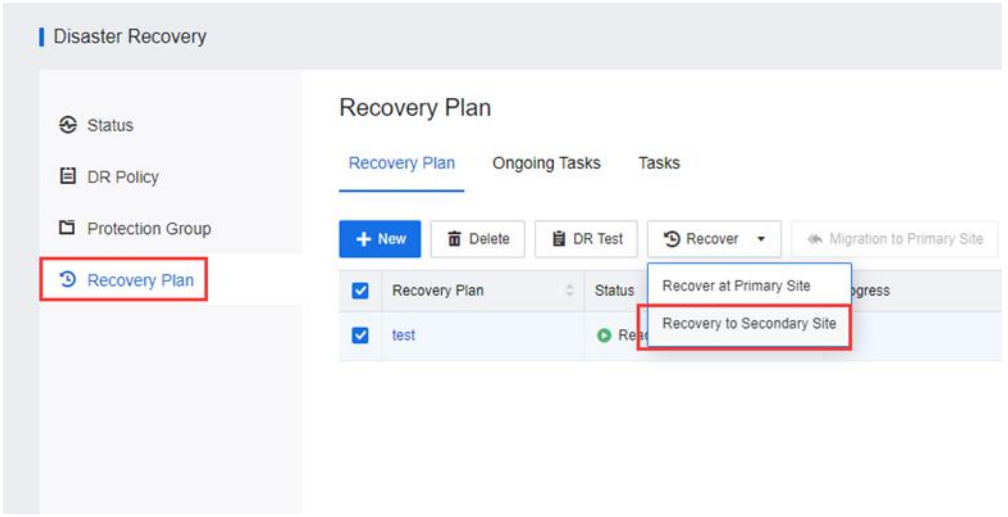
elastic IP or port mapping).

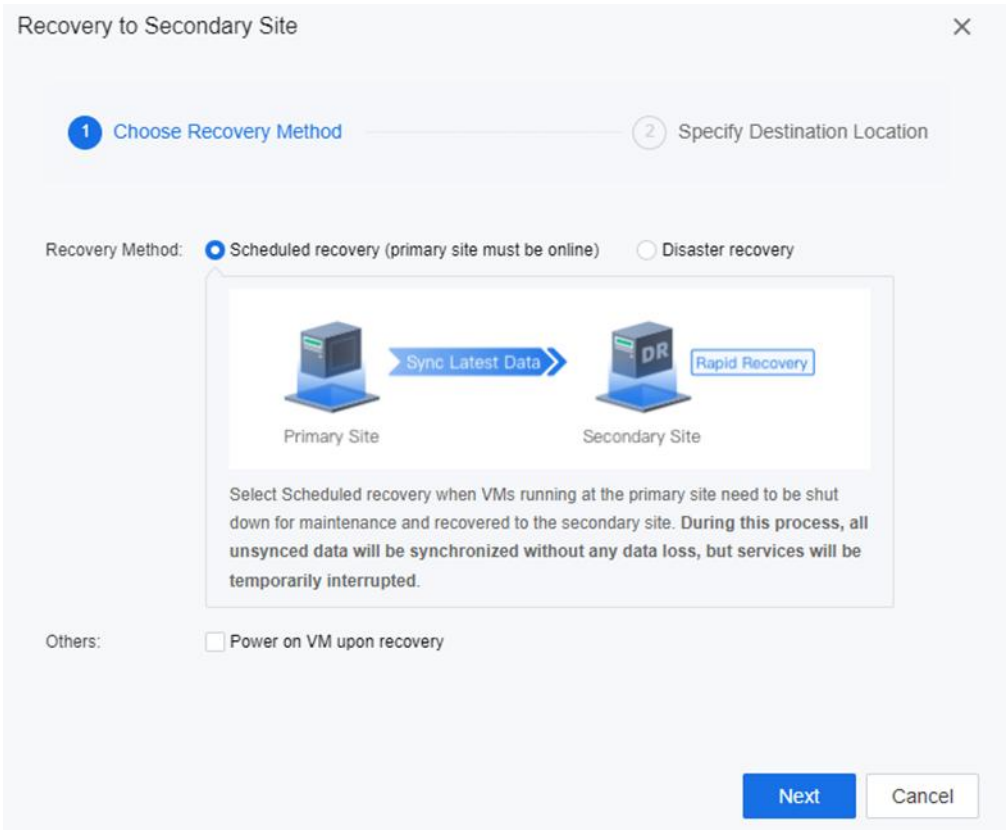
Step 5. When the primary site is normal, and the virtual machine fails, local recovery can be performed: Go to the **Recovery Plan** page and click **Recovery at Primary Site**. It is recommended to select **Create new virtual machine**, configure the destination location, and click **OK**.



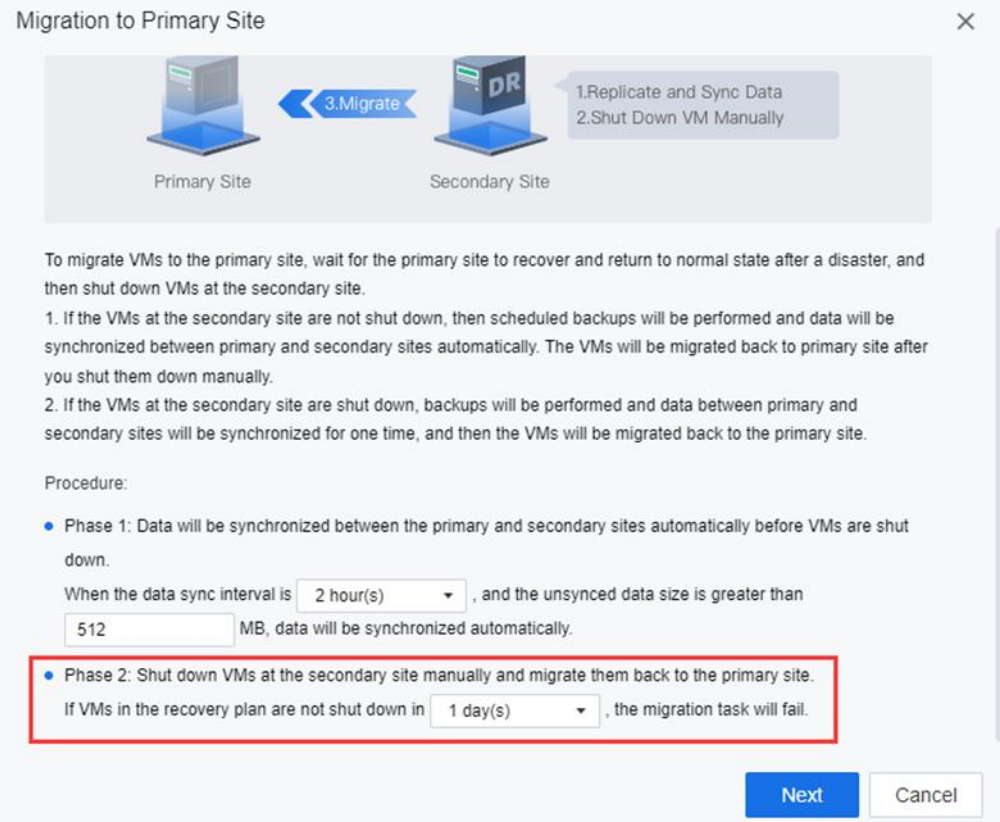


Step 6. When the primary site requires planned maintenance or a disaster occurs, the disaster recovery data of the secondary site can quickly recover the virtual machine from the secondary site to provide services: Go to the **Recovery Plan** page, and click **Recovery to Secondary Site**, choose the **Recovery Method** according to the actual recovery scenario, you can check **Power on VM upon recovery** checkbox, configure the recovery location, and click **OK**.





Step 7. After the primary site is recovered, the virtual machine can be migrated from the secondary site back to the primary site: Go to the **Recovery Plan** page, select the specific **Recovery Plan Name** and click **Migrate to Primary Site**, select the datastore for migration, and start migrating the virtual machine to the primary site. During the migration, the status will change to **Waiting for Shutdown**. At this time, you need to shut down the DR virtual machine manually and execute the migration task.



5.6.4 Auto Scaling

Features:

Sangfor SCP supports configuring auto-scaling for business by monitoring the load of virtual machines to achieve virtual machines creation or deletion. When the load of virtual machines exceeds the set conditions, SCP will automatically deploy a virtual machine to share the pressure of the production virtual machine to meet the resource requirement of applications when the production load pressure changes fluctuate widely and reduce human intervention.

5.6.4.1 Creating AS Group

Features:

The initial virtual machine will be deployed to join the AS group after the AS group is created.

Precautions:

1. The auto-scaling function only supports tenant VPC scenarios.

2. All nodes within the auto-scaling feature are loaded with vAD virtual services. If access is needed outside the tenant, bind the elastic IP for the vAD virtual services.
3. Auto-scaling VM is based on built-in image deployment. When creating the built-in image, ensure the production configuration, such as business service auto-startup, listening port, and database connection, are complete.
4. The threshold value monitored by the AS policy is the average value of all virtual machines in the AS group.
5. The AS group in the enabled state is not allowed to delete. Click the green button in the status bar to enable/disable it.
6. The AS group that has associated AS configuration and AS policy is not allowed to delete.

Prerequisite

1. Adequate resources quota has been allocated for the tenant.
2. 2. A load balancing (vAD) device has been created for the tenant.

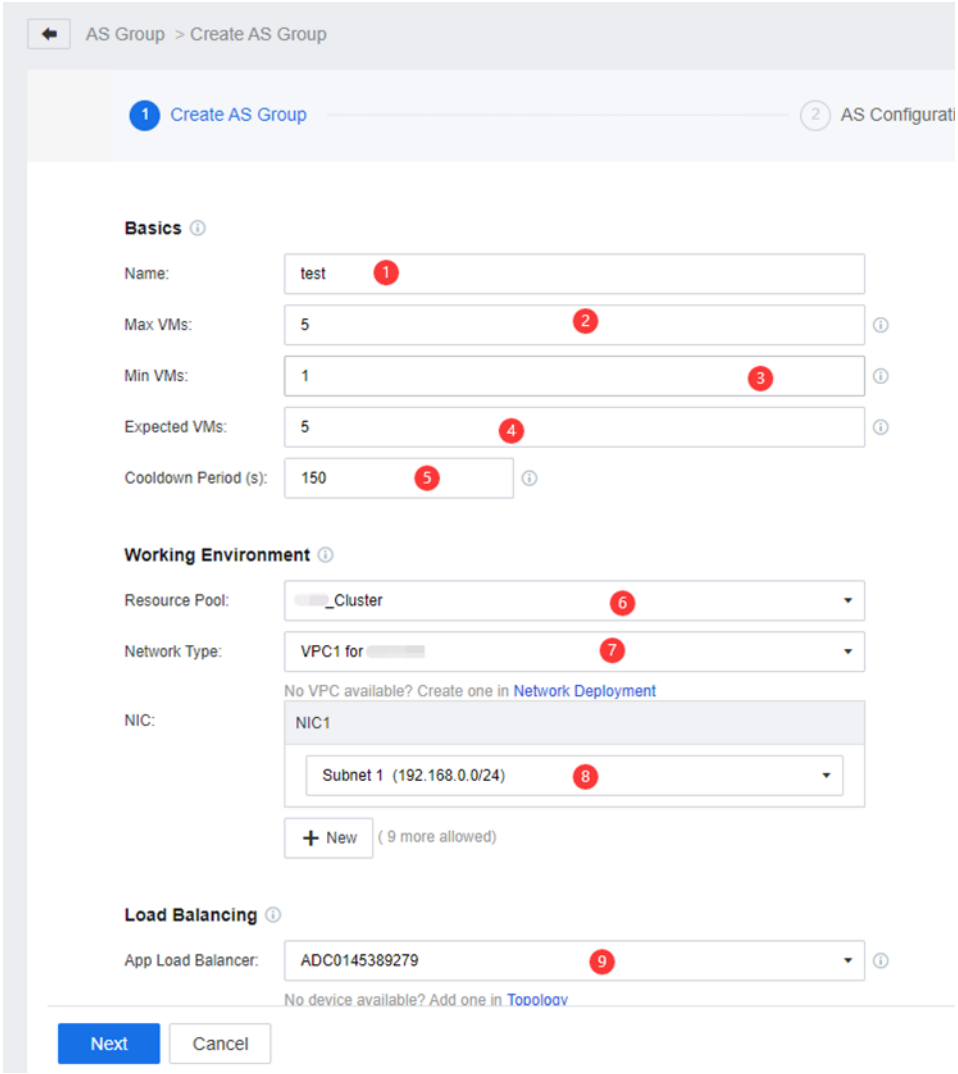
Steps:

Step 1. Log in to the tenant portal, navigate to **Reliability** and select **Auto Scaling**.

Step 2. Click **New** to create an AS Group by filling up the following information.

1. **Name** of the AS group.
2. **Max VMs:** Maximum number of VMs in an AS group when performing scaling.
3. **Min VMs:** Minimum number of VMs in an AS group when a scaling action is performed.
4. **Expected VMs:** Automatic scaling is performed to add the expected number of VMs after the AS group is created or edited.
5. **Cooldown Period(s):** A scaling cooldown helps you prevent your AS group from launching or terminating additional VMs before the effects of previous activities are visible.
6. **Resource Pool:** Select the resource pool where the tenant is located.
7. **Network Type:** Only tenant VPC is supported currently.

8. **NIC:** Select the tenant subnet to access.
9. **App Load Balancer:** Select the vAD planned for auto-scaling within the tenant.

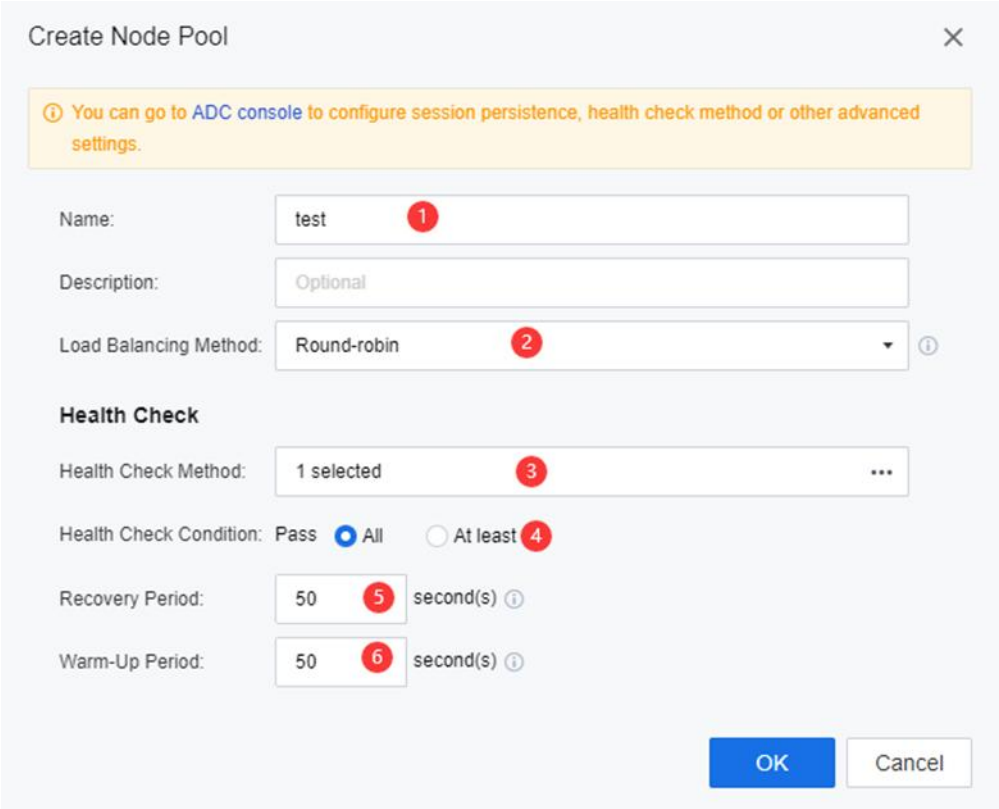


Step 3. Click **Node Pool** under **Load Balancing**, and a **Select Node Pool** window will appear and configure the following.

1. **Name** of the node pool.
2. **Load Balancing Method:** Passes each new connection request to the next node in line in a rotating sequential manner.
3. **Health Check Method:** Configure the method of vAD detection to VMs. Some of it required to be configured in vAD.
4. **Health Check Condition:** When multiple health check methods are configured, **At least,** or **All** checks are passed will be considered valid.
5. **Recovery Period:** When a failed node recovers, it gives the node time to get

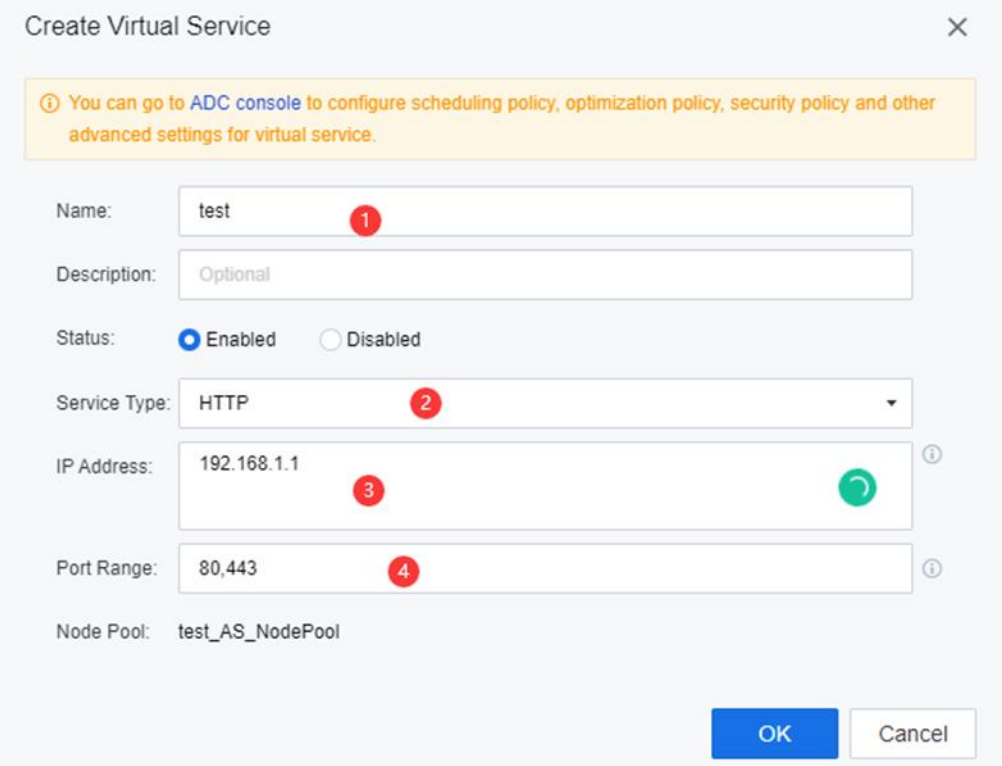
ready before returning to service. During this time, no requests will be sent to the node from the client. Range: 0-300. 0 indicates disabled.

6. **Warm-Up Period:** When a failed node recovers, this gives the node time to warm up. During this time, the traffic to the node will be slowly ramped up to prevent the node from being overwhelmed by more connections than it can handle as it starts up. **Range: 0-300** and **0** indicates disabled.

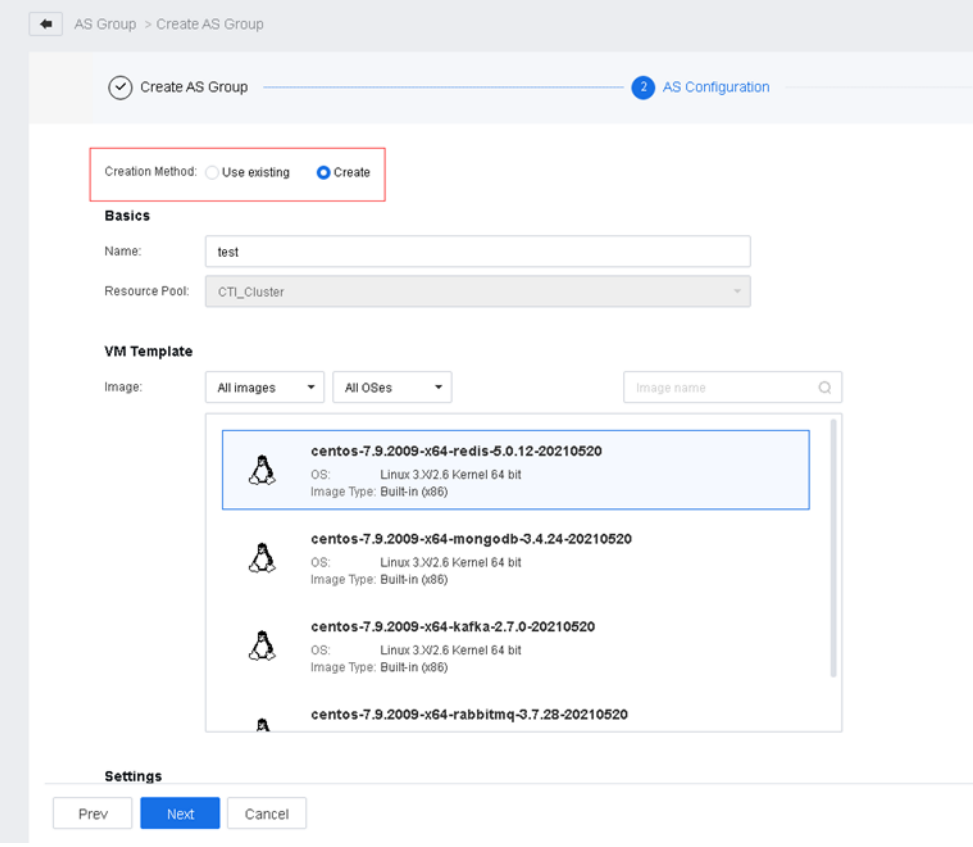


Step 4. Click **OK** to return to the **Create AS** Group page, look for **Virtual Service** under **Load Balancing, click New,** then configure the following.

1. Name of the virtual service.
2. **Service Type**: Select the service type.
3. **IP Address**: Input the IP address of the service provided by vAD to the outside network.
4. **Port Range**: Fill in the port range for the external service provided by vAD.

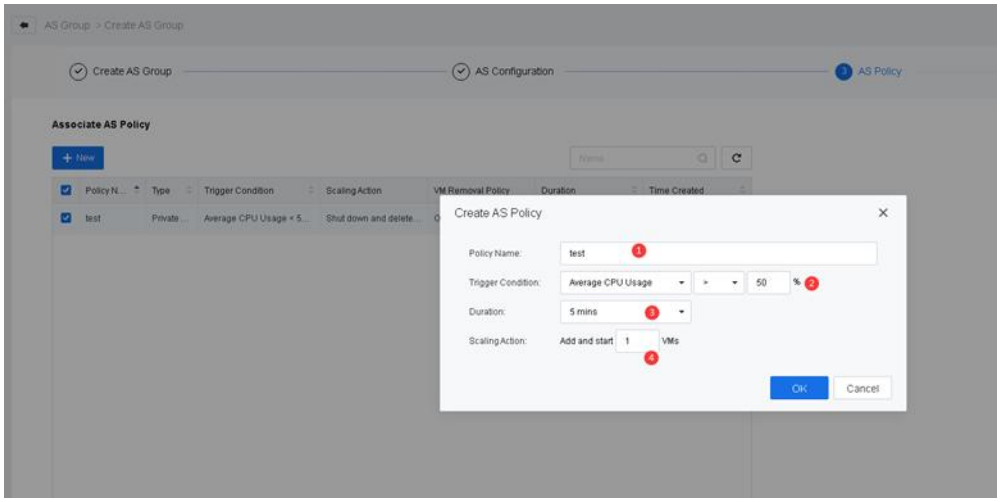


Step 5. Create a new AS configuration or use an existing AS configuration, which is the step of deploying a virtual machine using a built-in image.

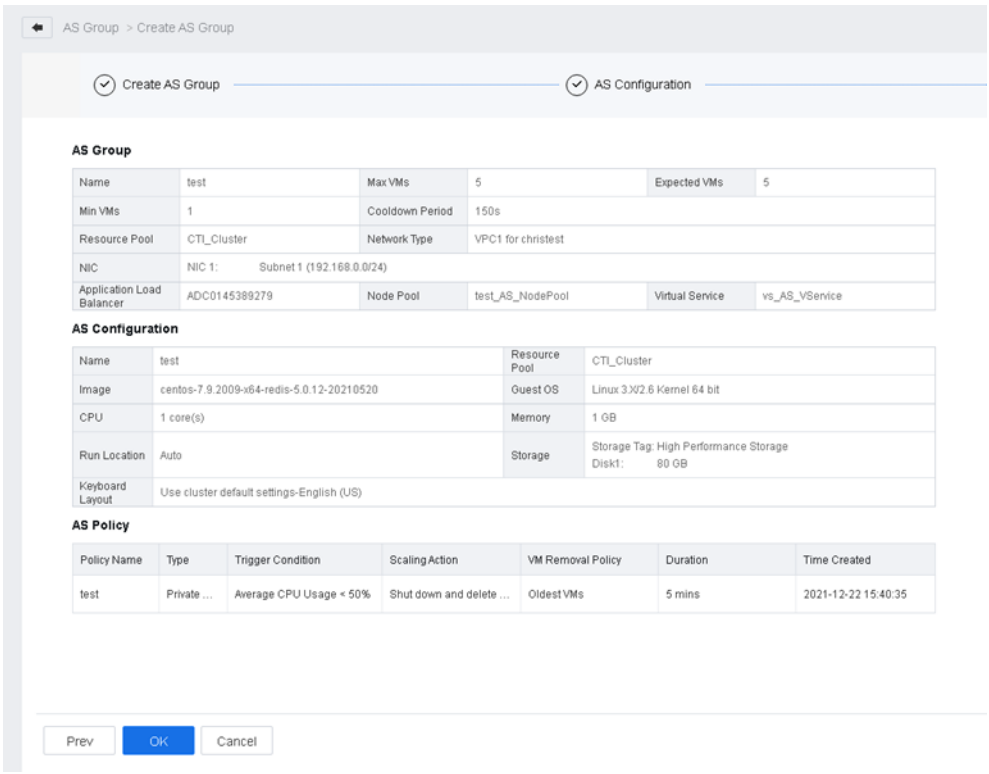


Step 6. Click **Next** to associate an existing or new AS policy.

1. Policy **Name**.
2. **Trigger Condition:** Support setting the threshold value for the average CPU or memory usage.
3. **Duration:** When all the virtual machines in the AS group have reached the trigger condition and exceed the duration, the scaling action will be executed.
4. **Scaling Action:** Create or delete the VMs. vAD exit mechanism will be used for deletion where it will not schedule new connections to this virtual machine or terminate existing connections. The virtual machine will be deleted when the existing connection is disconnected.

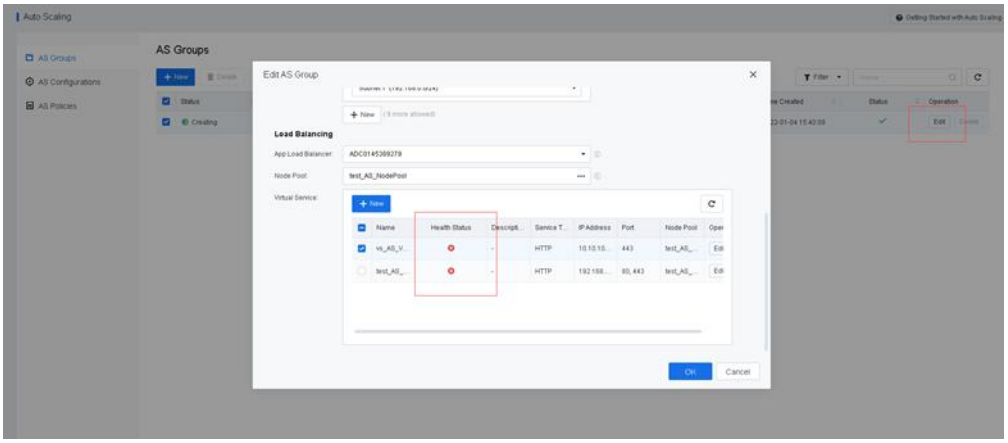


Step 7. Click **OK** to begin creating the AS policy and virtual machine.

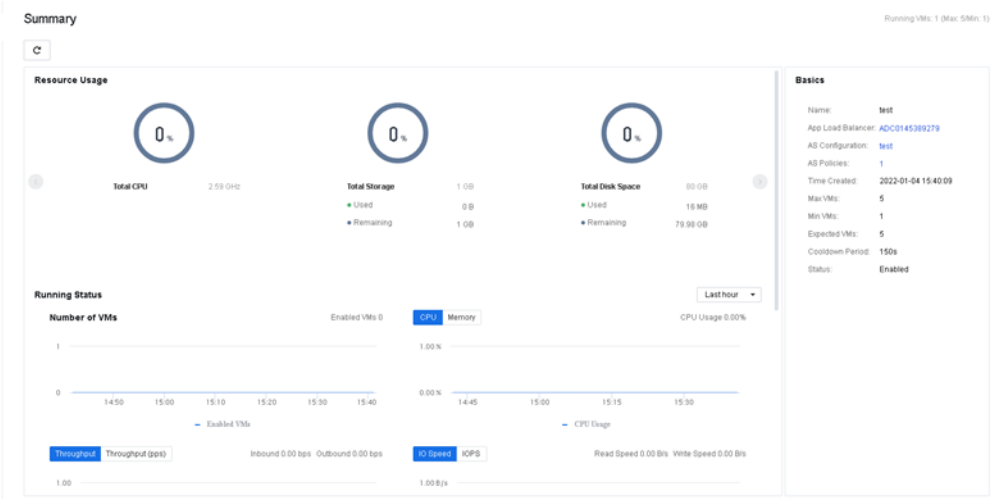


Step 8. The AS group has been created under the associated subnet.

Step 9. Click **Edit** to view the status of the node pool.



Step 10. Click the name of the AS group to view the detailed information about the AS group.



5.6.4.2 Creating AS Configuration

Features:

Create an overall AS configuration to set the specifications of the virtual machines in the AS policy.

Precautions:

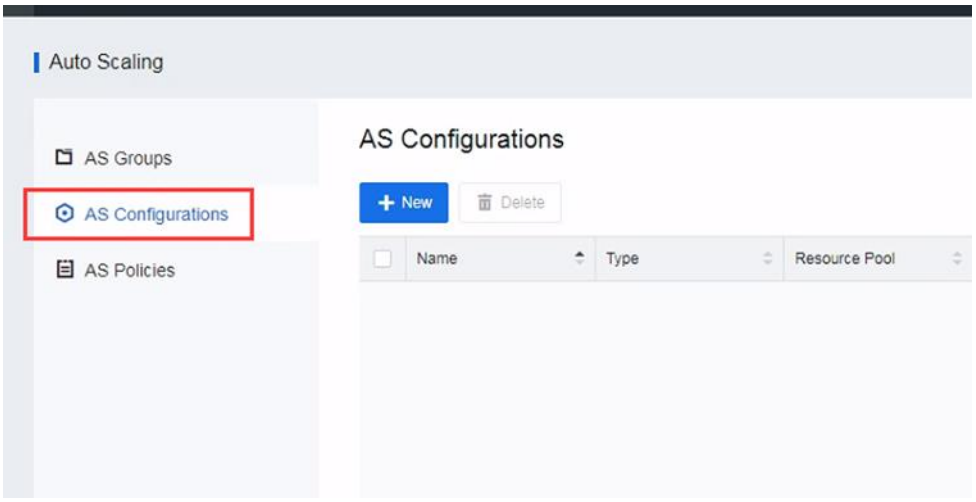
The auto-scaling virtual machine is based on built-in image deployment. Make sure that the production configuration such as business service auto-startup, listen port, and database connection is complete when creating the built-in image.

Prerequisite

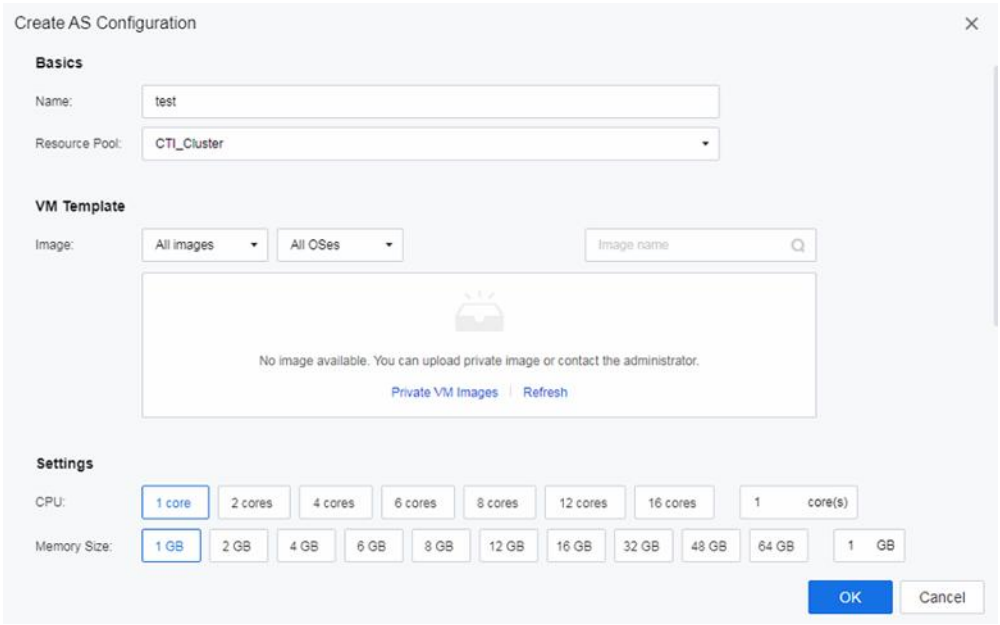
1. The built-in image has been created in advance according to the business requirements.
2. The AS configuration of the associated AS group is not allowed to delete.

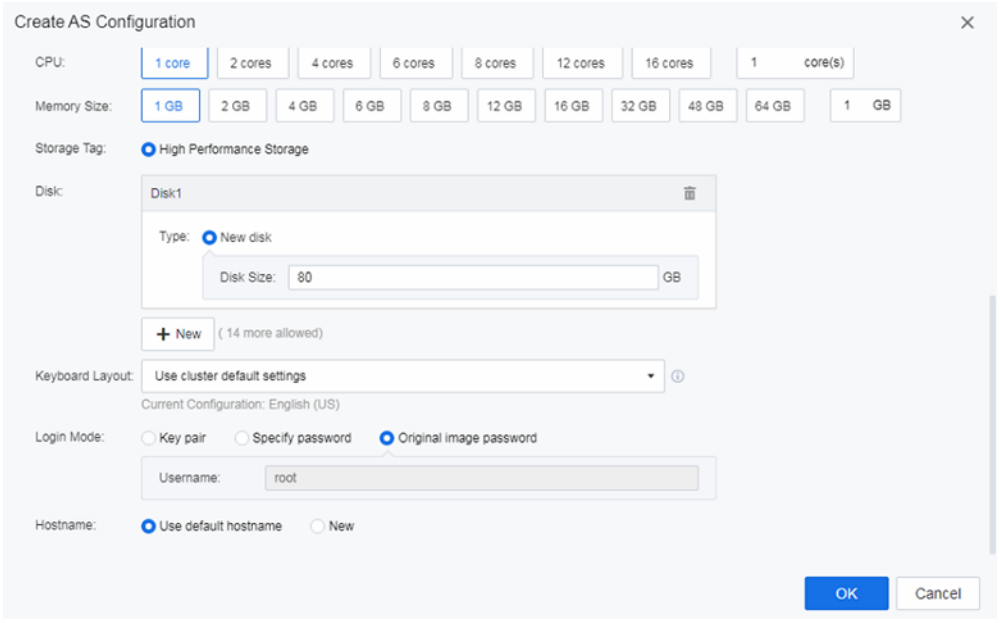
Steps:

Step 1. Log in to the tenant portal, and navigate to **Reliability** > **Auto Scaling** to choose **AS Configuration** to check the information of all the AS configurations.



Step 2. Click **New** to configure the virtual machine.





Step 3. Click **OK** to complete the link configuration. The created configuration can be found in the AS group.

5.6.4.3 Create AS Policy

Function Description:

Create an AS policy to set the scaling threshold and scaling action.

Precautions:

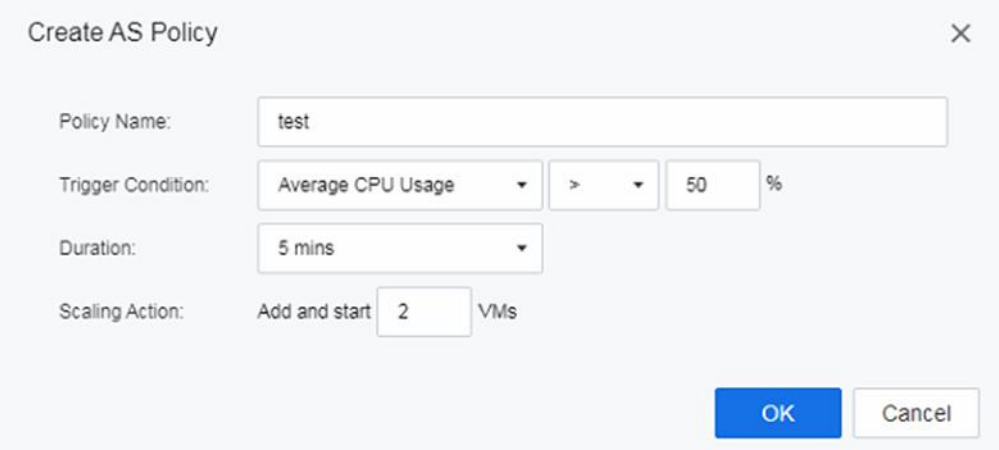
1. The policy associated with the AS group is not allowed to edit or deleted.
2. When the trigger condition is set as **Greater Than**, you can only configure for the **Add** and **Start** action. When the trigger condition is set as **Less Than**, you can only configure for the **Shutdown** and **Delete** action.
3. The threshold value monitored by the AS policy is the average value of all VMs in the AS group.

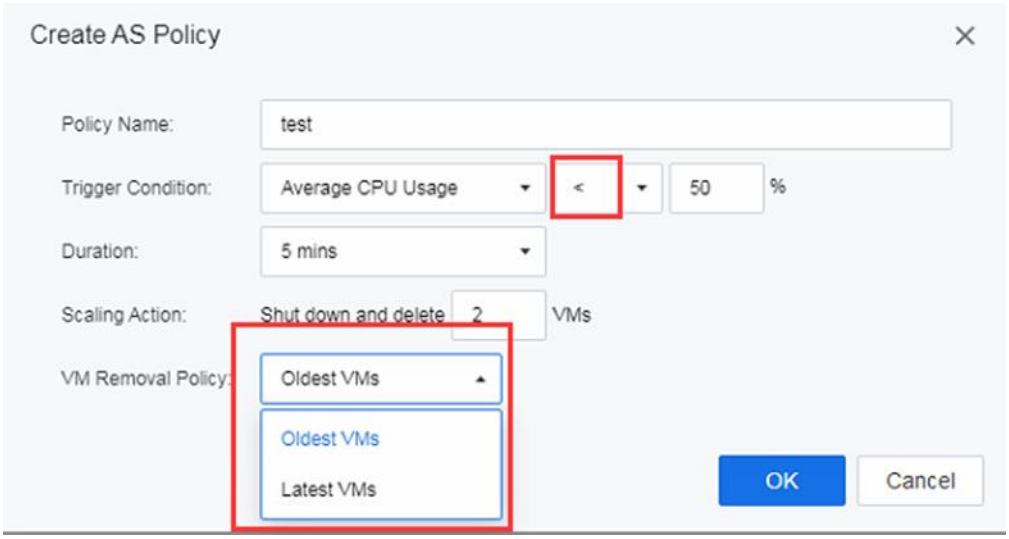
Prerequisite

N/A.

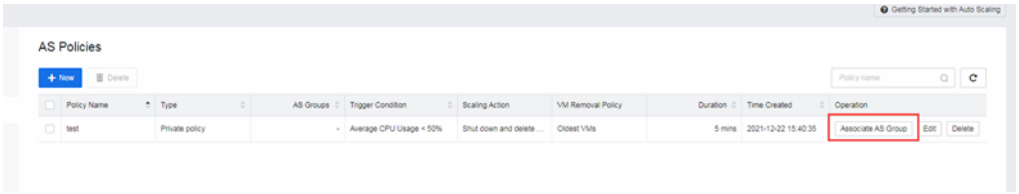
Steps:

Step 1. Log in to the tenant portal, navigate **Reliability** > **Auto Scaling,** and select **AS Policy**. Click **New** to create a new AS policy.





Step 2. Click **OK** to complete the policy creation and **Associate AS Group** to associate the policy to the corresponding AS group.



5.7 Monitor and Management

5.7.1 Monitoring Dashboard

Feature Description:

Tenants can monitor the virtual machine and elastic IP and display the monitoring information in charts by adding panels.

Precautions:

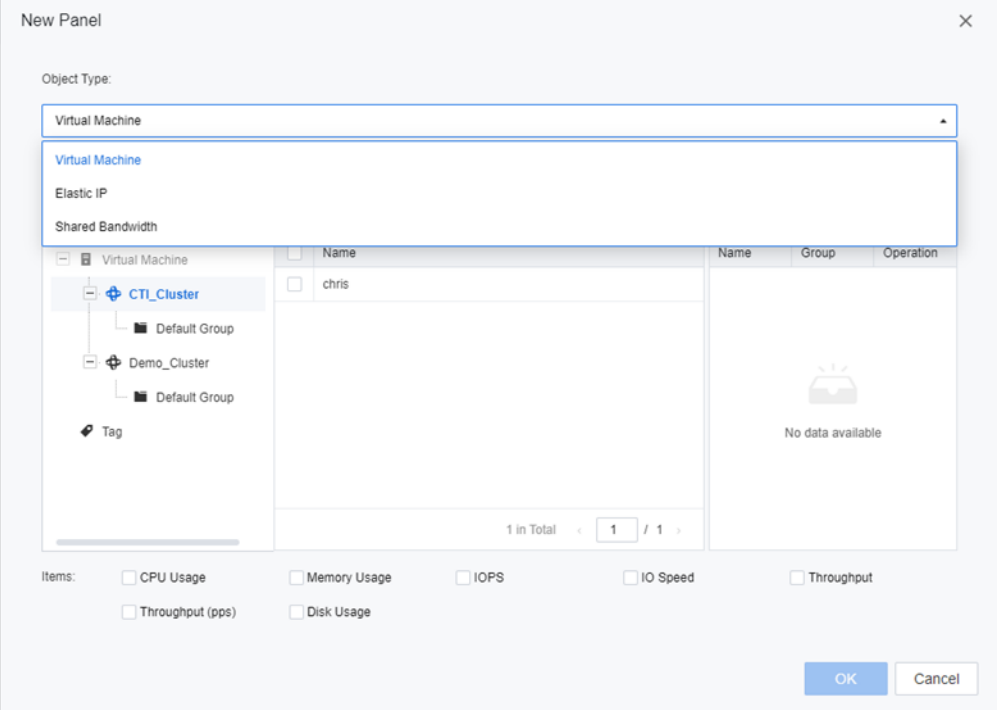
N/A.

Prerequisite

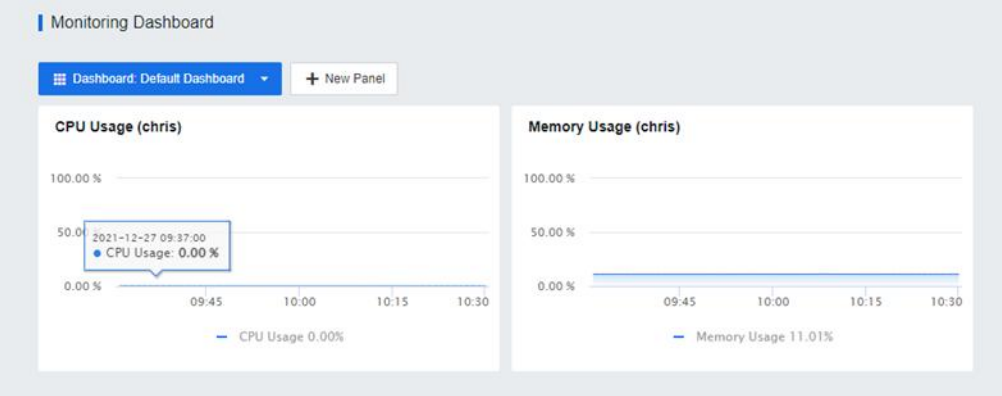
N/A.

Steps:

Step 1. Navigate to **Monitor Center** > **Monitoring Dashboard**, and click **New Panel.** Add the virtual machine, elastic IP, and shared bandwidth that requires to be monitored to the panel.



Step 2. After the addition is complete, you can monitor the virtual machine and elastic IP in the monitoring panel.



5.7.2 Alert

Feature Description:

Tenants can view all the alerts from the alert dashboard.

Precautions:

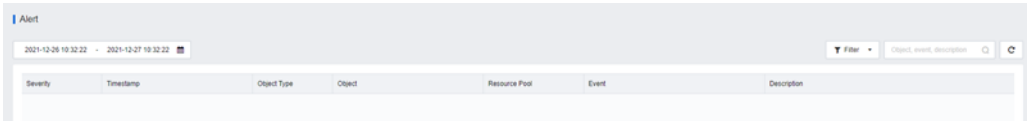
N/A.

Prerequisite

N/A.

Steps:

Step 1. Navigate to **Monitor Center** > **Alert** to view all the alerts.



5.7.3 Quota

Features:

Tenants can review the current resource usage from the quota dashboard.

Precautions:

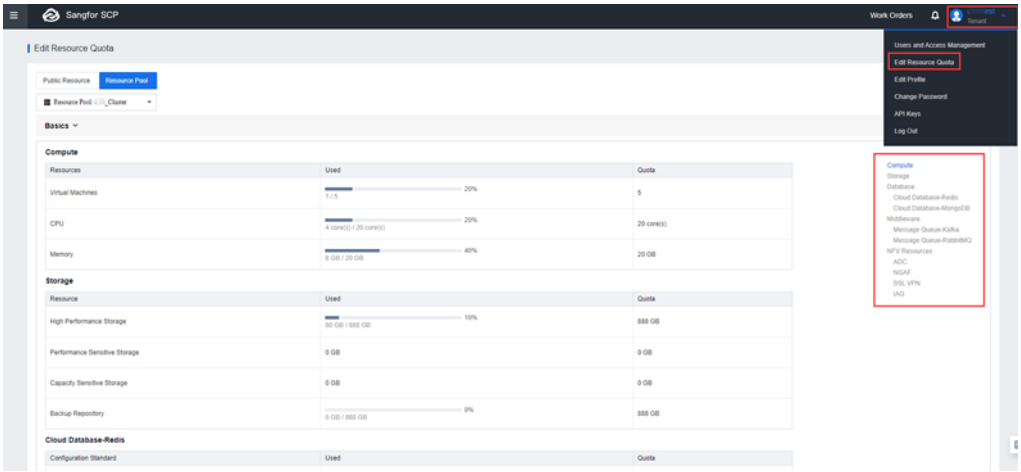
N/A.

Prerequisite

N/A.

Steps:

Navigate to the tenant profile at the top-right corner and select **Edit Resource Quota** to enter the **Quota Overview** interface. A tenant can view the usage of basic resources (computing, storage, network) and NFV resources (vAD, vNGAF, and SSL VPN).



5.7.4 Recycle Bin

Function Description:

After the tenant deletes the virtual machine, NFV device, and backup files, the deleted information will be moved to the recycle bin. Tenants can completely

delete or restore deleted information.

Precautions:

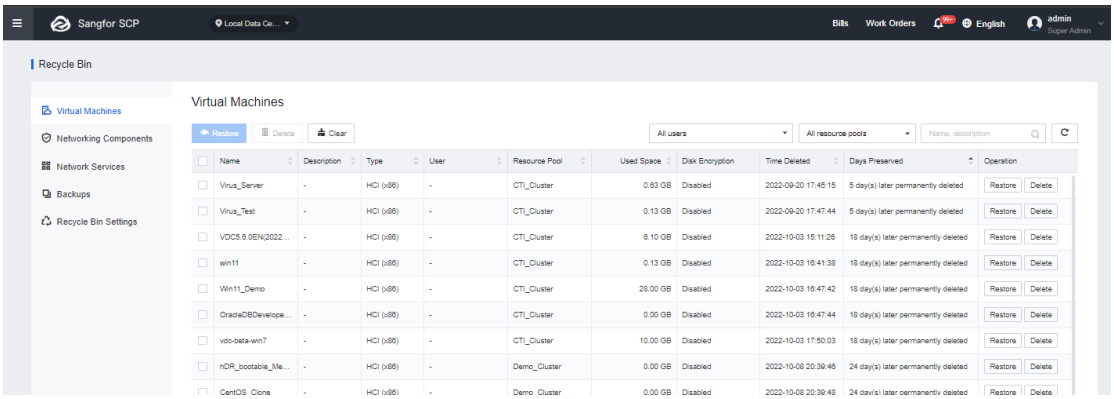
HCI6.8.0 and above are managed by SCP version 6.8.0 and above. Support modifying the number of days for file retention. Other versions do not support modification. The information in the recycle bin is saved for 30 days by default. After 30 days, the platform will automatically delete it.

Prerequisite:

None.

Steps:

1. Select **Management > Recycle Bin** to enter the Recycle Bin interface, where you can view deleted virtual machines, network components, NFV devices, and backup files.
2. Select the corresponding virtual machine, networking components, NFV device or backup file, and click **Restore** to restore the deleted virtual machine, NFV device or backup file. Click **Delete** to completely delete the deleted virtual machine, network element, NFV device, or backup file. Click **Clear** to completely delete all current files, network components, NFV devices, and virtual machine in the recycle bin.



3. Select **Recycle Bin Settings**, set the number of days to keep files, and click **Save**.

5.8 Bills

Function Description:

Tenants can view all expense records on the **Bills** dashboard. You can export the bills in Excel format.

5.9 Work Orders

Function Description:

Tenants can apply for resource quotas from the platform administrator at the **Work Orders**, approve work orders submitted by users, and view the approval history.

After submitting the work order, the tenant can cancel the work order before the administrator approves the work order to facilitate modification of the work order application content.

Precautions:

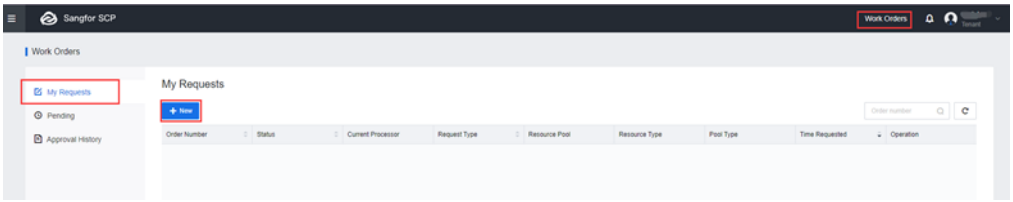
None.

Prerequisite

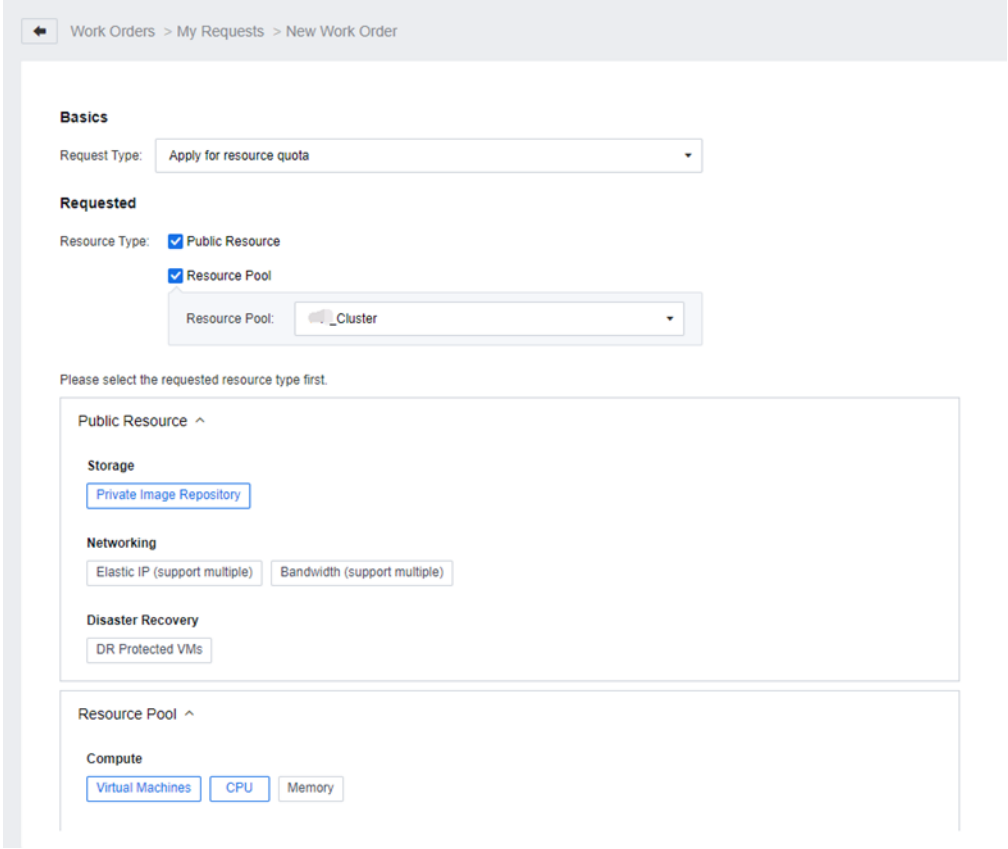
None.

Steps:

Step 1. Login tenant account from https://SCP IP, click **Work Orders**, select **My Requests**, and click **New** to apply for resource quotas.



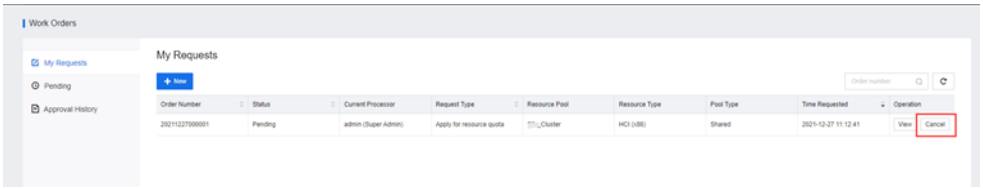
Step 2. Enter the number of resources to apply. The tenant can view the new total number of resources after applying for a quota from **New Quota**.

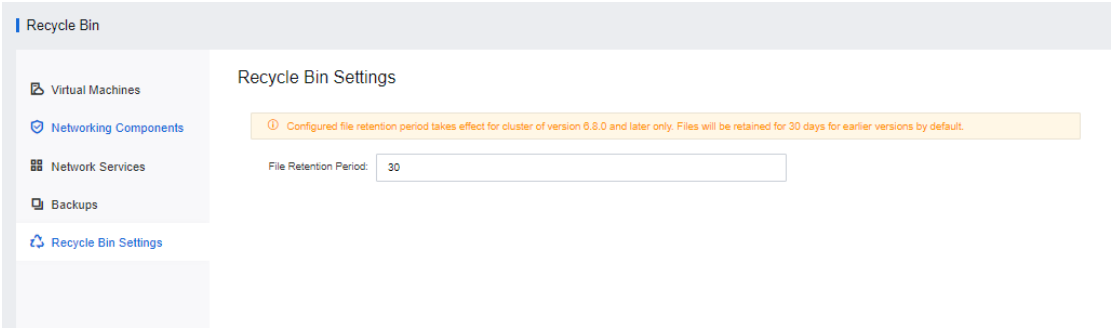


Selected:

Quota Type	Resource Type	Item	Resource Requested	New Quota	Operation
Public Resource	Storage	Private Image R...	10 GB	898 GB	
Resource Pool	Compute	CPU	10 core(s)	30 core(s)	
Resource Pool	Compute	Virtual Machines	2	7	

Step 3. Click **Apply Now** to submit an order request. Before the administrator approves the application, the submitted work order can be canceled, and modify the application information.





5.10 Tenant And Tenant Users Management

A tenant user is a basic unit in the tenant. If the tenant is a department of the company, the tenant user corresponds to the employees in the department.

5.10.1 Create User Account

Function Description:

Platform administrators can create tenant users under tenants, and tenants can also create tenant sub-accounts by themselves.

Precautions:

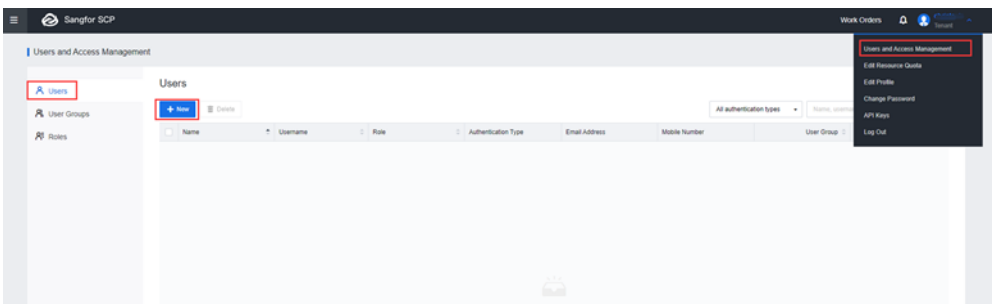
None.

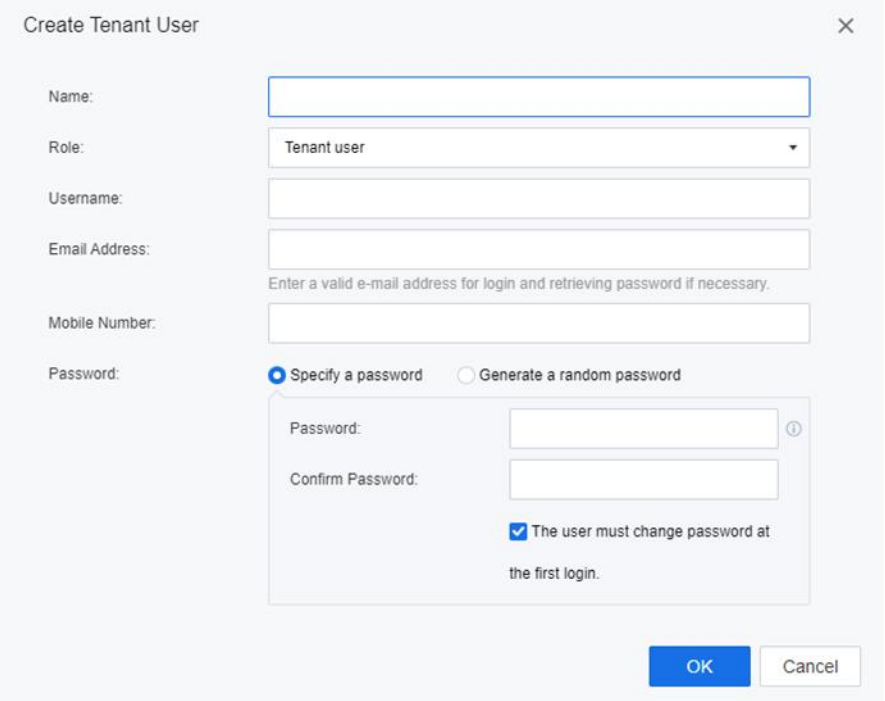
Prerequisite

None.

Steps:

Login tenant account from https://SCP IP, click **Users and Access Management** and then select **Users. Click New to create a tenant user account. Click New** to create a tenant VPC.





5.10.2 Edit Tenant User Account

Function Description:

The tenant can edit the tenant user account, including modifying the tenant user account's name, email, and mobile phone.

Precautions:

When a tenant user account uses the virtual machine under the tenant, the platform administrator cannot modify the tenant to which the tenant user account belongs. The virtual machine must be deleted or moved to recycle bin first.

Prerequisite

N/A.

Steps:

Login tenant account from https://SCP IP, click **User and Access Management, select** the corresponding tenant user, and click **Edit** for modification.

6 System Upgrade

Refer to the upgrade guide.

7 Common Troubleshooting

Search the Sangfor Community for troubleshooting guides.

8 Glossary

Terms	English Full Name	Definition
BGP	Border Gateway Protocol	Border Gateway Protocol is the only protocol that can properly handle multiple connections between unrelated routing domains. As a built-in line type of Sangfor Cloud Platform, it realizes multi-line interconnection
Backup Space	N/A	When using the backup function, the storage quota occupied by the tenant needs to provide the corresponding storage quota when applying for the tenant quota or when the administrator allocates the quota.
CDP	Continuous Data Protection	Continuous data protection is an advanced backup technology at the IO second level, which can record every data change and optimally achieve RPO=1s to protect data. Sangfor Cloud Platform adopts optimized CDP technology and provides customers with low-cost, easy-to-deploy, and high-value data protection solutions using the CDP module at the file layer.
Super Administrator	N/A	The super administrator (also known as the admin user) has all the operation and operation and maintenance management permissions. It is the role with the most permissions in the multi-tenant model of the entire Sangfor cloud platform.
DRS	Distributed Resource Scheduler	Dynamic resource scheduling technology. Sangfor Cloud Platform continuously and dynamically balances resources through the introduced automation mechanism, migrates virtual machines to hosts with more available resources, ensures that each virtual machine can call corresponding resources in a timely manner, and guarantees business systems performance.
Allocation	N/A	Platform administrators can assign virtual machines in the administrator's root directory to corresponding virtual machine groups or tenants, and tenants can also allocate virtual machines under their directories to

		corresponding virtual machine groups or tenant sub-accounts.
HA	High Available	A high-availability cluster usually requires two or more nodes to form a cluster. When an accident occurs on the node where the virtual machine with the HA function is enabled (the host is powered off, the network is disconnected, etc.) Select a node with sufficient resources to automatically restart the virtual machine to achieve uninterrupted or short business interruption. Sangfor cloud platform provides high-availability node services. When an abnormality is found, and the duration reaches the fault detection sensitivity set by the customer (for example, 5 minutes), the HA virtual machine will be switched to run on another node.
Deallocate	N/A	The platform administrator can deallocate the virtual machine whose permissions belong to the tenant to the administrator's root directory, and the tenant loses the use permission of the corresponding virtual machine. Tenants can also reclaim virtual machine corresponding to tenant sub-accounts.
Recycle Bin	N/A	It temporarily stores the deleted platform administrators, tenants, and other VM resources, network resources, and backup resources. In addition, the deleted resources can be recycled.
Work Order	N/A	The multi-tenant, self-service IaaS service provided by Sangfor Cloud Platform is a brand-new infrastructure delivery and usage model, which can abstract IT physical resources into elastic virtual resource pools provided on demand, including virtual machine, storage, network, Network security, providing external services in the form of consumer units (i.e., tenants or virtual data centers) and providing users with these consumer units and other infrastructure including virtual machine and operating system images through fully automated self-service access Schema and

		application service templates.
Cluster	N/A	The physical hosts with the HCI virtualization software installed are uniformly added to a management platform for maintenance, which is convenient for business deployment and can also improve the effective utilization of resources. Generally, it is used in conjunction with virtual storage. Sangfor cloud platform can add multiple clusters to perform unified resource management in the form of resource pools.
Role	N/A	Sangfor cloud platform built-in user types, different roles have different permissions and functions. The platform preset roles are divided into admin, tenant, and tenant user.
Image	N/A	An elastic server template that includes software and necessary configuration, at least the operating system, and can also include application software (such as database software, development tools, etc.) and proprietary software. Sangfor SCP images can be divided into Public VM Images, Private VM Images, and Network Device Images.
Clone	N/A	Generate an identical virtual machine through cloning to improve business deployment efficiency.
Snapshot	N/A	The status record of a certain moment of data storage, Sangfor cloud platform records the status of qcow2 at the snapshot moment by taking a snapshot of qcow2, that is, the data location described by the qcow2 file at that time. The data recovery of the virtual machine can be performed through the snapshot at this moment.
Template	N/A	Take a current virtual machine as the main body, convert it into a template (shutdown and locked state), and then derive N virtual machines consistent with the current template status. The image file of the derived virtual machine refers to the template image file and its incremental image and can configure the data disk.

NFV	Network Function Virtualization	Network function virtualization. Sangfor cloud platform realizes various network function resources required in the network through NFV, allocates and flexibly schedules on demand to realize network function virtualization in cloud architecture.
Quota	N/A	The usage and allocation of basic resources (computing, network, storage resources) and NFV resources in the Sangfor cloud platform. Tenants can apply to the administrator to use related resources. Administrators can also learn about the resource usage of the entire cloud platform through quota usage.
Direct line	N/A	The virtual machine in the VPC needs to communicate with the tenant's local data center under the cloud or the equipment hosted in the equipment room. Two different parts of the network.
SCP	Sangfor Cloud Platform	Sangfor cloud computing platform is the general term for the entire cloud platform management architecture.
Private Image Repository	N/A	The storage quota occupied by cloud platform tenants for uploading images or creating images needs to be provided when applying for tenant quotas or when assigning quotas by administrators.
Elastic IP	N/A	For the IP addresses that can be accessed outside the Sangfor cloud platform, you can bind the elastic IP to the corresponding virtual machine in the tenant or the VPC egress router to access resources outside the VPC.
VPC	Virtual Private Cloud	For the IP addresses that can be accessed outside the Sangfor cloud platform, you can bind the elastic IP to the corresponding virtual machine in the tenant or the VPC egress router to access resources outside the VPC.
VXLAN	Virtual Extensible LAN	A network virtualization technology. An extension of VLAN technology can penetrate the third-layer network to expand the second layer. The central two-tier virtual migration and multi-tenancy requirements.

Tenant	N/A	The tenant administrator has the management rights of all resources and tenant sub-accounts in the tenant and is the second-level management role in the Sangfor multi-tenancy model.
Tenant User	N/A	Tenant users have administrative rights to the virtual machine resources associated with them. The tenant user is the third-level role in Sangfor's multi-tenancy model.
Resource Pool	N/A	The collection of cluster resources on the Sangfor cloud platform can associate clusters that have been added to the cloud platform to different resource pools, manage resource pool resources through the cloud platform, and allocate resources to tenants for use.
Resource Reservation	N/A	Reserve a certain resource space on some nodes. The system or other virtual machines will not use this part of the resources. When a node fails or is switched for disaster recovery, the reserved node resources can immediately restore the virtual machine, reducing the risk of business failure recovery due to insufficient resources. Risk of failback failure.
Create Image	N/A	The platform administrator can select a virtual machine configured according to requirements and use it as a template to create an image. The image created by this method will retain all the software and data of the virtual machine system disk. Using this method to create an image requires the target virtual machine to be shut down and installed with an operating system and Sangfor vmTools.
Shared Service Network	N/A	Sangfor SCP introduces public service regions, designates a public service edge for each resource pool, and builds a public service network as a dedicated channel between public service regions and resource pool tenants.
DR test virtual machine	N/A	During the disaster recovery drill, a new test virtual machine will be generated at the secondary site. The drill virtual machine is not configured with any connection and will not

		affect the disaster recovery node and business network.
Application Center Service Mapping Routing	N/A	Application center service mapping routing: The router deployed between the SCP and the public service network egress implements address communication from the application center to the public service network through address translation.

9 Abbreviations

Abbreviations	English Full Name
AC	Access Control
AD	Application Delivery
NGAF	Application Firewall
aHM	Heterogeneous Management
AI	Artificial Intelligence
API	Application Programming Interface
BMC	Baseboard Manager Controller
CDP	Continuous Data Protection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DRS	Dynamic Resource Scheduling (DRS)
HA	High-Availability
HCI	Hyper-Converged Infrastructure
IaaS	Infrastructure as a Service
ICMP	Internet Control Message Protocol
IPMI	Intelligent Platform Management Interface
LDAP	Lightweight Directory Access Protocol
NAT	Network Address Translation
NFV	Network Functions Virtualization
NGFW	Next Generation Application Firewall
NTP	Network Time Protocol
PaaS	Platform as a Service
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SCP	Sangfor Cloud Platform
SMTP	SimpleMail Transfer Protocol
SSO	Single Sign On
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

vAD	Virtual Application Delivery
vAF	Virtual Next General Application Firewall
VPC	Virtual Private Cloud

