



SANGFOR

aCMP

User Manual

Version 5.8.6



Change Log

Date	Change Description
Oct 22, 2018	Edited the aCMP user manual

CONTENT

Chapter 1 Overview	5
1.1 Brief Introduction of aCMP Products	5
1.2 aCMP Architecture	8
1.3 aCMP Key Characteristics	9
Chapter 2 Installation and Upgrading	18
2.1 New deployment	18
2.2 Deployment of Operating and Standby Units (If Necessary)	20
2.3 Network Configuration	24
2.4 aCMP Activation	28
2.5 Add Physical Resources	33
2.6 aCloud Cluster Licensing	37
2.7 NFV Licensing	38
2.8 Division of Availability Zone	40
2.9 Upgrade.....	42
2.10 Delete Cluster	45
Chapter 3 Operation Maintenance and Management.....	48
3.1 Basic Management	49
3.1.1 System Configuration	49
3.1.2 System Maintenance	52
3.1.3 Business Maintenance.....	53
3.2 Resource Management.....	54
3.2.1 Image Management	54
3.2.2 Management of virtual machine	63
3.3 Reliability Center	78
3.3.1 Holistic View	78
3.3.2 Business Reliability	81
3.3.3 Disaster Recovery Plan	88
3.3.4 aCMP Reliability.....	109
3.3.5 Hardware Reliability	113
3.3 Operations Center	115
3.3.1 Users.....	115
3.3.2 Work Order.....	124
3.3.3 Billing	131

3.4	Monitoring Center	133
3.5	Network Administration	133
3.5.1	Network Topology.....	133
3.5.2	Distributed Firewalls	136
Chapter4	FAQ	138

Chapter 1 Overview

SANGFOR Cloud Management Platform aCMP can manage cross-region clusters and provide heterogeneous management support for VMware data centers, which can divide the managed pool of resources into multiple logically availability zones, realizes the customized approval process and billing functions through the setting of classified administrator authority. It also enhances the network management and security among tenants, and tenants can configure their own firewall, and the flexible image management can effectively reduce the workload of platform management personnel in operation and maintenance. On the other hand, in terms of business reliability, through remote disaster recovery services, it provides users with a complete virtual machine-level remote disaster recovery plan.

This chapter mainly introduces and explains the SANGFOR aCMP products in detail, including product introduction, architecture and key features.

1.1 Brief Introduction of aCMP Products

SANGFOR aCMP cloud management platform can provide abundant management capabilities. First of all, in the resource creation phase, it can put multiple data centers under heterogeneous management. These data centers may be either cross-regional clusters or VMware data centers. In terms of authorization, it supports uniform authorization; in other words, In case of heterogeneous management of multiple aCMP clusters, only one aCMP authorized import is need, while all the authorizations of other clusters under heterogeneous management may be distributed as needed through the aCMP authorization. On the tenant side, it has abundant tenant management functions. On the one hand, the administrator may customize the approval process, and on the other hand, the tenant may submit the independent service work order application resources, which should be used and charged reasonably through multiple levels of resources charging functions. In terms of security, in multi-tenant scenarios, it supports tenants to configure their own distributed firewall policies without conflicting with platform administrators' policies; in terms of management, a single cluster can support up to 64 hosts, support the tenants' subnet topology display, and can provide API interfaces conforming to the openstack specification for third parties; in terms of hardware, it provides support for INTEL's latest V5 CPU.

On the other hand, SANGFOR operation management platform aCMP integrates three centers: Reliability Center, Operations Center and Monitoring Center. Among them, Reliability Center can provide users with a complete virtual machine-level remote disaster preparedness plan, including disaster recovery plan, disaster recovery drill, virtual machine recovery and relocation, visual operation and maintenance, etc. "Operations Center" can provide users with a wide range of

management options, including multi-tenant, autonomous work order, flow billing, authority management and VMware heterogeneous management capabilities; and "Monitoring Center" can provide users with a multi-dimensional monitoring perspective, which supports the monitoring from both the platform and business levels to ensure the business runs normally in all respects.

The list of SANGFOR aCMP product features is shown in the following table:



: This table only lists the basic functions supported by SANGFOR aCMP.

Please consult the after-sales technical service engineer of the local office for specific configuration implementation and other functions.

Table 1-1 aCMP Product Function List

Affiliated Components	Function Items	Descriptions of Functions
aCMP cloud management platform	Multi-tenant	Support multi-tenant access
aCMP cloud management platform	Self-service work order	Support tenant work order self-service application
aCMP cloud management platform	Customization of approval process	Support the layout approval process and support multi-level examination and approval.
aCMP cloud management platform	Billing and measurement	Charging for tenants' CPU, memory and storage
aCMP cloud management platform	Support VMware VDC functions	Support the editing of VMware virtual machine configuration on cloud management platform (supporting CPU editing, memory, hard disk, network).
aCMP cloud management platform	Multi-tenant distributed firewall	Multi-tenant scenario: it supports tenants to configure their own distributed firewall policies without conflicting with the policies configured by super administrators.

aCMP cloud management platform	Tenant topology display	Multi-tenant scenario: support the administrator zooming method to display the tenant virtual network topology, supports the tenant sub-topology rendering.
aCMP cloud management platform	Multi cluster & multi-data center management	Support cross-regional cluster management and support the heterogeneous management of VMware
aCMP cloud management platform	Authority management	Set different administrative authorities for different administrators.
aCMP cloud management platform	Image management	Support image distribution and management of different partitions
aCMP cloud management platform	Unified authorization	Authorization for managing single or multiple acloud clusters on the cloud management platform
aCMP cloud management platform	Integration capability	Cloud management provides API to third party in line with openstack specification.
aCMP cloud management platform	Reliable Center	General Drawing of Provision of Reliability Services
aCMP cloud management platform	Disaster recovery management	Provide a complete VR remote disaster recovery plan
aCloud	Data striping	Further optimize virtual storage performance
aCloud	Big cluster	A single cluster supports up to 64 hosts
aCloud	Support INTEL V5CPU	Provide the latest INTEL CPU support

The recommended deployment modes are as follows:

1. The aCMP is deployed on the aCloud cluster in the form of virtual machine.
2. aCloud cluster IP and user password are added voluntarily to aCMP to conduct heterogeneous management over aCloud cluster.
3. vcenter cluster user IP and password are added voluntarily to aCMP to conduct heterogeneous management over VMware.



Note: aCMP does not currently support deployment on VMware and physical machines.

1.2 aCMP Architecture

From the perspective of business stratification, the architecture of SANGFOR aCMP cloud management platform is as follows:

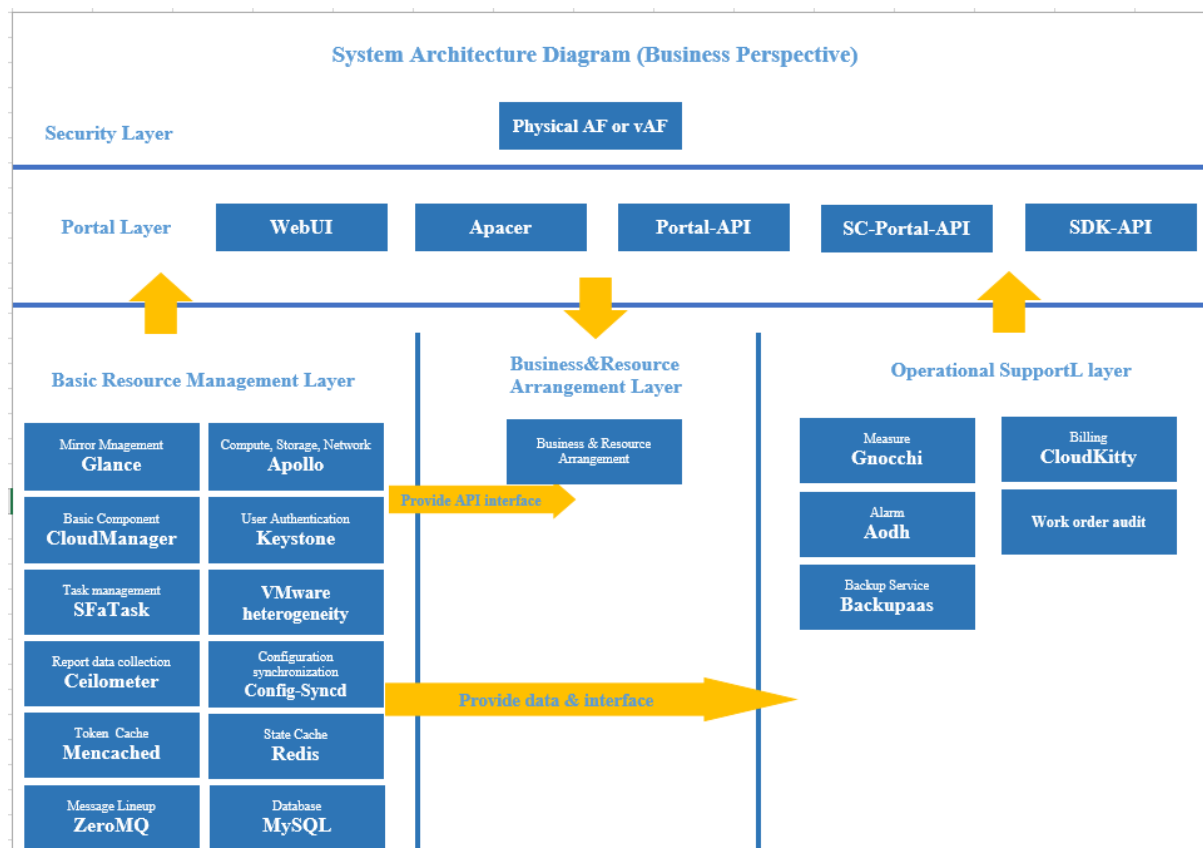


Fig. 1-1 aCMP System Architecture Diagram

In view of the above Fig. 1-1, it is briefly explained as follows:

The micro-service architecture is adopted at the overall back-end, which supports horizontal scaling, low coupling, building block-type, stateless and inter-module REST API communication and maintains decoupling;

- With the separation of aCMP and aCloud architectures, cloud management architectures can provide rapid evolution and upgrade based on the actual needs;
- aCMP is decoupled from aCloud architecture to ensure aCloud architecture is stable with high performance;
- With the front-end display and back-end separation, back-end configuration customization, it can quickly integrate and display data;
- Standardized API interface can facilitate the integrated development by a third party;
- Internal RPM management shall be used to support module decoupling and upgrade;
- The MongoDB's front-end reading/writing separation architecture supports large concurrency;
- The three-level role system based on keystone extension (admin, tenant and user) has more flexible management dimensions than the two-level role of Openstack (admin and tenant);
- Based on the self-developed Phoenix framework on Openstack, it solves the problem that Openstack service architecture is too redundant while maintaining the advantages of Openstack architecture;
- The Gnocchi module redeveloped based on Openstack has been greatly improved compared with the performance of official Gnocchi;

1.3 aCMP Key Characteristics

● Multi-cluster Management

aCMP unifies the management of resources such as infrastructure, availability zones, cloud services and tenant applications.

The deployment mode of aCMP 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 Fig. 1-2:

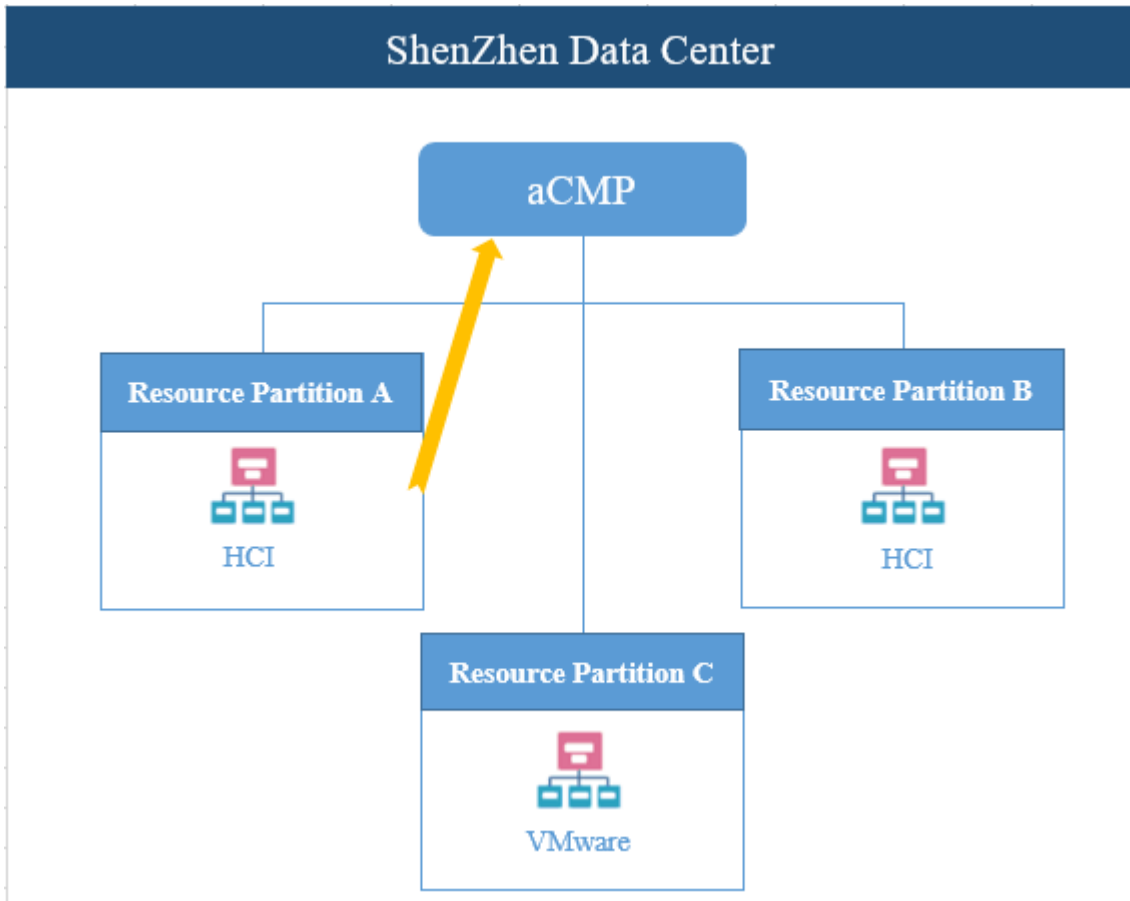


Fig. 1-2 Multi-cluster Deployment of Single Data Center

At the same time, aCMP supports the cross-regional heterogeneous management of multiple clusters from multiple data centers. Its deployment logic topology is shown in Fig. 1-3:

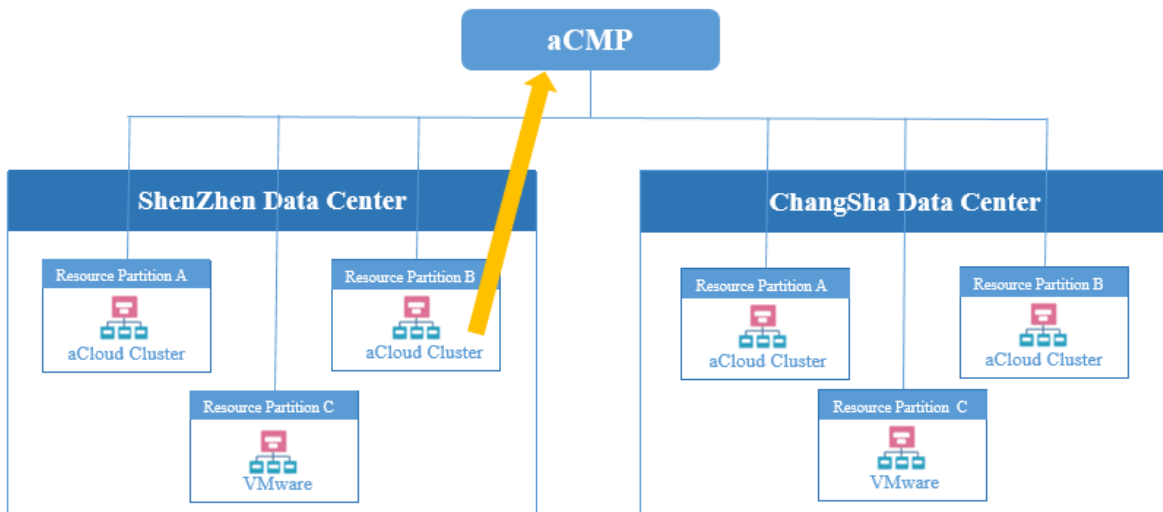


Fig. 1-3 Multi-cluster Deployment of Multi-Data Center

● Multi-tenant management

In order to meet the operational management requirements of the platform for the organization, SANGFOR aCMP can set up a maximum of three user management levels, namely platform management, organization management and end users. The relationship between management responsibilities and levels is shown in Figure 1-4.

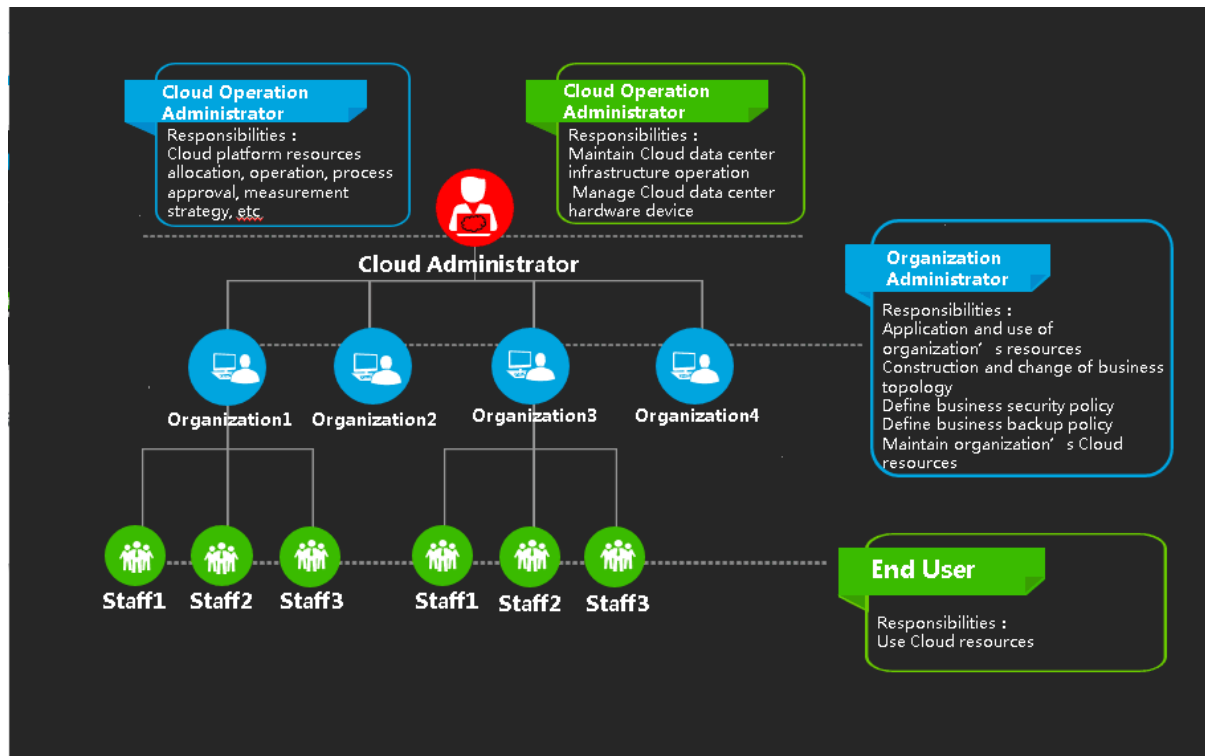


Figure 1-4 aCMP User Management Level

● Self-service function

Orders will be automatically generated after users applying for or managing 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 process is shown in Fig. 1-5.

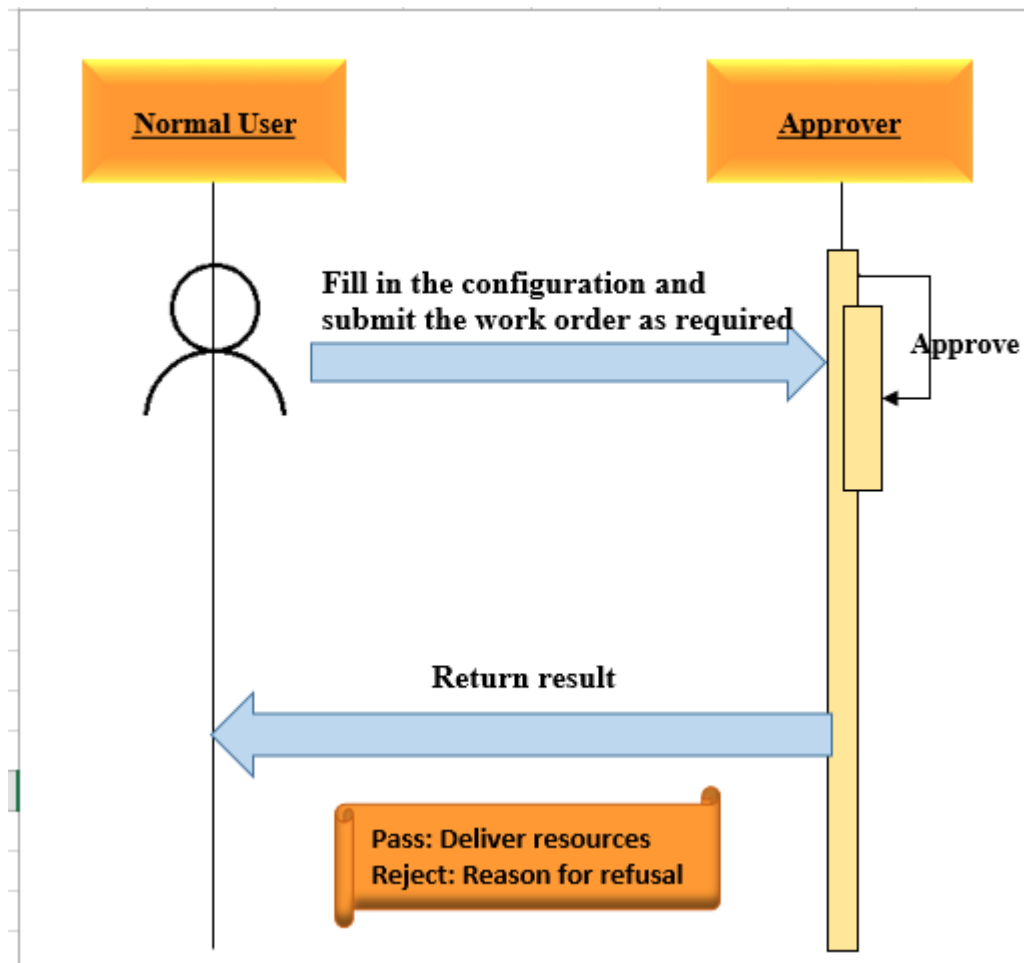


Fig. 1-5 Application Process of Self-service Work Order

- Multi-tenant Distributed Firewall

SANGFOR aCMP can provide tenants with space isolation, support tenants to configure their own distributed firewall policies, without conflicting with platform administrators' configuration policies. The logical diagram of the failure domain is shown in Fig. 1-6.

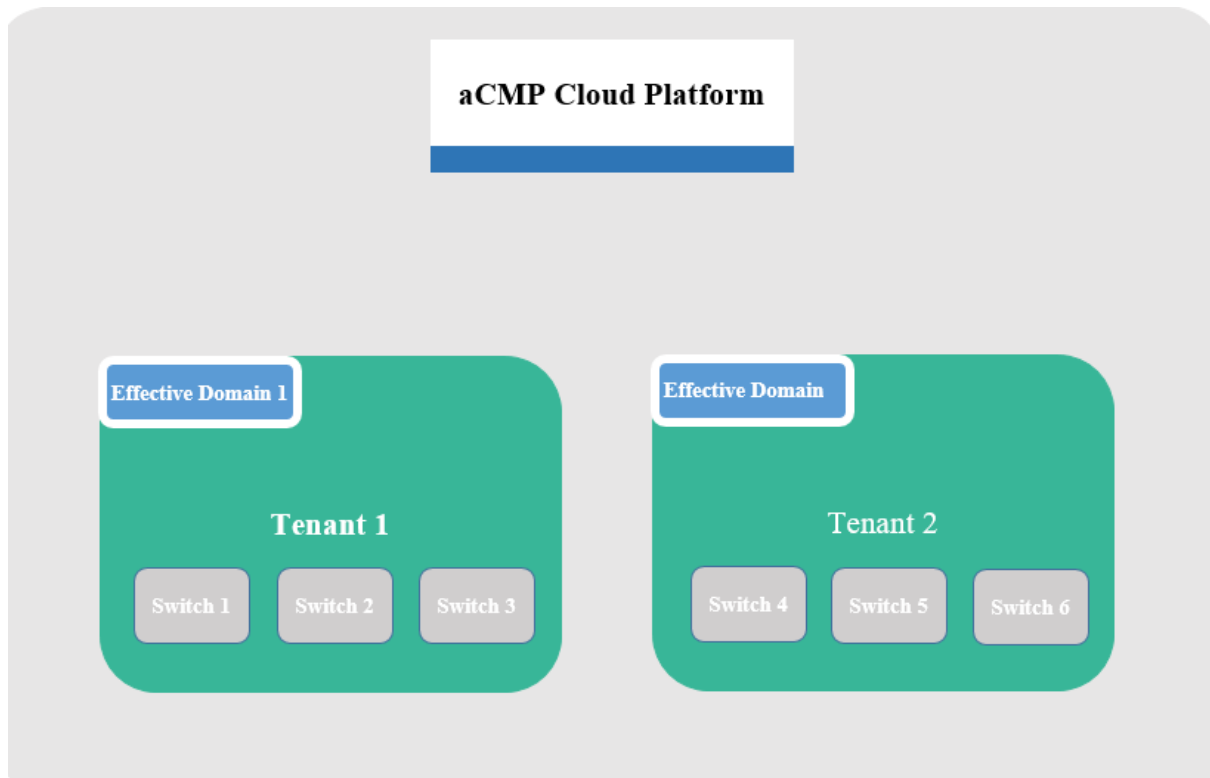


Fig. 1-6 Multi-tenant Distributed Firewall

Distributed firewall rules within each tenant will only be issued to its own switch to take effect, to achieve the firewall rule isolation between tenants and between tenants and platforms.

● Image unified management

- Provide unified image management functions to achieve unified creation and management of images on all aCloud availability zones.
- In the multi-tenant mode, the administrators can customize the organization administrator. In the organization, the public image provided by the platform administrator can be used in the organization, or the customized private 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 in Fig. 1-7:

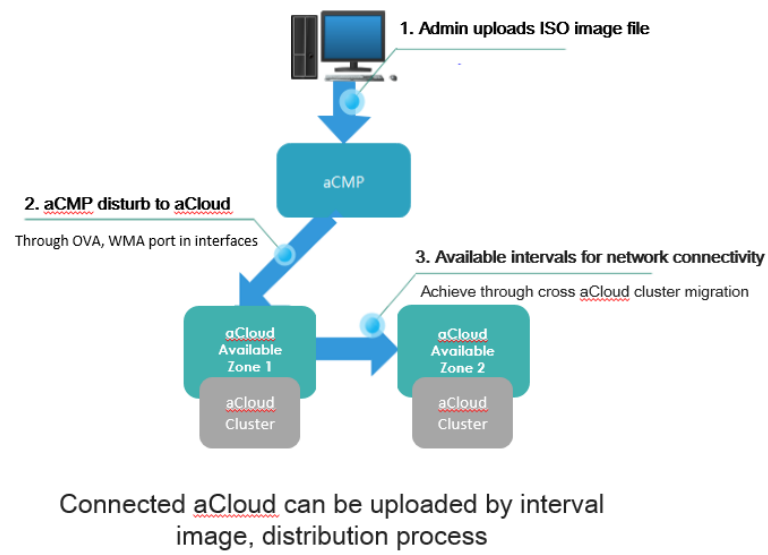


Fig. 1-7 Image Management

● Unified Licensing

The whole cloud management platform only needs one authorization to satisfy the authorization of all hosts under the cloud management platform, realizes the unified management and flexible control of authorization, and solves the problems that authorization cannot drift between clusters and the change of extended authorization. The mode of authorization is shown in Fig. 1-8:

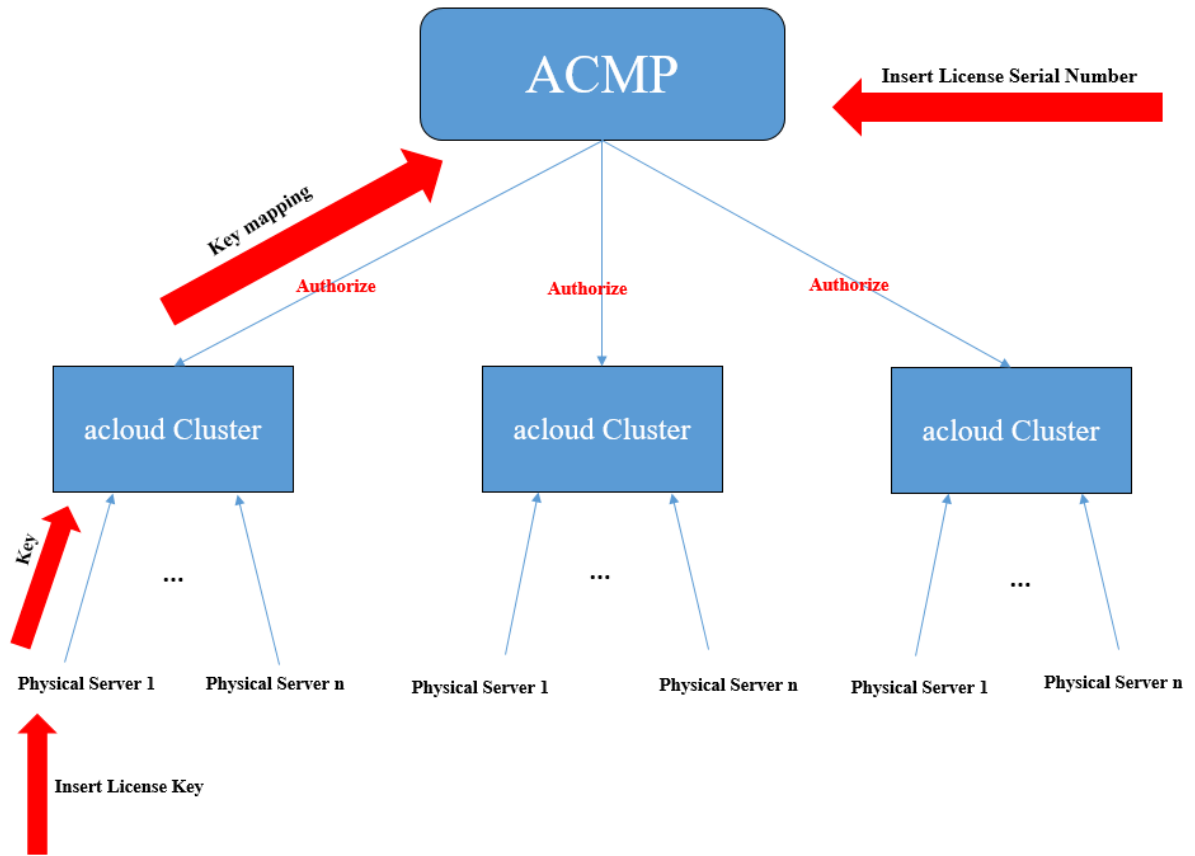


Fig. 1-8 Authorized Management

- **Standard API Interface**

SANGFOR aCMP 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 in Figs. 1-9 and 1-10:

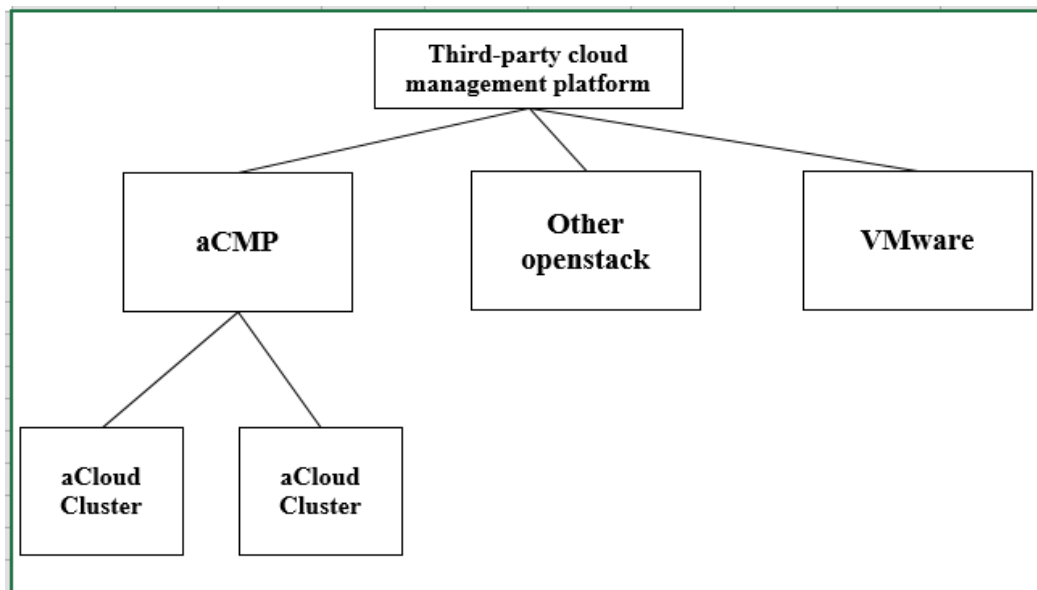


Fig. 1-9 Unified Interface

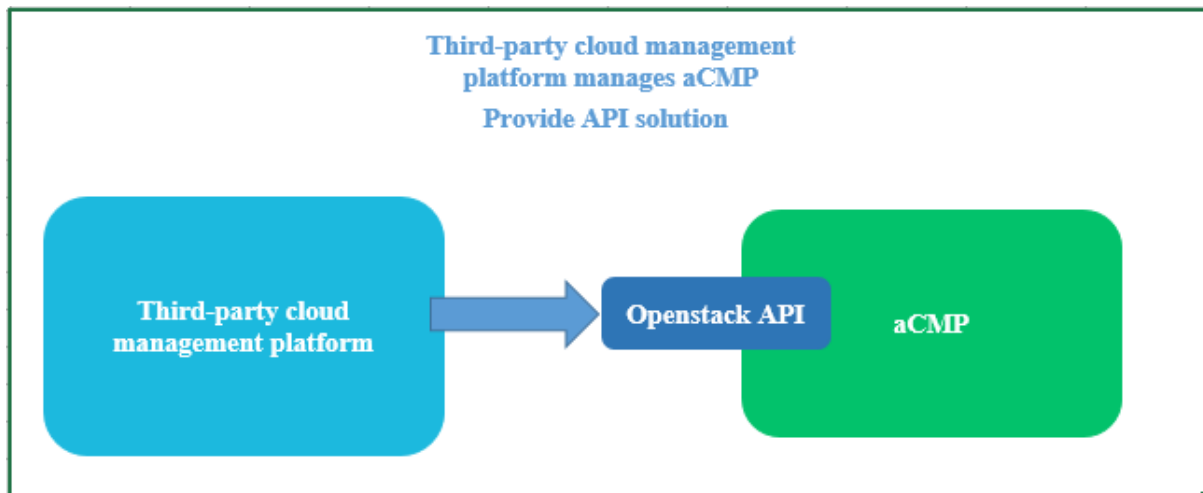


Fig. 1-10 Third Party Integration

- **Big Cluster Deployment**

SANGFOR aCMP cloud management platform can support the deployment of a maximum of 64 servers in the single cluster.

- **Customized Approval Process**

Flexible work order approval process to meet different customer management requirements.

- **Management of Measurement and Billing**

- Transparency and visualization of multi-tenant computing resource usage
- Transform the cost center of the data center into the profit center by charging for resources used by the secondary units and subsidiaries by the quantity
- Convenience for the industry cloud to charge for resources used by each tenant and facilitate the resource settlement with the tenant
- Provide resource availability report which can be exported.

- **Put VMware VDC under heterogeneous management**

It can unify the heterogeneous management of VMware data center and provide a unified management mode of aCloud and VMware.

- **Hardware Support**

It supports aCloud platform to support INTEL v5 CPU server.

● Disaster recovery services

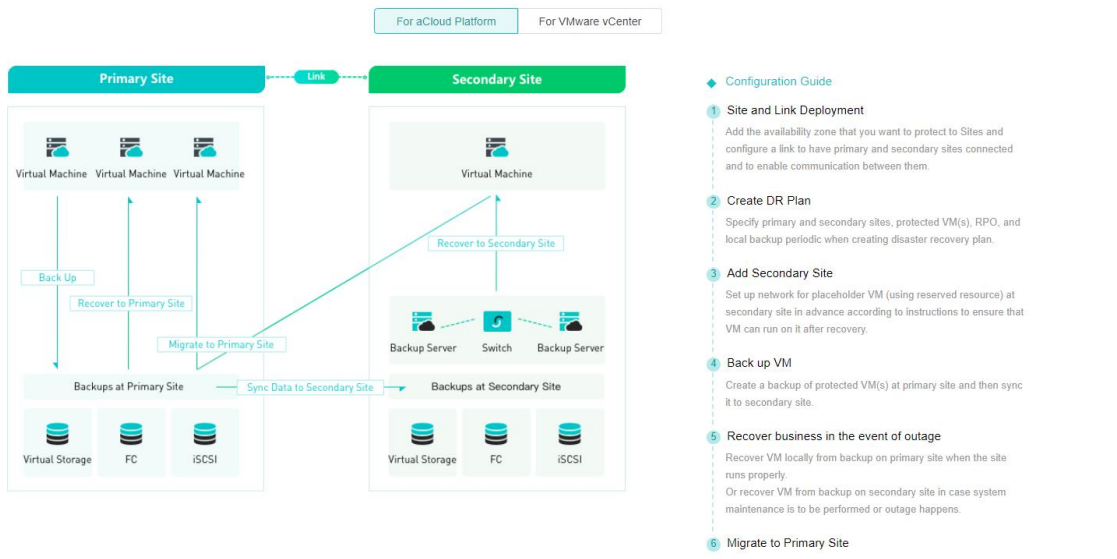


Figure 1-11

SANGFOR disaster recovery plans provide a "local backup - remote disaster recovery" plan, where the primary site configures storage (external storage or VS) for the purpose of local backup storage, and the secondary site configures an aCloud cluster as the disaster recovery center.

● Reliability Center

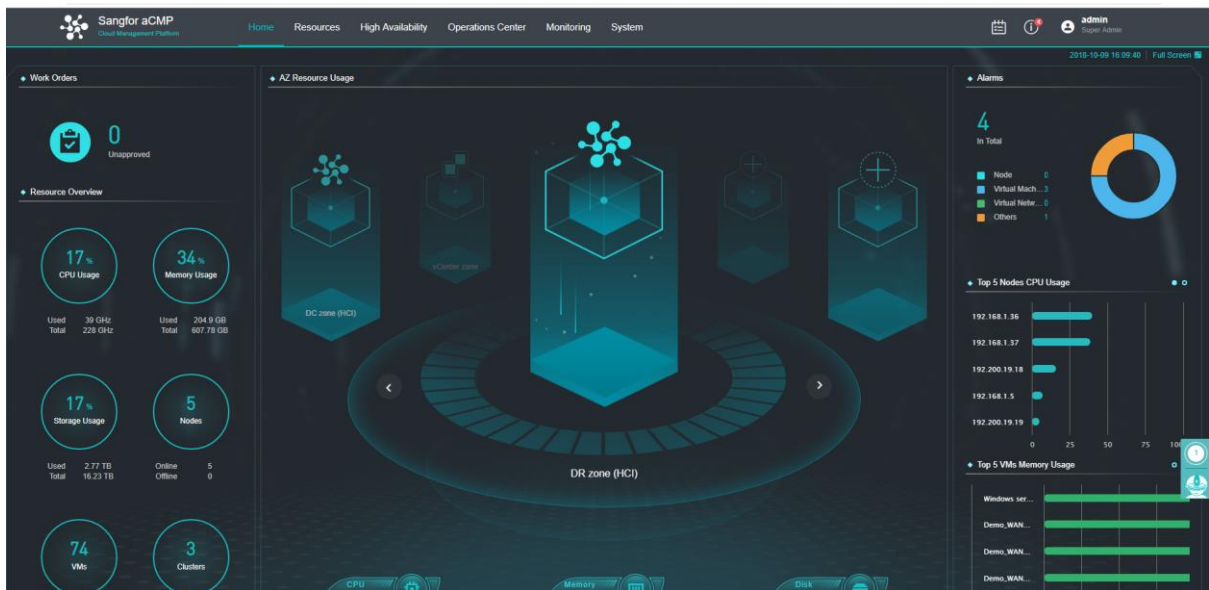


Figure 1-12

- Provide a complete business protection service, integrated in a unified platform, which is reusable and reliable.

-
- Simplest operation and maintenance mode of visualization with reliable resources and one-key availability of services

Chapter 2 Installation and Upgrading

2.1 New deployment

[Function description]

Deploy a new SANGFORE aCMP cloud management platform.

[Prerequisites]

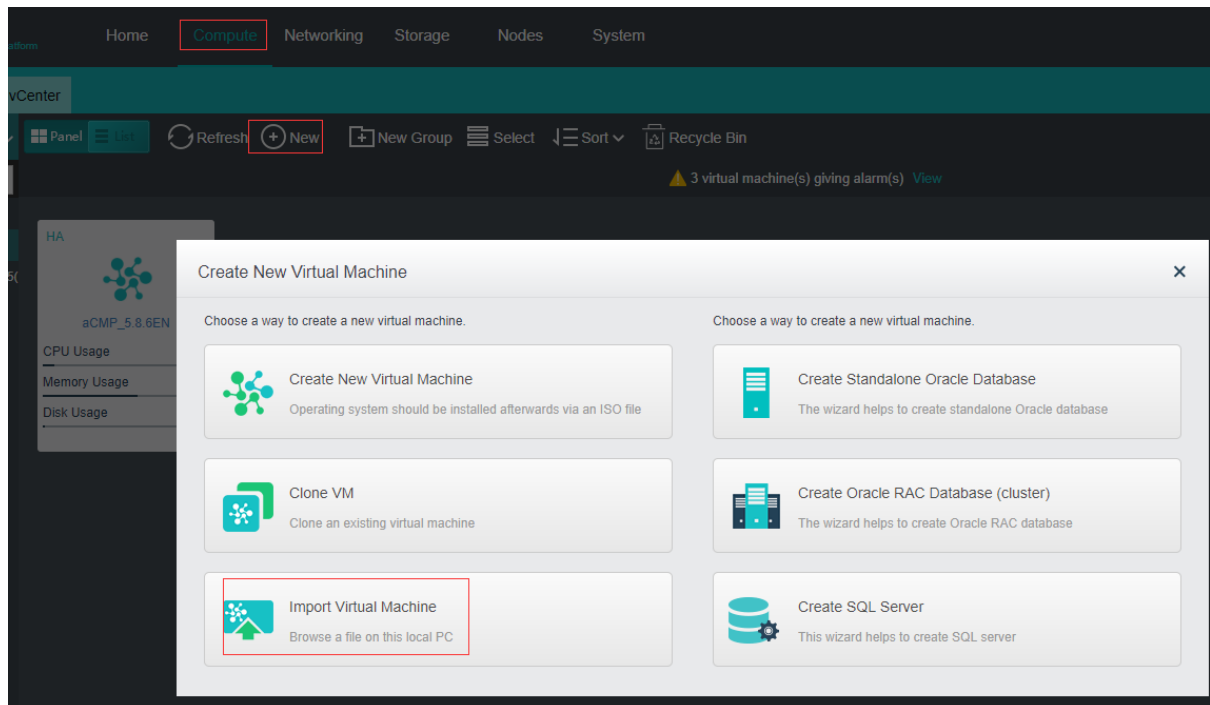
1. The SANGFOR enterprise-level cloud aCloud platform has been correctly deployed.
2. The aCMP cloud management image installation package is prepared.

[Operating steps]

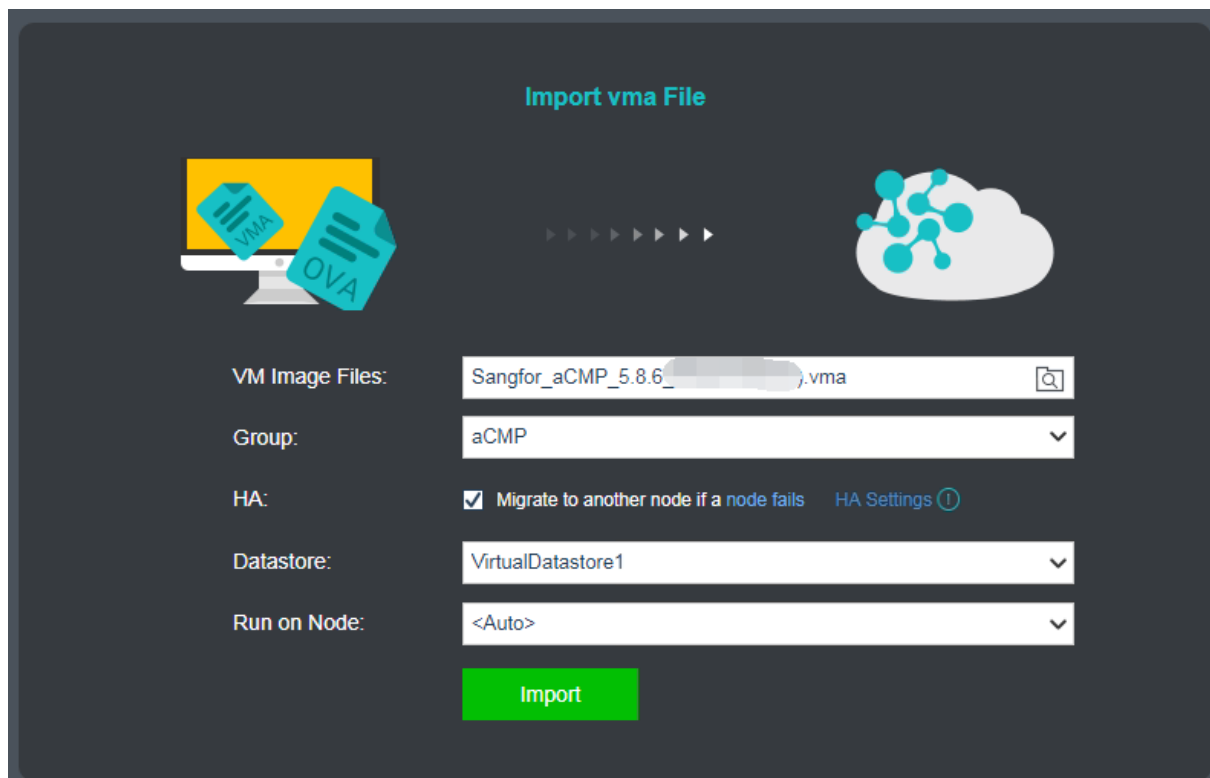
Log onto aCloud platform console:

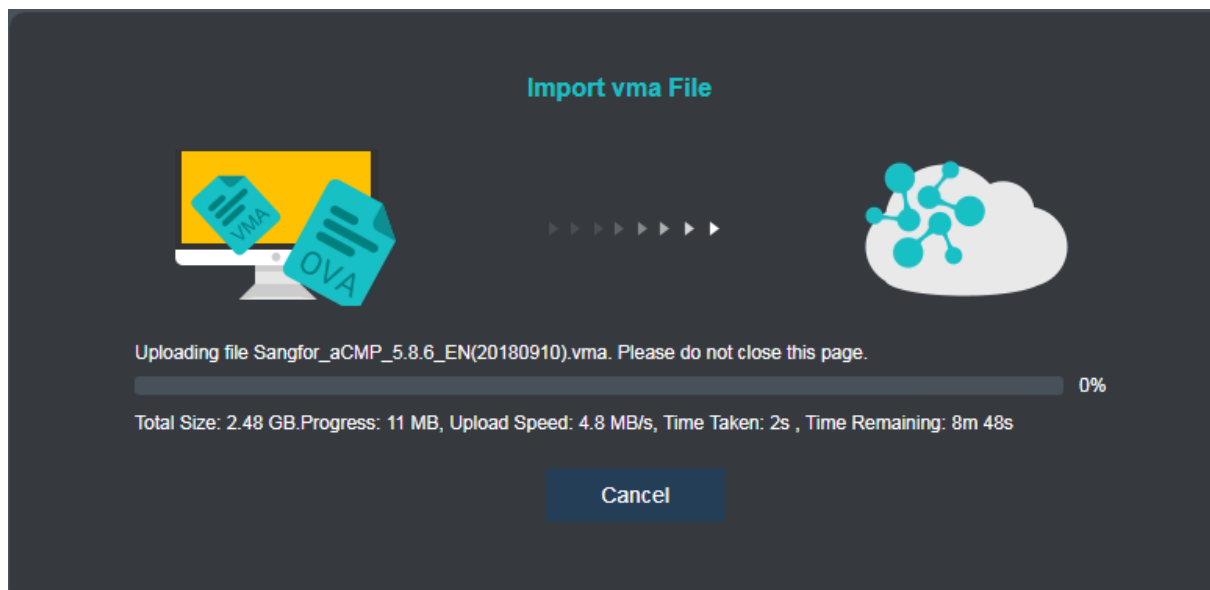


1. Click 『Compute』 → 『New』 → 『import Virtual Machine』 ":

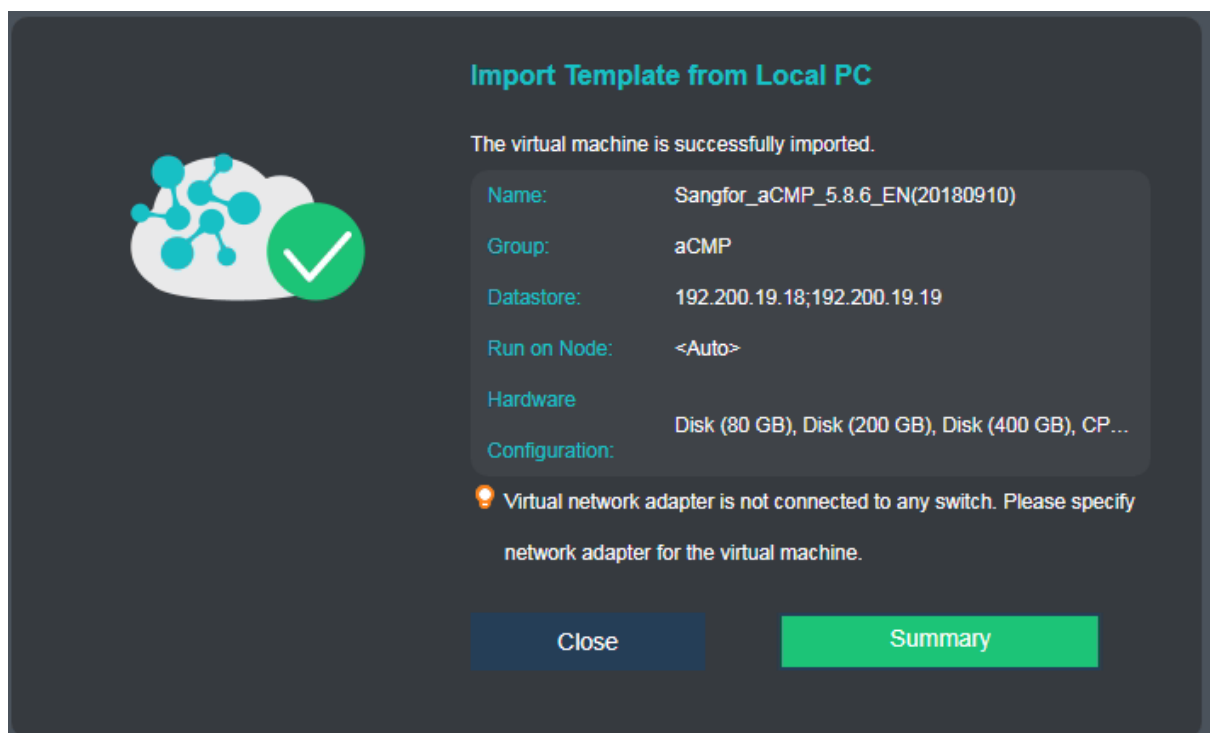


2. Select aCMP virtual machine, select the corresponding grouping, storage location and running location and click "start the Import" to display the upload interface;





3. After the upload is successful, it is necessary to transfer the virtual machine to further configure the network. For details, please refer to Section 2.3 Network Configuration.



2.2 Deployment of Operating and Standby Units (If Necessary)

[Function Description]

SANGFOR aCMP 5.8.6 supports operating and standby deployment. When the aCMP master node is unavailable, the aCMP standby node can be switched to the master node to ensure the high availability of the management platform.

[Note]

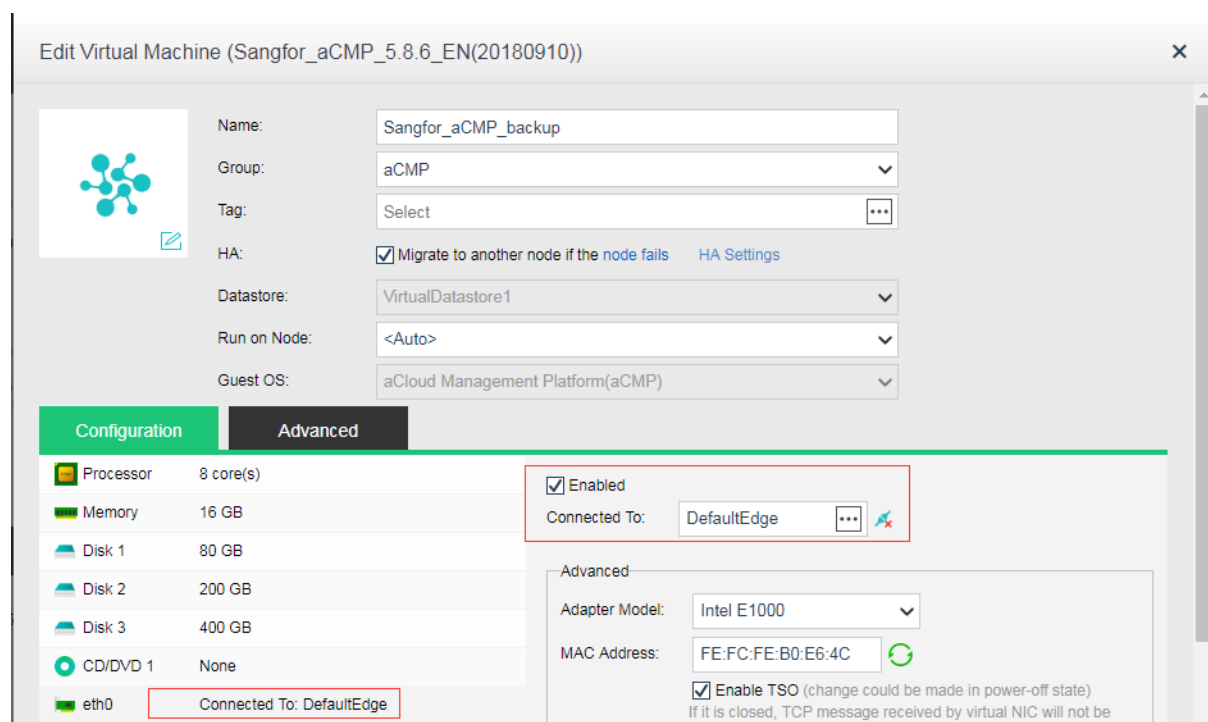
Make sure that the IP of the configured aCMP does not conflict with IP addresses of other hosts, and the network between the operating and standby aCMP is well connected.

[Prerequisites]

aCloud Platform and aCMP Virtual Machine of SANGFOR Enterprise-level Cloud have been accurately deployed

[Operating steps]

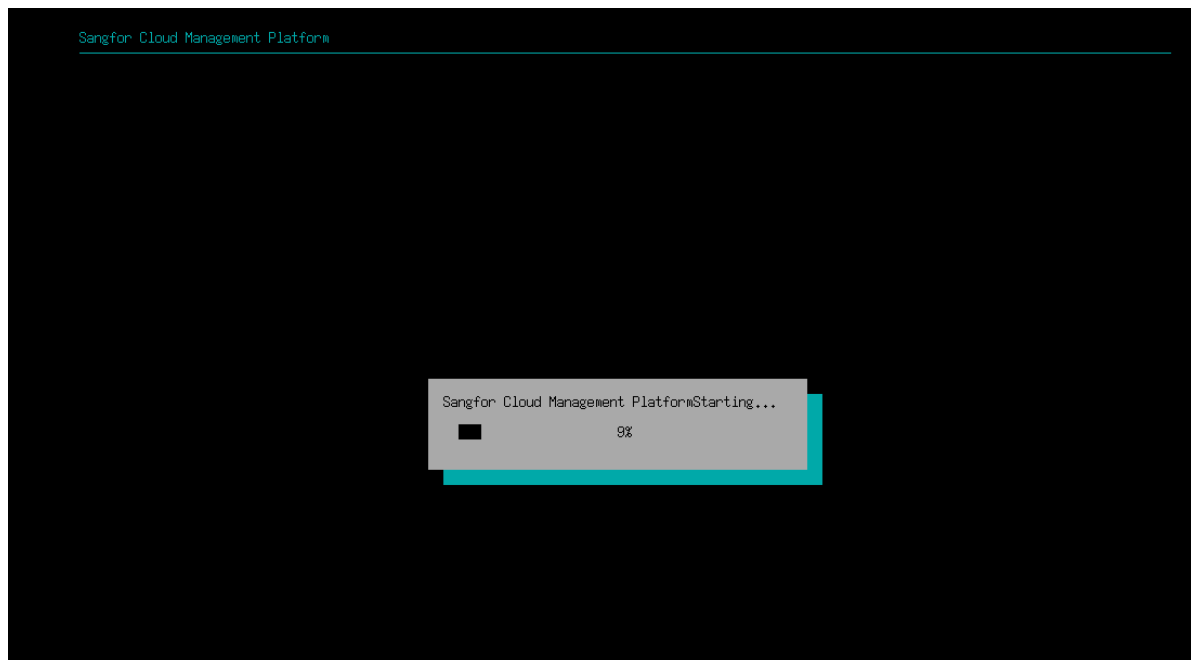
1. Select the newly imported standby aCMP virtual machine (See 2.1 for the detail steps), click 『More』 → 『Edit』 to edit the network card and connect the wires with the second/third-level aCloud platform management network and then click OK;



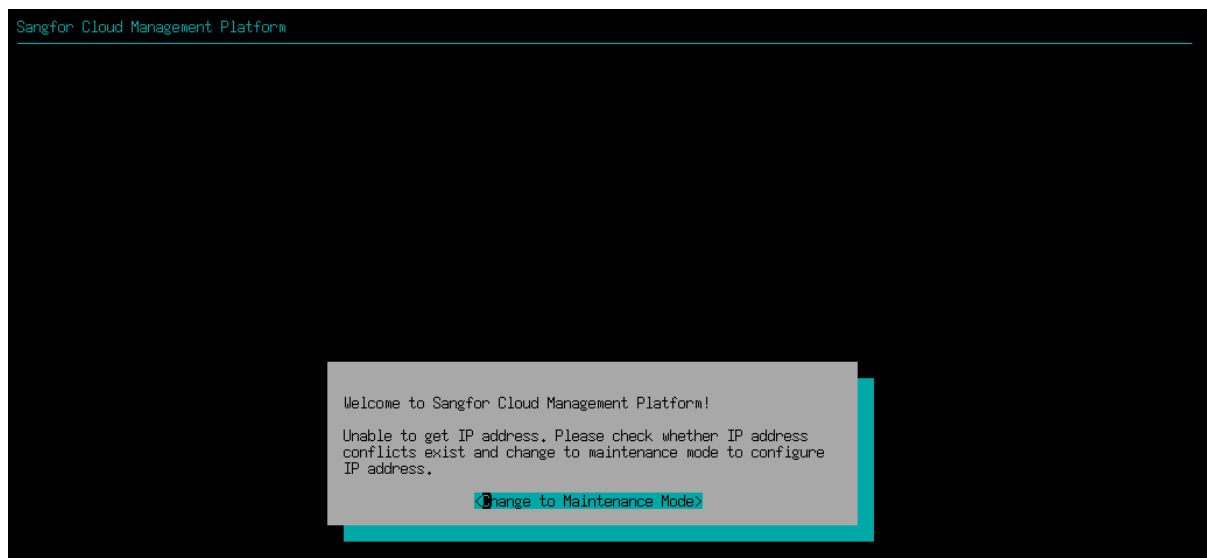
2. Start the imported aCMP virtual machine, log in the console of aCMP virtual machine to modify aCMP password. The steps to modify are detailed in “Network Configuration” in Section 2.3 of this Chapter;

Immediately after the starting, the following will be displayed on the console

interface:



The following configuration interface will appear after shutdown:



Later, one IP is also configured for the standby aCMP in reference to Section 2.3.

3. Log in the home page of main aCMP and click 『Reliability Center』 → 『aCMP Failover』

index/index/#/

Home Resources **Reliability Center** Operations Center Monitoring System

Availability Zones (AZ)

Get Started Business Reliability aCMP Reliability Hardware Reliability

Holistic View Scheduled Backup/CDP Overload Check Hardware Health Check

Disaster Recovery Network Check

VM Failover Data Replication

Resource Scheduling Data Reconstruction

Node Reservation **aCMP Failover**

Reliability Center > aCMP Failover

Refresh Add aCMP Node

aCMP Failover

aCMP high availability requires active and standby aCMP be configured. In case active aCMP fails, administrator can visit standby aCMP GUI and change its status to active, which ensures availability of cloud management platform.

aCMP IP	Status	Active/Standby	Operation
192.168.19.172	Online	Active(Current Node)	-
192.168.19.173	Online	Standby	Switch to Active Delete

4. Click **Add aCMP Node**, input IP address and password of standby aCMP and click **OK**;

Add aCMP Node ✕

Configuration Guide:

1. Add a new aCMP and specify its IP address, username and password.
2. This aCMP will work as a standby unit and related configurations and data will be synced to it from the current platform.
3. Visit standby aCMP GUI by specified IP address and change its status to active in case the primary aCMP fails.

aCMP IP:

Username:

Password:

After the adding, one aCMP in a standby state can be seen on the configuration page.

Reliability Center > aCMP Failover

Refresh Add aCMP Node

aCMP Failover

aCMP high availability requires active and standby aCMP be configured. In case active aCMP fails, administrator can visit standby aCMP GUI and change its status to active, which ensures availability of cloud management platform.

aCMP IP	Status	Active/Standby	Operation
192.168.19.172	Online	Active(Current Node)	-
192.168.19.173	Online	Standby	Switch to Active Delete

2.3 Network Configuration

[Function Description]

After aCMP cloud management platform is imported successfully, its network setting shall be conducted. So that aCMP can get access to aCloud cluster network and only in this way aCMP can enable the heterogeneous management of other clusters where the network is accessible.

[Note]

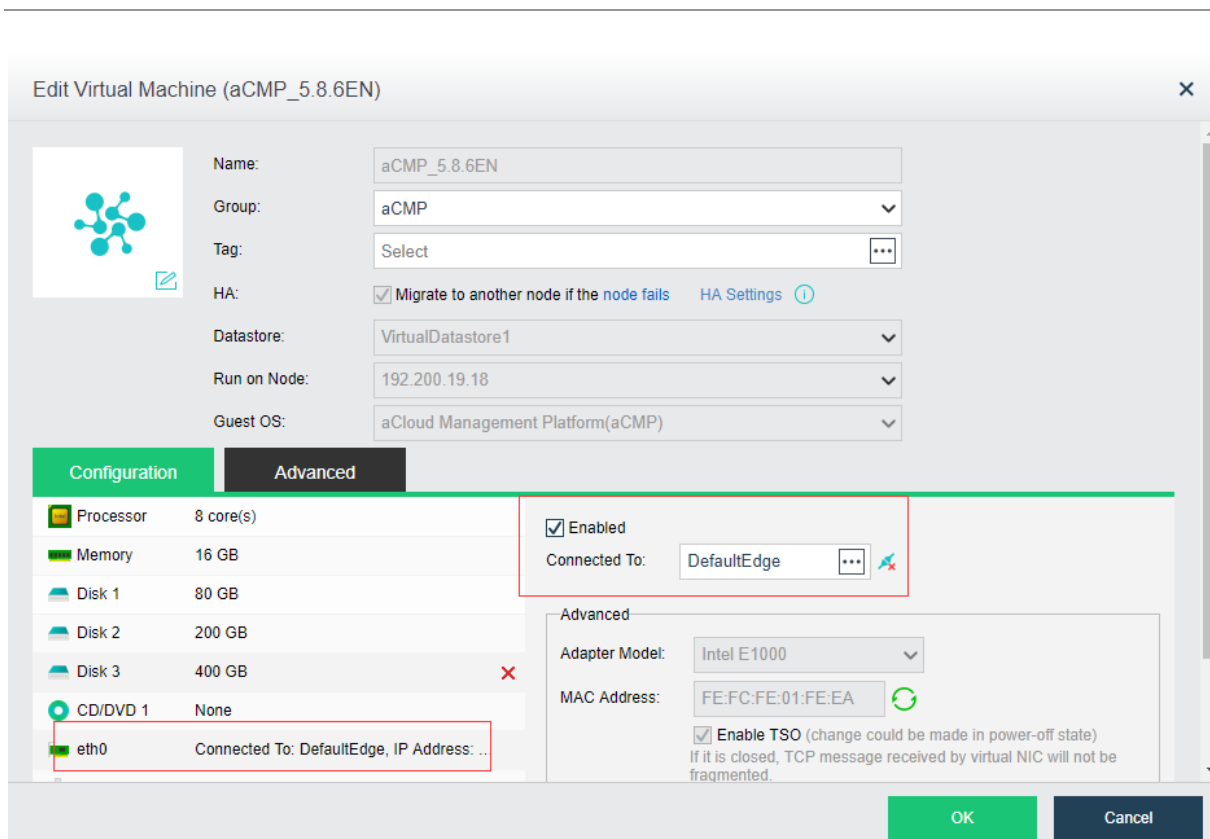
Please guarantee no conflict between the IP of aCMP and the IP address of other hosts.

[Prerequisites]

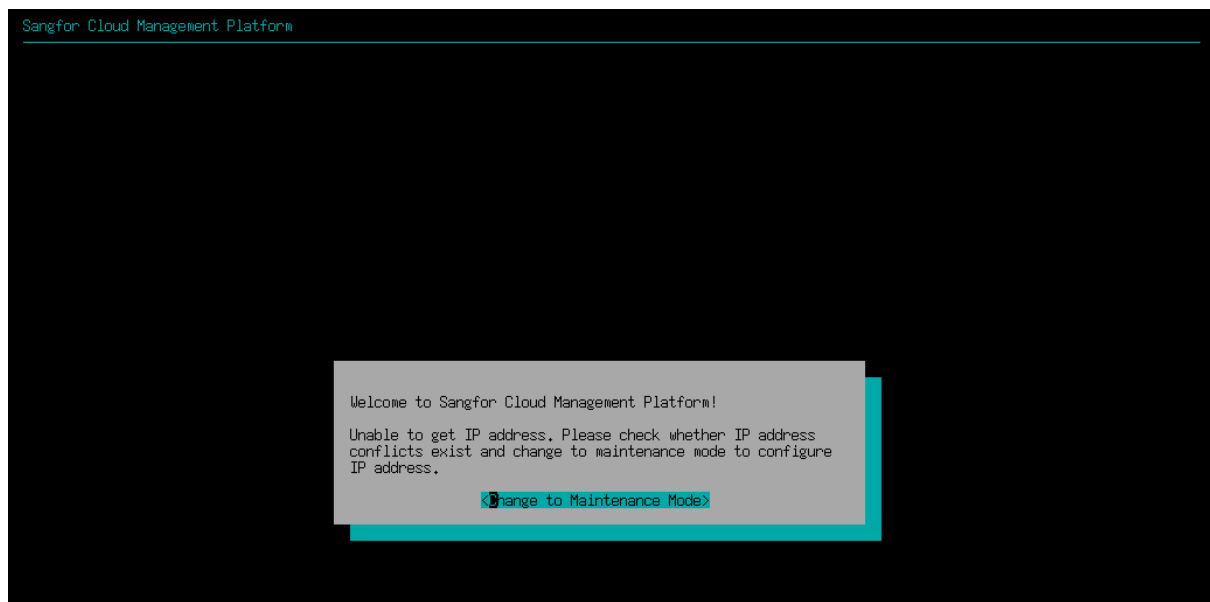
aCloud Platform and aCMP Virtual Machine of SANGFOR Enterprise-level Cloud have been accurately deployed

[Operating Steps]

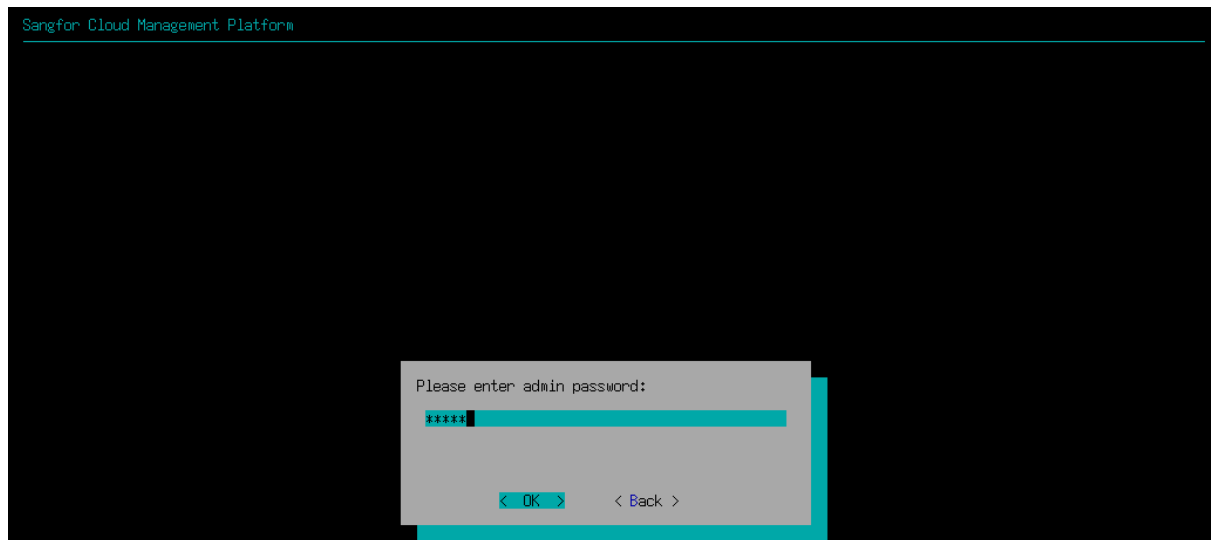
1. Select the imported aCMP virtual machine, click 『More』 → 『Edit』 to edit the network card and connect the wires with the second/third-level aCloud platform management network and then click the **OK**;



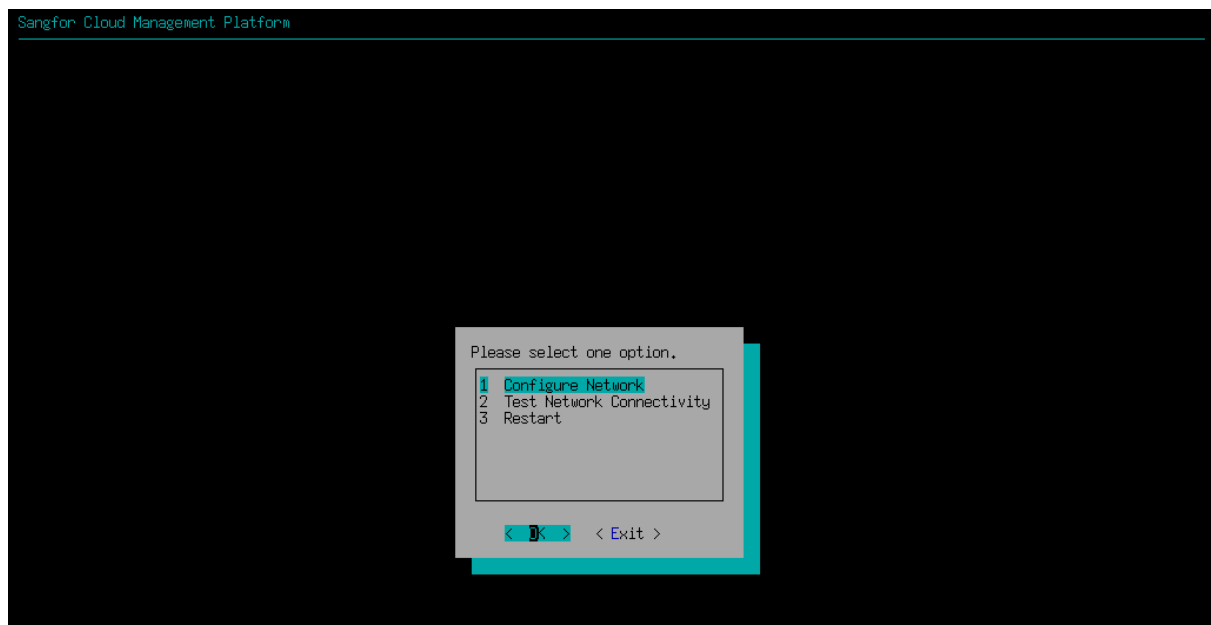
2. Start the imported aCMP virtual machine and log in the console of aCMP virtual machine;



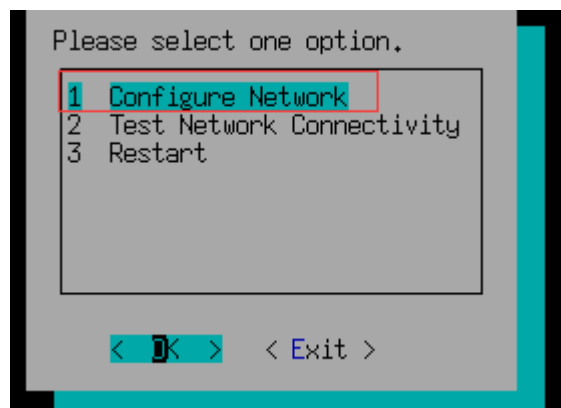
3. Have a random click on the console of virtual machine, press the key "enter" in the keyboard to enter into the maintenance mode and then enter password (the initial password is admin); after the password is entered, select the option OK and then press the key "enter" in the keyboard to enter a configuration interface.

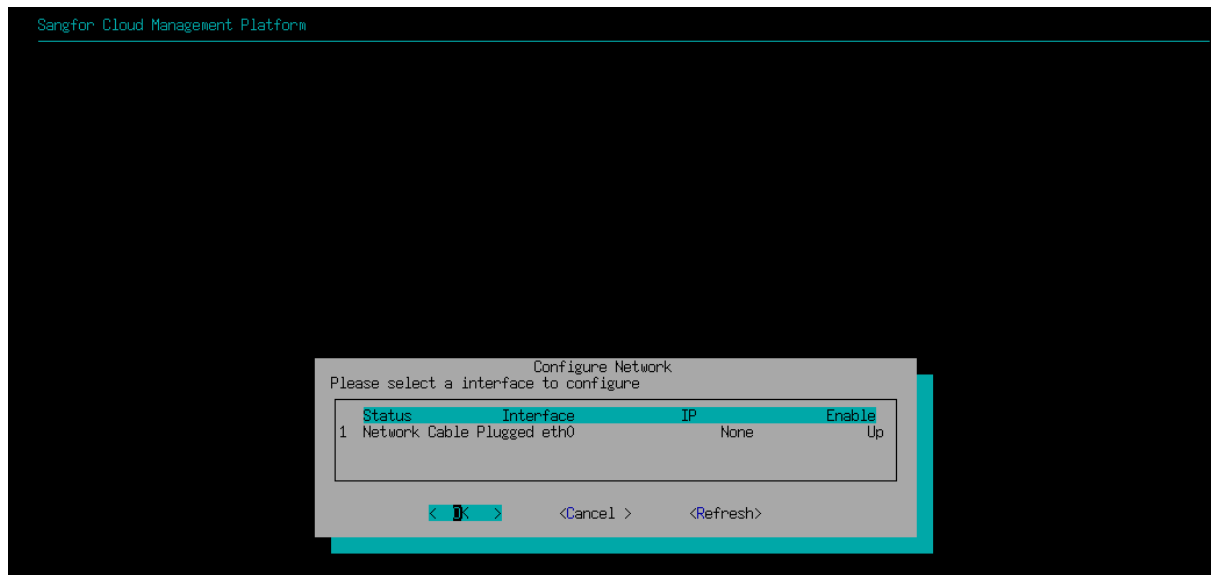


Click OK to enter the following interface:

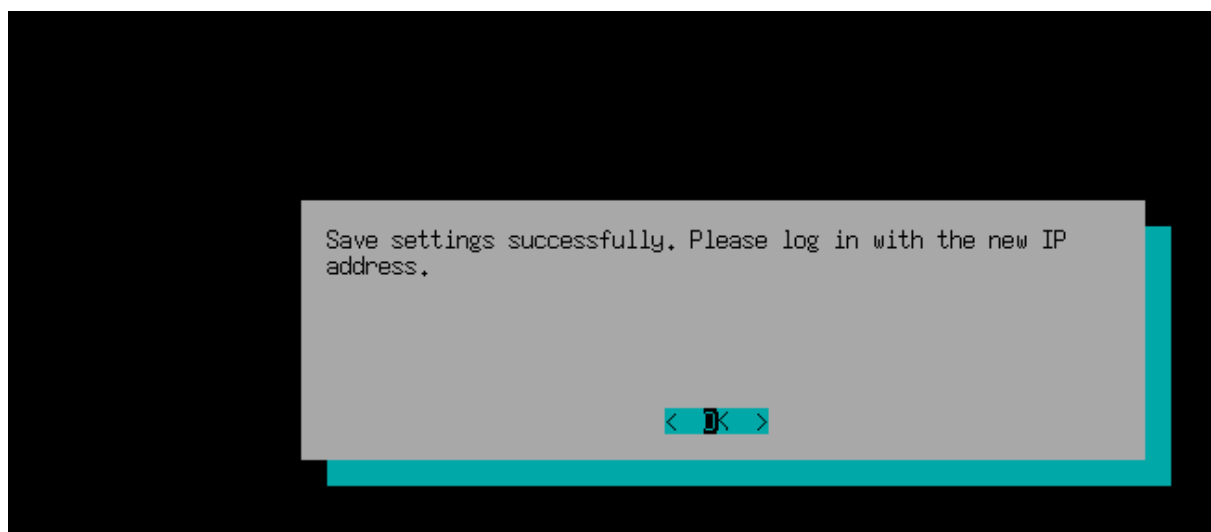
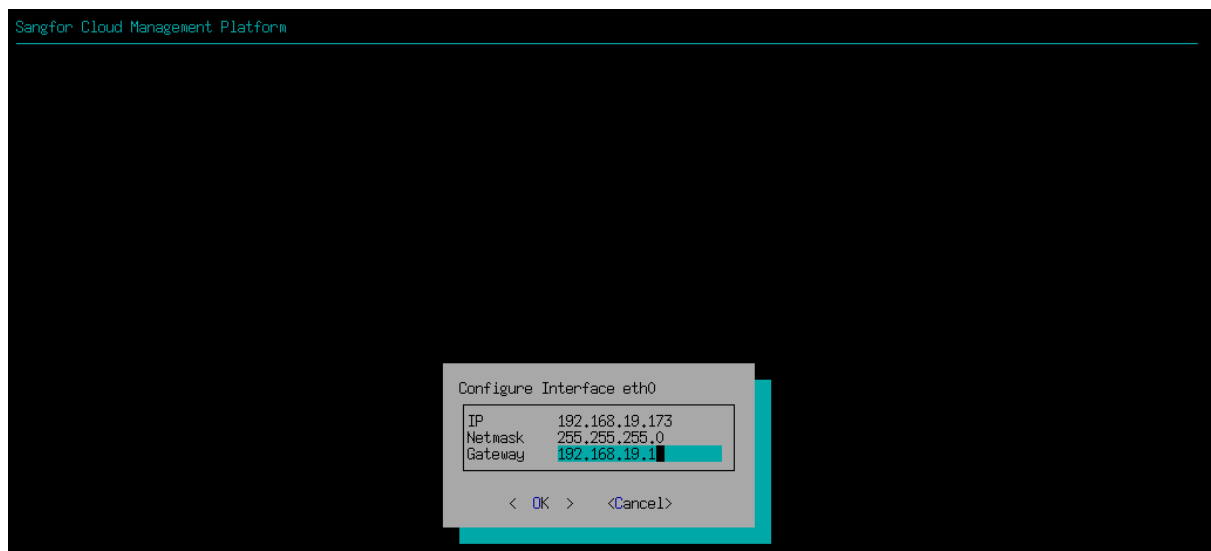


4. Click the key “↑↓” in the keyboard to select 『Network Configuration』 and press the key “enter” in the keyboard;

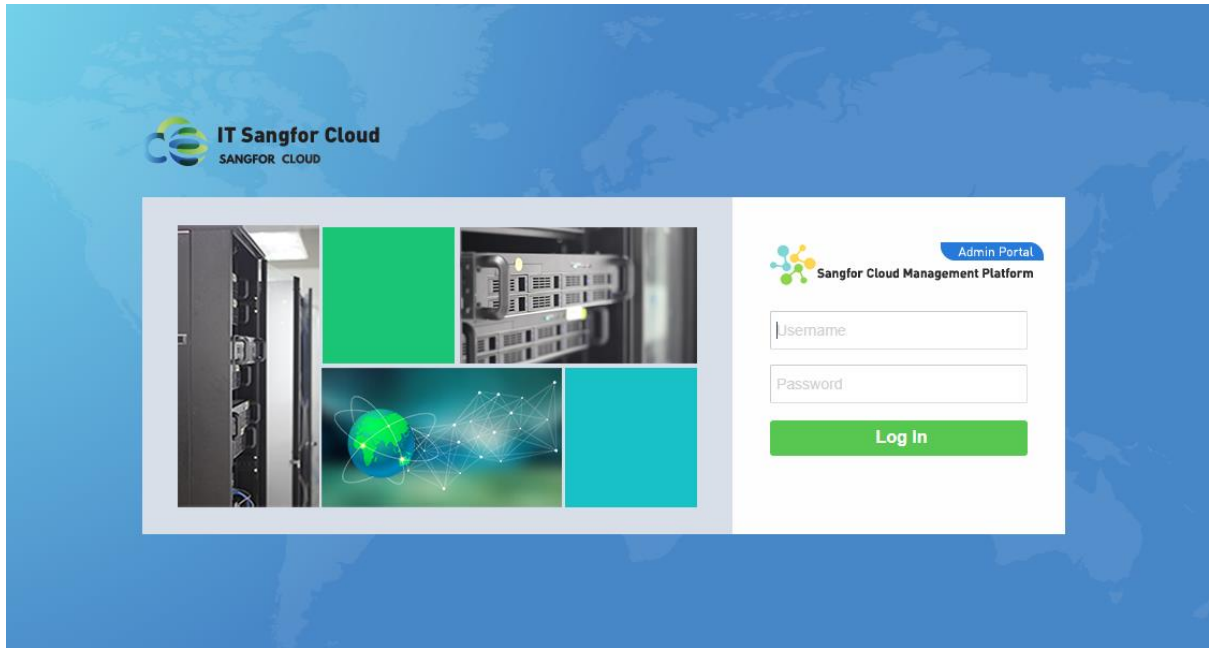




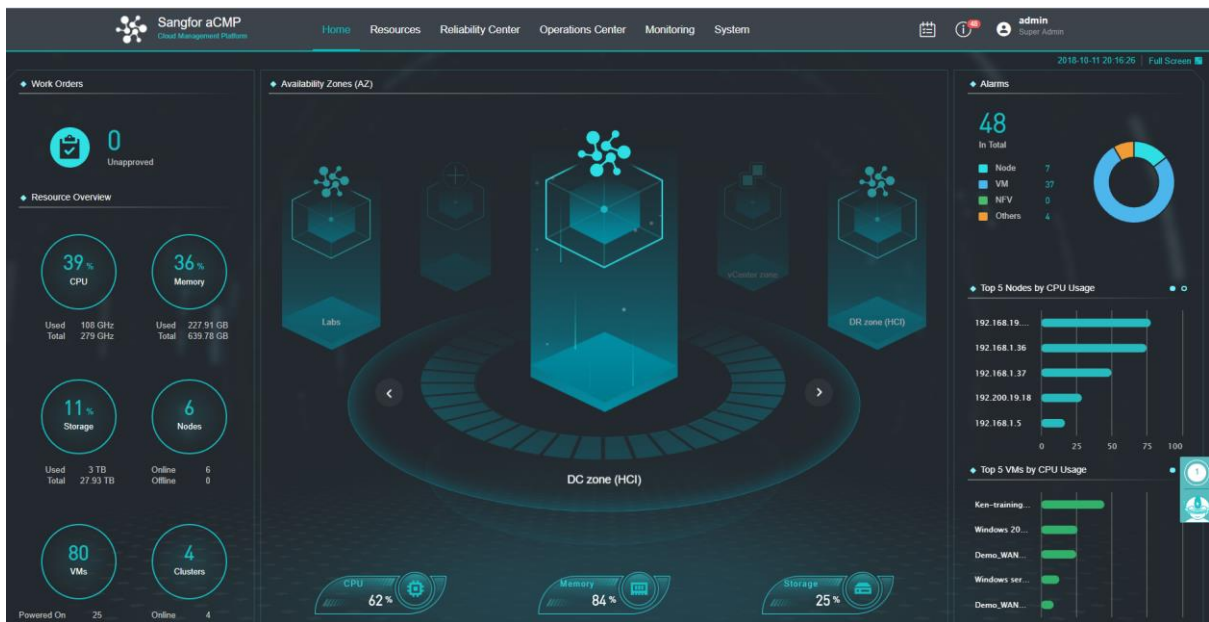
5. Set the IP address, mask and gateway and click OK;



6. Open the browser, enter IP:4430 set in https:// and press the key "enter";



7. The default account and password are admin/admin. For the safety of your account, please do the modification.



2.4 aCMP Activation

[Function Description]

Activate aCMP and give authorization to the cluster for networking.

[Prerequisites]

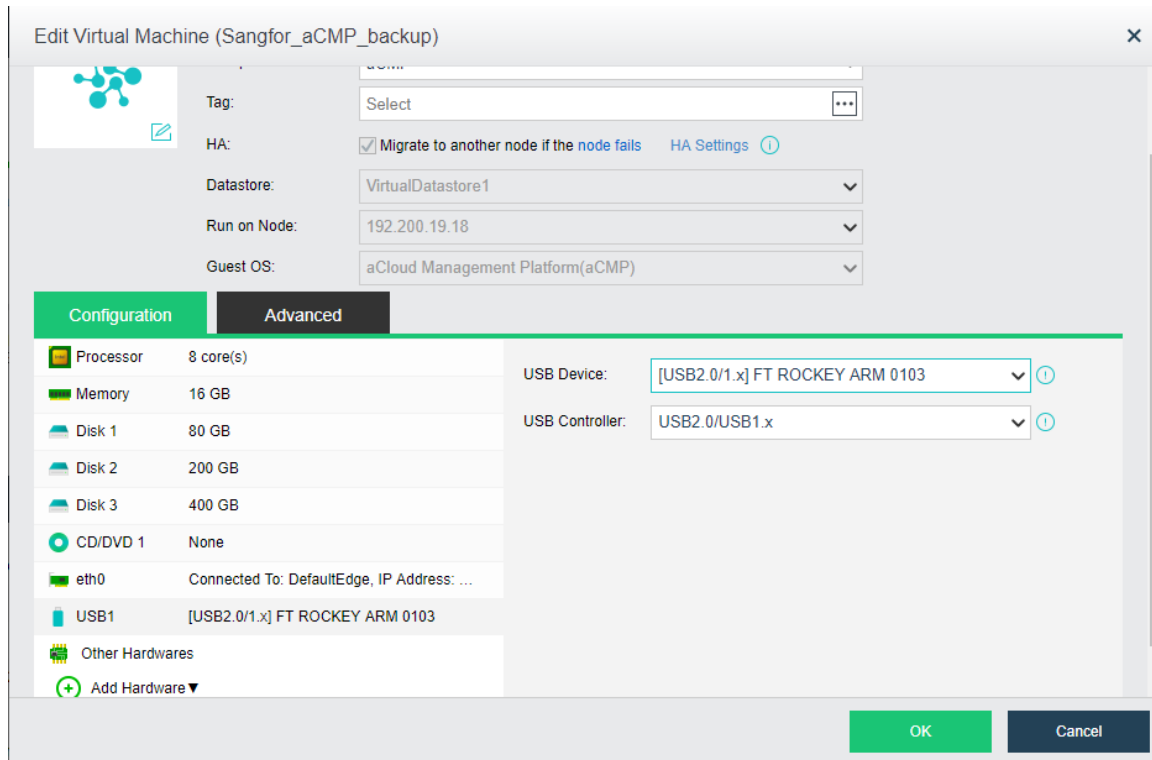
1. aCloud Platform and aCMP virtual machine of SANGFOR Enterprise-level

Cloud have been accurately deployed

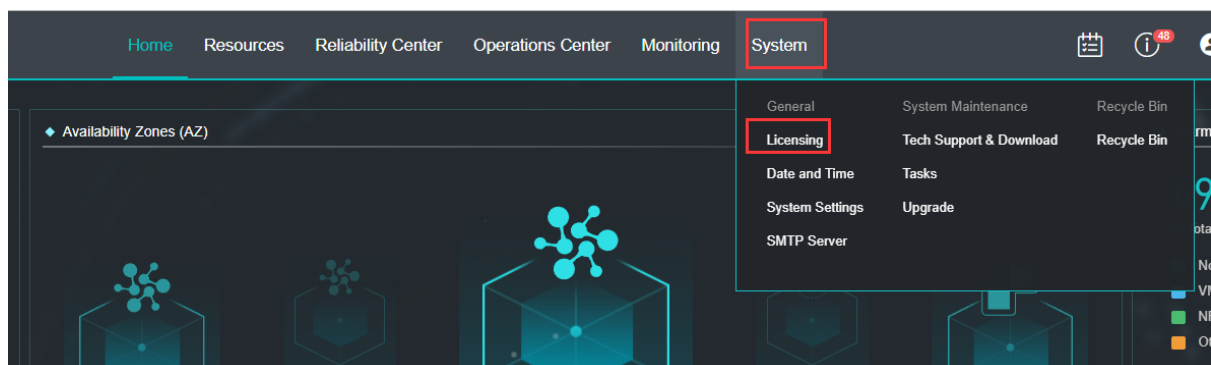
2. Prepare the serial number and key for activation

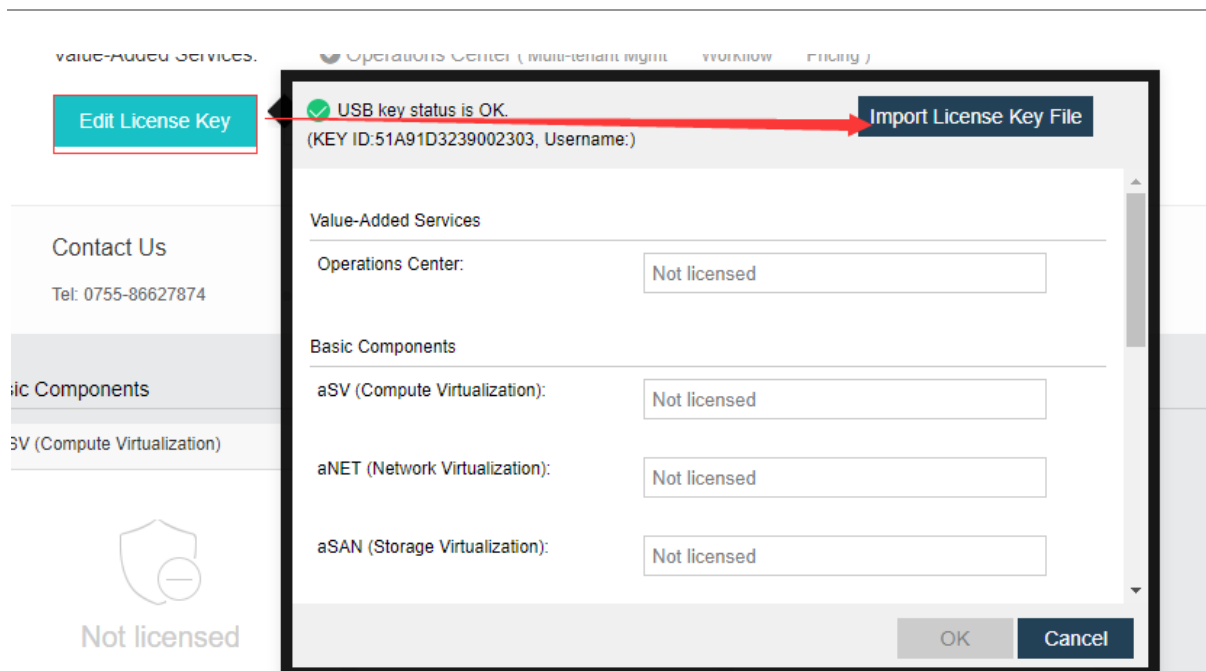
[Operating Steps]

1. Click aCMP virtual machine → 『Edit』 → add USB hardware → map key to the virtual machine;

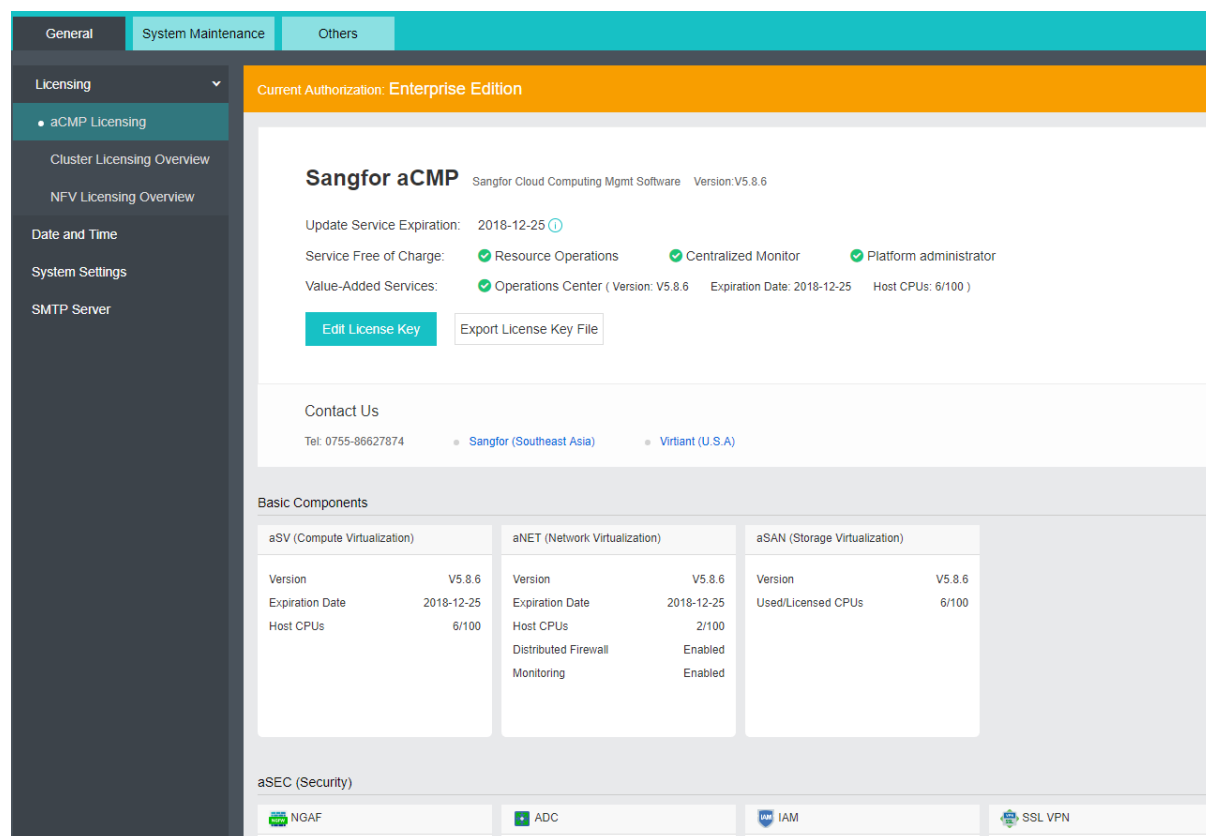


2. After successful mapping, log in the home page of aCMP, click 『System』 → 『Licensing』 → 『General』 to enter the authorization page of aCMP, click 『Edit License Key』 and select the ready authorization document (with a .lic suffix),

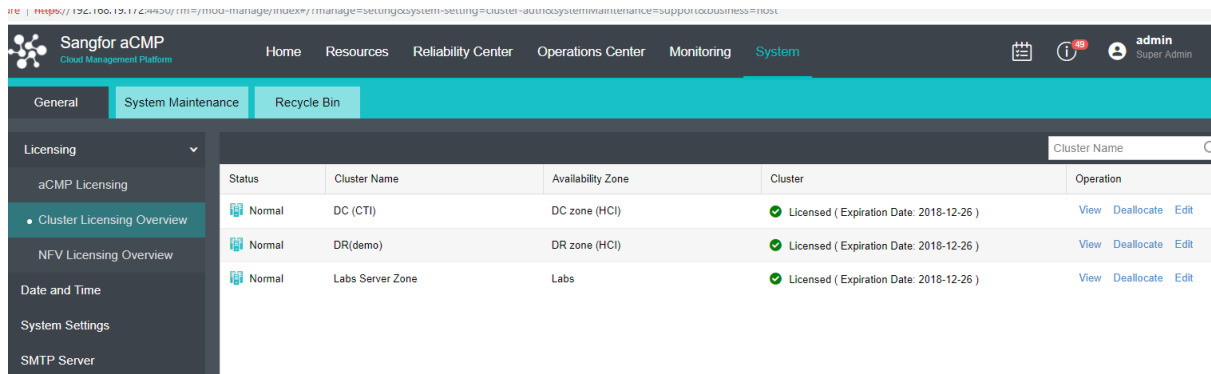




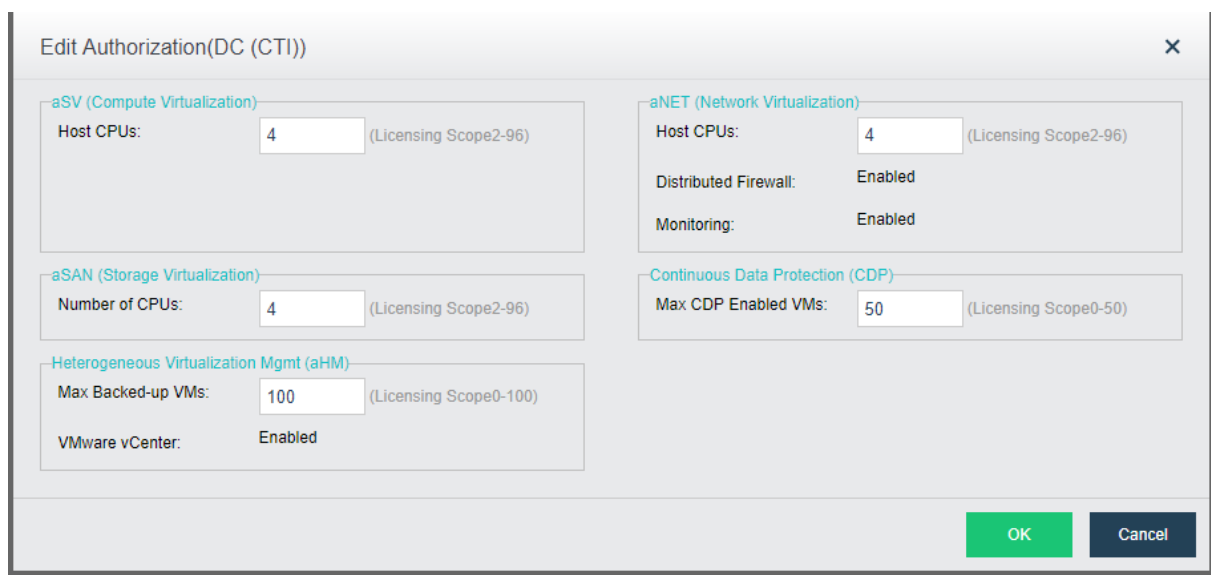
After successful import, the information of the corresponding serial number can be viewed;



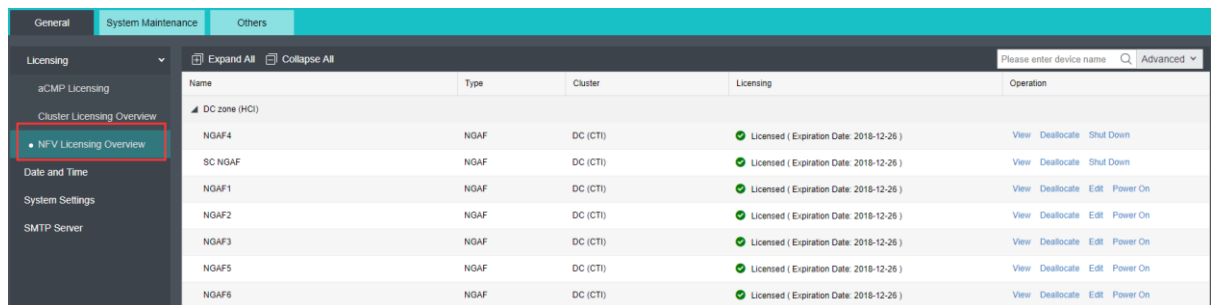
3. Click 『Cluster Licensing Overview』 to license the newly added clusters and also license, revoke or modify the existing clusters;



Click Edit to display the following configuration and you can configure the licensing related to aSV, aNET, aSAN, CDP and aHM of the corresponding clusters on this interface.



- Click 『NFV Licensing Overview』 and you can license, revoke, view and edit (only in shutdown mode) NFV of the clusters.



Only the NFV in shutdown mode can be edited with authorization and you can just click Edit to conduct the licensed editing;

NGAF Licensing

Device Name: NGAF1

Configuration Standard: 100Mbps

Licensed Resources

Branch VPN Sites: 5

SSL VPN Users: 5

Server Access Verification: 5

Mobile VPN Users: 5

Licensed Features

Cross-ISP Access Optimization	IPSec VPN	IPS
Antivirus	Web App Protection	
Bandwidth Management	Application Control	
Web Filter	Data Leak Protection	APT Detection
RT Vulnerability Scanner	Software Upgrade	

Licensed Hardware Usage

Type	Free	Licensed Number	Usage
100Mbps	3	10	70%
200Mbps	10	10	0%
400Mbps	10	10	0%
800Mbps	10	10	0%
1.6Gbps	10	10	0%

Licensed Resource Usage

Type	Free	Licensed Number	Usage
Branch VPN Sites	61	100	39%
SSL VPN Users	39	100	61%
Server Access Veri...	39	100	61%
Mobile VPN Users	40	100	60%

Click Deallocate and you can revoke the authorization of NFV devices, as shown in the following diagram:

(CTI)	✔ Licensed (Expiration Date: 2018-12-26)	View	Deallocate	Shut Down
(CTI)	✔ Licensed (Expiration Date: 2018-12-26)	View	Deallocate	Shut Down

The configuration of authorization revocation can be effective only after aCMP administrator enters the password to confirm:

Alert

Are you sure that you want to revoke authorization of NGAF4?
It becomes unauthorized after revocation and business may get interrupted. Please operate with caution.

Enter password (admin) to confirm this operation

.....

OK Cancel

Click shut Down and you can continue to shut down the corresponding NFV:

Name	Type	Cluster	Licensing	Operation
DC zone (HCI)				
NGAF4	NGAF	DC (CTI)	✔ Licensed (Expiration Date: 2018-12-26)	View Deallocate Shut Down
SC NGAF	NGAF	DC (CTI)	✔ Licensed (Expiration Date: 2018-12-26)	View Deallocate Shut Down

Click Power On and you can start the corresponding NFV:

NGAF1	NGAF	DC (CTI)	✔ Licensed (Expiration Date: 2018-12-26)	View	Deallocate	Edit	Power On
NGAF2	NGAF	DC (CTI)	✔ Licensed (Expiration Date: 2018-12-26)	View	Deallocate	Edit	Power On
NGAF3	NGAF	DC (CTI)	✔ Licensed (Expiration Date: 2018-12-26)	View	Deallocate	Edit	Power On

Click View and you can view the authorization details of the corresponding NFV:

DC zone (HCI)							
NGAF4	NGAF	DC (CTI)	✔ Licensed (Expiration Date: 2018-12-26)	View	Deallocate	Shut Down	
SC NGAF	NGAF	DC (CTI)	✔ Licensed (Expiration Date: 2018-12-26)	View	Deallocate	Shut Down	
NGAF1	NGAF	DC (CTI)	✔ Licensed (Expiration Date: 2018-12-26)	View	Deallocate	Edit	Power On

Licensing

Device Name: NGAF
 Authorization Method: 100Mbps

Resource Distribution

Branch VPN Sites: 8
 SSL VPN Users: 30
 Server Access Verification: 30
 Mobile VPN Users: 30

Licensed Features

IPS

RT Vulnerability Scanner

Bandwidth Management

Web Filter

Application Control

URL Database

IPS Vulnerability Database

Application Signature Database

Data Leak Protection Database

Data Leak Protection

Software Upgrade

Anti-Virus Database

Cross-ISP Access Optimization

Web App Protection

APT Detection

IPSec VPN

WAF Signature Database

Malware Signature Database

Antivirus

2.5 Add Physical Resources

[Function Description]

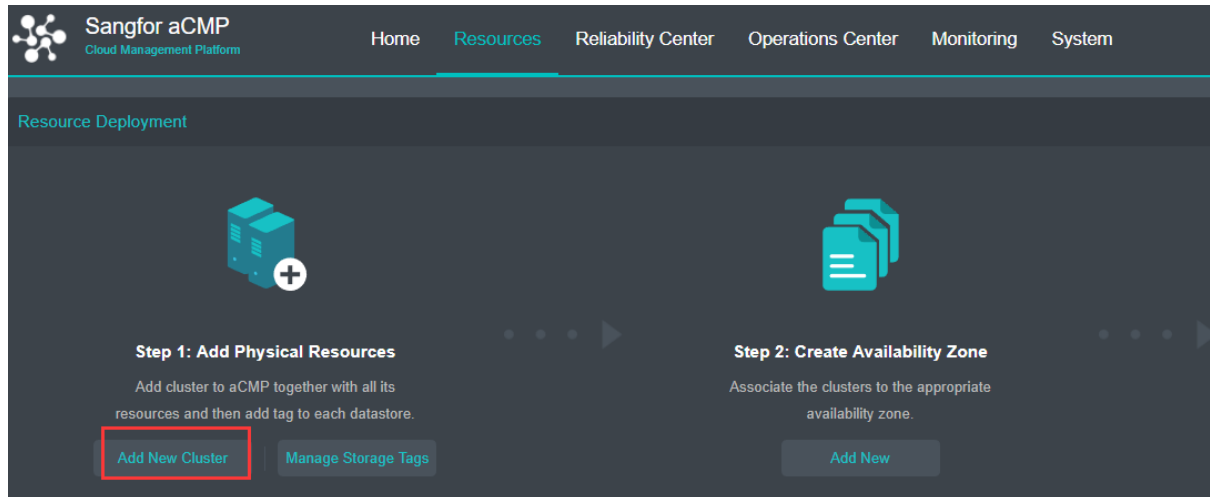
SANGFOR aCMP supports the heterogeneous management of many aCloud clusters and also the heterogeneous management of VMware data centers. When the unified management of many data centers or many clusters is required, aCMP shall be deployed to conduct the heterogeneous management of all the clusters.

[Prerequisites]

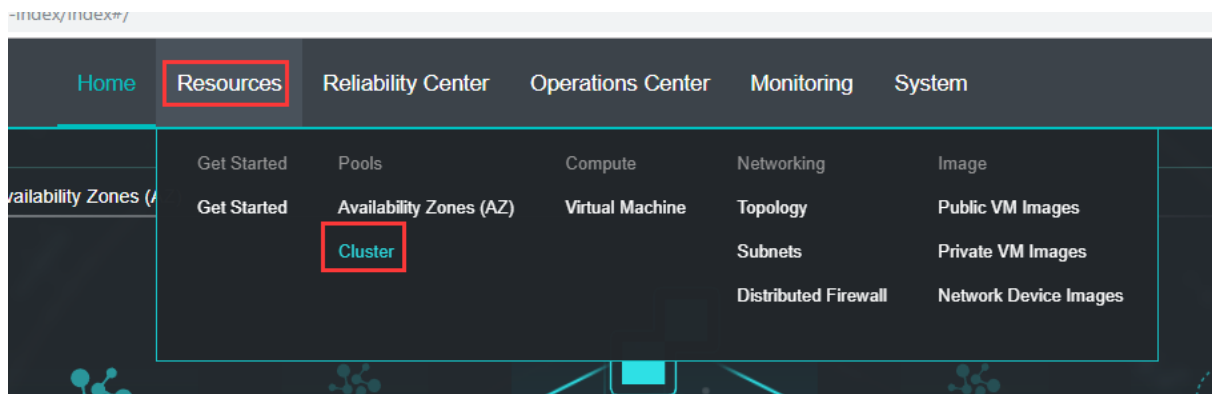
SANGFOR aCMP can get access to the network of aCloud platforms or VMware platform.

[Operating Steps]

1. Log in the home page of aCMP platform, select 『Resources』 → 『Get Started』 and click **Add Cluster**, as given in the following diagram:



- Or, select 『Resources』 → 『Clusters』 on the home page of aCMP platform and click **New** on the popped page.



2. Enter the IP, username, password, name, description and type of cluster according to the requirement; keep the default values if the port is unchanged; click **Next**;

Pools > Cluster > Add New Cluster

1 Basics 2 Add Tags 3 Confirm

Cluster Name: DR(demo)

Description: Description

Cluster Type: aCloud

Cluster IP: 192.200.19.20

Not verify cluster IP address
(Select this if cluster IP is mapped, to avoid connection failure)

Username: admin

Password:

Port: 443

Next Cancel

3. You can set the different tags for the different storage volumes according to the actual situations of the clusters; the default tags include: “high performance”, “good performance” and “large capacity”. These tags can be changed according to the actual situation. You can do the editing on the page 『Cluster』 → 『Tags』 . After the setting, click Next

1 Basics 2 Add Tags 3 Confirm

Associate datastore with a tag according to its performance or hard disk adopted by it. A matching datastore will be chosen based on specified storage tag when creating virtual machine.

Refresh Tags

Status	Name	Storage Type	Capacity	Tag
Normal	VirtualDatastore1	Virtual Storage	10.84 TB	None None High Performance Good Performance Large Capacity

Back Next Cancel

Cluster > Tags

Refresh How to Tag Storage Performance

Tag	Description	Operation
High Perf...	Tag for SSD with high IO speed, to create high-end virtual machines	Edit
Good Per...	Good IO read/write performance. Generally, this tag is for old-styled storage.	Edit
Large Ca...	Fair IO read/write performance but large capacity and high security, cost-effective	Edit

4. Finally, Check that the information is correct and then click **OK**

Pools > Cluster > Add New Cluster

Basics Add Tags 3 Confirm

Cluster Name: DR(demo)
 Description:
 Cluster Type: aCloud
 Cluster IP: 192.200.19.20
 Port: 443

Tagging Storage:

Name	Storage Type	Performance	Capacity
VirtualDatastore1	Virtual Storage	Good Performance	10.84 TB

Back OK Cancel

5. If the cluster is added to this aCMP cloud management platform for the first time, licensing message will be given. Conduct the licensing in reference to “Section 2.5 Licensing”.

192.200.19.20 aCloud 5.8.6 19.59 GHz / 163.27 GHz 12% 147.45 G

192.168.19.200 17.84 GE

Message ✕

This cluster you are adding has not been licensed.
 Before using cluster resources, you should license the cluster first.
 Please license it in System > General > Licensing [Cluster License](#).

Close

2.6 aCloud Cluster Licensing

[Function Description]

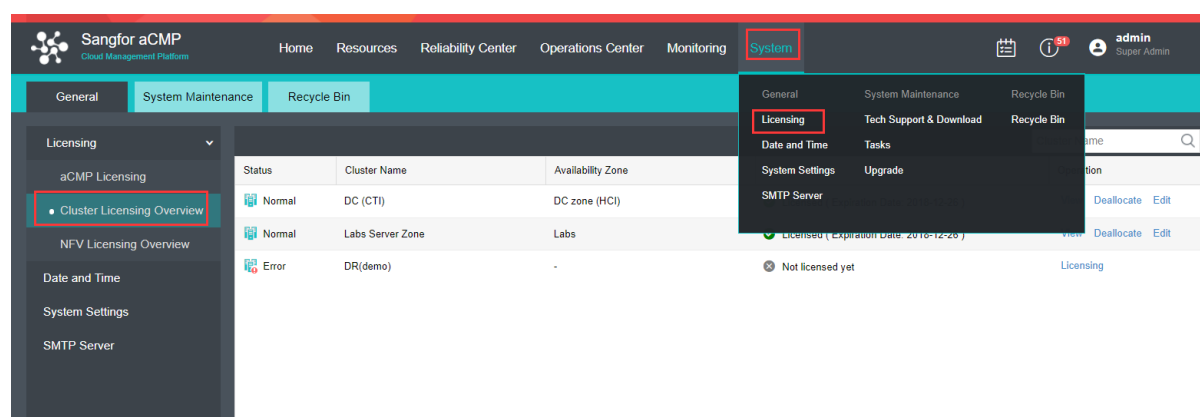
After aCloud cluster is successfully added on SANGFOR aCMP platform, it shall be authorized to guarantee the availability of aCloud cluster service, or the authorization of aCloud cluster shall be cancelled and aCloud cluster shall be edited. All these operations are carried out on this page.

[Prerequisites]

SANGFOR aCMP has been imported, licensed and activated and the authorization is sufficient for aCloud clusters under the heterogeneous management.

[Operating Steps]

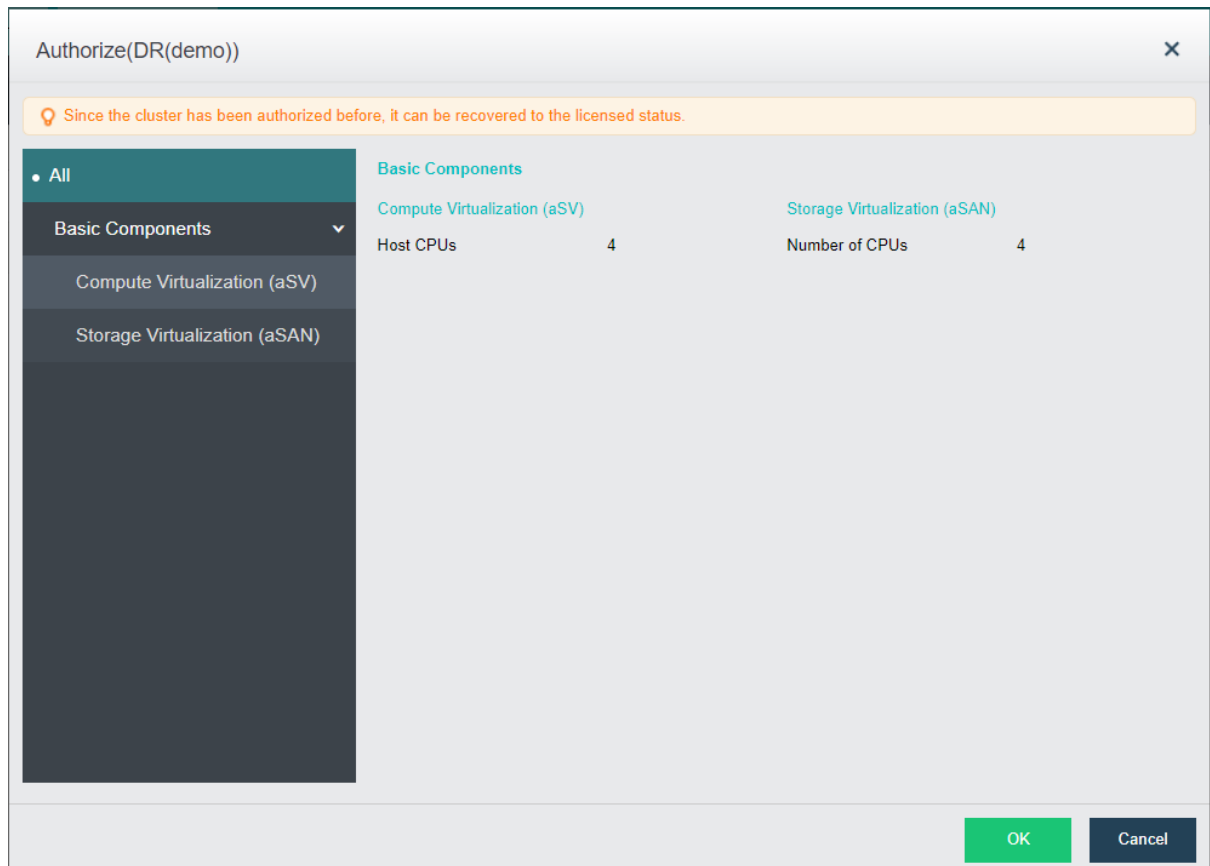
1. Log in the home page of aCMP platform, select 『Management』 → 『Serial Number』 → 『Cluster Licensing Overview』, check the licensed clusters and click **Licensing** to license the clusters.



2. Click 『Licensing』 on the right side of the clusters in an abnormal state;

Status	Cluster Name	Availability Zone	Cluster	Operation
Normal	DC (CTI)	DC zone (HCI)	✔ Licensed (Expiration Date: 2018-12-26)	View Deallocate Edit
Normal	Labs Server Zone	Labs	✔ Licensed (Expiration Date: 2018-12-26)	View Deallocate Edit
Error	DR(demo)	-	✘ Not licensed yet	Licensing

After authorization allocation, click **OK** to complete the licensing;



3. After licensing success, you can view, edit and revoke the authorization of clusters on the licensing interface.

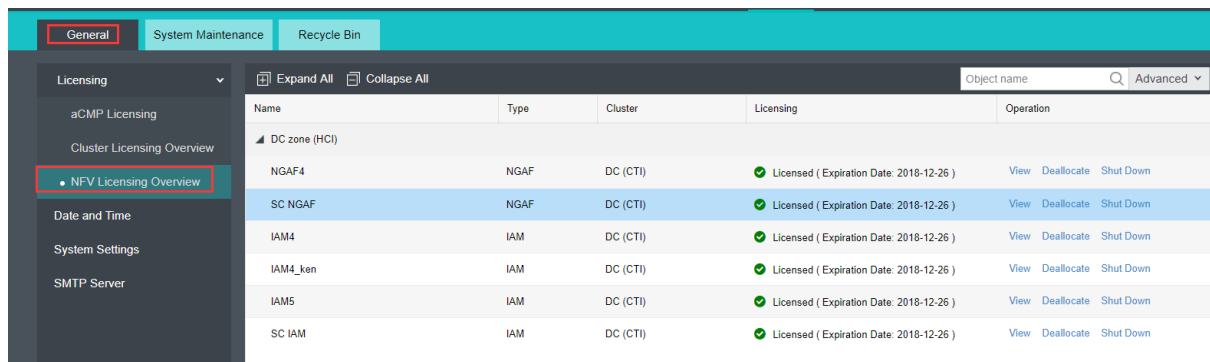
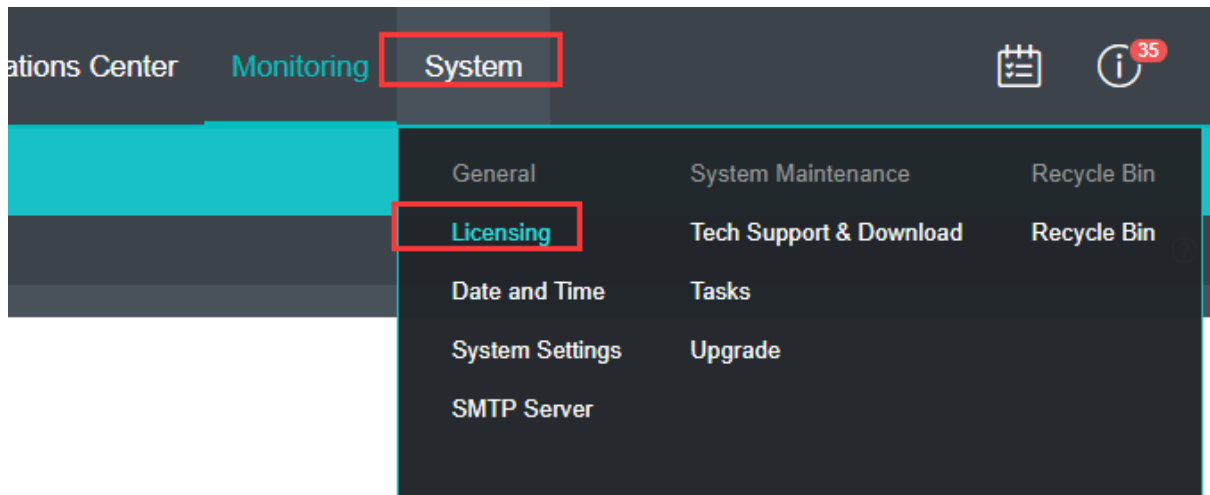
Status	Cluster Name	Availability Zone	Cluster	Operation
Normal	DC (CTI)	DC zone (HCI)	✔ Licensed (Expiration Date: 2018-12-26)	View Deallocate Edit
Normal	DR(demo)	DR zone (HCI)	✔ Licensed (Expiration Date: 2018-12-26)	View Deallocate Edit
Normal	Labs Server Zone	Labs	✔ Licensed (Expiration Date: 2018-12-26)	View Deallocate Edit

2.7 NFV Licensing

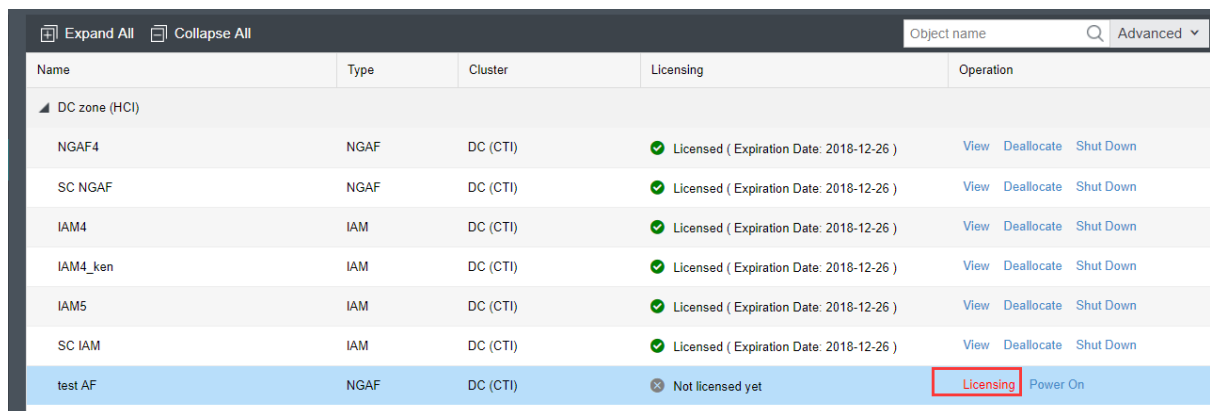
After the aCloud cluster is managed by aCMP, the virtual network device can only be deployed on the aCMP. NFV device requires to authorize through aCMP so that the advanced function in NFV can be used normally.

【Steps】

1. Select 『System』 → 『Licensing』 → 『NFV Licensing Overview』 to check which device is not authorized. Then select unauthorized device and click **Licensing** button.



2. Select unauthorize NFV device and click **licensing** which locate on the right side. After assigning corresponding authorization, click **OK** button.



NGAF Licensing

Device Name: test AF

Configuration Standard: Not licensed yet

Licensed Resources

Branch VPN Sites: 0

SSL VPN Users: 0

Server Access Verification: 0

Mobile VPN Users: 0

Licensed Features

Cross-ISP Access Optimization	IPSec VPN	IPS
Antivirus	Web App Protection	
Bandwidth Management	Application Control	
Web Filter	Data Leak Protection	APT Detection
RT Vulnerability Scanner	Software Upgrade	
IPS Vulnerability Database	WAF Signature Database	
Anti-Virus Database	Malware Signature Database	
Data Leak Protection Database	URL Database	
Application Signature Database		

Licensed Hardware Usage

Type	Free	Total	Usage
100Mbps	8	10	20%
200Mbps	10	10	0%
400Mbps	10	10	0%
800Mbps	10	10	0%
1.6Gbps	10	10	0%

Licensed Resource Usage

Type	Free	Total	Usage
Branch VPN Sites	82	100	18%
SSL VPN Users	60	100	40%
Server Access Veri...	60	100	40%
Mobile VPN Users	60	100	40%

OK Cancel

3. The authorized NFV can be view, edit and deallocate.

DC zone (HCI)

Device Name	Configuration Standard	Configuration Standard	Status	View	Deallocate	Shut Down
NGAF4	NGAF	DC (CTI)	Licensed (Expiration Date: 2018-12-26)	View	Deallocate	Shut Down
SC NGAF	NGAF	DC (CTI)	Licensed (Expiration Date: 2018-12-26)	View	Deallocate	Shut Down
IAM4	IAM	DC (CTI)	Licensed (Expiration Date: 2018-12-26)	View	Deallocate	Shut Down
IAM4_ken	IAM	DC (CTI)	Licensed (Expiration Date: 2018-12-26)	View	Deallocate	Shut Down
IAM5	IAM	DC (CTI)	Licensed (Expiration Date: 2018-12-26)	View	Deallocate	Shut Down
SC IAM	IAM	DC (CTI)	Licensed (Expiration Date: 2018-12-26)	View	Deallocate	Shut Down
test AF	NGAF	DC (CTI)	Not licensed yet	Licensing	Power On	

2.8 Division of Availability Zone

[Function Description]

After the heterogeneous management of clusters, the existing different clusters shall be divided into the different availability zones. The concept of availability zone is oriented based on data center. Generally, availability zones can include many clusters. The division of the logical conception of availability zone can effectively help the administrator to manage the platform.



: Only one cluster can be added in the availability zone of this version.

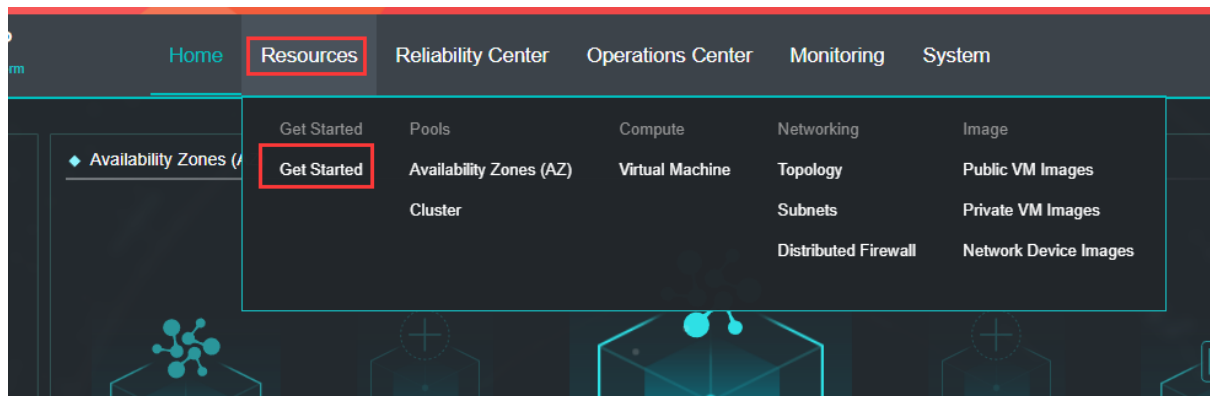
[Prerequisites]

SANGFOR aCMP has added the cluster successfully.

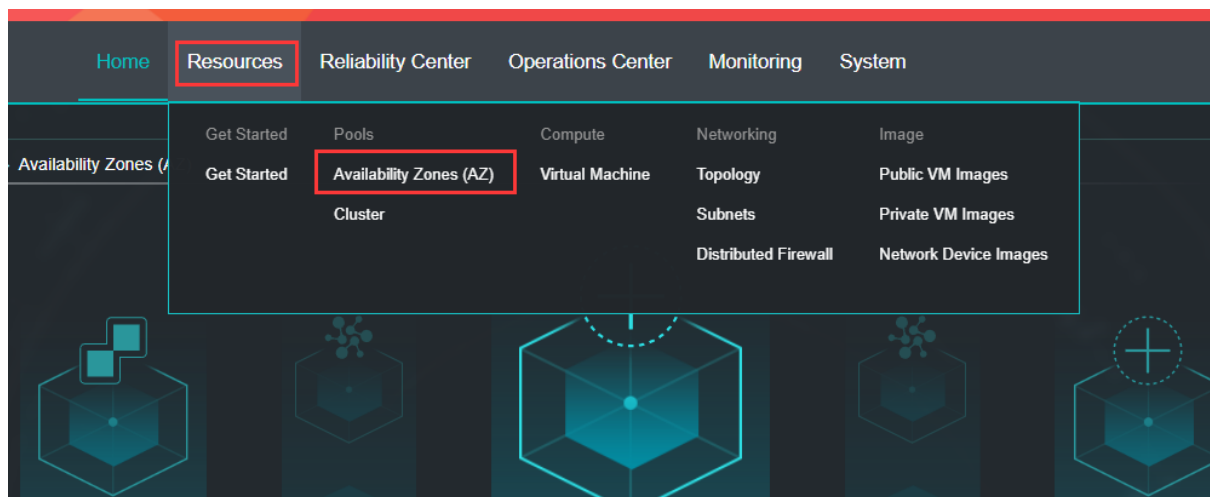
[Operating Steps]

1. Log in the home page of aCMP and click 『Resources』 → 『Get Started』 , as given in the following diagram:

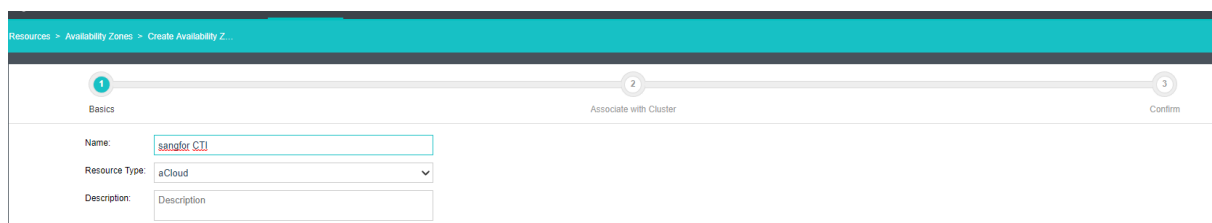
Click **Create Availability Zone** in Step 2, as given in the following figure:



Or, click 『Resources』 → 『Availability Zone』 and click **Create** on the popped page to enter the of availability zone configuration:

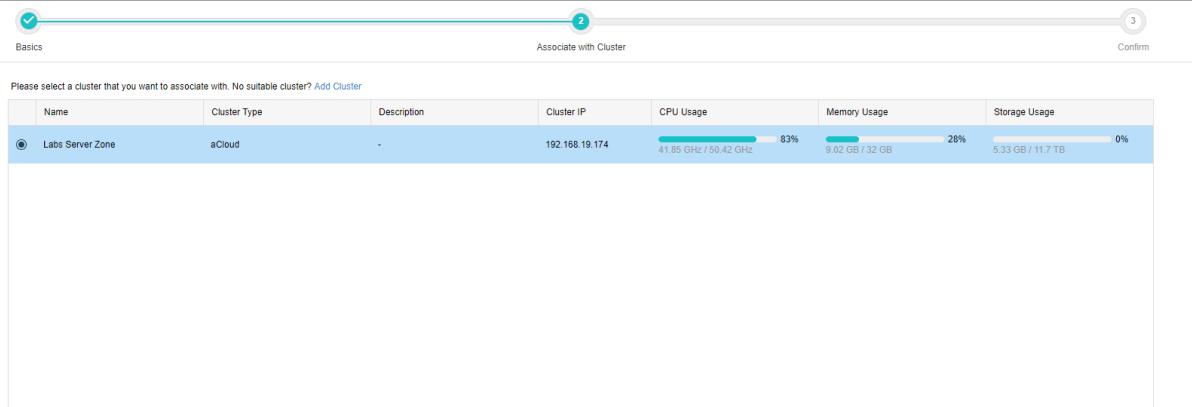


2. Fill in the relevant information and click **Next**

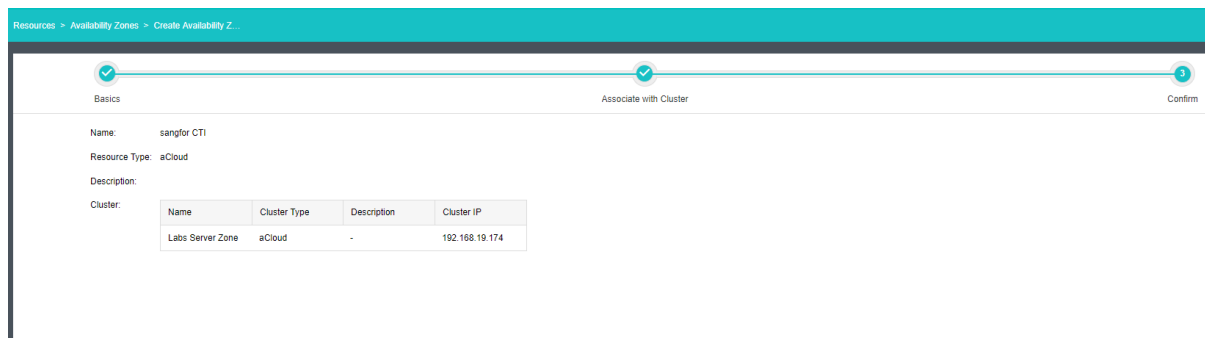
A screenshot of the 'Create Availability Zone' configuration page in the SANGFOR aCMP interface. The page has a teal header with the breadcrumb 'Resources > Availability Zones > Create Availability Z...'. Below the header is a progress bar with three steps: 'Basics', 'Associate with Cluster', and 'Confirm'. The 'Basics' step is active. The form includes a 'Name' field with the value 'sangfor CTI', a 'Resource Type' dropdown menu set to 'aCloud', and a 'Description' field with the value 'Description'.

3. Select the cluster to be added to this availability zone. If there is no suitable

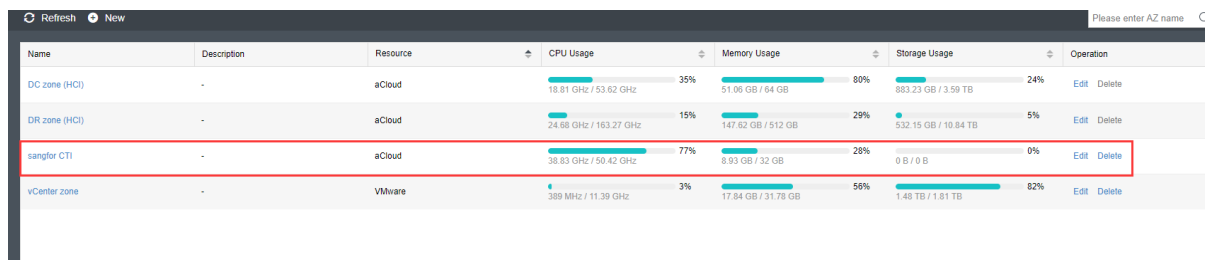
cluster, you can click Add Cluster. See “Section 3.2.1” for the operation details. After configuration completion, click **Next**;



4. Check that the information is correct and then click **OK**.



5. After completion, you can see the added availability zone and then you can edit and delete this availability zone.



2.9 Upgrade

[Function Description]

SANGFOR aCMP5.8.6 has executed the perfection of the cloud management platform in many aspects; in case of using demands, Upgrade Package can be loaded to

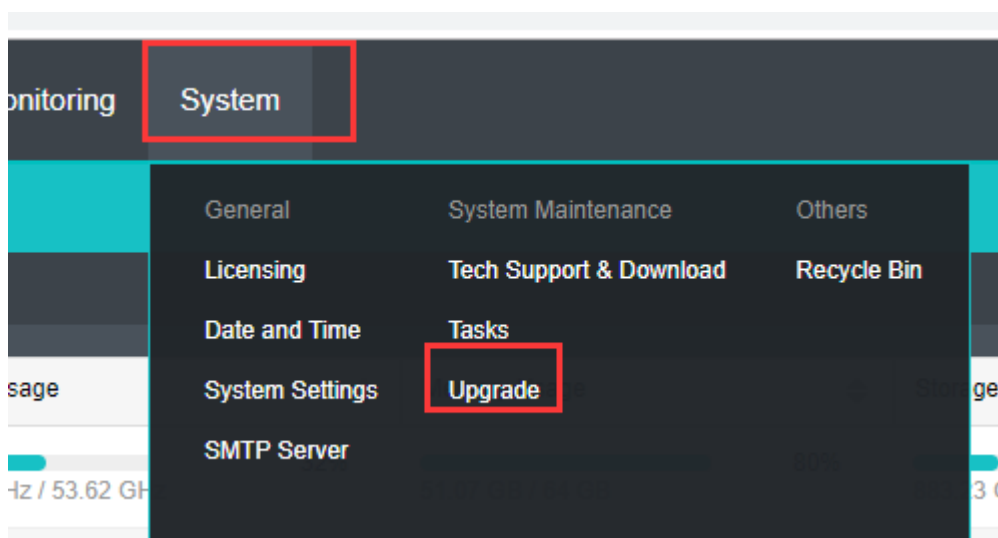
upgrade aCMP so that the versions of aCMP and aCloud can be consistent.

[Prerequisites]

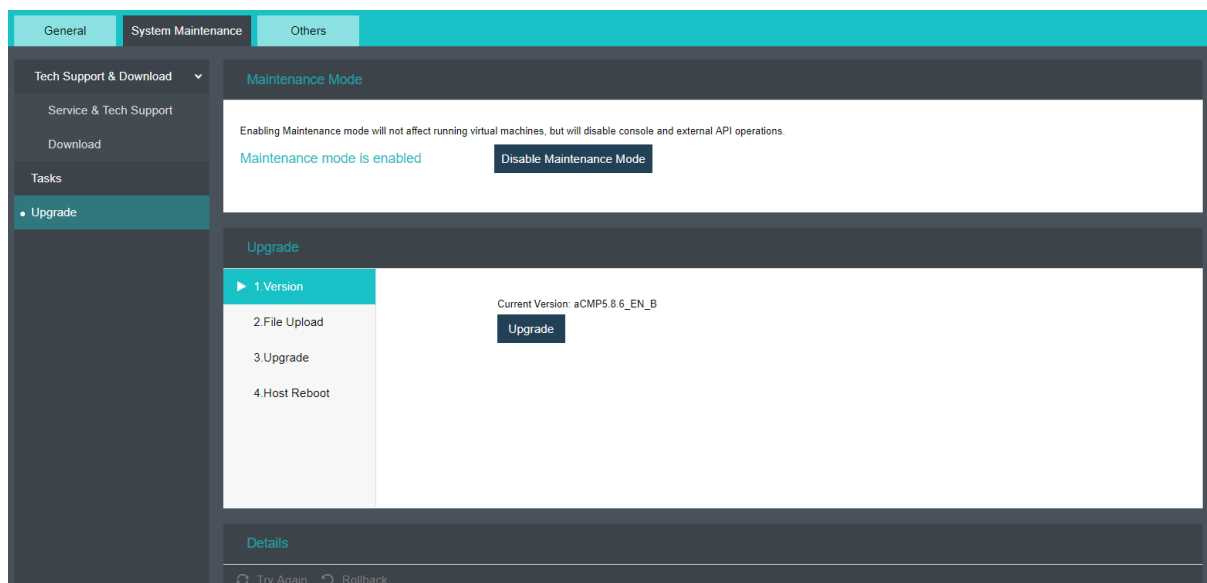
1. aCMP of other earlier versions have been deployed in the platform.
2. Upgrade Package of aCMP cloud management image has been prepared.

[Operating Steps]

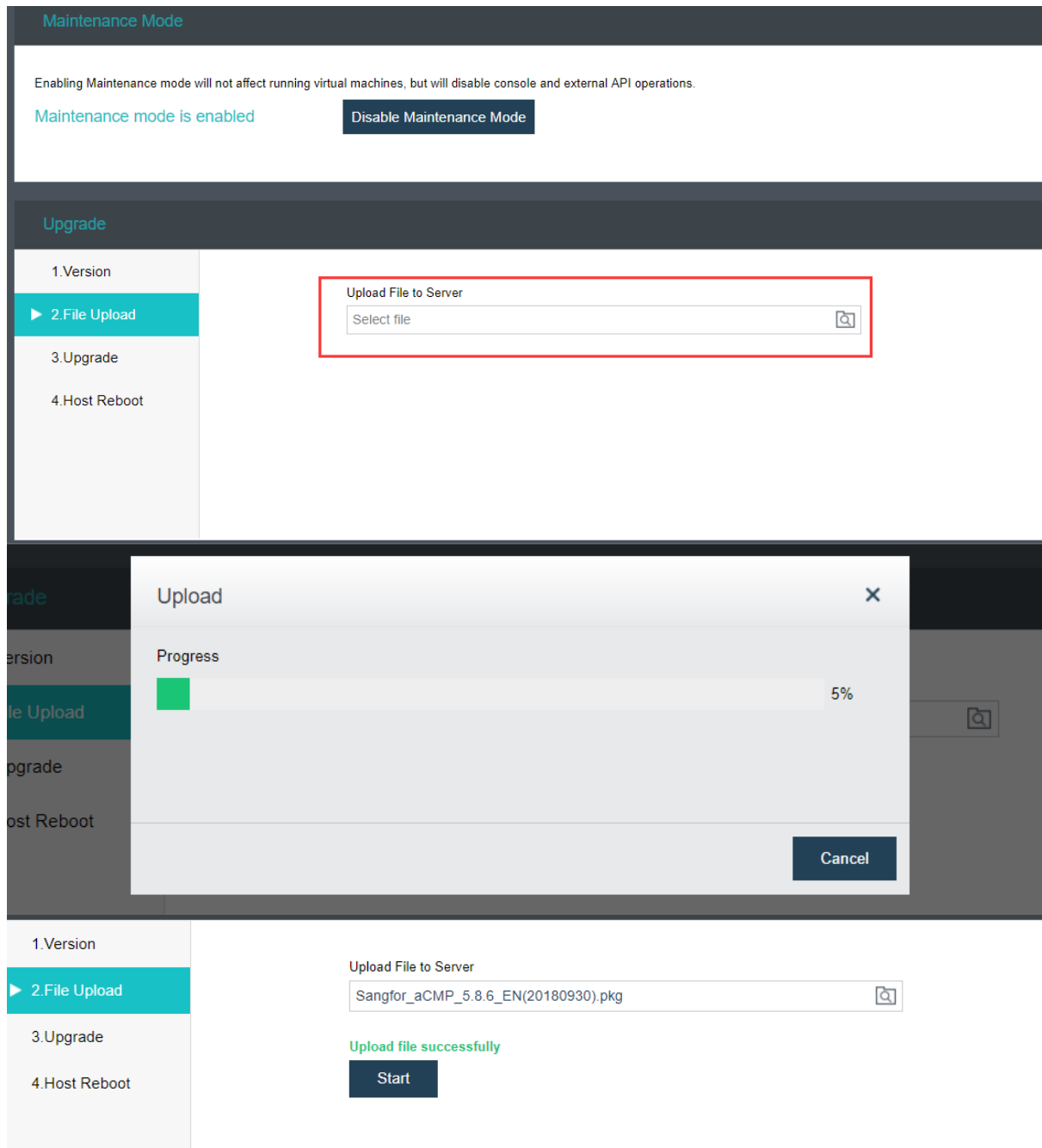
1. Log in the home page of aCMP platform console and click 『System』 → 『Upgrade』 to enter the device upgrade page;



2. Click 『Maintenance Mode is Enabled』 and then click 『Upgrade』 ;



3. Select Upload file to server;



4. After uploading successfully, click **Start**; after upgrading success, restart aCMP virtual machine;

The screenshot displays two sections of the aCMP platform console. The top section, titled "Maintenance Mode", contains the text "Enabling Maintenance mode will not affect running virtual machines, but will disable console and external API operations." Below this, it states "Maintenance mode is enabled" with a "Disable Maintenance Mode" button. The bottom section, titled "Upgrade", features a sidebar with steps: "1.Version", "2.File Upload", "3.Upgrade", and "4.Host Reboot" (which is highlighted with a blue bar and a play icon). The main area shows a progress bar for "4.Host Reboot" that is 100% complete, labeled "Completed". Below the progress bar, it says "It takes effect after platform restart." and includes a "Restart This Platform" button.



: During the upgrading process, the clusters in running will not be influenced; however, aCMP disables any other operations.

2.10 Delete Cluster

[Function Description]

If any cluster under the heterogeneous management of aCMP is required no more due to some demands, aCMP cluster can be deleted.

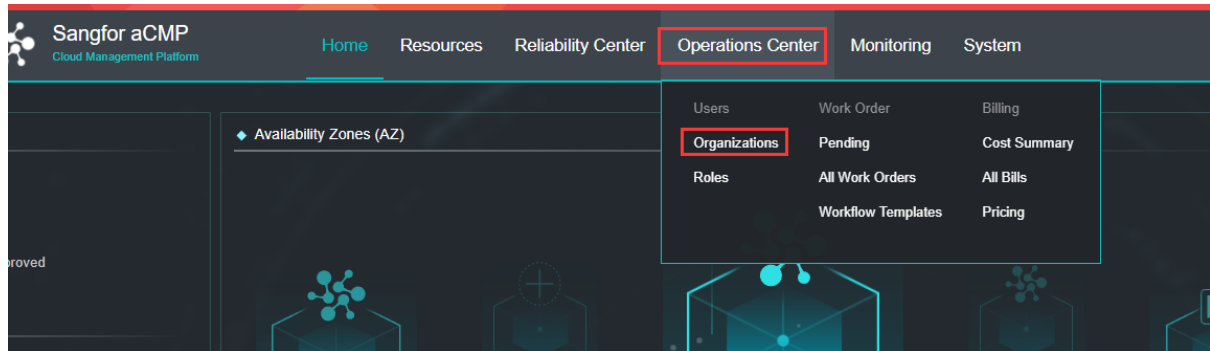
[Prerequisites]

If the cluster shall be deleted, the corresponding availability zone shall also be deleted.

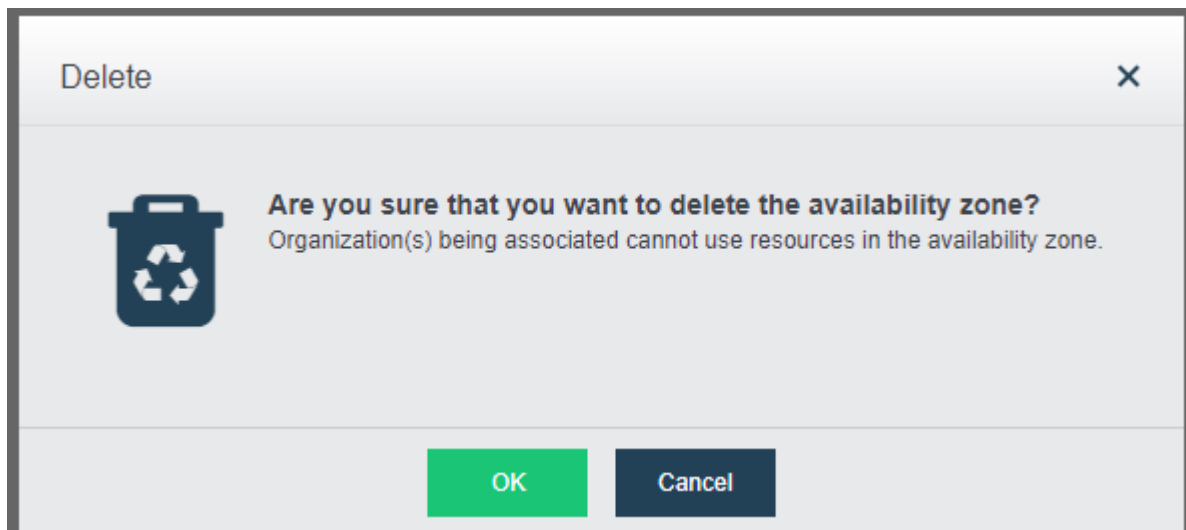
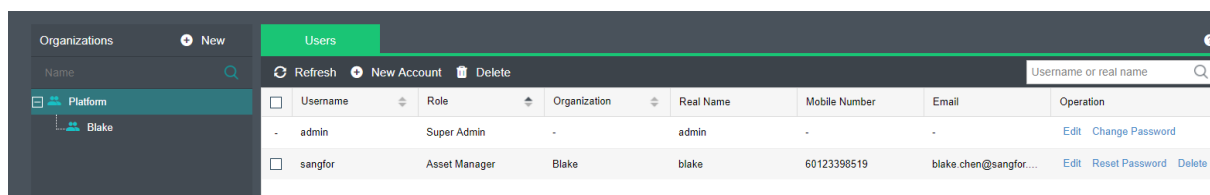
If the availability zone shall be deleted, the organizations and users created in the availability zone shall also be deleted.

[Operating Steps]

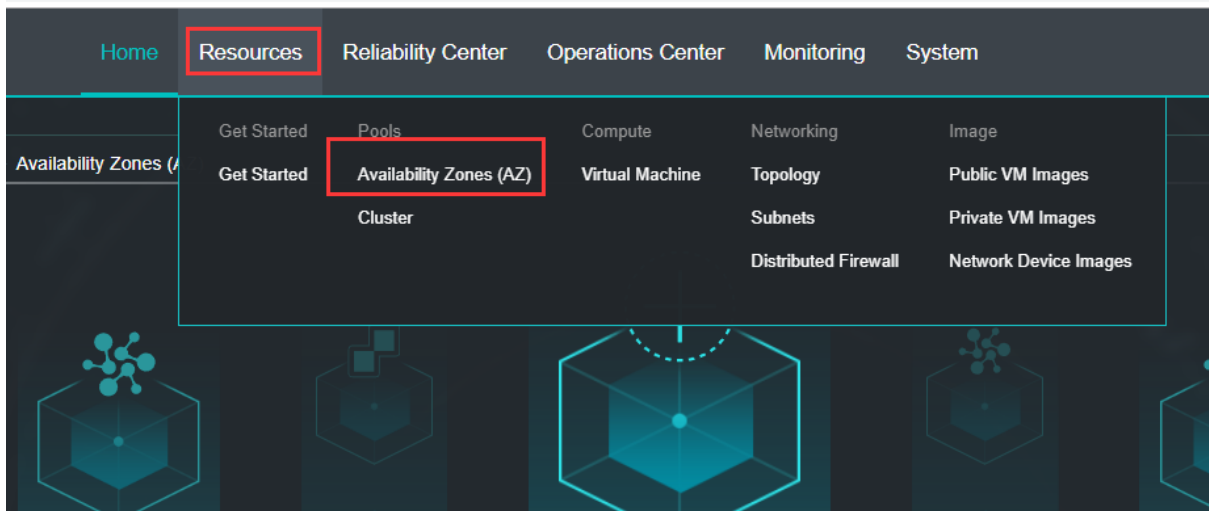
1. Log in the home page of aCMP platform console and click 『Operations Center』 → 『Organizations』 to enter the organization management interface:



2. Click 『Availability Zone』 to find all the associated users to be deleted, remove the corresponding user and click **OK**;

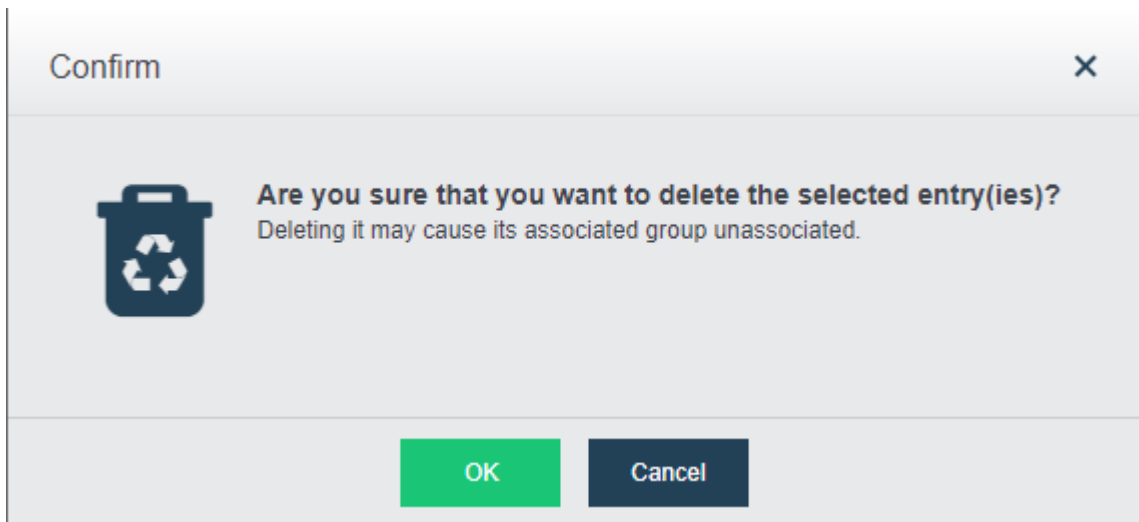


3. After all the associated organizations of the availability zone to be deleted are removed, click 『Resources』 → 『Availability Zone』 and you can find that Delete of the corresponding availability zone changes to be clickable; Click Delete and then click OK on the popped window;

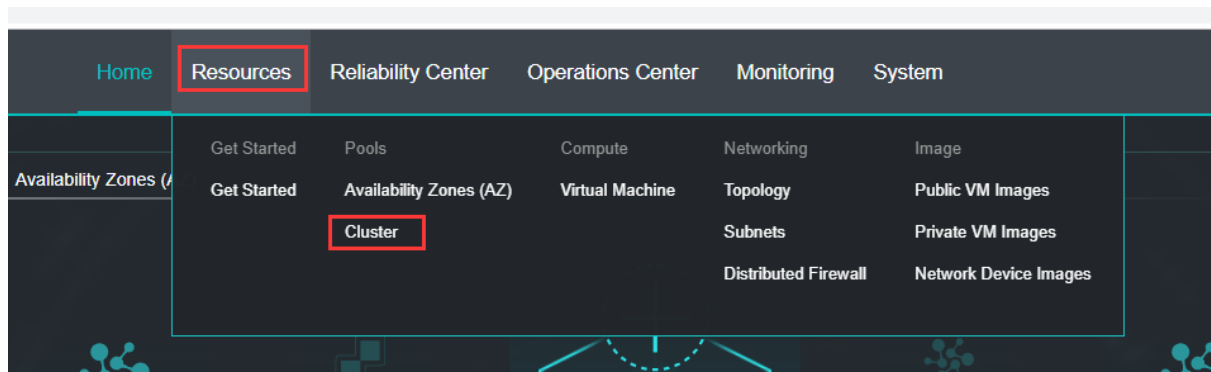


The screenshot shows the VMware vSphere Clusters page. The table below displays the following data:

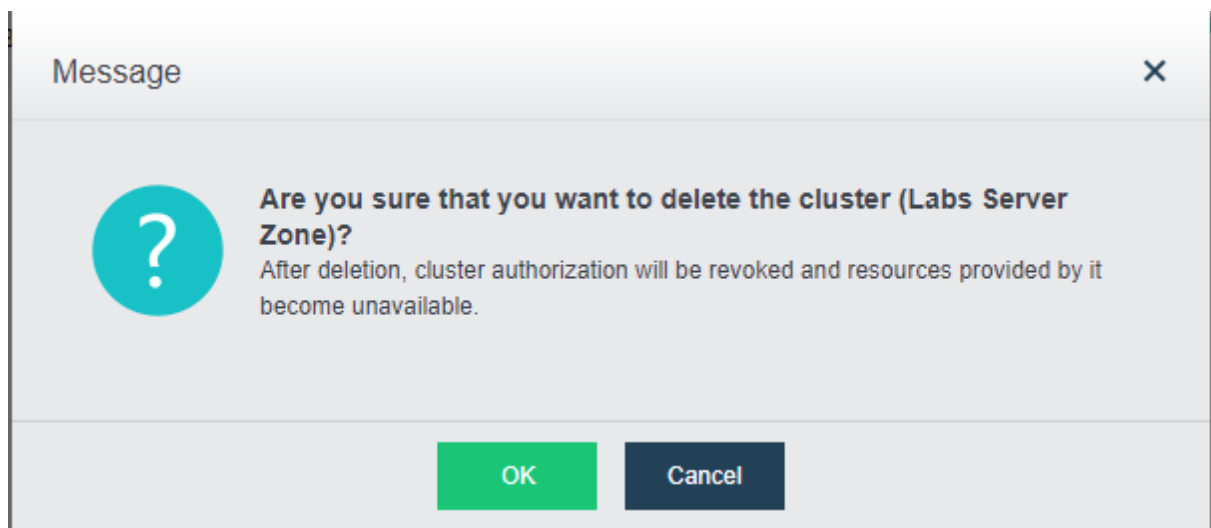
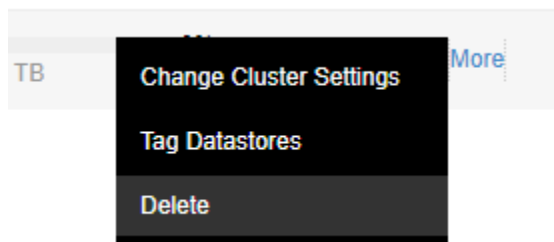
Name	Description	Resource	CPU Usage	Memory Usage	Storage Usage	Operation
DC zone (HCI)	-	aCloud	27.08 GHz / 53.62 GHz 51%	51.28 GB / 64 GB 80%	885.51 GB / 3.59 TB 24%	Edit Delete
DR zone (HCI)	-	aCloud	32.94 GHz / 163.27 GHz 20%	147.74 GB / 512 GB 29%	532.92 GB / 10.84 TB 5%	Edit Delete
sangfor CTI	-	aCloud	42.36 GHz / 50.42 GHz 84%	9.25 GB / 32 GB 29%	0 B / 0 B 0%	Edit Delete
vCenter zone	-	VMware	364 MHz / 11.39 GHz 3%	17.84 GB / 31.78 GB 56%	1.48 TB / 1.81 TB 82%	Edit Delete



4. Click 『Resources』 → 『Clusters』 to find the cluster to be deleted, click “More”-“Delete” and then click **OK** on the popped window to delete the cluster, as shown in the following diagram:



Status	Name	Description	Availability Zones	Cluster IP	Cluster Type	Version	CPU Usage	Memory Usage	Storage Usage	Operation
Normal	DC (CTI)	-	DC zone (HCI)	192.168.1.35	aCloud	5.8.6	24.98 GHz / 53.62 GHz 47%	51.34 GB / 64 GB 80%	688.39 GB / 3.98 TB 24%	Visit Edit More
Normal	DR(demo)	-	DR zone (HCI)	192.200.19.20	aCloud	5.8.6	25.16 GHz / 163.27 GHz 15%	147.67 GB / 512 GB 29%	534.68 GB / 10.84 TB 5%	Visit Edit More
Normal	ESXi	-	vCenter zone	192.168.19.200	VMware	6.5.0	406 MHz / 11.39 GHz 4%	17.84 GB / 31.78 GB 56%	1.48 TB / 1.81 TB 82%	Edit More
Normal	Labs Server Zone	-	-	192.168.19.174	aCloud	5.8.6	34.29 GHz / 58.42 GHz 68%	9.09 GB / 32 GB 28%	5.33 GB / 11.7 TB 0%	Visit Edit More



Chapter3 Operation Maintenance and Management

3.1 Basic Management

3.1.1 System Configuration

3.1.1.1 Time and Date Configuration

[Function Description]

As for time setting of aCMP platform, SANGFOR aCMP supports both the time customization and the automatic acquisition of NTP time.

[Prerequisites]

aCloud platform and aCMP virtual machine of SANGFOR Enterprise-level Cloud have been correctly deployed. If NTP time shall be acquired, it shall be guaranteed that aCMP can get access to NTP server network.

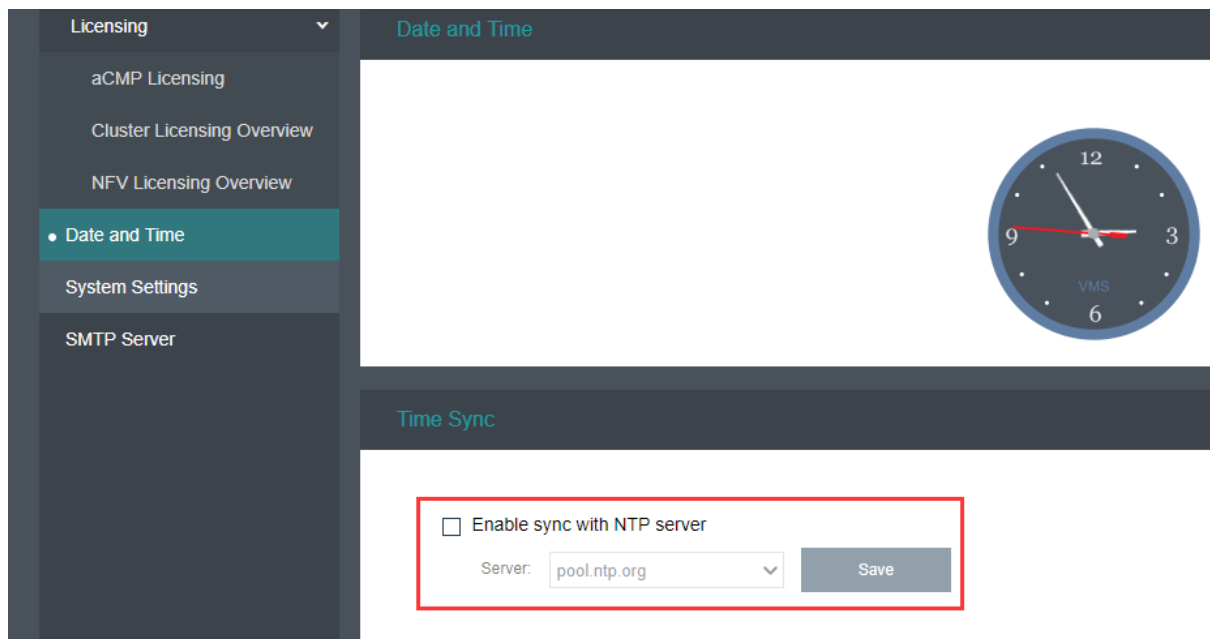
[Operating Steps]

1. Log in the home page of aCMP platform and select 『System』 → 『Date and Time』 ;

The screenshot displays the Sangfor aCMP Cloud Management Platform interface. The top navigation bar includes 'Home', 'Resources', 'Reliability Center', 'Operations Center', 'Monitoring', and 'System'. The 'System' menu is expanded, showing options like 'General', 'System Maintenance', 'Recycle Bin', 'Licensing', 'Tech Support & Download', 'Tasks', 'System Settings', and 'SMTP Server'. The 'Date and Time' option is highlighted. Below the navigation, the 'Date and Time' configuration page is shown, featuring a clock, the current time '14:53:25', the date '2018-10-10 Wednesday', and the time zone '(UTC+08:00) Irkutsk, Beijing'. A 'Change' button is visible. The 'Time Sync' section includes a checkbox for 'Enable sync with NTP server' and a 'Server' dropdown menu with 'pool.ntp.org' selected, followed by a 'Save' button.

2. Click 『Change』 to enter the time setting; you can customize the time or get the local time;

3. SANGFOR aCMP supports the synchronization of NTP server; please do the setting as required.



3.1.1.2 IP Setting of the Platform

[Function Description]

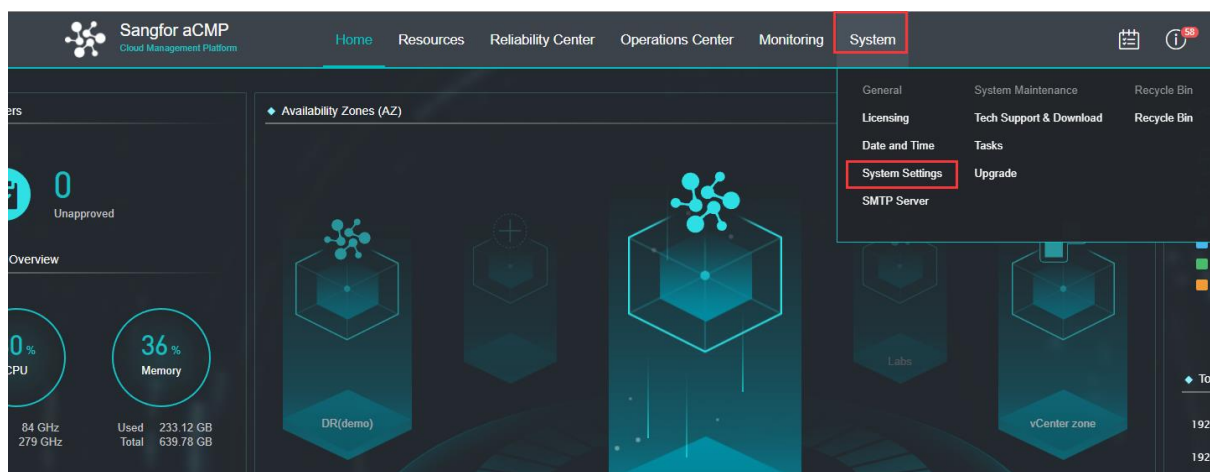
SANGFOR aCMP supports the change of IP as required and the DNS and route configuration of aCMP via the network satisfying the different scenarios.

[Prerequisites]

IP and gateway have been correctly planned.

[Operating Steps]

1. Log in the home page of aCMP platform and select 『System』 → 『System Configuration』 ;



2. Configure IP according to the actual situation of network and configure the route and the platform DNS according to the requirement.

The screenshot displays the 'System Settings' configuration page in the SANGFOR aCMP management interface. The left sidebar contains navigation options: General, System Maintenance, Others, Licensing, aCMP Licensing, Cluster Licensing Overview, NFV Licensing Overview, Date and Time, System Settings (selected), and SMTP Server. The main content area is divided into three sections, each with a red box highlighting its configuration fields:

- System Settings:** A note states 'Cloud management platform (CMP) supports web-based access on specified IP address'. Below this are three input fields: 'IP Address (eth0)' with the value '192.168.19.172', 'Netmask' with '255.255.255.0', and 'Default Gateway' with '192.168.19.1'. A green 'Save' button is located below these fields.
- Routing:** A table with columns 'Dst IP', 'Netmask', 'Next-Hop IP', and 'Operation'. The table is currently empty, displaying 'No data available'. Above the table are 'New' and 'Delete' buttons.
- DNS Servers:** Two input fields for 'Preferred DNS' and 'Alternate DNS'. A green 'Save' button is located below these fields.

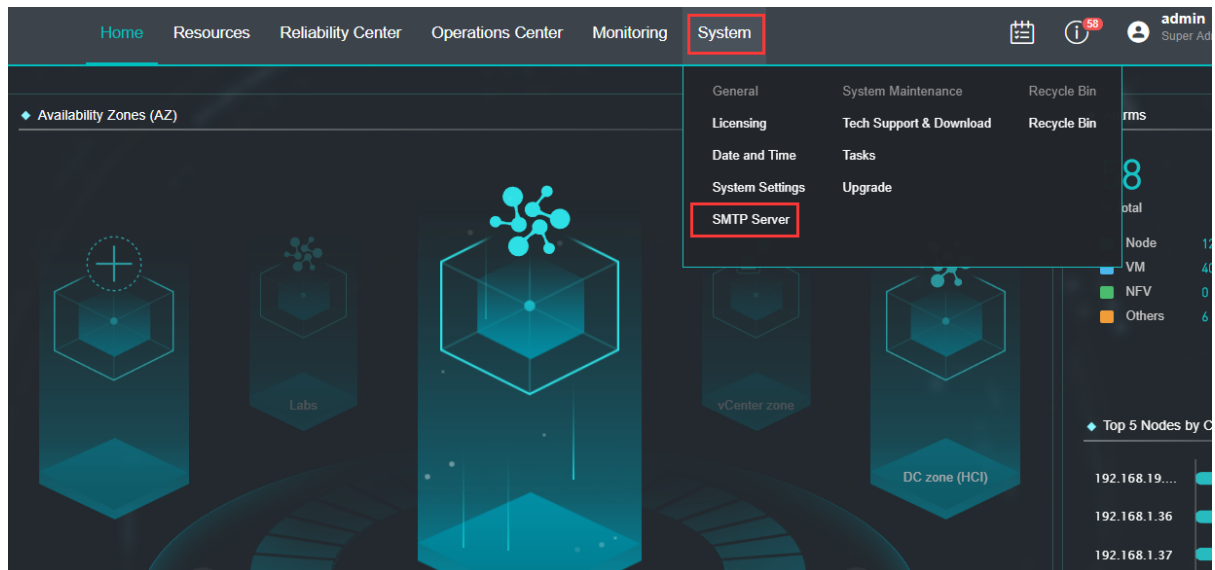
3.1.1.3 Mailbox Setting

[Function Description]

SANGFOR aCMP is configured with Mailbox and you can send the alarm by Mailbox. The customer can master the running state of clusters at any time.

[Operating Steps]

1. Log in the home page of aCMP platform and select 『System』 → 『SMTP Server』 ;



2. Fill in Mailbox address and smtp server address according to the actual situation; if the sending server requires authentication of the username and password, the corresponding username and password shall be entered and the testing shall be carried out.

3.1.2 System Maintenance

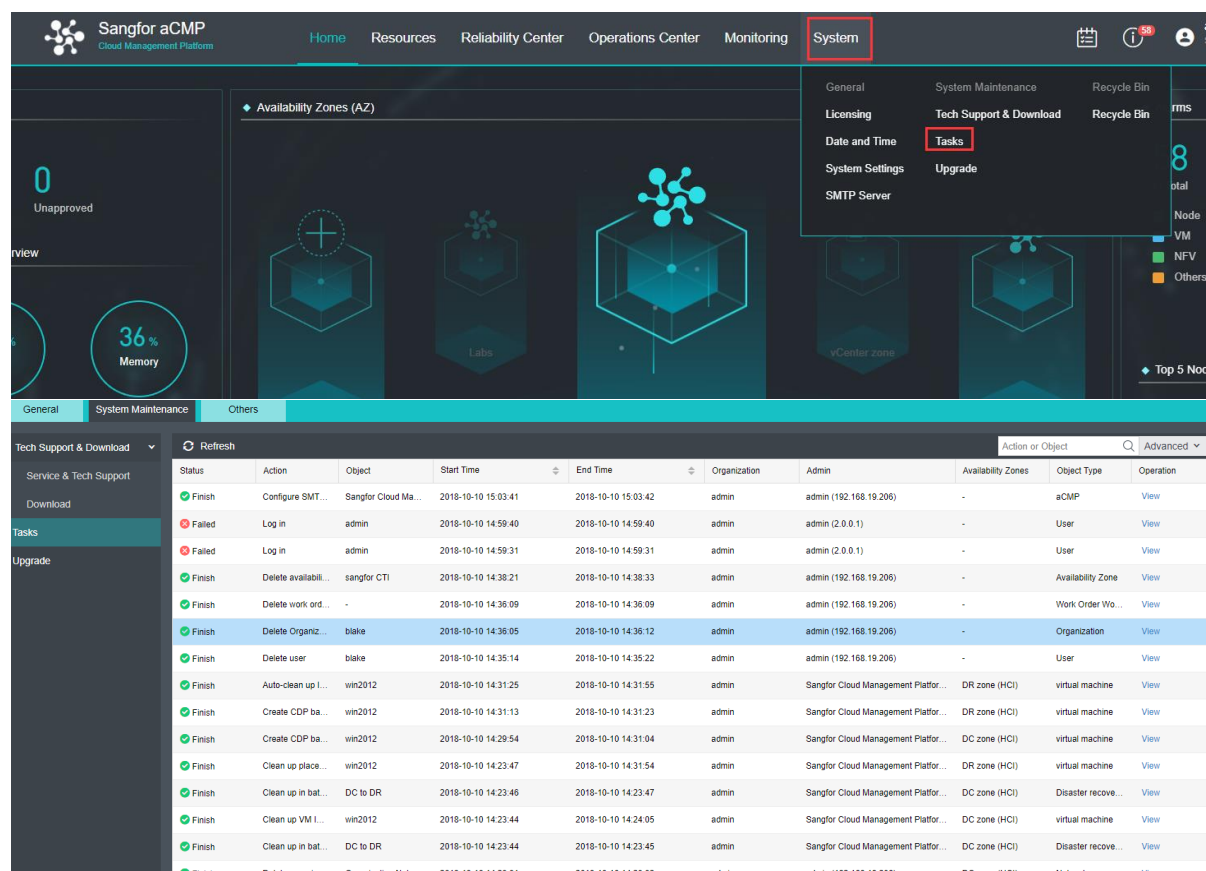
3.1.2.1 View of Tasks Logs

[Function Description]

SANGFOR aCMP will record all the operation logs and synchronously the operation results. For example, the administrator can examine the historical operation records on this page to orientate the fault causes.

[Operating Steps]

1. Log in the home page of aCMP platform and select 『System』 → 『Tasks』 ;



Status	Action	Object	Start Time	End Time	Organization	Admin	Availability Zones	Object Type	Operation
Finish	Configure SMT...	Sangfor Cloud Ma...	2018-10-10 15:03:41	2018-10-10 15:03:42	admin	admin (192.168.19.206)	-	aCMP	View
Failed	Log in	admin	2018-10-10 14:59:40	2018-10-10 14:59:40	admin	admin (2.0.0.1)	-	User	View
Failed	Log in	admin	2018-10-10 14:59:31	2018-10-10 14:59:31	admin	admin (2.0.0.1)	-	User	View
Finish	Delete availabili...	sangfor CTI	2018-10-10 14:38:21	2018-10-10 14:38:33	admin	admin (192.168.19.206)	-	Availability Zone	View
Finish	Delete work ord...	-	2018-10-10 14:36:09	2018-10-10 14:36:09	admin	admin (192.168.19.206)	-	Work Order Wo...	View
Finish	Delete Organiz...	blake	2018-10-10 14:36:05	2018-10-10 14:36:12	admin	admin (192.168.19.206)	-	Organization	View
Finish	Delete user	blake	2018-10-10 14:35:14	2018-10-10 14:35:22	admin	admin (192.168.19.206)	-	User	View
Finish	Auto-clean up l...	win2012	2018-10-10 14:31:25	2018-10-10 14:31:55	admin	Sangfor Cloud Management Platfor...	DR zone (HCI)	virtual machine	View
Finish	Create CDP ba...	win2012	2018-10-10 14:31:13	2018-10-10 14:31:23	admin	Sangfor Cloud Management Platfor...	DR zone (HCI)	virtual machine	View
Finish	Create CDP ba...	win2012	2018-10-10 14:29:54	2018-10-10 14:31:04	admin	Sangfor Cloud Management Platfor...	DC zone (HCI)	virtual machine	View
Finish	Clean up place...	win2012	2018-10-10 14:23:47	2018-10-10 14:31:54	admin	Sangfor Cloud Management Platfor...	DR zone (HCI)	virtual machine	View
Finish	Clean up in bat...	DC to DR	2018-10-10 14:23:46	2018-10-10 14:23:47	admin	Sangfor Cloud Management Platfor...	DC zone (HCI)	Disaster recove...	View
Finish	Clean up VM l...	win2012	2018-10-10 14:23:44	2018-10-10 14:24:05	admin	Sangfor Cloud Management Platfor...	DC zone (HCI)	virtual machine	View
Finish	Clean up in bat...	DC to DR	2018-10-10 14:23:44	2018-10-10 14:23:45	admin	Sangfor Cloud Management Platfor...	DC zone (HCI)	Disaster recove...	View
Finish	Delete organiza...	Organization Netw...	2018-10-10 14:20:01	2018-10-10 14:20:02	admin	admin (192.168.19.206)	DC zone (HCI)	Network	View

3.1.3 Business Maintenance

3.1.3.1 Recycle Bin

[Function Description]

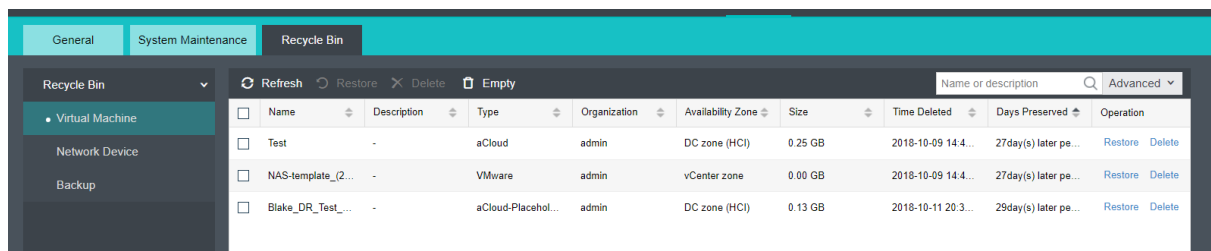
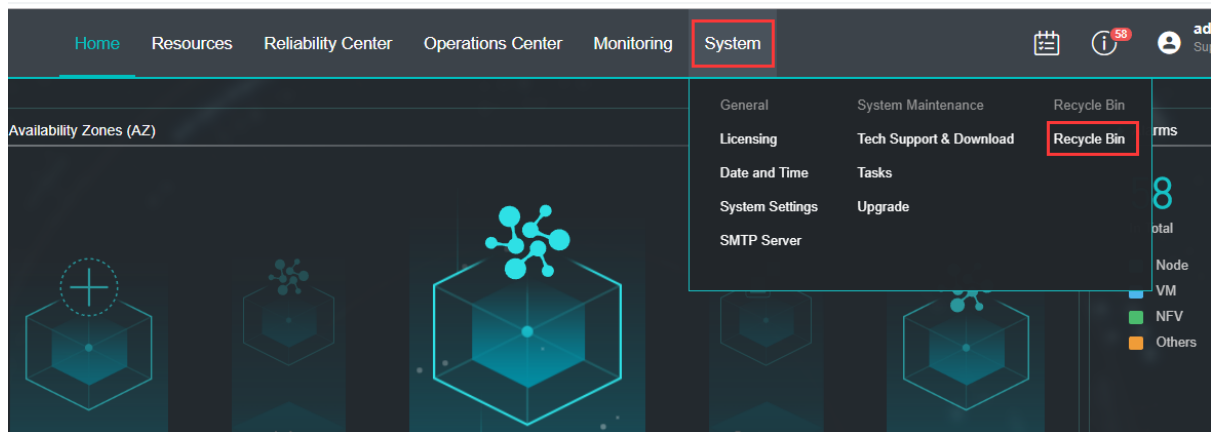
SANGFOR aCMP strongly protects the data safety of the platform. When the administrator deletes the virtual machine and network devices of the platform, these devices will be moved into recycle bin to keep for a while. They are recoverable during this period but not recoverable once timeout or manually and completely deleted.

[Note]

Virtual machine cannot be recovered once deleted from recycle bin; please do the operation carefully.

[Operating Steps]

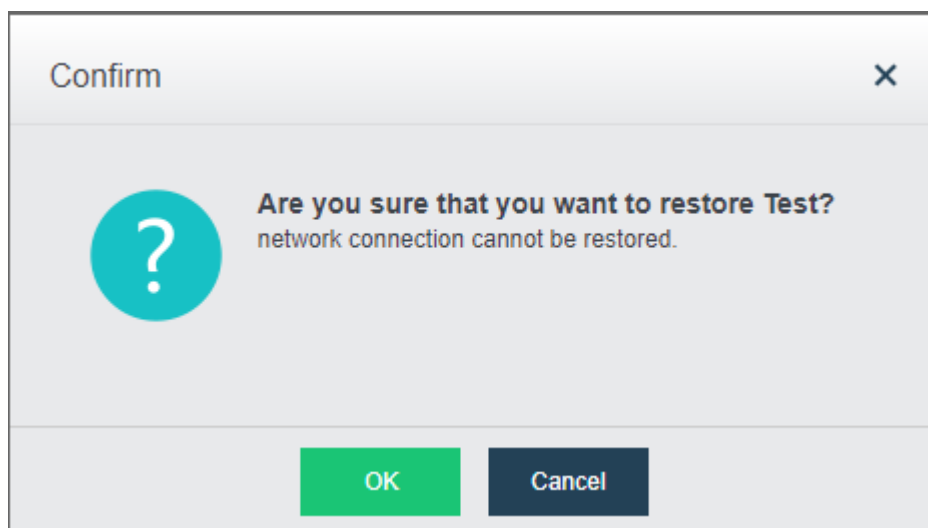
1. Log in the home page of aCMP platform and select 『System』 → 『Recycle Bin』 to enter the recycle bin interface;



2. Tick the virtual machine or network device to be deleted and click **Restore** or **Delete** to restore or delete the virtual machine in the recycle bin.



Note: This deletion operation will completely delete the data of virtual machine or network device; please do the operation carefully.



3.2 Resource Management

3.2.1 Image Management

3.2.1.1 Public Image Management

[Function Description]

The administrator can upload the images to all availability zones or organizations for use. Image is divided into public image and private image and the relevant explanation is given as follows:

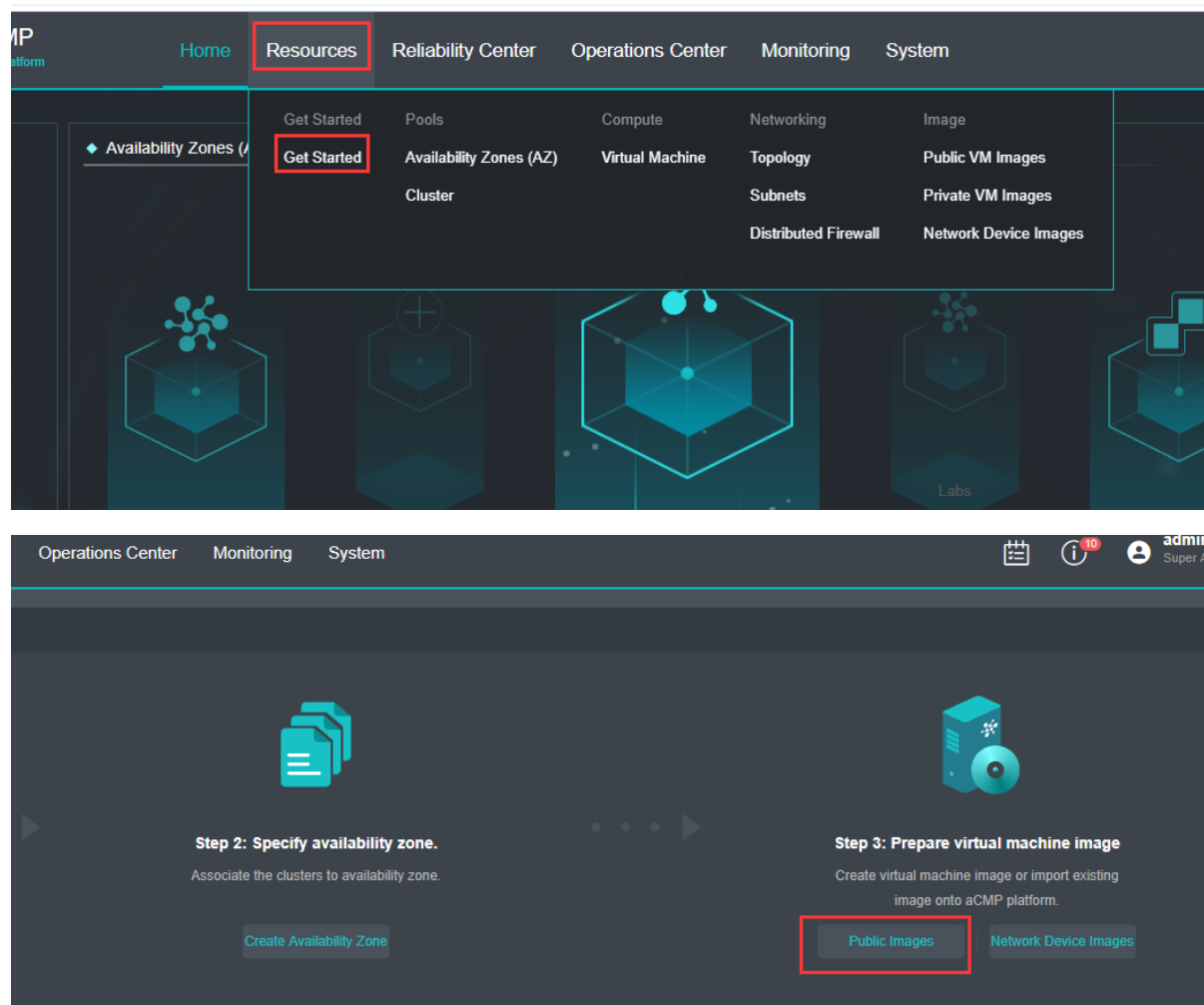
- **Public Image:** it is created by platform administrator and can be used by both platform administrator and tenants.
- **Private Images:** created by tenant administrator and used only among tenants
- **Network Device Images:** template images of NFV, uploaded by platform administrator

[Prerequisites]

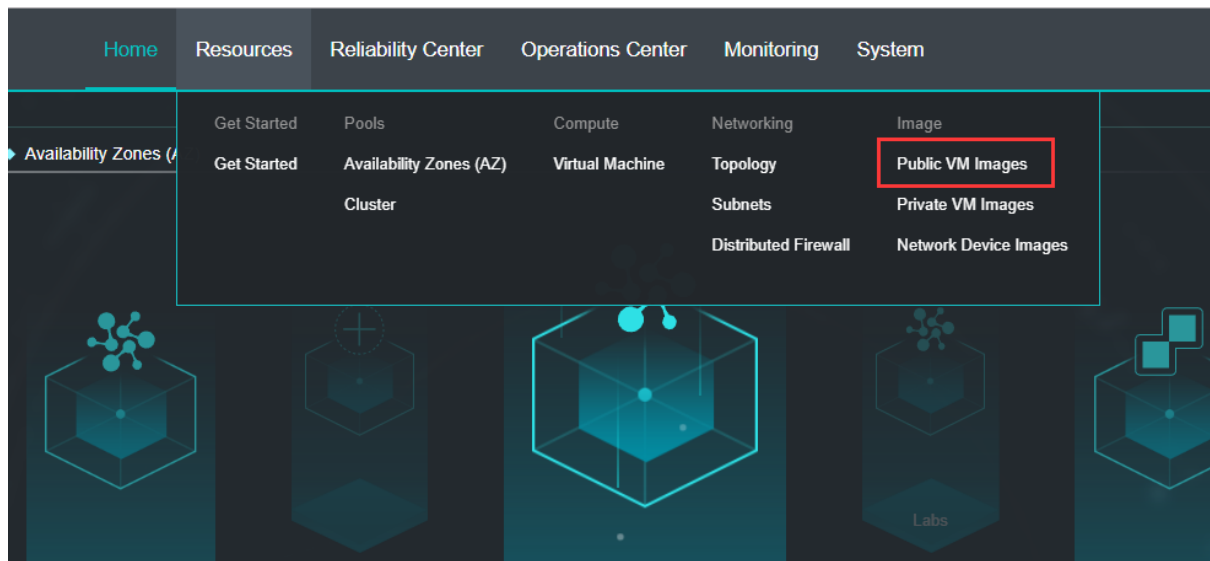
SANGFOR aCMP has sufficient image storage space

[Operating Steps]

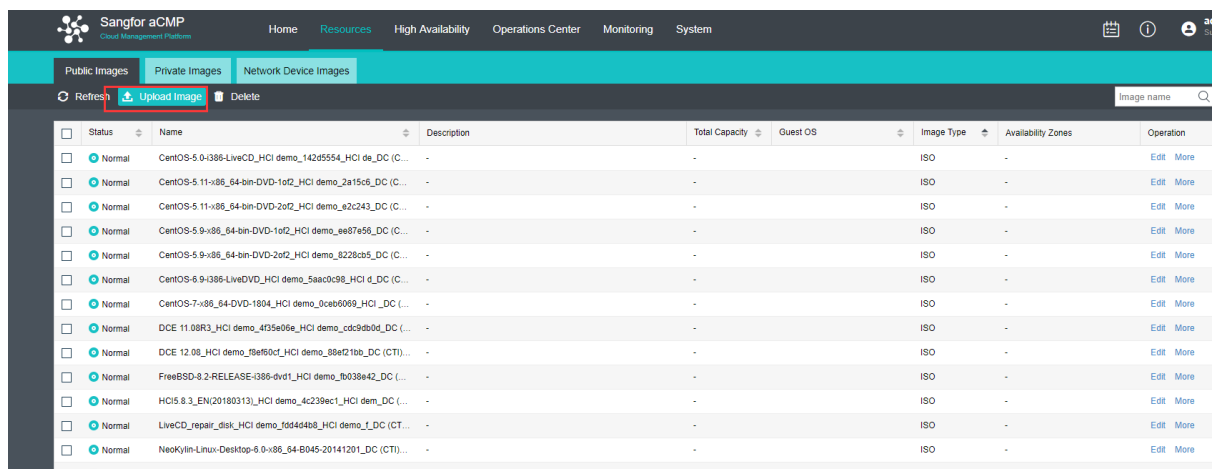
1. Log in the home page of aCMP platform, select 『Resources』 → 『Get Started』 , click Public Images to enter the Public Images Management Interface as shown in the following figure:



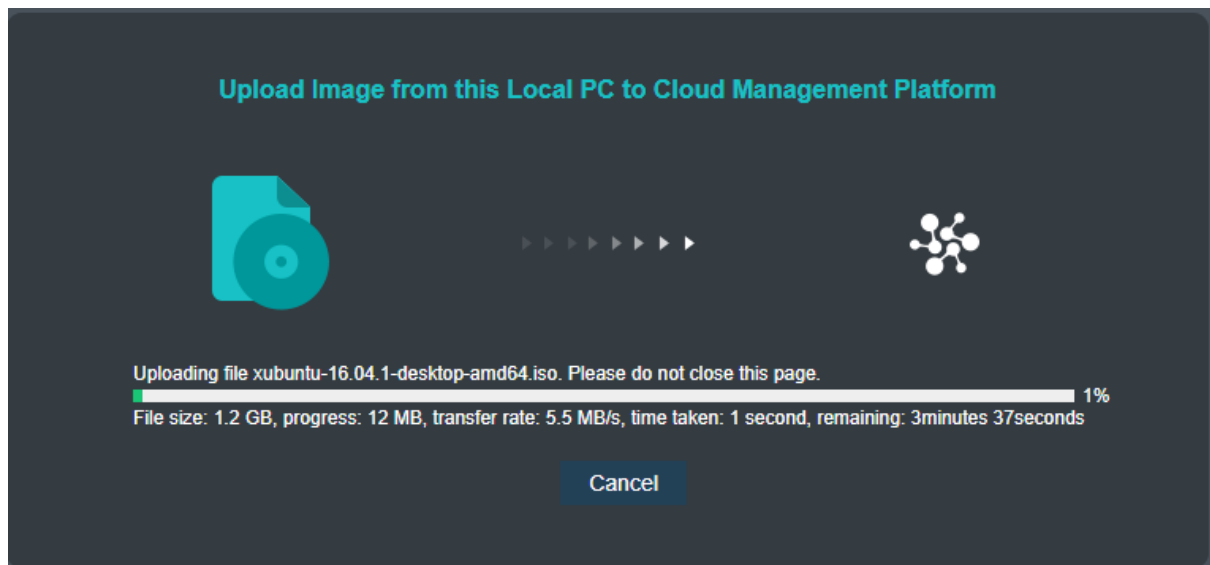
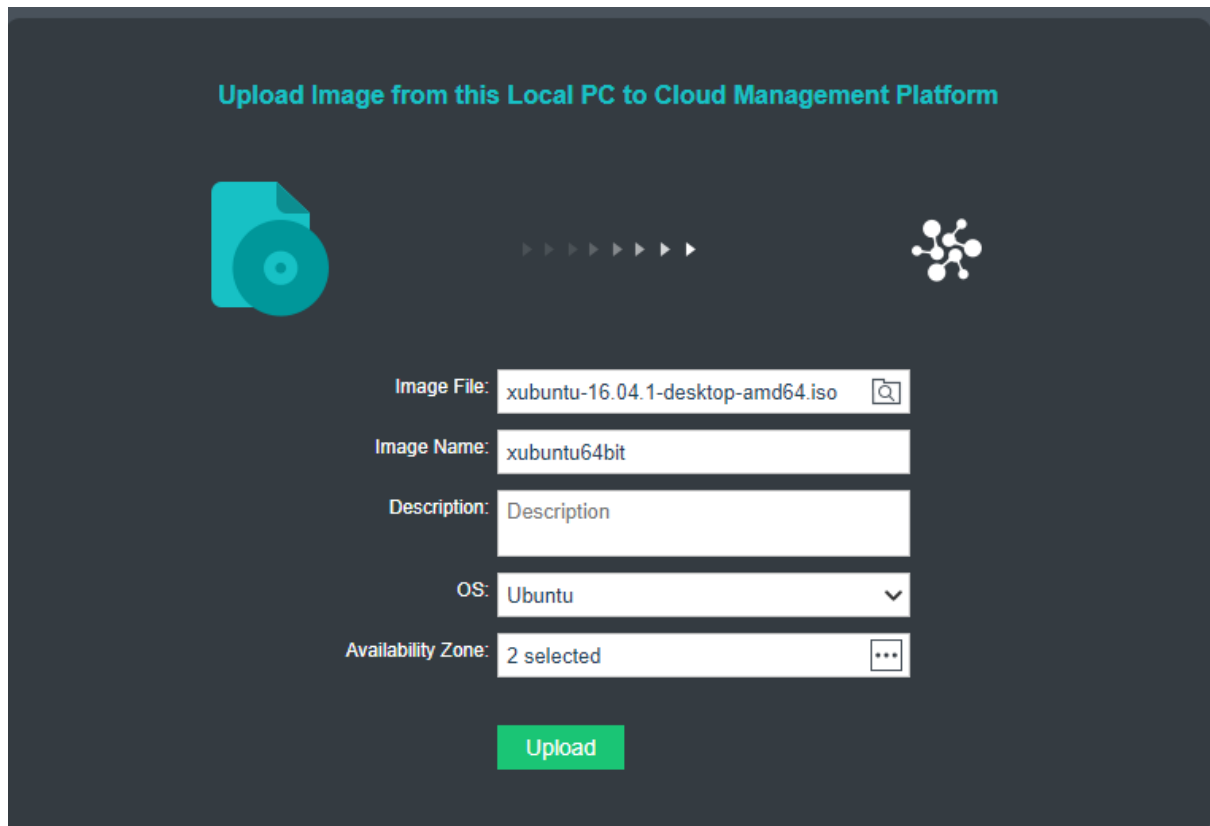
Or select 『Resources』 → 『Public VM Images』 to enter the VM Images Management Interface;



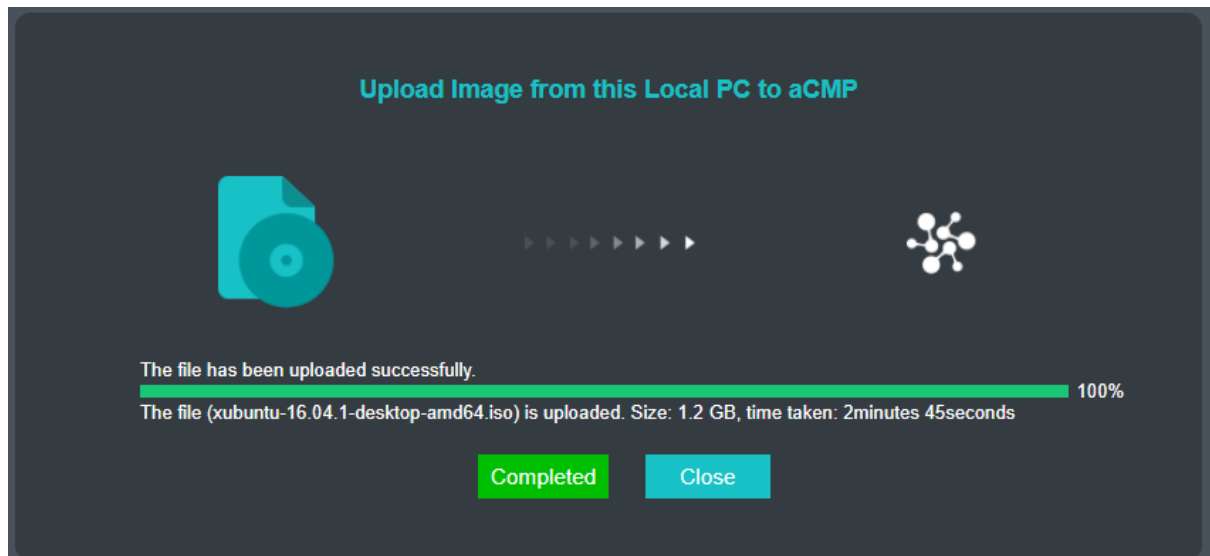
2. On the current page, you can see all existing images on aCMP, including public images, private images and network device images. The Public Images page is selected by default. Click the **Upload Image**;



3. Select local images to be uploaded; fill in the corresponding information; select the corresponding operating system and availability zone, and click Upload;



4. Upon the completion of uploading, click **Completed** to continue to upload or click **Close**.



3.2.1.2 Management of Private Images

[Function description]

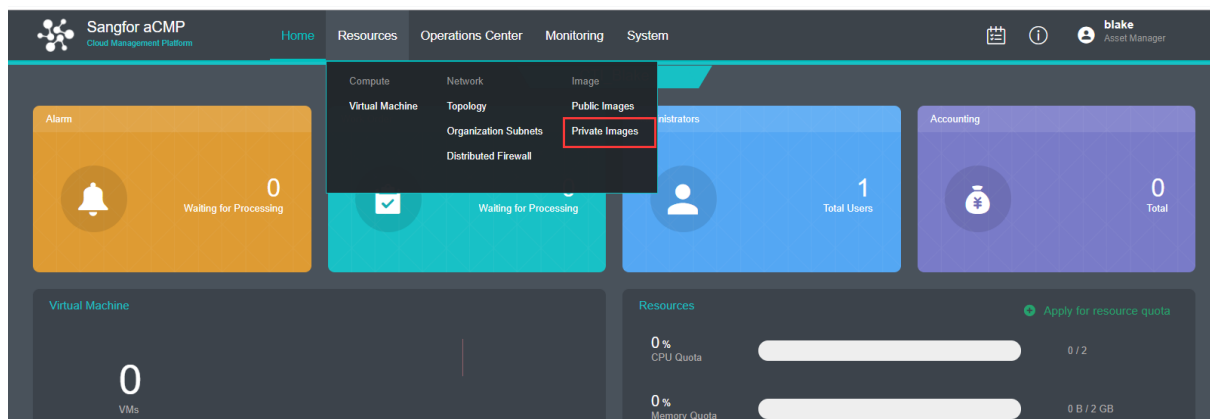
If the platform administrator does not assign the required image to the organization administrator, the latter can also upload private images according to his own needs. Private images can only be used within the organization.

[Prerequisites]

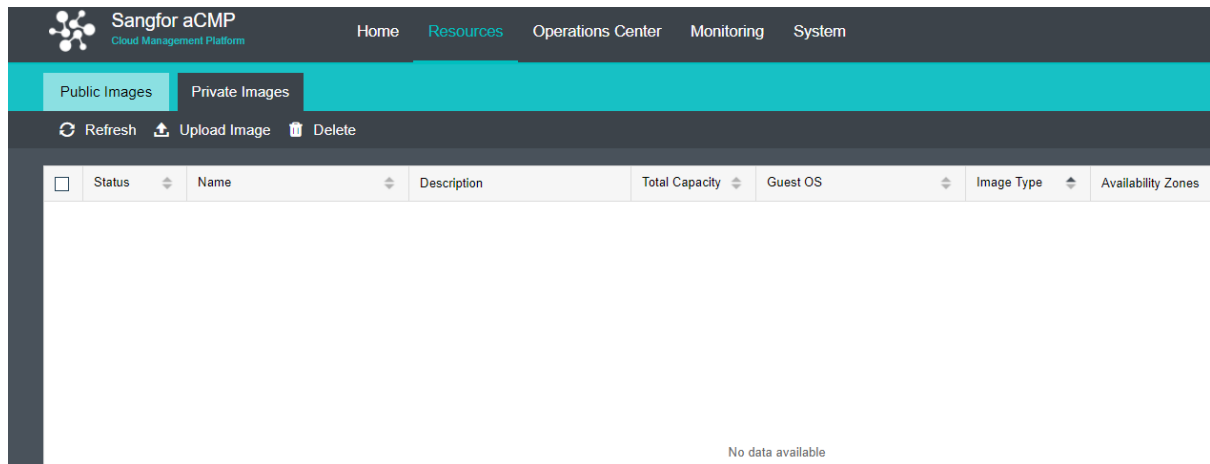
Prepare the ISO file to be uploaded

[Operating Steps]

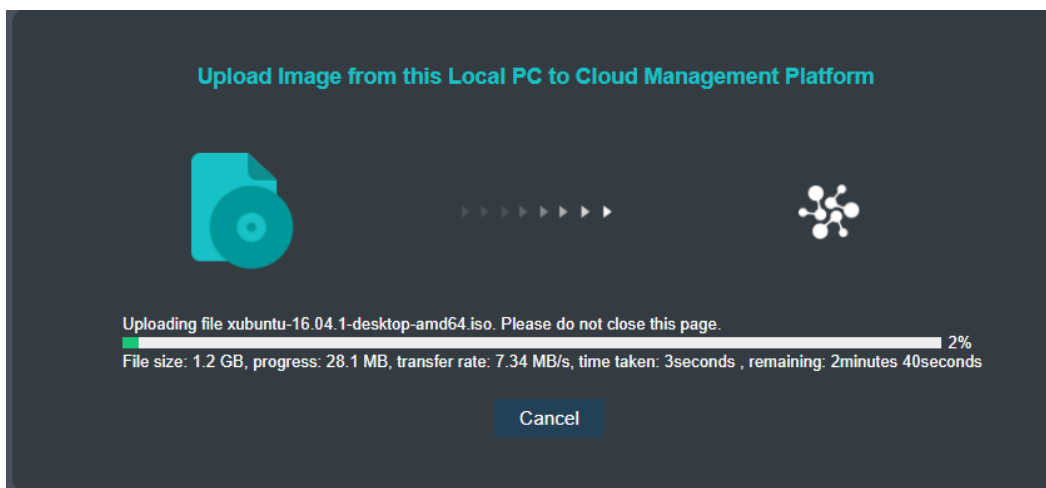
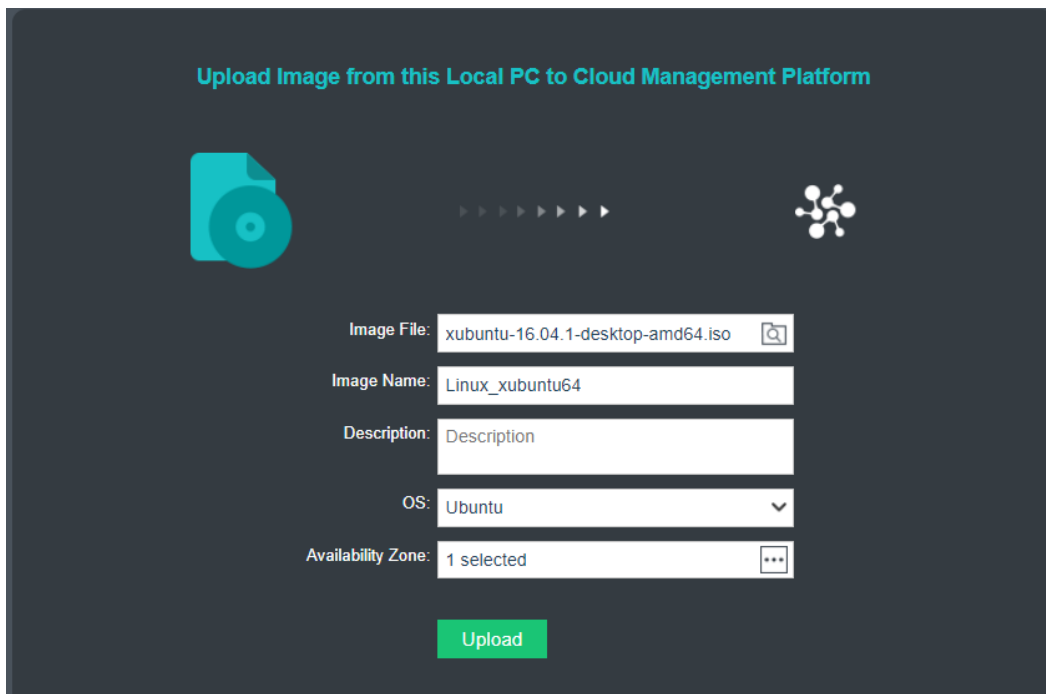
1. Log in to the home page of aCMP organization administrator (<https://IP>); select 『Resources』 → 『Private Images』 ; click Upload Image



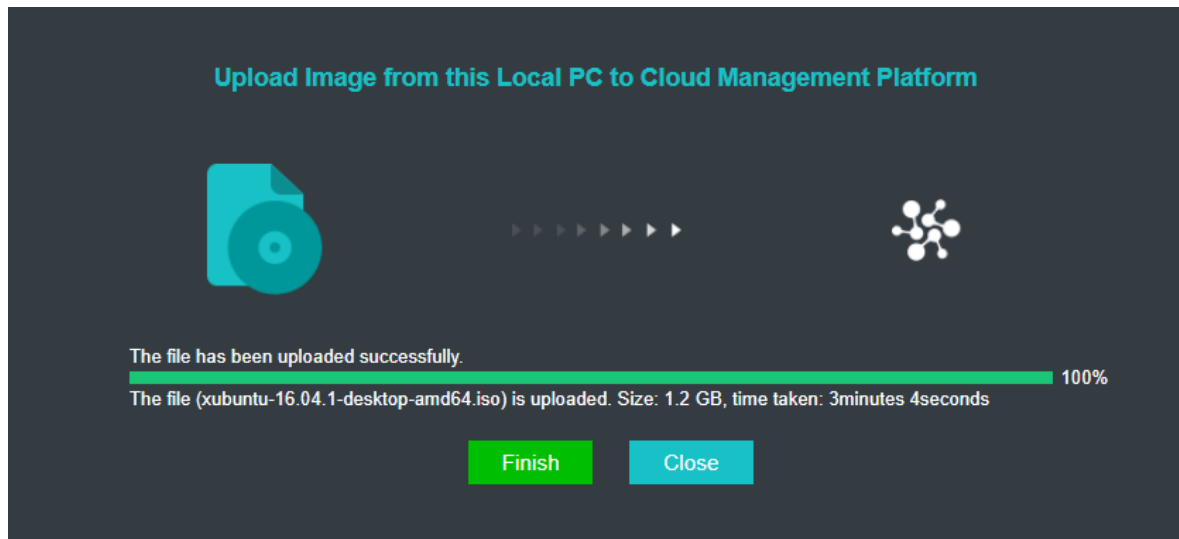
The following configuration page will be displayed after login:



2. Select the images to be uploaded, configure accordingly; click Upload



3. Upon the completion of uploading, click **Completed** to continue to upload or click **Close**. See the following figure:



3.2.1.3 Management of Network Device Images

[Function Description]

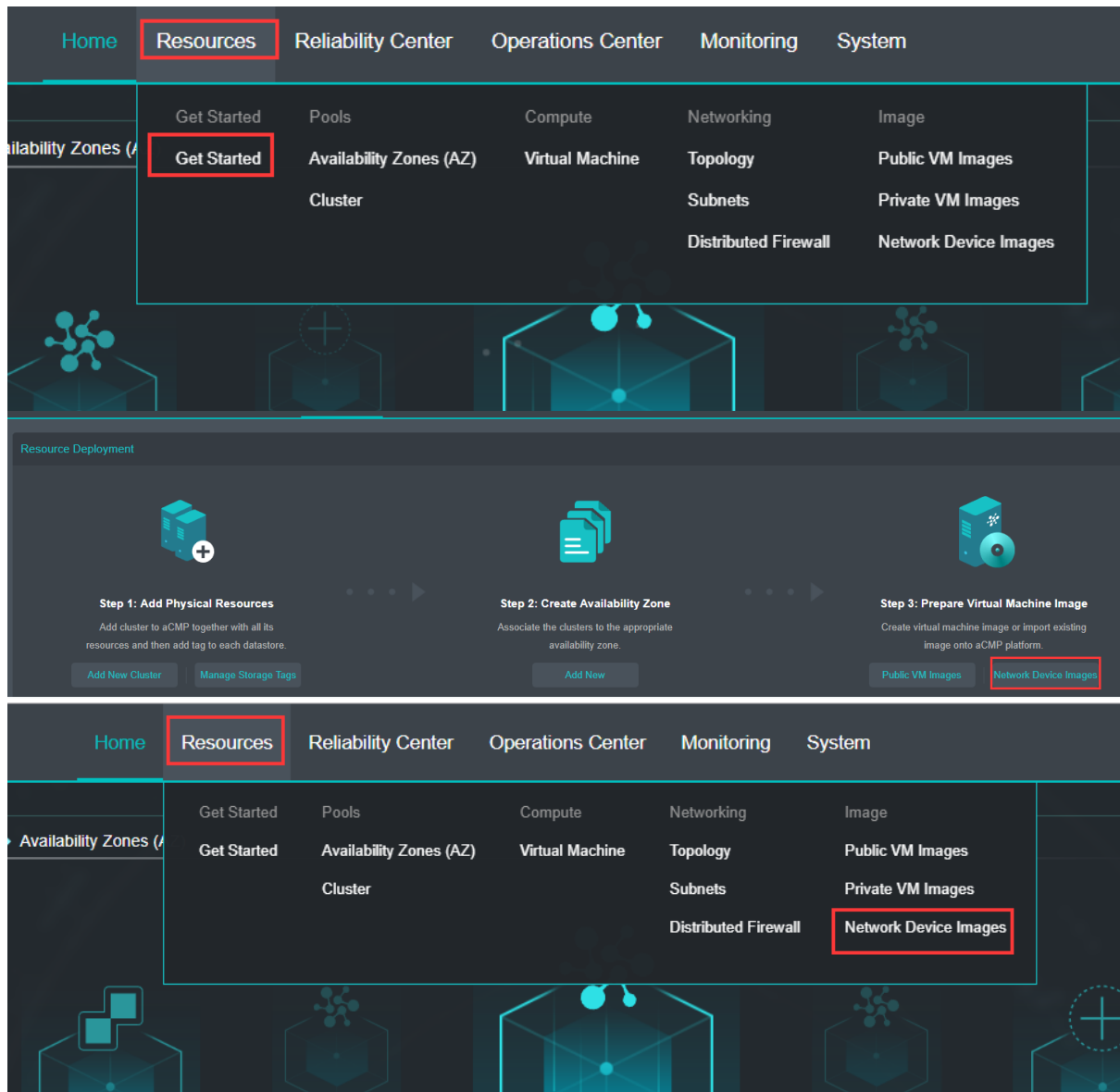
If the networking requirements of virtual network include network security components, such as vAD and vAC (please download security components from the official website of SANGFOR), you need to upload the corresponding network device images via which the corresponding security component instance can be created. The platform administrator can manage virtual network images through the management function of network device images.

[Prerequisites]

1. SANGFOR aCMP has sufficient images storage
2. Prepare network device images and authorization

[Operating Steps]

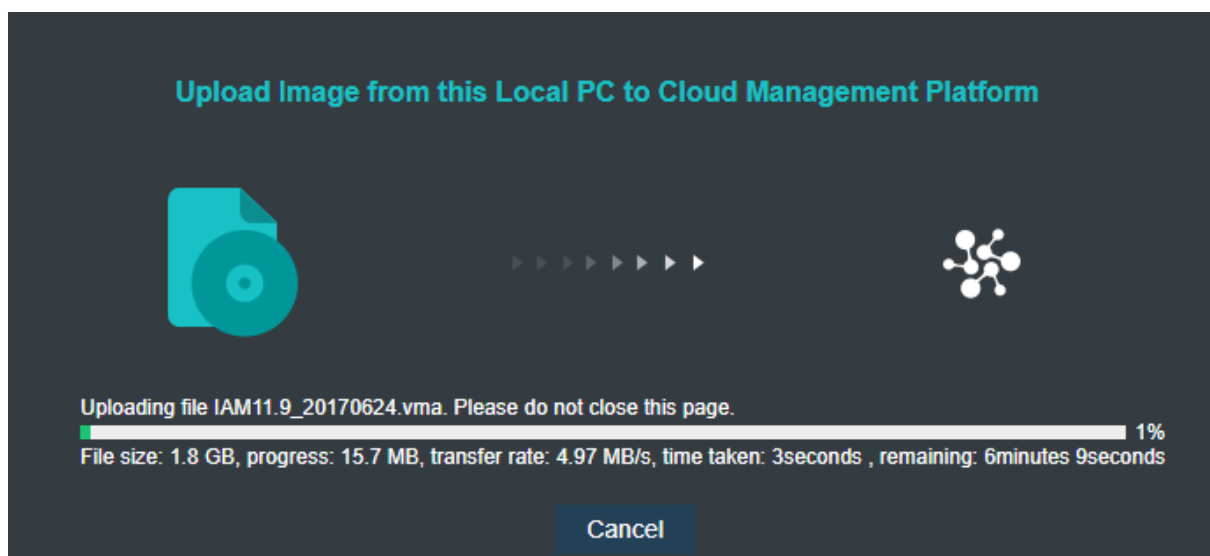
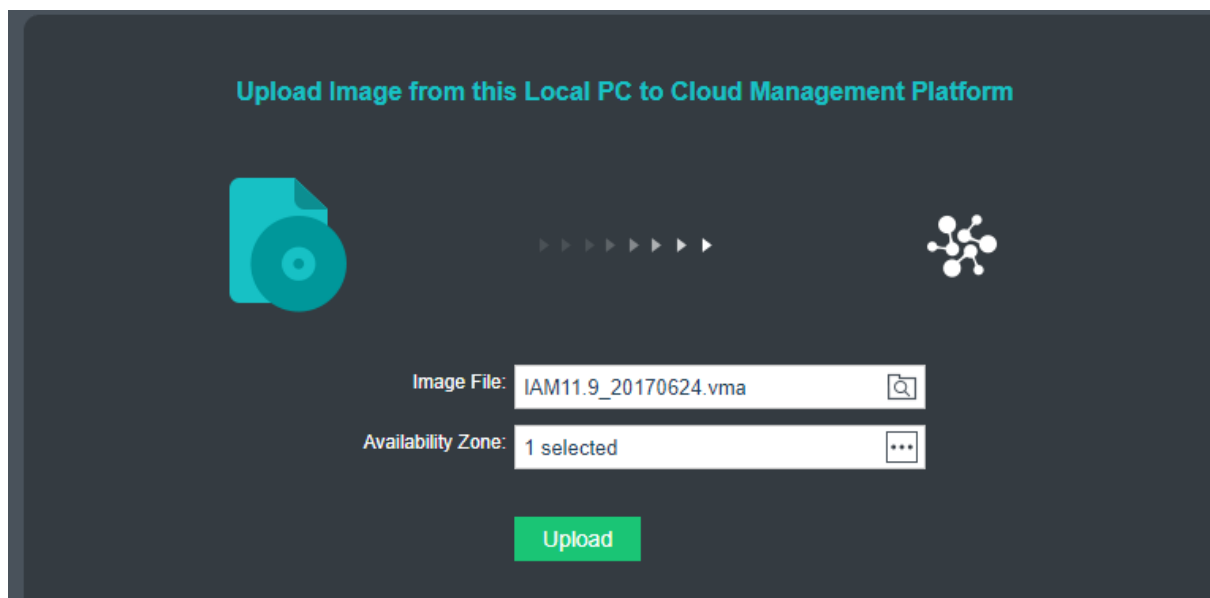
1. Log in to the home page of aCMP platform, select 『Resources』 → 『Get Started』, click **Upload Network Device Template**; or directly select 『Resources』 → 『Network Device Images』 to enter network device images management page;



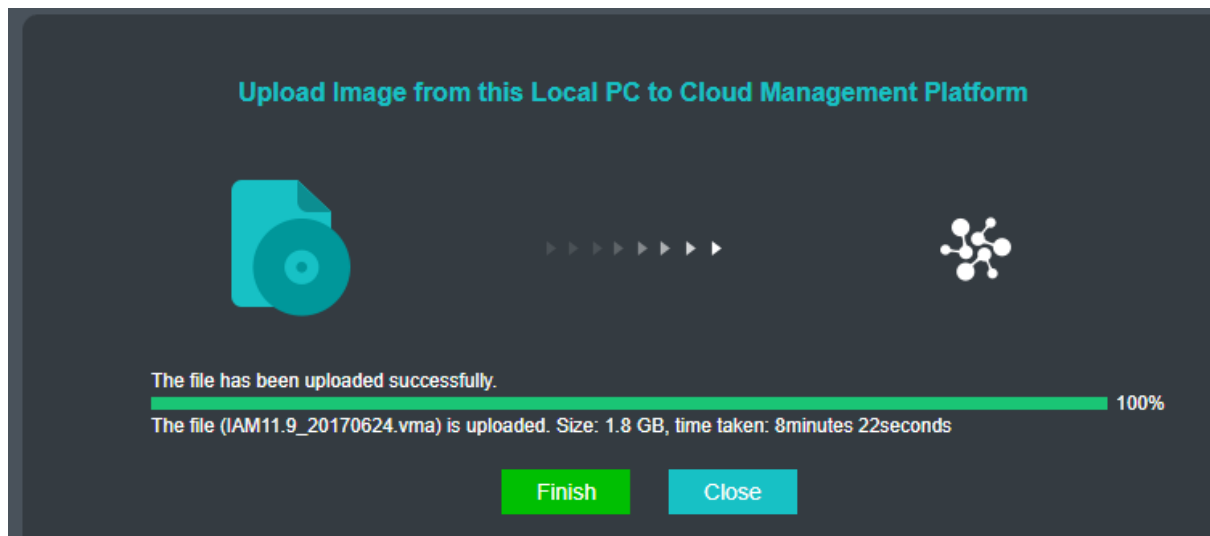
2. On the current page, you can see all existing images on aCMP, including public images, private images and network device images. Select 『Network Device Images』 tab and Click Upload Image.

Public Images				Private Images				Network Device Images			
Refresh				Upload Image				Delete			
<input type="checkbox"/>	Name	Status	Version								
<input type="checkbox"/>	▲ SSL		-								
<input type="checkbox"/>	SSLM7.5_20171011	● Normal	M7.5								
<input type="checkbox"/>	▲ IAM		-								
<input type="checkbox"/>	IAM11.9_20170624	● Normal	11.9								
<input type="checkbox"/>	▲ AF		-								
<input type="checkbox"/>	AF7.1R3_20170830	● Normal	7.1R3								

3. Select the local images to be uploaded; select the availability zone; and click Upload.



-
4. Upon the completion of uploading, click **Completed** to continue to upload or click **Close**.



3.2.2 Management of virtual machine

Virtual machine is the basic unit of SANGFOR aCMP for providing services; and the administrator can create, export, delete and perform various operations on the virtual machine at his own discretion. Users can manage the virtual machine by creating a virtual machine or making a template.

3.2.2.1 Creation of full virtual machine

[Function description]

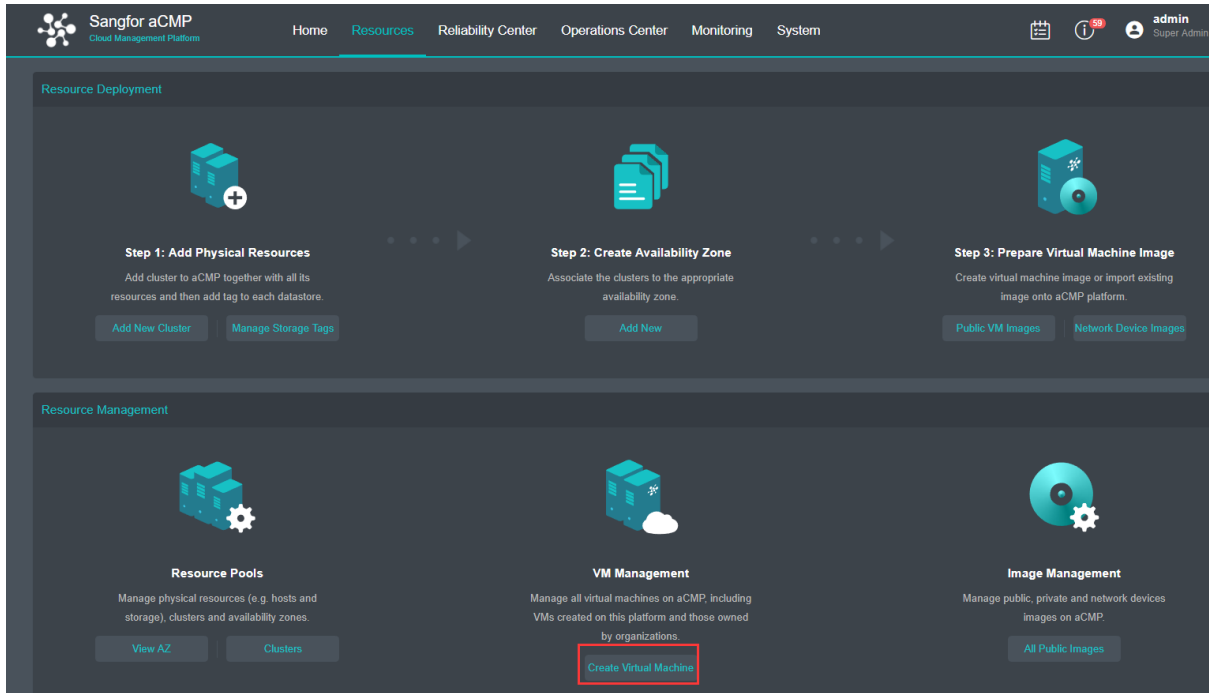
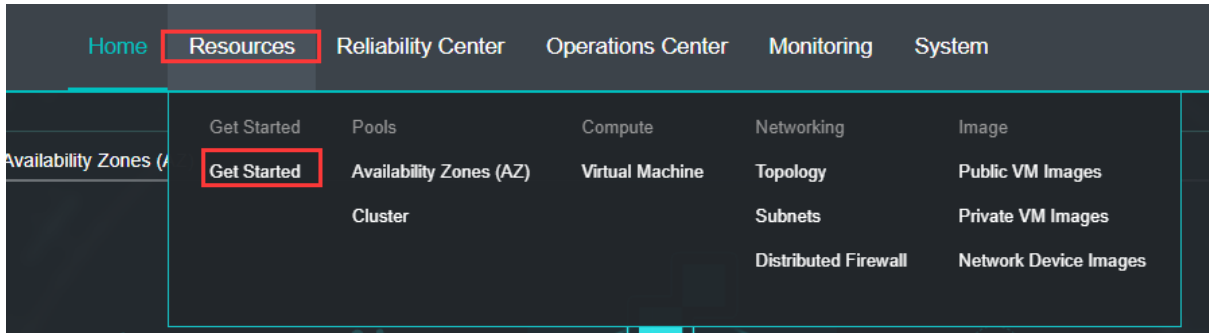
This function is used for creating new virtual machine resources

[Prerequisites]

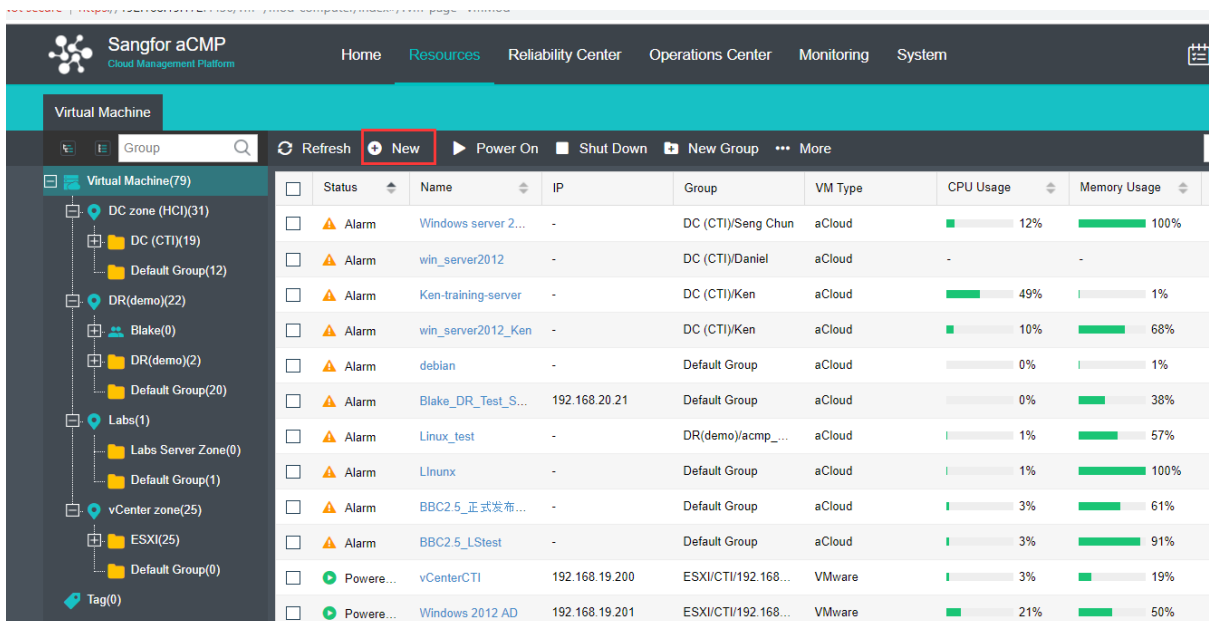
The ISO file required for creating a virtual machine has been uploaded

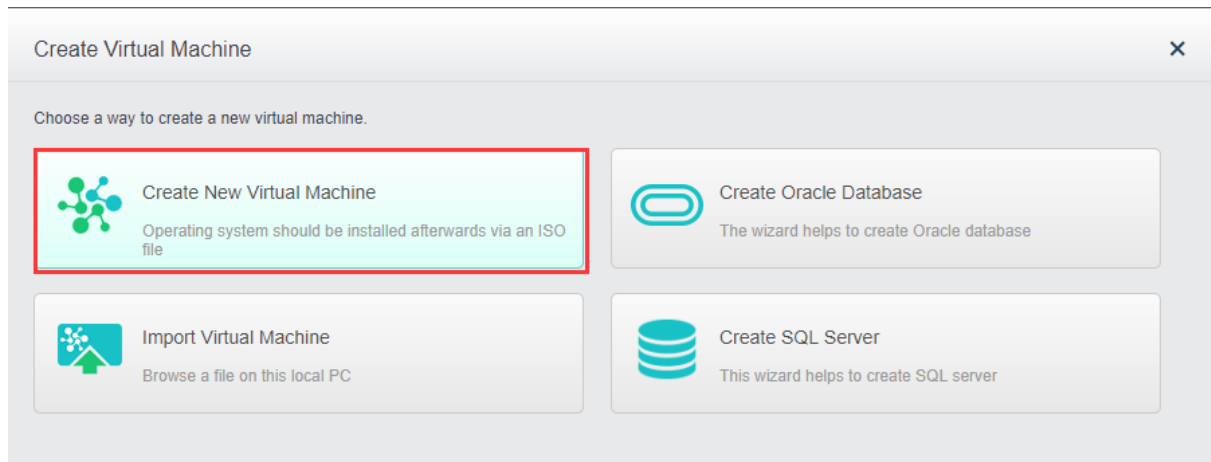
[Operating steps]

1. Log in to the home page of aCMP platform, select 『Resources』 → 『Get Started』, click **Create Virtual Machine**; or click 『Resources』 → 『Virtual Machine』; see the following figure:

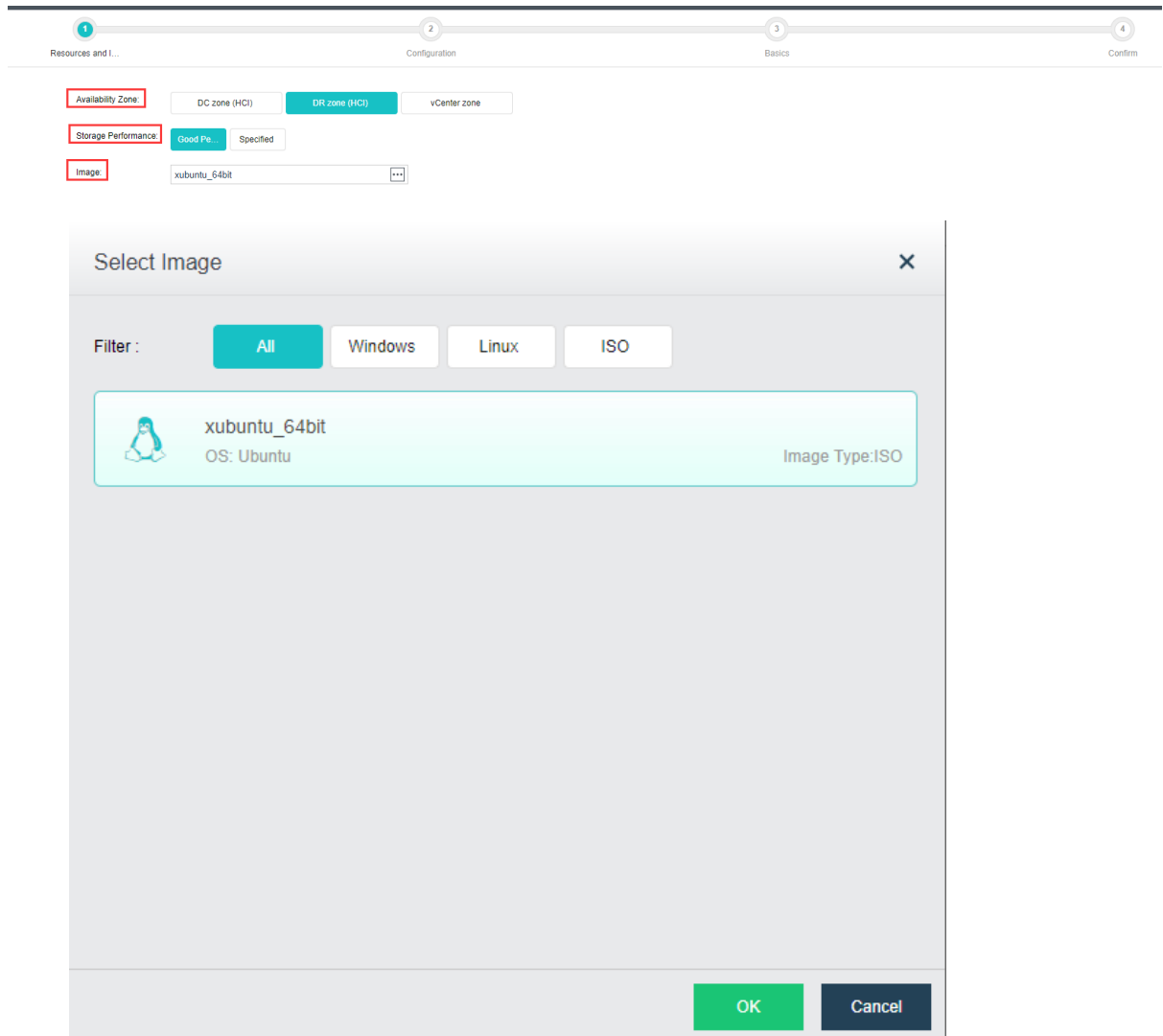


2. Click **New**, select **Create New Virtual Machine** in the **【Create Virtual Machine】**.





3. Configure virtual machine images and availability zone, configure memory property, select the corresponding images, click **Next**;



4. Configure the parameters and network of virtual machine according to the actual demand and click **Next**;

Resources > Virtual Machine > Create Virtual Machine

Resources and I... Configuration Basics Confirm

VMs: 1

CPU: 1 CPU Core(s) **2 CPU Core(s)** 4 CPU Core(s) 6 CPU Core(s) 8 CPU Core(s) 12 CPU Core(s) 16 CPU Core(s) core(s)

Custom Options

Memory: 1 GB 2 GB **4 GB** 6 GB 8 GB 12 GB 16 GB 32 GB 48 GB 64 GB GB

Custom Options

Datatore: Disk 1

New disk Existing disk Physical Disk Shared Disks

Disk Capacity: 80 GB

Pre-allocation

+ Add Disk (2 more disks can be added)

USB Device: **+** Add USB Device (12 more USB devices can be added)

Network: eth0

Enabled

Realtek RTL8139

fa:fc:fe:b9:40:0b

DefaultEdge

Back Next Cancel

Configure advanced options;

Advanced

Boot Order: 1 Disk 1 2 CD/DVD 3 None

Others:

Power on at node startup

High priority

Reboot if fault occurs (due to stuck, blue screen, etc., requiring vmTools be installed)

Enable CPU hot add (change could be made in power-off state) Guest OSes Support

Enable memory hot add (change could be made in power-off state) Guest OSes Support

Enable UUID generator (every time UUID generator is enabled, a new UUID will be generated)

Remote Debugging: Enable memory reclaiming (detect and reclaim free memory of idle virtual machine)

Back Next Cancel

5. Fill in the basic information of virtual machine, click **Next**;

Resources > Virtual Machine > Create Virtual Machine

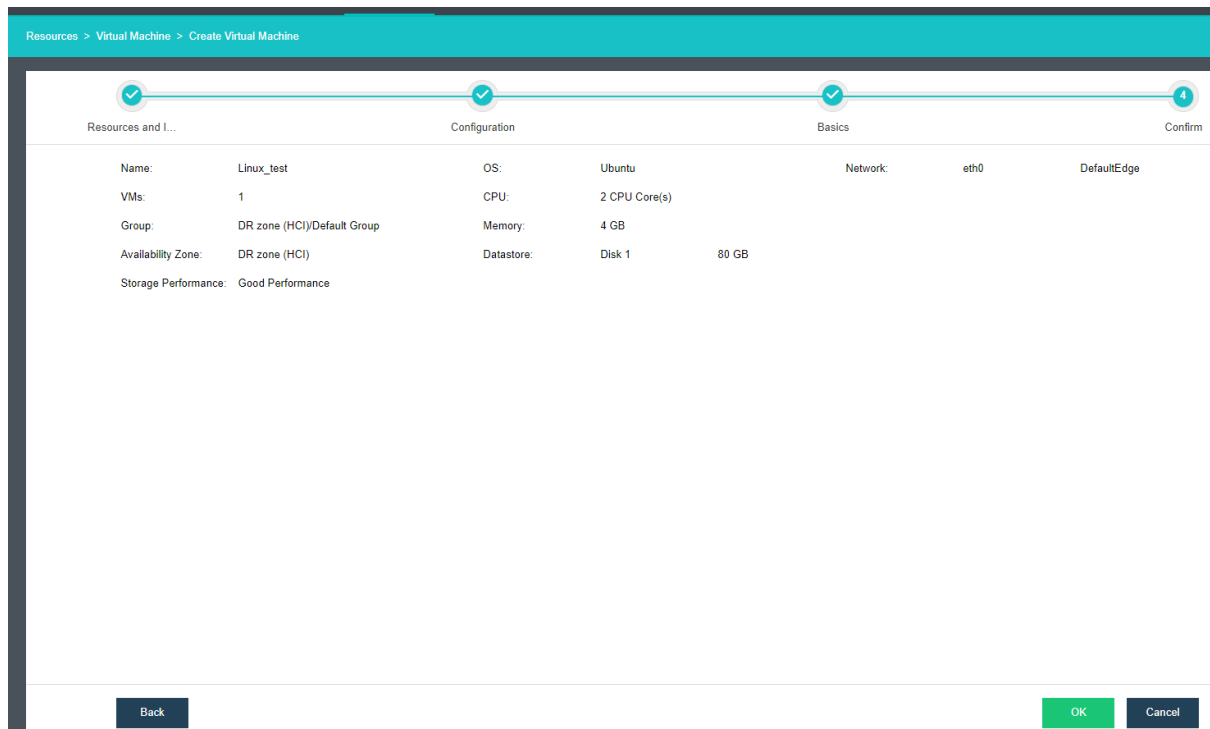
Resources and I... Configuration Basics Confirm

Name: Linux_test

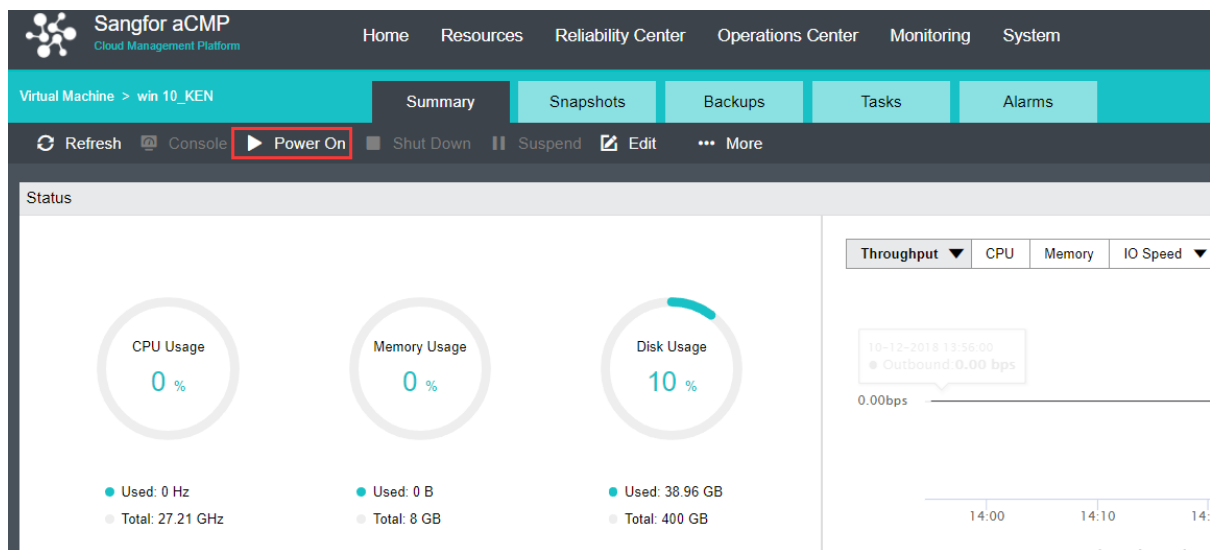
Description: Description

Group: DR zone (HCI)Default Group

6. Click **OK** to finally confirm the information.



7. It should be noted that the virtual machine created by ISO needs to manually perform the installation steps of the operating system after powering on and entering the console for the first time.



Click Console to enter the operating system installation interface after powering on:



3.2.2.2 Export of Virtual Machine

[Function Description]

This function is applicable to the virtual machine.

[Operating Steps]

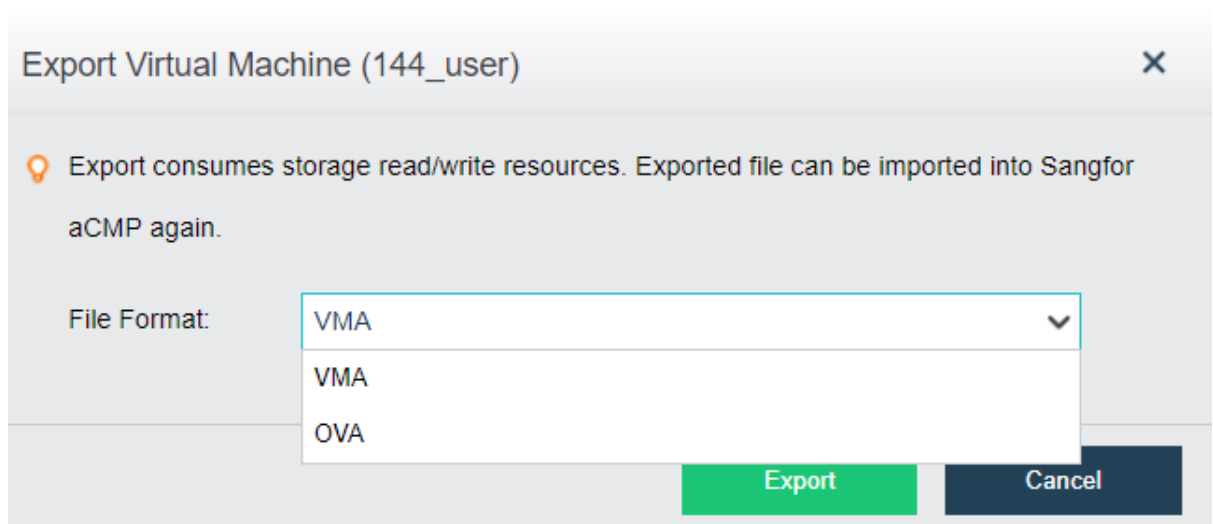
1. Log in to the home page of aCMP platform, click 『Resources』 → 『Virtual Machine』 option; select the virtual machine to be exported; click **More** on the right; click **Export** option;



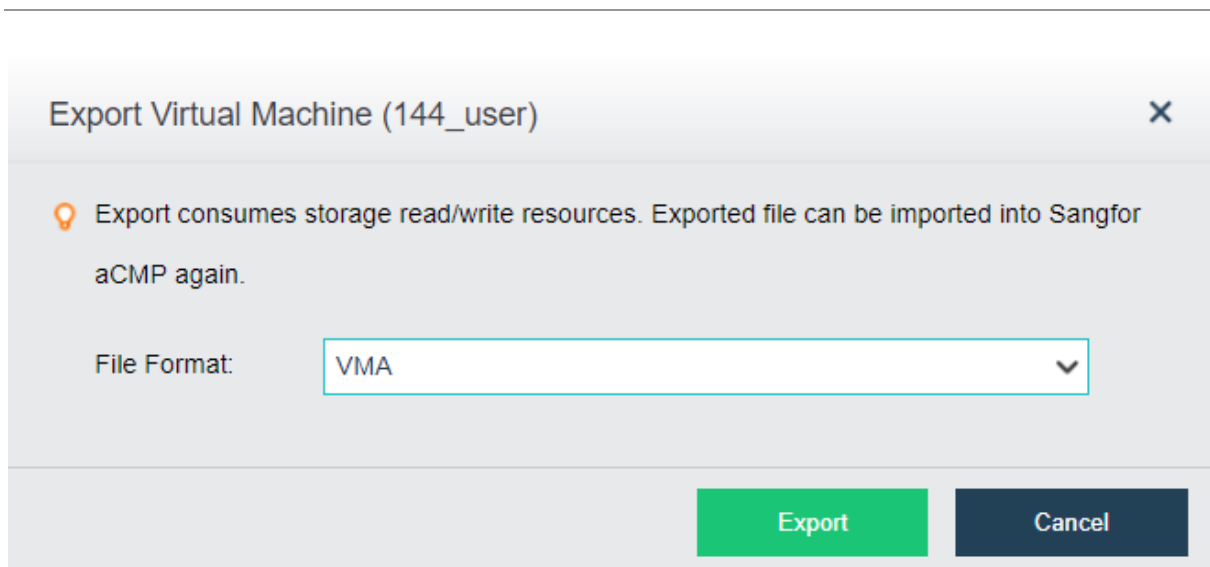
Note: the virtual machine in operation can be exported.

Power...	IP	Group	Cloud	Progress 1	Progress 2	Progress 3	More
Power...	146_user	Default Group	aCloud	0%	36%	51%	more
Power...	146_user	146.0.0.10	Default Group	aCloud	0%	47%	Console
Power...	Demo_WANO_SD...	-	Default Group	aCloud	8%	100%	Power On
Power...	149_user	149.0.0.10	Default Group	aCloud	0%	47%	Shut Down
Power...	Demo_WANO_SD...	-	Default Group	aCloud	8%	100%	Suspend
Power...	144_user	144.0.0.10	Default Group	aCloud	0%	47%	Reset
Power...	147_user	147.0.0.10	Default Group	aCloud	0%	34%	Power Off
Power...	Demo_WANO_SD...	-	Default Group	aCloud	16%	96%	Tag
Power...	145_user	145.0.0.10	Default Group	aCloud	0%	47%	Clone
Power...	Demo_WANO_SD...	-	Default Group	aCloud	8%	100%	Edit
Power...	Demo_WANO_SD...	-	Default Group	aCloud	8%	100%	Create image
Power...	142_user	142.0.0.10	Default Group	aCloud	0%	45%	Snapshots
Power...	Demo_WANO_SD...	-	Default Group	aCloud	15%	100%	Export
Power...	Lab-server template	192.200.19.20, 19...	Default Group	aCloud	0%	31%	Migrate
Power...	win2012	192.168.1.222	Default Group	aCloud	0%	16%	Backups
							Backup

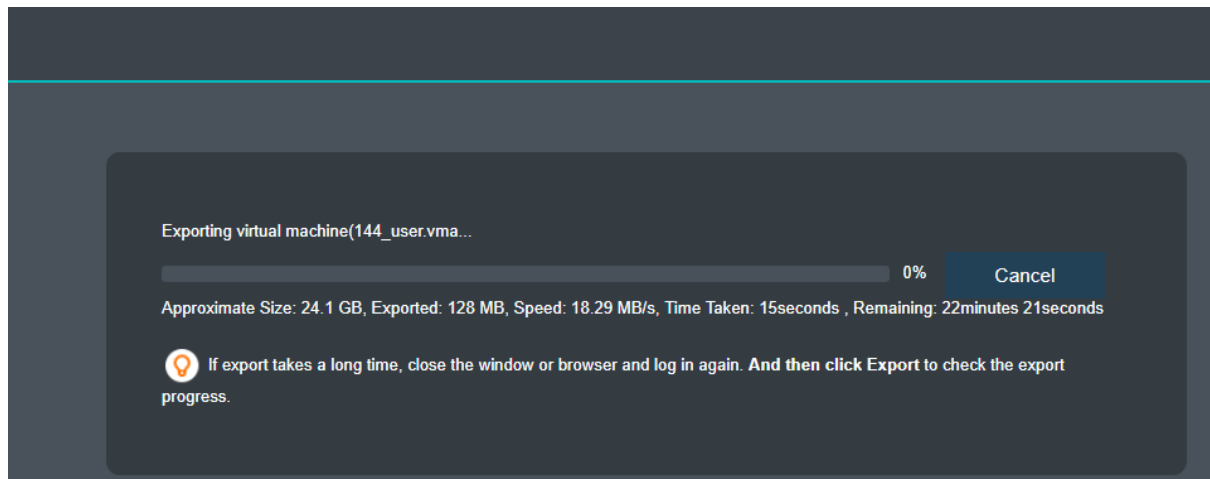
2. Select the desired export format; OVA and VMA formats are available; click Start Export;



: VMA, OVA formats; the corresponding export selections are different. To export VMA format, directly click Start Export. To export OVA format, however, you need to select the version number in the Virtual Machine Version. The version of the virtual machine is the version number of VMware Station.



3. Wait for the virtual machine to produce an export file and download the export file;



3.2.2.3 Import of virtual machine

[Function Description]

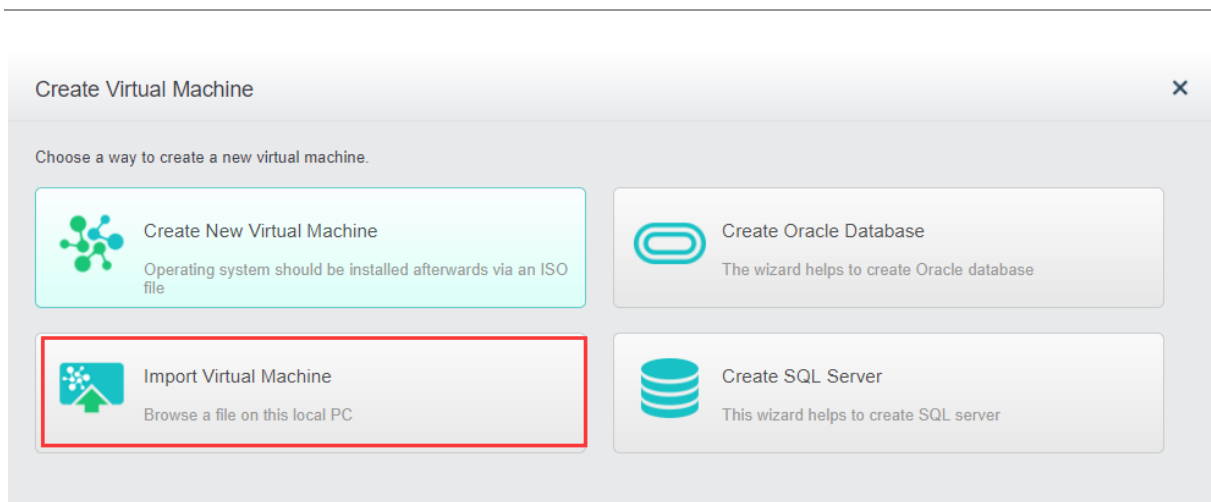
This function is applicable to import the virtual machine to aCloud cluster via aCMP.

[Prerequisites]

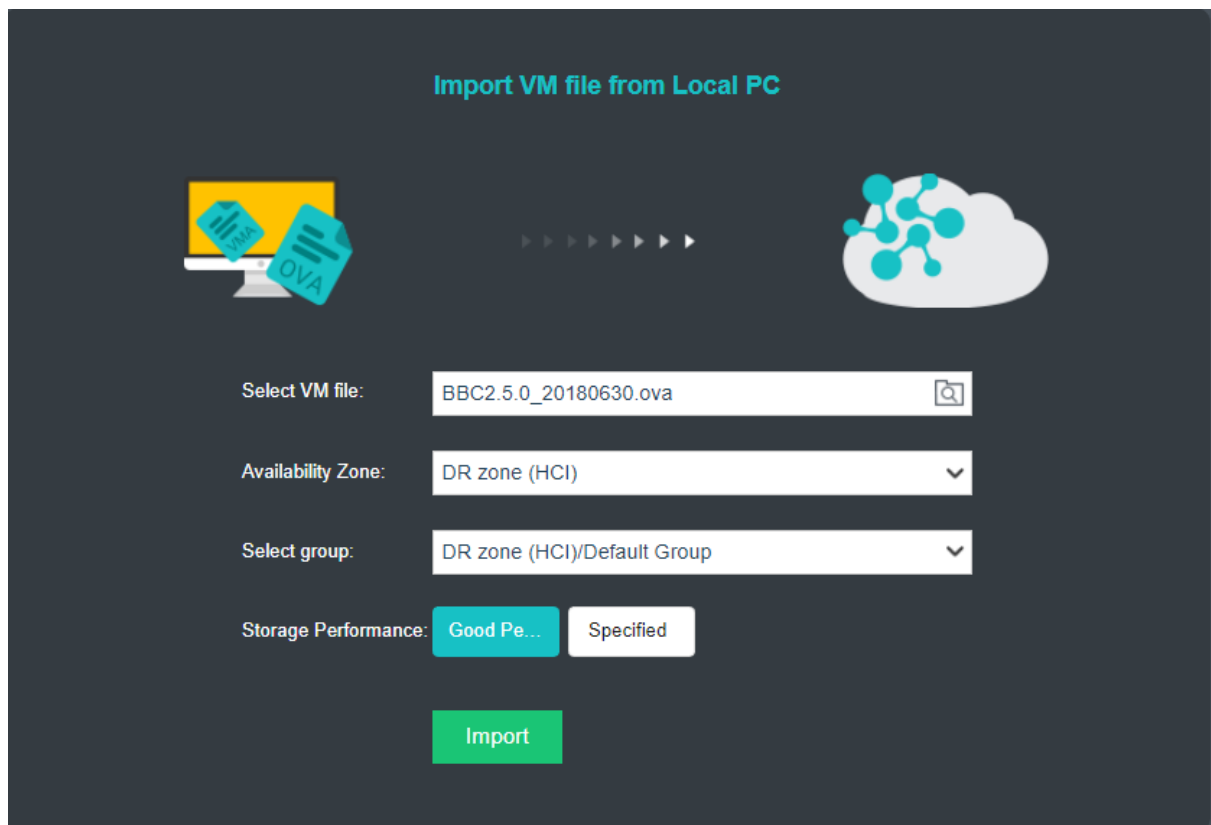
Prepare the VMA file or OVA file corresponding to the virtual machine.

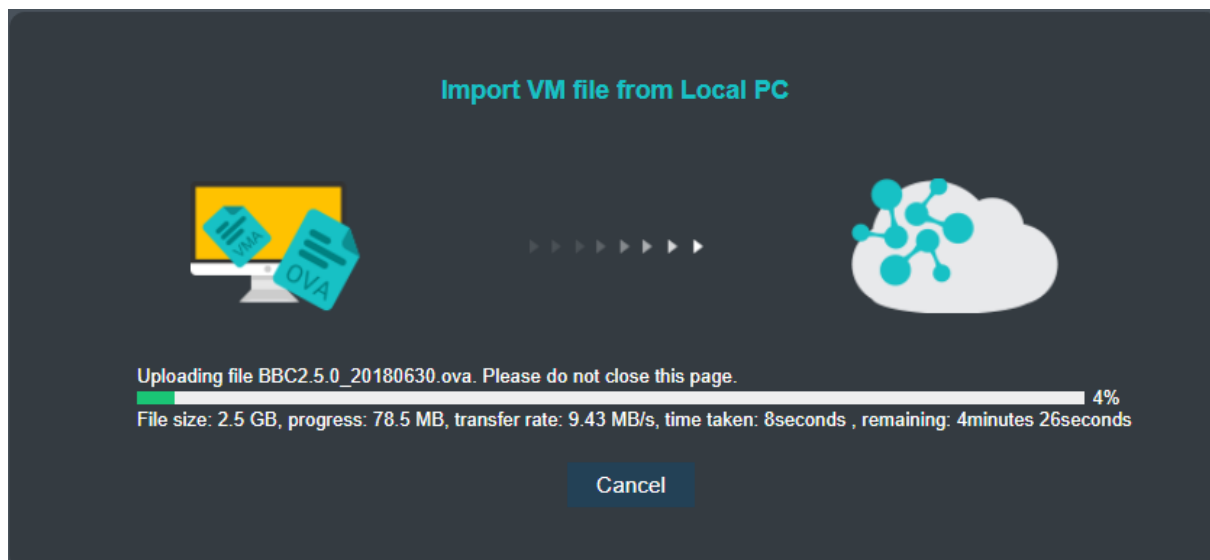
[Operating Steps]

1. Log in to the home page of aCMP platform, click 『Resources』 → 『Virtual Machine』 option; click **New**; select **Import Virtual Machine** in **【Create Virtual Machine】** window;

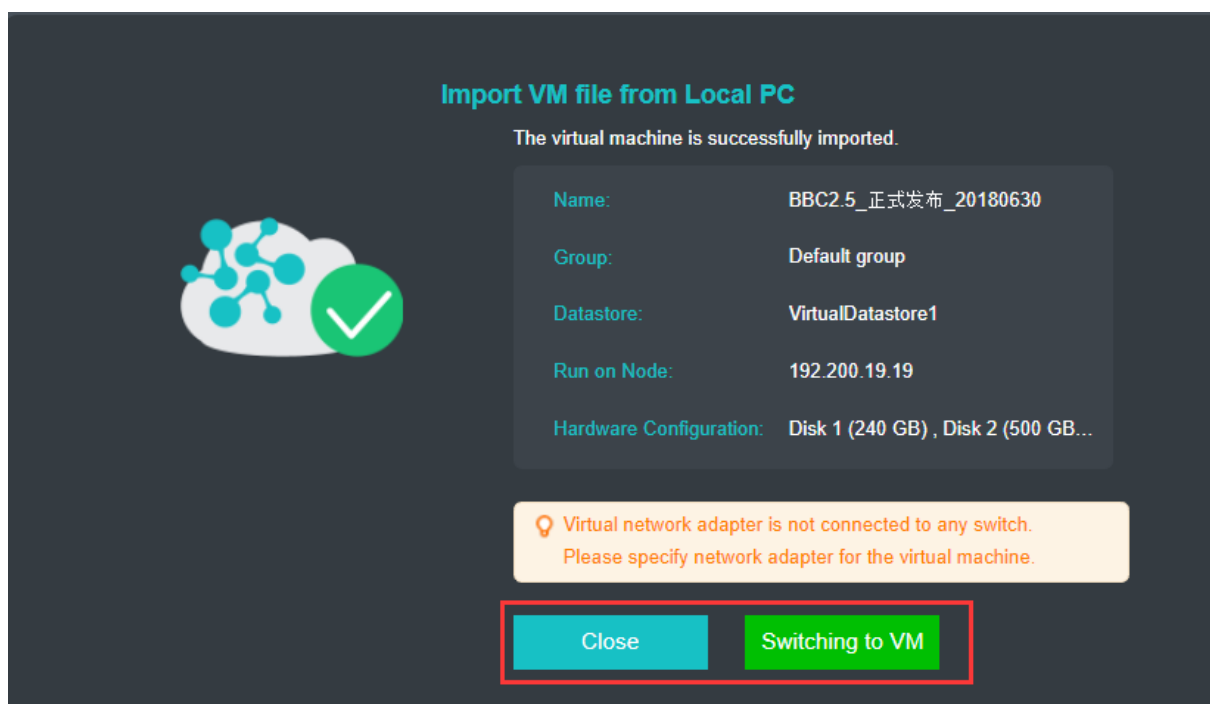


2. Select the virtual machine to be imported and the corresponding virtual machine parameters; click **Import**;





3. After import, click **Close** or **Switching to VM** to edit the virtual machine.



: When importing the virtual machine, its network card is not connected to the switch. You can click **Switching to VM** to configure the virtual machine.

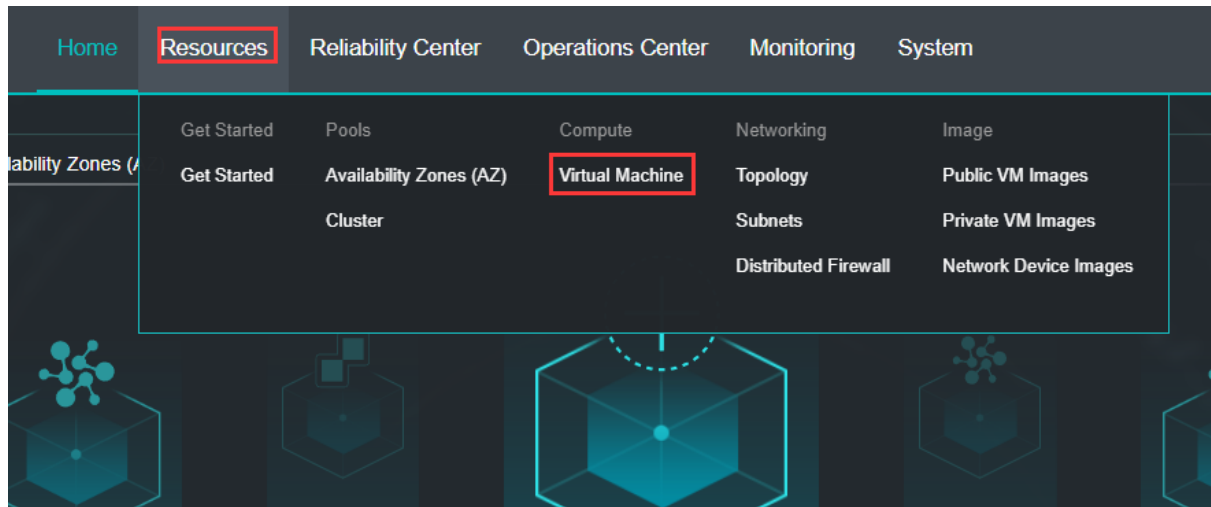
3.2.3.4 Migration of Virtual Machine

[Function Description]

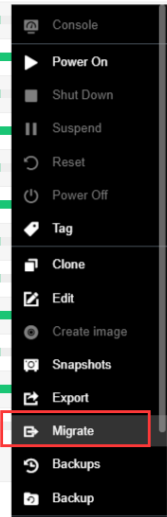
This function is used for migrating the virtual machine and supports the migration of virtual machines across availability zone.

[Operating Steps]

1. Log in to the home page of aCMP platform, select 『Resources』 → 『Virtual Machine』 ; select the virtual machine to be migrated; click 『More』 → 『Migrate』 ;



<input type="checkbox"/>	Power...	146_user	146.0.0.10	Default Group	aCloud	0%	47%	53%	More
<input type="checkbox"/>	Power...	Demo_WANO_SD...	-	Default Group	aCloud	8%	100%		
<input type="checkbox"/>	Power...	149_user	149.0.0.10	Default Group	aCloud	0%	47%		
<input type="checkbox"/>	Power...	Demo_WANO_SD...	-	Default Group	aCloud	10%	100%		
<input type="checkbox"/>	Power...	147_user	147.0.0.10	Default Group	aCloud	1%	34%		
<input type="checkbox"/>	Power...	Demo_WANO_SD...	-	Default Group	aCloud	12%	96%		
<input type="checkbox"/>	Power...	145_user	145.0.0.10	Default Group	aCloud	0%	47%		
<input type="checkbox"/>	Power...	Demo_WANO_SD...	-	Default Group	aCloud	6%	100%		
<input type="checkbox"/>	Power...	Demo_WANO_SD...	-	Default Group	aCloud	9%	100%		
<input type="checkbox"/>	Power...	142_user	142.0.0.10	Default Group	aCloud	0%	45%		
<input type="checkbox"/>	Power...	Demo_WANO_SD...	-	Default Group	aCloud	12%	100%		
<input type="checkbox"/>	Power...	Lab-server template	192.200.19.20, 19...	Default Group	aCloud	0%	31%		
<input type="checkbox"/>	Power...	win2012	DR	192.168.1.222	Default Group	aCloud	0%	16%	
<input type="checkbox"/>	Power...	144_user	144.0.0.10	Default Group	aCloud	-	-	-	
<input type="checkbox"/>	Power...	Demo_WANO_SD...	-	Default Group	aCloud	-	-	-	
<input checked="" type="checkbox"/>	Power...	BBC2.5	-	Default Group	aCloud	-	-	-	More



2. Select the availability zone, cluster, running position and storage of migration; click **OK**;

Migrate
✕

Current Location

Name:

Availability Zone:

Cluster:

Run on Node:

Datastore:

Destination Location

Name:

Availability Zone:

Cluster:

Run on Node:

Datastore:

➔

Power on aCloud virtual machine upon migration completion

OK
Cancel



When migrating the virtual machine, the target location may be the availability zone where the virtual machine is located, or other availability zone; in case of migration upon powering on, migrate to the aCloud cluster and the machine is kept on and to VMware cluster and the machine is off; you may also check “Start aCloud Virtual Machine Automatically after Migration” and you need to check “Automatically Turn off aCloud Virtual Machine to Complete Migration”, or you have to manually turn off the machine to complete the migration; in case of migration in off state, the machine will be always in off state after migration, but you may check “Automatically Start aCloud Virtual Machine after Migration”.

3. You can see the progress of migration in the task bar.

Tasks
✕

All
Disaster Recovery

Status	Action	Object	Start Time	End Time	Admin	Operation
<div style="width: 37%; height: 10px; background: linear-gradient(to right, #009688, #ccc);"></div> 37%	Migrate virtual m...	BBC2... ..	2018-10-10 18:22:37	-	admin (192.168.19.206)	View Cancel
✔ Finish	Migrate virtual m...	win_server_2003	2018-10-10 18:21:22	2018-10-10 18:21:40	admin (192.168.19.206)	View
✔ Finish	Edit cluster auth...	Labs Server Zone	2018-10-10 18:16:21	2018-10-10 18:16:25	admin (192.168.19.206)	View
✘ Failed	Add availability z...	Labs	2018-10-10 18:11:10	2018-10-10 18:11:10	admin (192.168.19.206)	View
✘ Failed	Add availability z...	Labs	2018-10-10 18:11:09	2018-10-10 18:11:10	admin (192.168.19.206)	View
✔ Finish	Add availability z...	Labs	2018-10-10 18:11:07	2018-10-10 18:11:16	admin (192.168.19.206)	View
✔ Finish	Log in	admin	2018-10-10 18:07:21	2018-10-10 18:07:21	admin (192.168.19.206)	View
✔ Finish	Upload image	Linux_subuntu64	2018-10-10 18:00:35	2018-10-10 18:03:41	blake (192.168.19.206)	View

3.2.3.5 Allocation of Virtual Machine

[Function Description]

This function is applicable to the allocation of virtual machine, which can be allocated to the organization or organization members.

[Operating Steps]

1. Log in to the home page of aCMP platform, select 『Resources』 → 『Virtual Machine』 ; select the virtual machine to be allocated; click 『More』 → 『Allocate』 ;

Name	IP	Group	Cloud	Progress 1	Progress 2	Progress 3
Power... 146_user	146.0.0.10	Default Group	aCloud	0%	47%	53%
Power... Demo_WANO_SD...	-	Default Group	aCloud	6%	100%	
Power... 149_user	149.0.0.10	Default Group	aCloud	0%	47%	
Power... Demo_WANO_SD...	-	Default Group	aCloud	10%	100%	
Power... 147_user	147.0.0.10	Default Group	aCloud	0%	34%	
Power... Demo_WANO_SD...	-	Default Group	aCloud	6%	96%	
Power... 145_user	145.0.0.10	Default Group	aCloud	0%	47%	
Power... Demo_WANO_SD...	-	Default Group	aCloud	5%	100%	
Power... Demo_WANO_SD...	-	Default Group	aCloud	10%	100%	
Power... 142_user	142.0.0.10	Default Group	aCloud	0%	45%	
Power... Demo_WANO_SD...	-	Default Group	aCloud	8%	100%	
Power... Lab-server template	192.200.19.20, 19...	Default Group	aCloud	0%	31%	
Power... win2012	192.168.1.222	Default Group	aCloud	0%	16%	
Power... 144_user	144.0.0.10	Default Group	aCloud	-	-	-
Power... Demo_WANO_SD...	-	Default Group	aCloud	-	-	-



: 1. allocating aCloud virtual machine to the organization will disconnect the network of the virtual machine; after allocation, the virtual machine can be found in the default group or organization member of the corresponding organization. The network of the virtual machine should be configured manually.

2. Select the organization and organization member (can be null) to be allocated; click OK;

Assign Virtual machines
✕

Select organization:

Select users:

💡 Assigning virtual machines from HCI platform to organization will disconnect them. You may find the associated default organization or cloud user and check the virtual machine later when you finish assignment, and change VM network settings manually.

OK
Cancel



: Do not allocate the virtual machine across availability zone.

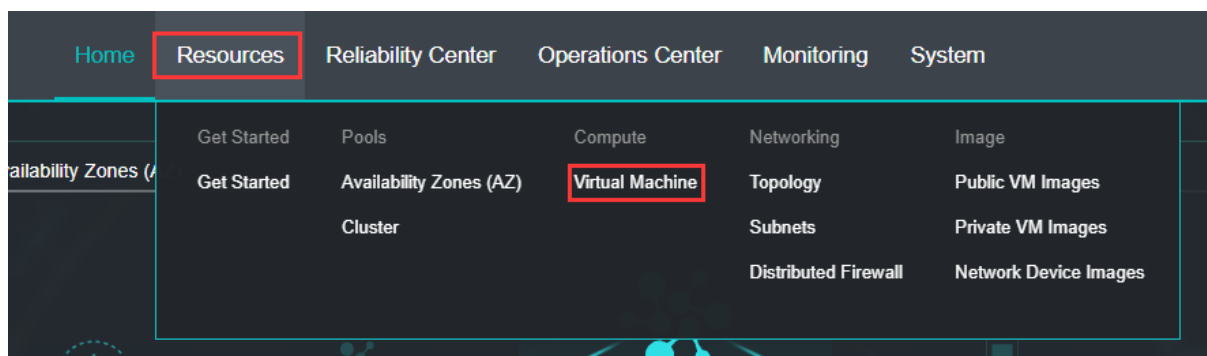
3.2.3.6 Deallocation of Virtual Machine

[Function Description]

This function is applicable to the de-allocation of virtual machine.

[Operating Steps]

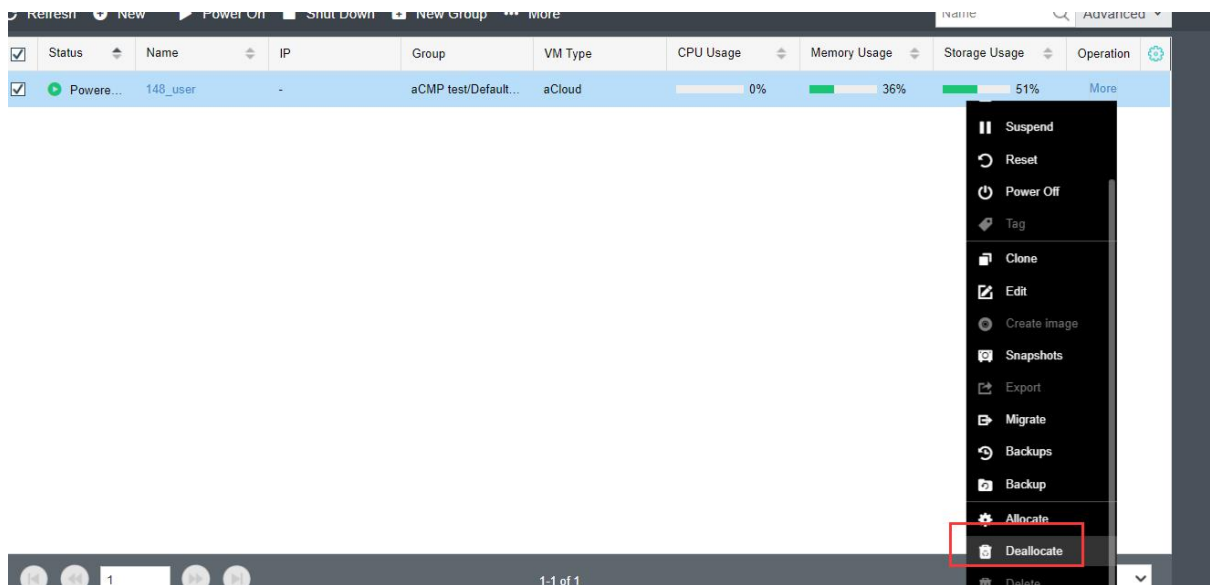
1. Log in to the home page of aCMP platform, select 『Resources』 → 『Virtual Machine』 ; select the organization or organization member of the virtual machine to be de-allocated;



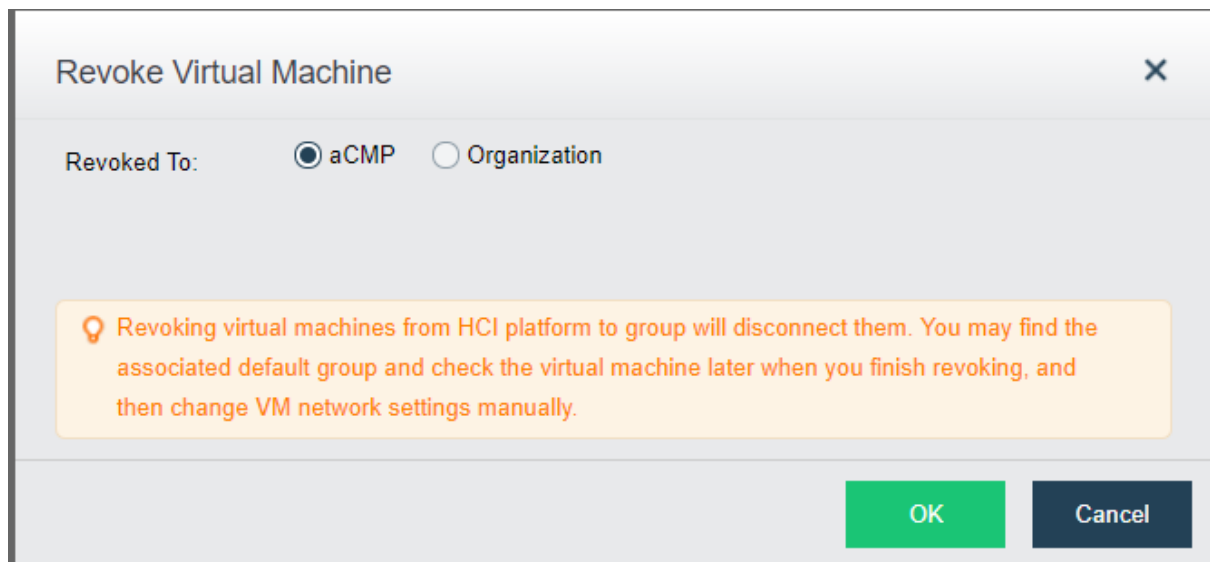
Status	Name	IP	Group	VM Type	CPU Usage	Memory Usage	Storage Usage	Operation
Alarm	Linux	-	Default Group	aCloud	1%	100%	12%	More
Alarm	BBC2	-	Default Group	aCloud	3%	58%	2%	More
Alarm	BBC2_5_LStest	-	Default Group	aCloud	3%	85%	2%	More
Alarm	Linux_test	-	Default Group	aCloud	1%	26%	0%	More
Powered On	Demo_WANO_SD...	-	Default Group	aCloud	9%	100%	18%	More
Powered On	148_user	-	Default Group	aCloud	0%	36%	51%	More
Powered On	146_user	146.0.0.10	Default Group	aCloud	0%	47%	53%	More
Powered On	Demo_WANO_SD...	-	Default Group	aCloud	15%	100%	18%	More
Powered On	149_user	149.0.0.10	Default Group	aCloud	0%	47%	53%	More
Powered On	Demo_WANO SD...	-	Default Group	aCloud	11%	100%	19%	More



- 1) The virtual machine allocated with no organization or organization member cannot be de-allocated.
- 2) Select the virtual machine to be de-allocated; click 『More』 → 『De-allocate』 ;



- 2 In case of a virtual machine owned by an organization member, the virtual machine may be de-allocated to the organization or cloud management platform, or can only de-allocated to cloud management platform;



3. You can see the progress of de-allocation in the task bar.

3.3 Reliability Center

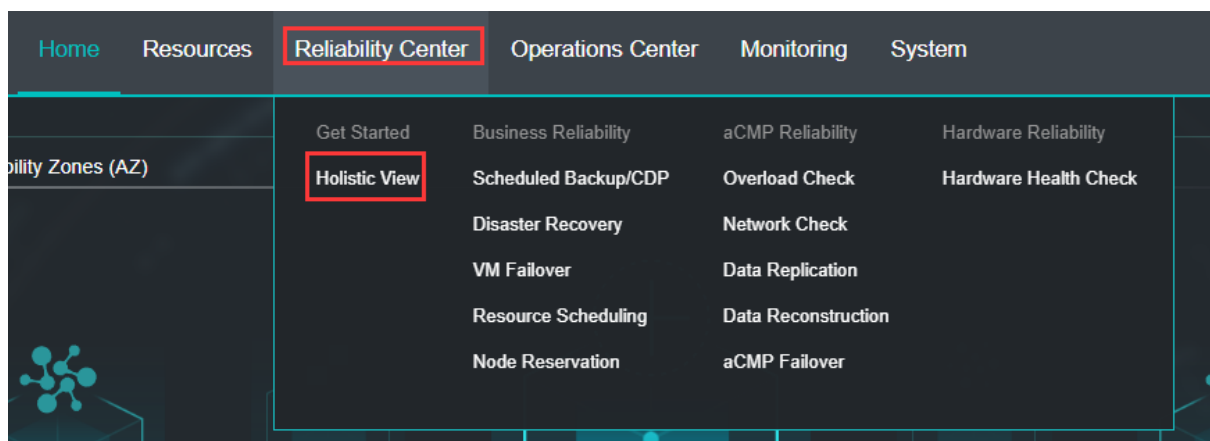
3.3.1 Holistic View

[Function Description]

This function provides visualized and minimal operation and maintenance mode. One-click acquisition of reliable resources and services is available. The administrator can obtain the overall operation conditions of the platform through this interface and can quickly find out the specific problem.

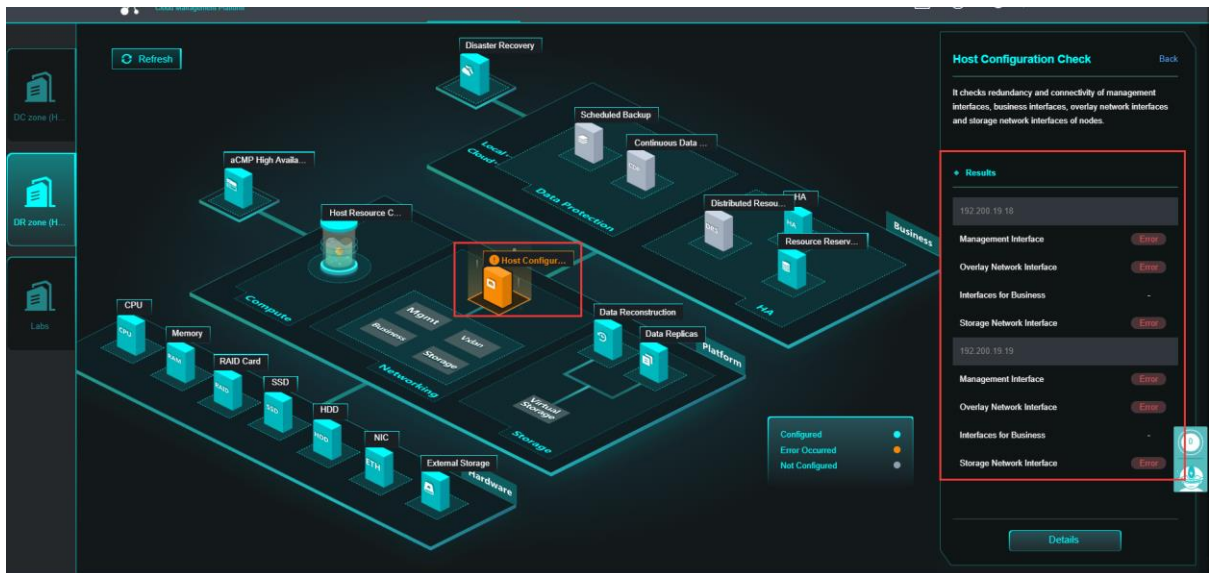
[Operating Steps]

1. Log in to the home page of aCMP platform, select 『Reliability Center』 → 『Holistic View』 to enter Holistic View page;





1. Grey means that this function is unavailable or that services have not been configured; yellow means that abnormal services are detected; green means that services have been configured
2. Different sites are displayed on the left side; click any service that you want to view in the main interface to view the corresponding detailed status;



2. Click Details tab to enter the **Details** page.

High Availability > Host Configuration Check

Host Configuration Check Check Now
 Last Check Time 2018-10-10 19:32:42

It checks redundancy and connectivity of management interfaces, business interfaces, overlay network interfaces and storage network interfaces of nodes.

Node Name	NIC MTU configuration check	Subnet Mask Consistency	IP Address Conflict Check	Interface Multiplexing	Interface Redundancy
192.200.19.18.eth0	✓ 1500	✓ 255.255.255.0	✓ Normal	✓ Normal	⚠ Not configured
192.200.19.19.eth1	✓ 1500	✓ 255.255.255.0	✓ Normal	✓ Normal	⚠ Not configured

Entities Description >>
 Solutions >>

On this page:

Clicking **Check Now** can detect again to eliminate false alarm; the following interface will appear after clicking it:

Confirm ✕

To not affect cluster performance, we recommend cluster health check be performed when the running business system is not busy.

Are you sure that you want to perform health check now?

OK
Cancel

Click OK to check; and the detection results will be given again:

Host Configuration Check Checking...
 Last Check Time 2018-10-10 19:34:43

It checks redundancy and connectivity of management interfaces, business interfaces, overlay network interfaces and storage network interfaces of nodes.

Node Name	NIC MTU configuration check	Subnet Mask Consistency	IP Address Conflict Check	Interface Multiplexing	Interface Redundancy

『Entities Description』 can view the decision rule of each detection item; see the following figure:

Entities Description >>

MTU:

Check whether MTU of management interfaces on all nodes are the same.

MTU of management interfaces should be identical: ❌

Netmask Consistency:

Check whether netmask of the management interfaces of all the nodes are the same.

Netmasks are inconsistent: ❌

IP Address Conflict:

Check whether IP address of the Management interface conflicts with any interface or device.

IP address conflict exists: ❌

Reuse of Management Interface:

Check whether management interface uses the same interface with edge or overlay network interface.

Management interface is reused: ❌

Aggregate Interface:

Check whether management interface is an aggregate interface.

It is not an aggregate interface: ⚠️

『Solutions』 provides reference solutions for current abnormality; see the following figure:

Solutions >>

MTU:

If MTU of management interfaces are not the same, it may make clustered node unable to communicate with each other and perform operations like backup, etc. Please configure the same MTU for management interfaces of all hosts.

Netmask Consistency:

If netmasks of management interfaces are not the same, it may make clustered nodes unable to communicate with each other and perform operations like backup, etc. Please configure the same netmask for management interfaces of all hosts.

IP Address Conflict:

If management interface address conflicts with any interface or device, it may cause network error. Please configure another IP address for the management interface.

Reuse of Management Interface:

Please set another interface as management interface and make sure that it does not use the same interface with overlay network interface or edge.

Aggregate Interface:

If the interface is not an aggregate interface, single point of failure may occur, which will affect business continuity.

3.3.2 Business Reliability

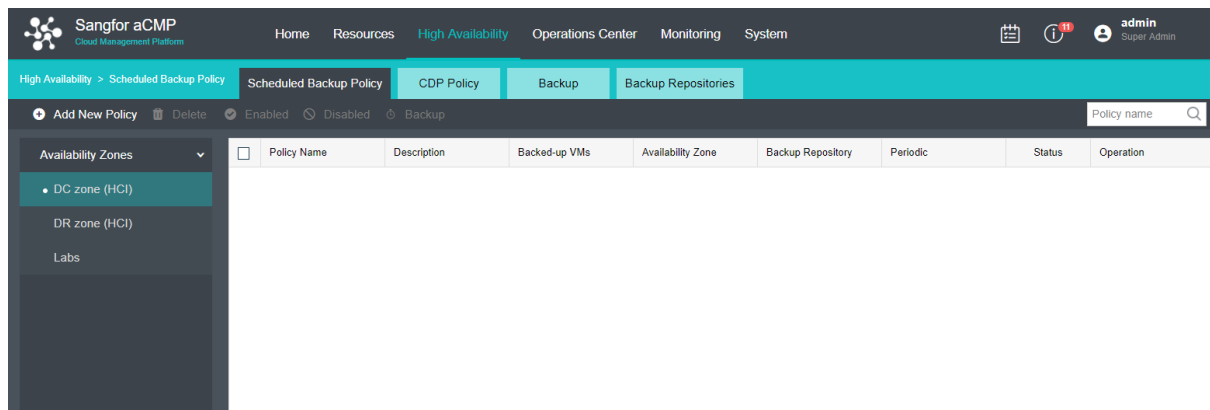
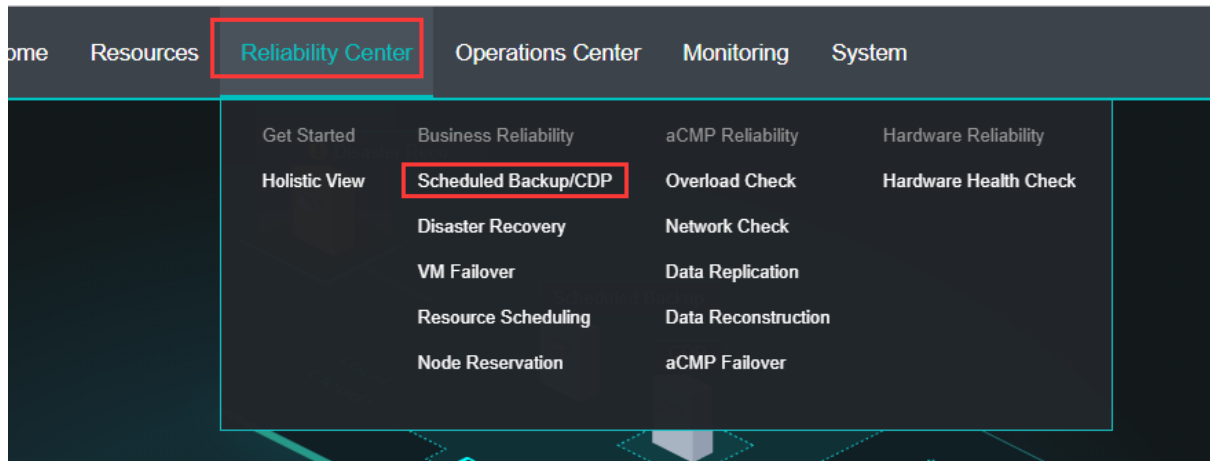
3.3.2.1 Configuration Backup and CDP

[Function Description]

This function provides local backup and CDP service for the virtual machine and provides grade protection for service by distinguishing different service grades. Local backup can periodically back up the data; and CDP can provide real-time data protection.

[Operating Steps]

1. Log in to the home page of aCMP platform, select 『Reliability Center』 → 『Scheduled Backup/CDP』 to enter backup and CDP configuration interface as shown in the following figure:



2. Configure the matching backup policy and CDP backup policy on the configuration page as required.



: The method to configure detailed backup policy and CDP policy is the same as the configuration method on aCloud. For specific configuration, please refer to the corresponding version of aCloud user manual.

3.3.2.2 HA Fault Migration

[Function Description]

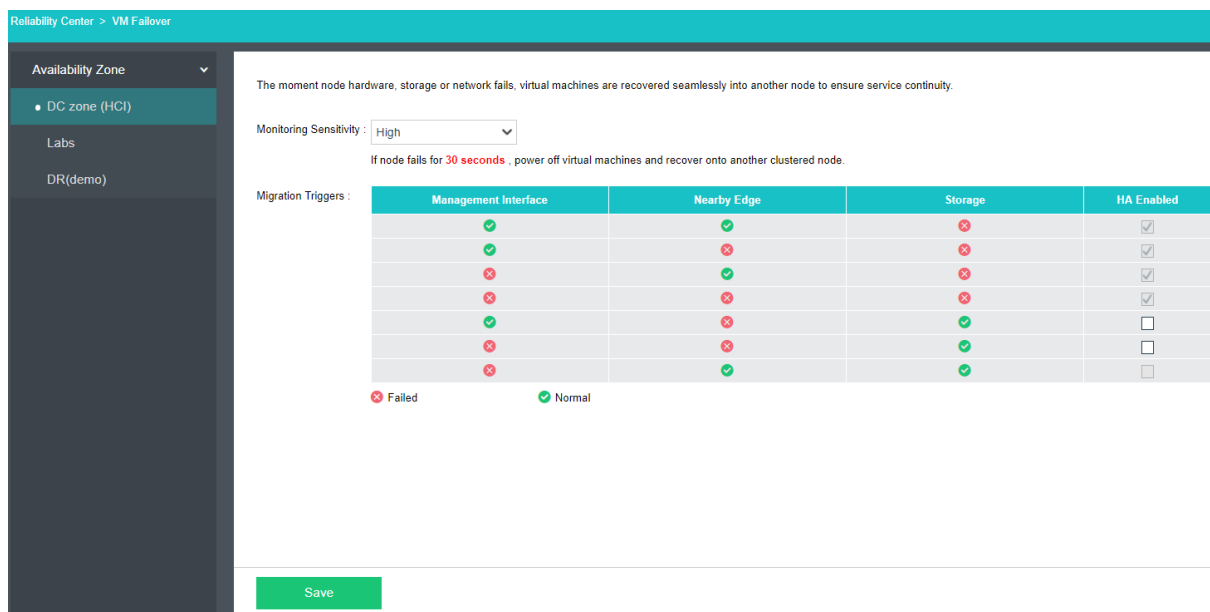
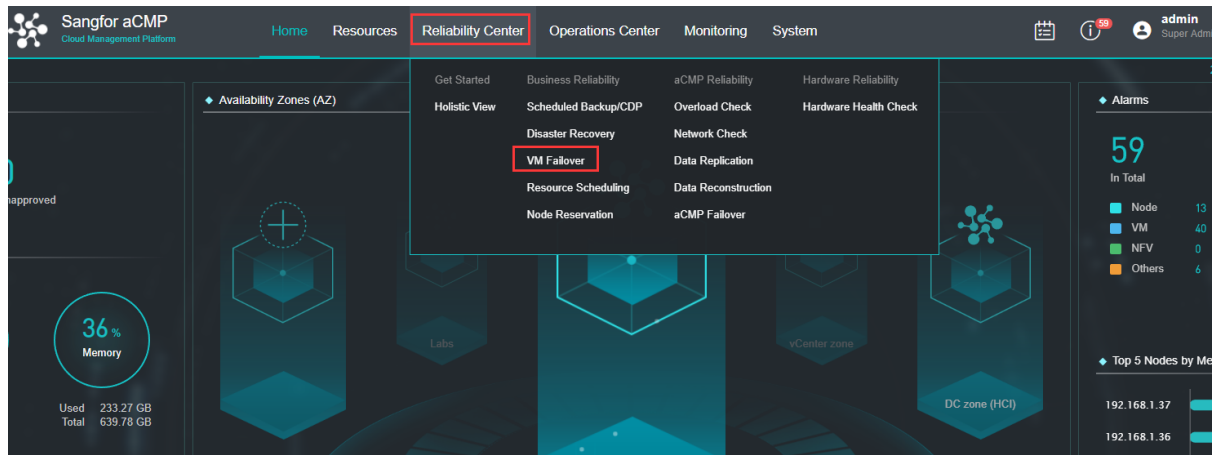
This function provides high availability services for the virtual machine. When a host in the cluster fails, the virtual machine running on the fault host may automatically and quickly choose other appropriate host via fault migration to ensure the high availability of the virtual machine.

[Prerequisites]

HA function should be checked for relevant virtual machine.

[Operating Steps]

1. Log in to the home page of aCMP platform, select 『Reliability Center』 → 『VM Failover』 to enter the Fault Migration (HA) page;



: Different fault detection sensitivity may be selected. This setting is for the entire cluster.

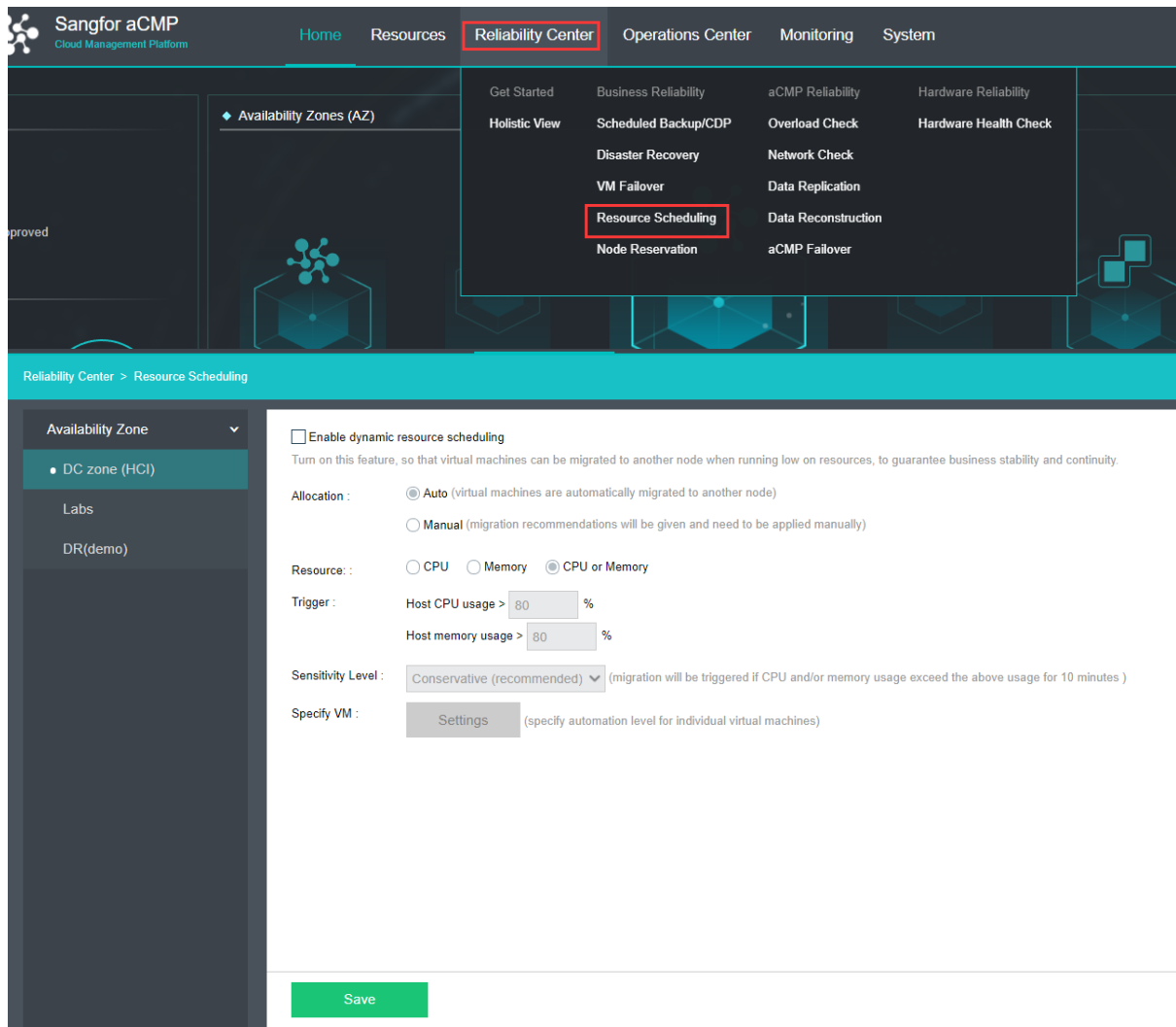
3.3.2.3 Resource Scheduling

[Function Description]

When this function is enabled, the system realizes the intelligent scheduling of the running position of the virtual machine according to the resource load of each host to ensure the continuous and stable operation of the business.

[Operating Steps]

1. Log in to the home page of aCMP platform, select 『Reliability Center』 → 『Resource Scheduling』 to enter the Resource Scheduling page; see the following figure:



【Availability Zones】 You may select the resource scheduling policy for the effective area to be configured

On this page:

Scheduling mode—automatic: the system will implement automatic scheduling according to the resource load of the cluster and the rules.

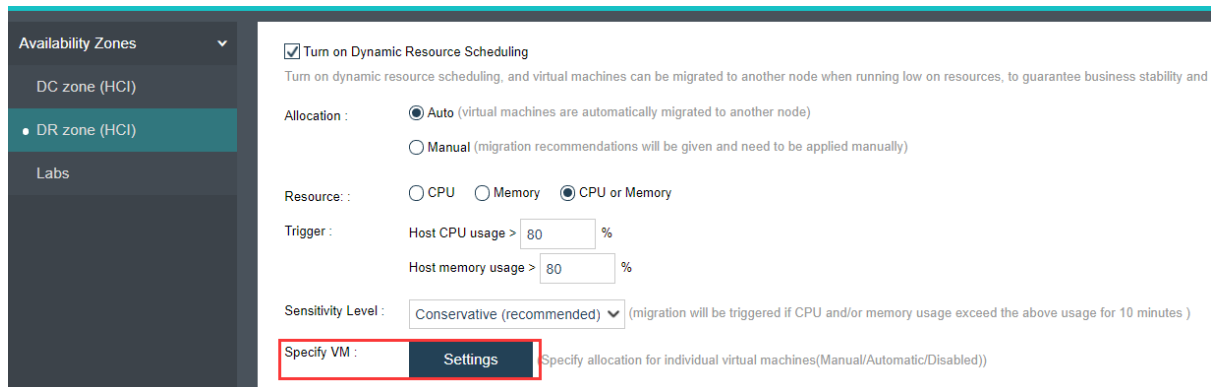
Scheduling mode—manual: the system will give scheduling suggestion according to resource load. Users need to execute the scheduling suggestion manually.

Resource: the variable that triggers scheduling execution or gives scheduling suggestion can only be set as CPU, memory, or either.

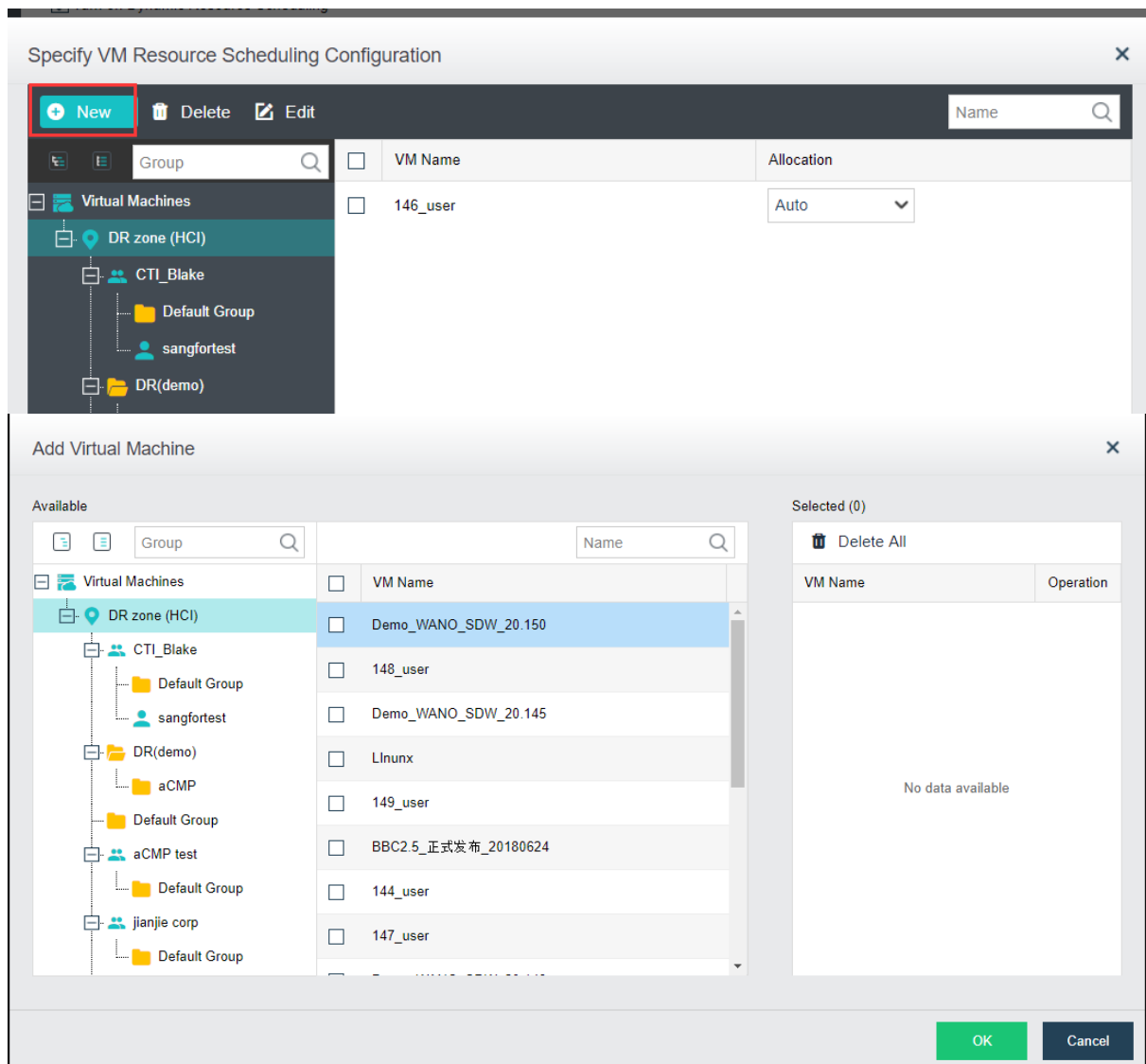
Trigger: the triggering condition that triggers scheduling execution or gives scheduling suggestion

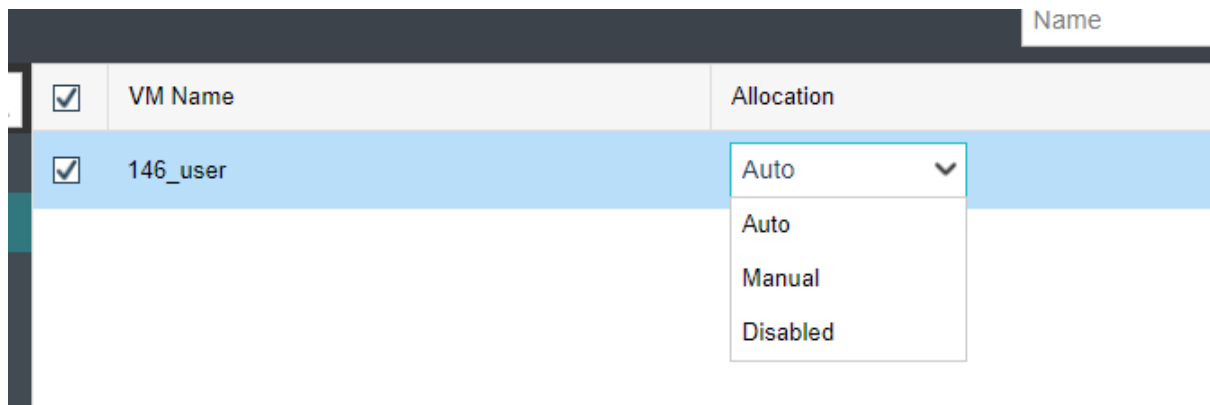
Sensitivity Level: in corresponding mode, if the system detects that the measure factor reaches the threshold and lasts for a certain time, it will schedule cluster resource.

2. Click Settings to configure corresponding scheduling mode for specific virtual machine;

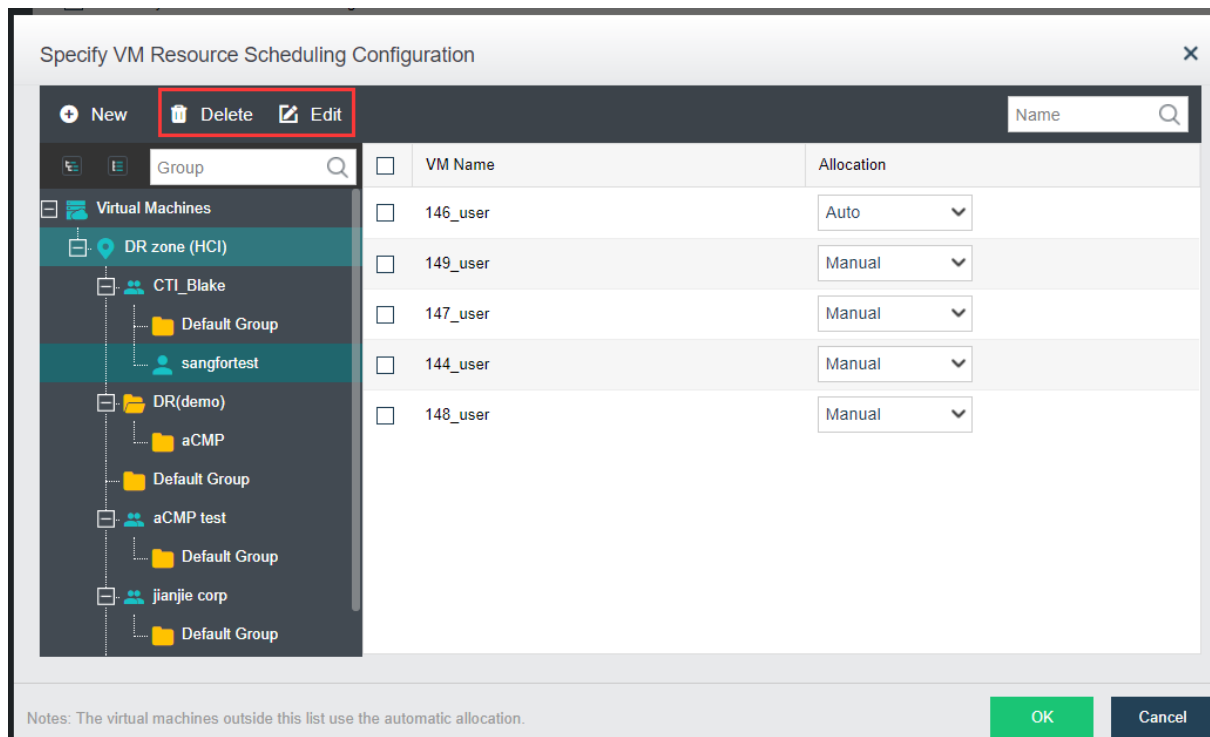


3. Meanwhile, batch configuration of virtual machine is also available. Click **New**; select virtual machine and scheduling mode, then click **OK**;





4. Similarly, the current configuration may be modified or deleted.



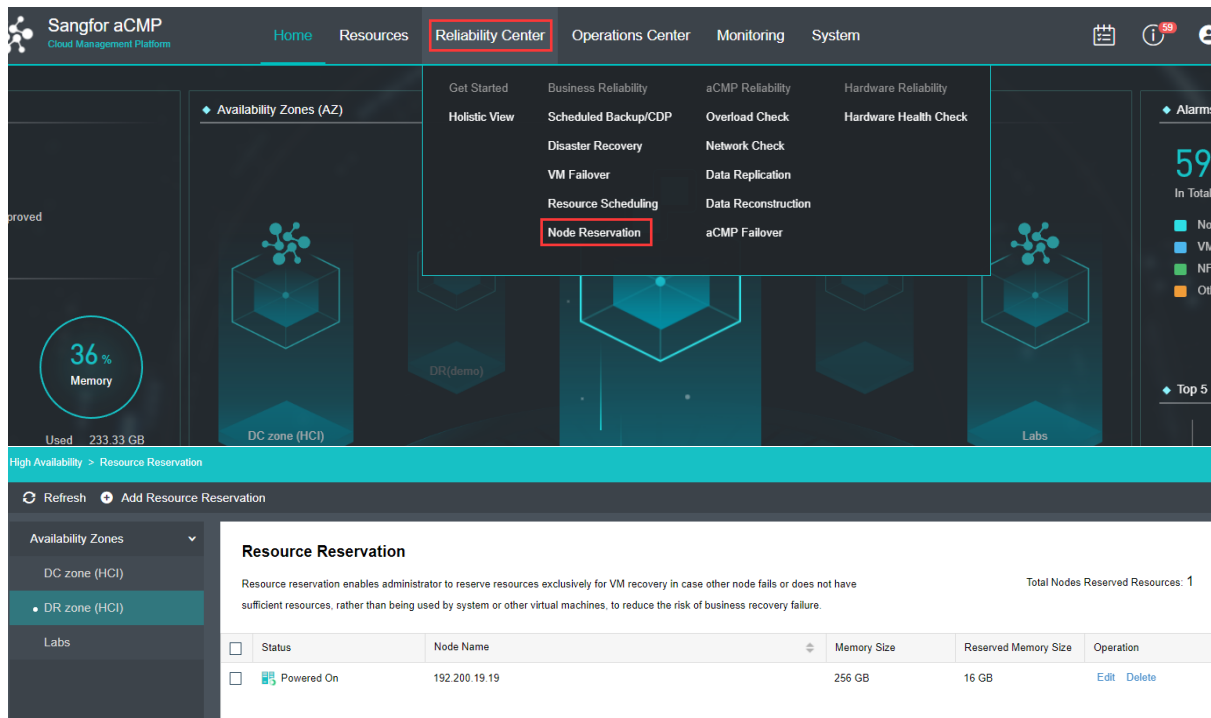
3.3.2.4 Resource Reservation

[Function Description]

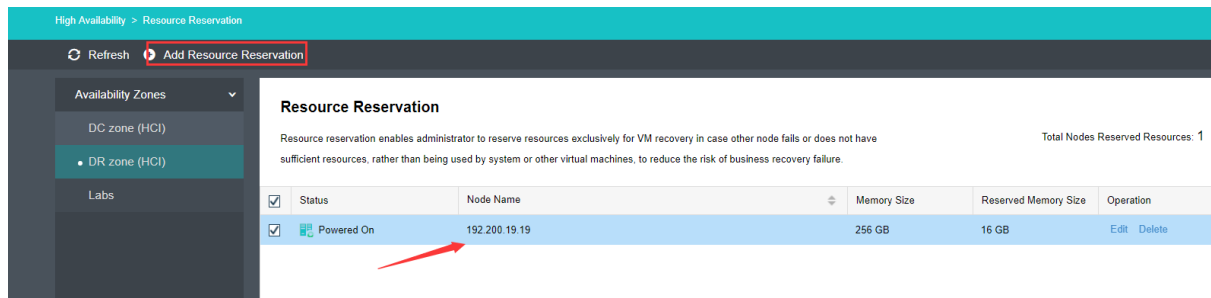
When this function is enabled, resource reservation refers to the reservation of some resource space on partial hosts. This part of resource will not be used by the system or other virtual machine. In case of the failure of a host or disaster recovery switch, the cloud virtual machine may be immediately recovered with the reserved host resource to reduce the risk of the failure of the recovery from business failure due to lack of resources.

[Operating Steps]

1. Log in to the home page of aCMP platform, select 『Reliability Center』 → 『Node Reservation』 to enter Resource Reservation Configuration;



2. The current reservation conditions can be seen on the main page; click **Add Resource Reservation** to enter Host Resource Reservation Configuration page;



3. Configure "Availability Zones", "Node Reserved Resource", "Reserved Memory Size" and other parameters; click **OK**;

Add Resource Reservation ✕

💡 Specify a node and reserve certain amount of its memory resource for VM recovery in case another node fails or runs low on memory.

Availability Zone:

Node Reserved Resource:

Memory Size : 256 GB

Reserved Memory Size: GB

OK
Cancel

4. The reservation items just added can be seen on the interface and can be edited or deleted.

Refresh
Add Resource Reservation

Availability Zones

DC zone (HCI)

DR zone (HCI)

Labs

Resource Reservation

Resource reservation enables administrator to reserve resources exclusively for VM recovery in case other node fails or does not have sufficient resources, rather than being used by system or other virtual machines, to reduce the risk of business recovery failure.

Total Nodes Reserved Resources: 2

<input type="checkbox"/>	Status	Node Name	Memory Size	Reserved Memory Size	Operation
<input type="checkbox"/>	Powered On	192.200.19.19	256 GB	16 GB	Edit Delete
<input type="checkbox"/>	Powered On	192.200.19.18	256 GB	16 GB	Edit Delete

3.3.3 Disaster Recovery Plan

Disaster recovery service provides users with complete virtual machine-level disaster recovery program, including disaster recovery plan, recovery to secondary site, incremental return to the primary site, visual operation and maintenance and other characteristics. The program can help users to quickly grasp and obtain the capability of remote disaster recovery, making disaster recovery no longer a “high-end” proprietary service.

3.3.3.1 Configuration of DR plan

[Function Description]

The disaster recovery plan of SANGFOR is a “local backup-remote disaster recovery” program. A storage is configured as the primary site as the destination

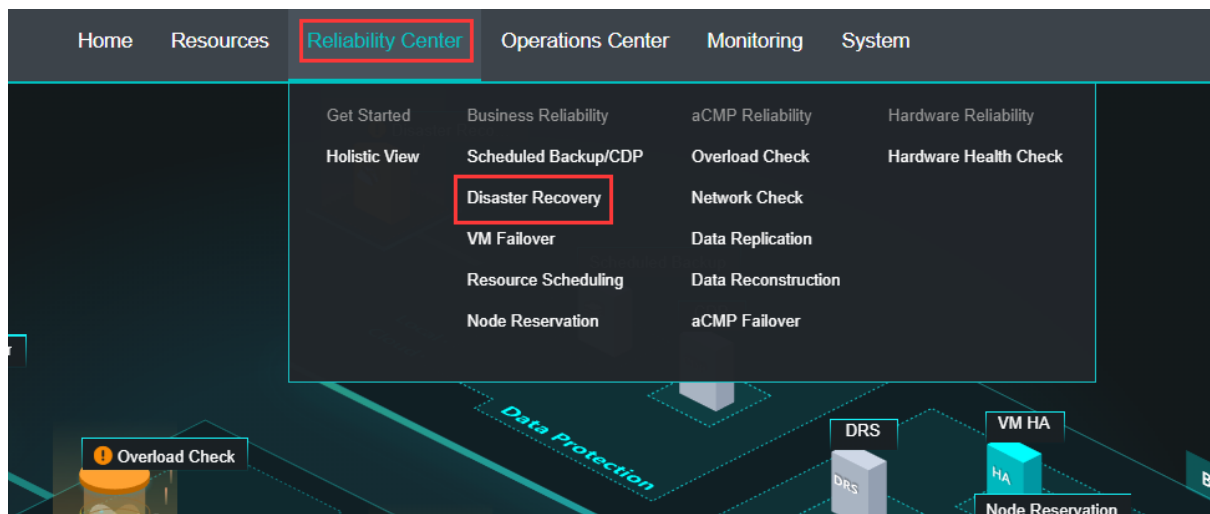
storage for local backup. aCloud cluster is configured on the secondary site as a disaster recovery center.

[Prerequisites]

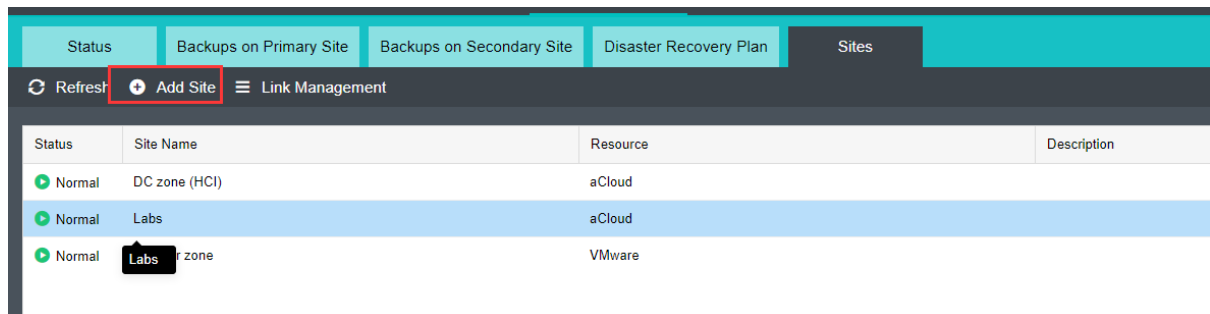
Prepare SANGFOR aCMP management resources and plan corresponding primary and secondary sites for disaster recovery

[Operating Steps]

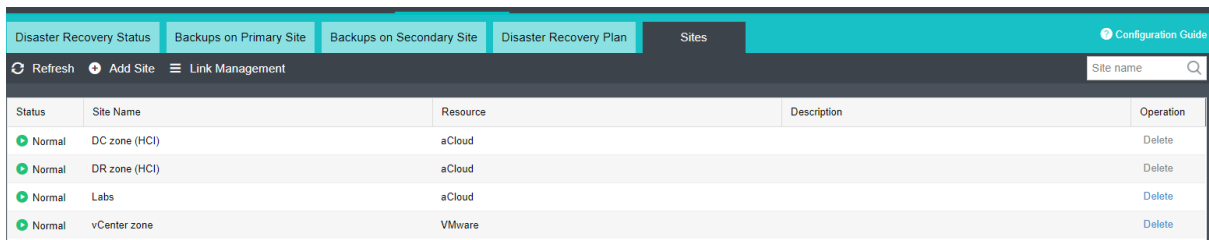
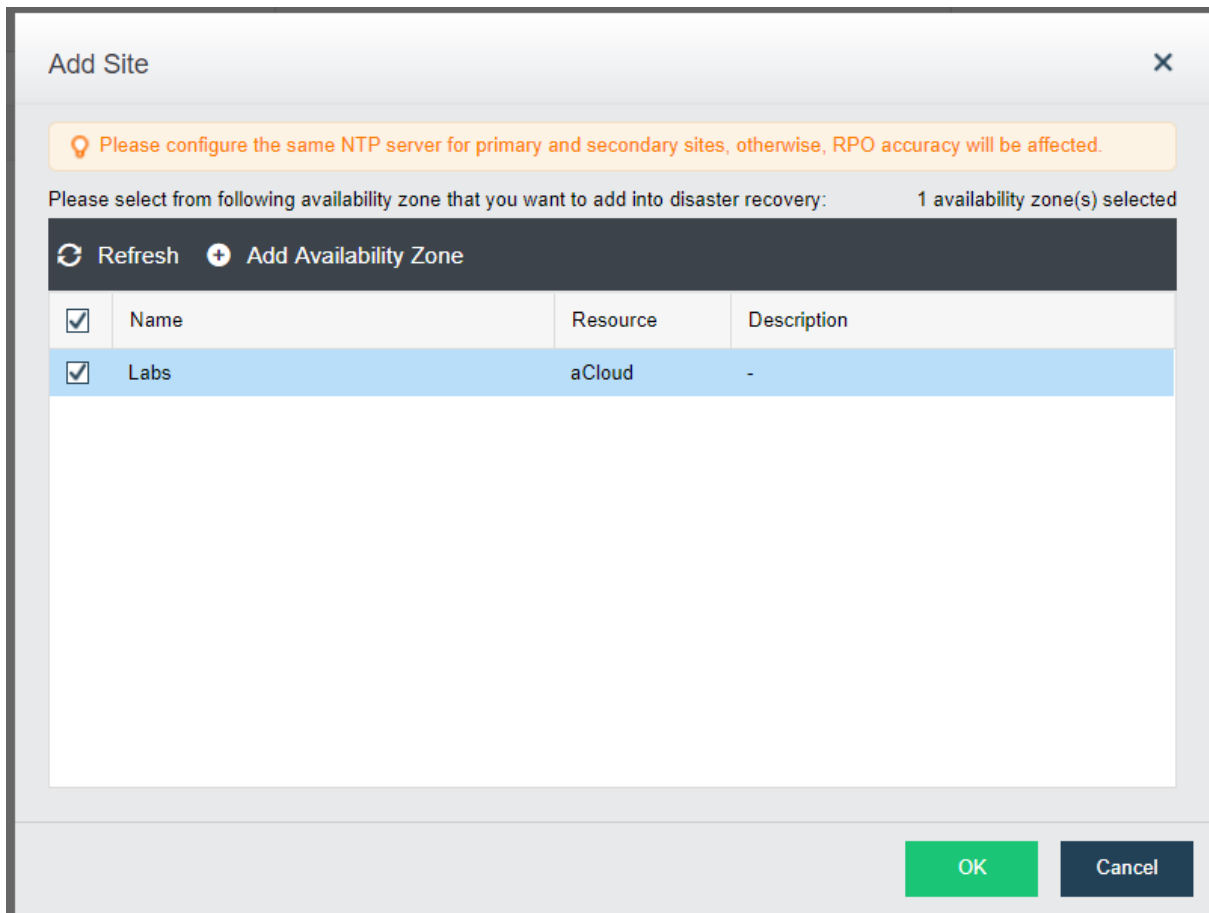
1. Log in to the home page of aCMP platform, select 『Reliability Center』 → 『Disaster Recovery』 to enter Disaster Recovery management interface;



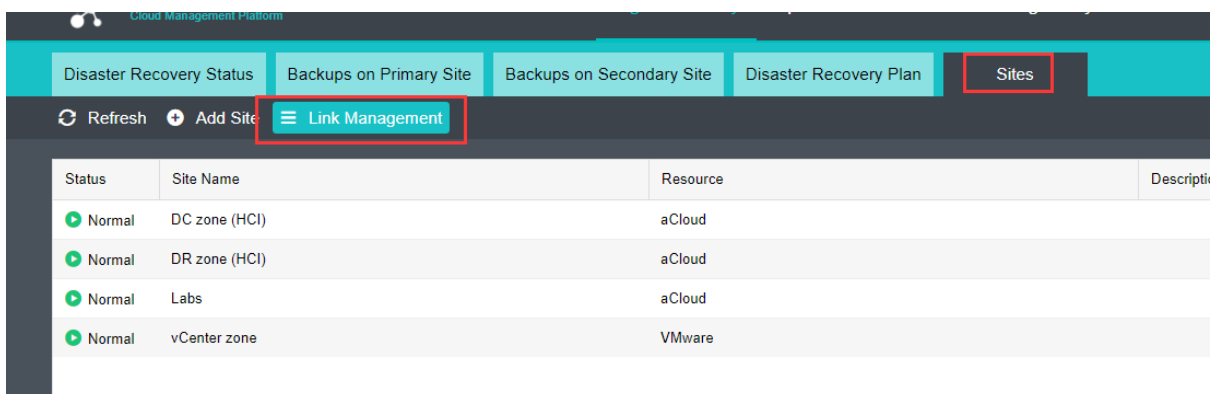
2. Select 『Sites』 and click **Add Site**;



As shown in the following figure, select the availability zones to be added with disaster recovery service; click **OK**. If you do not see the target availability zones, you may click Add Availability Zones to enter the Add Availability Zones interface to add availability zones. For specific operating steps, please refer to Section 2.8 of Chapter 2. You can see the availability zones that have been successfully added. The corresponding availability zones can be removed;

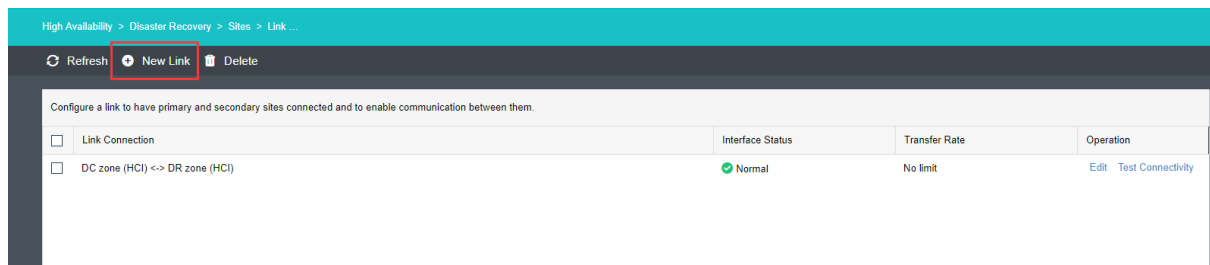


3. Select **【Sites】**, click Link Management for the deployment and configuration of the links among sites.

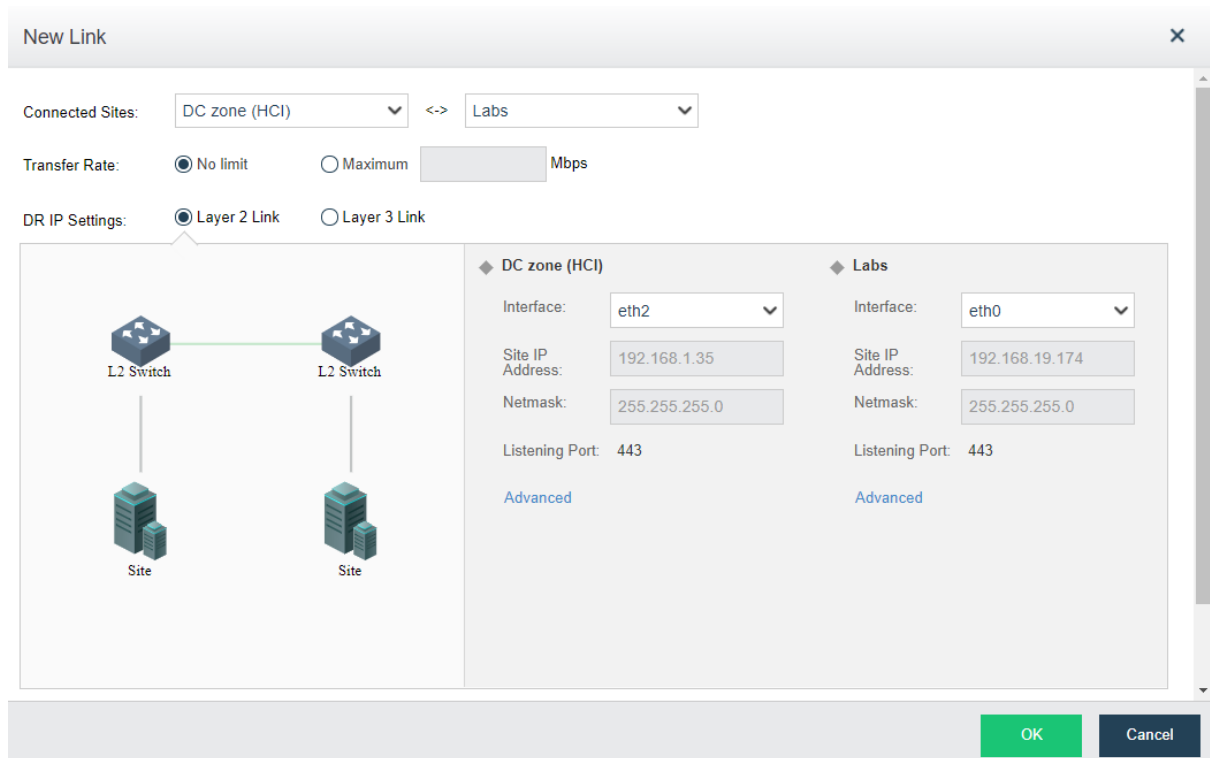


The following configuration interface will appear after clicking Link Management;

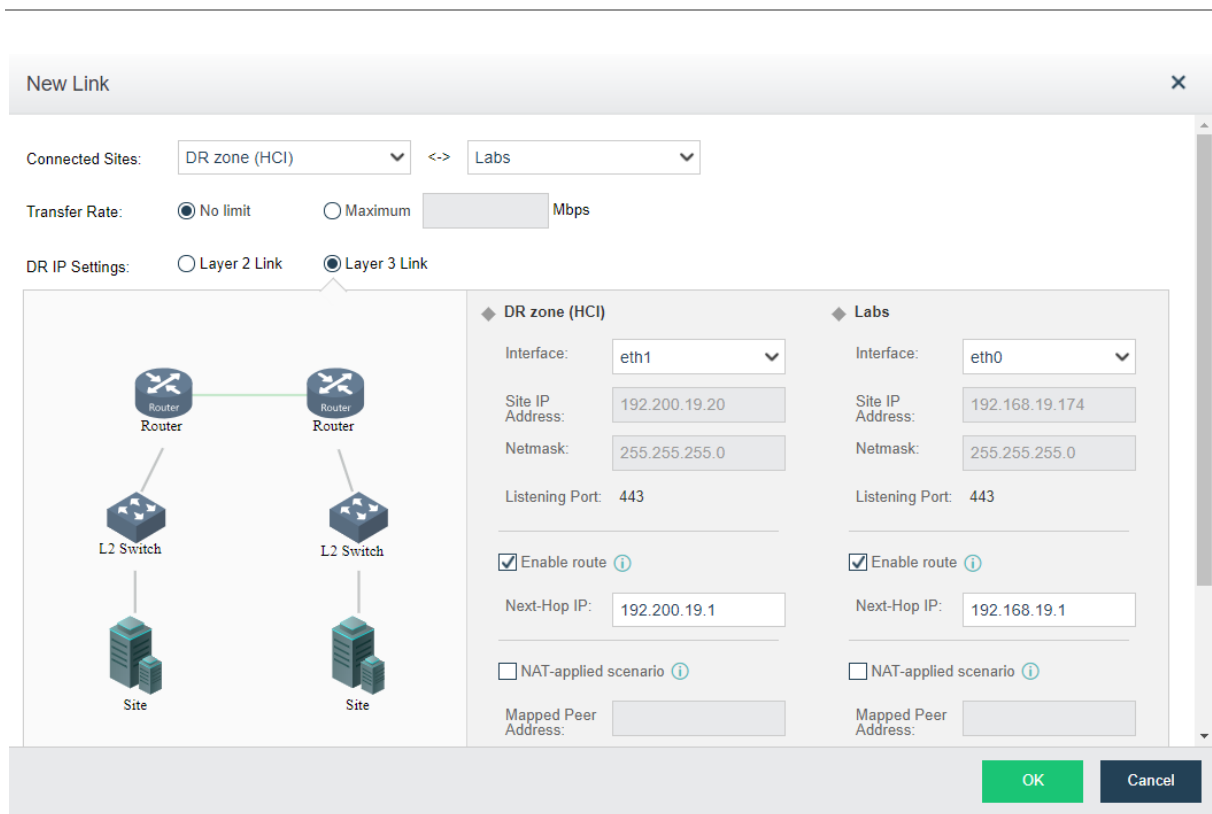
click New Link can add new DR links.



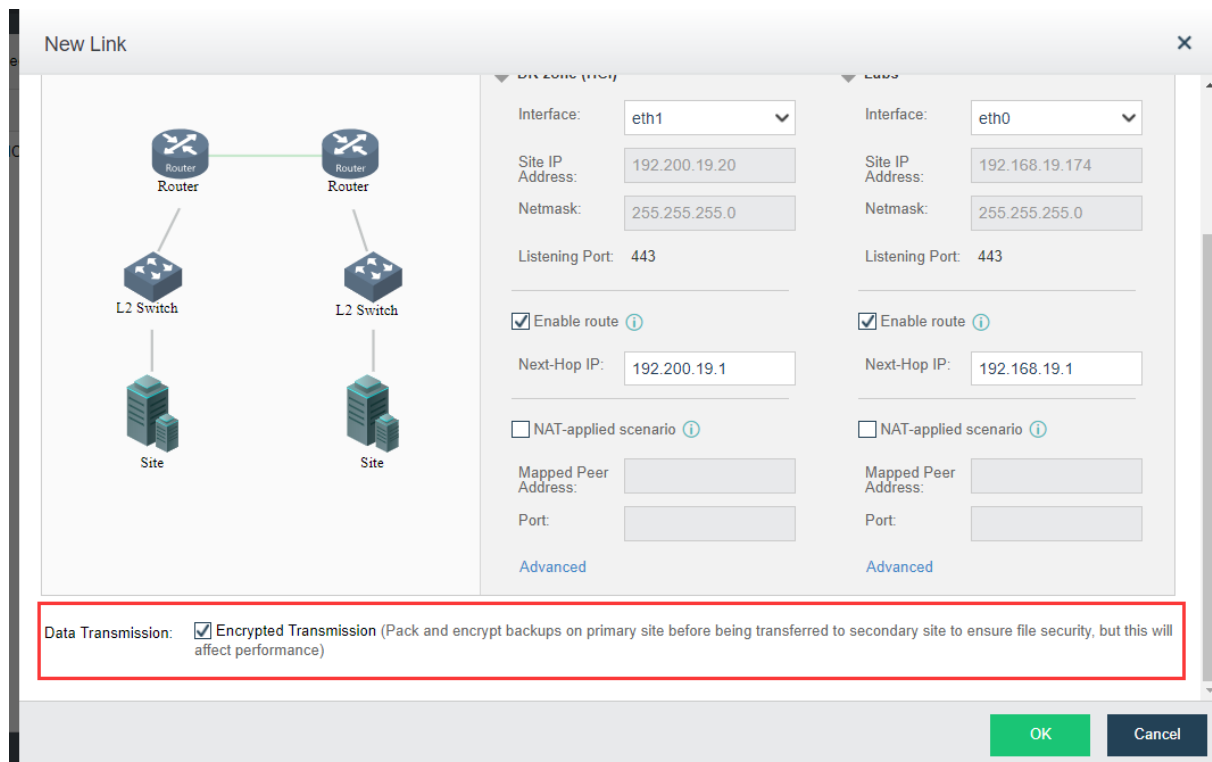
The configuration of Layer 2 Link is as follows:



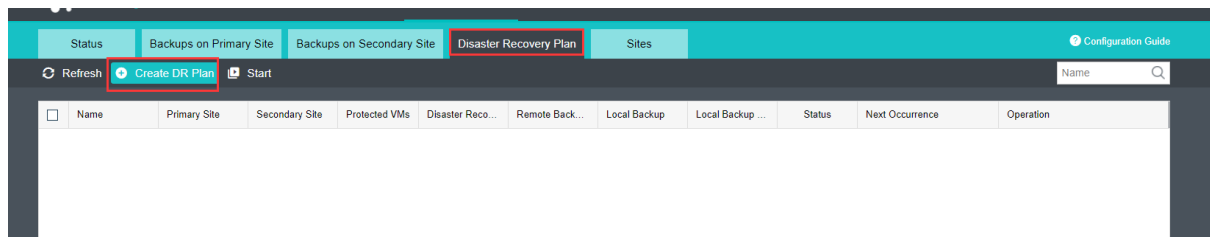
The configuration of Layer 3 Link is as follows:



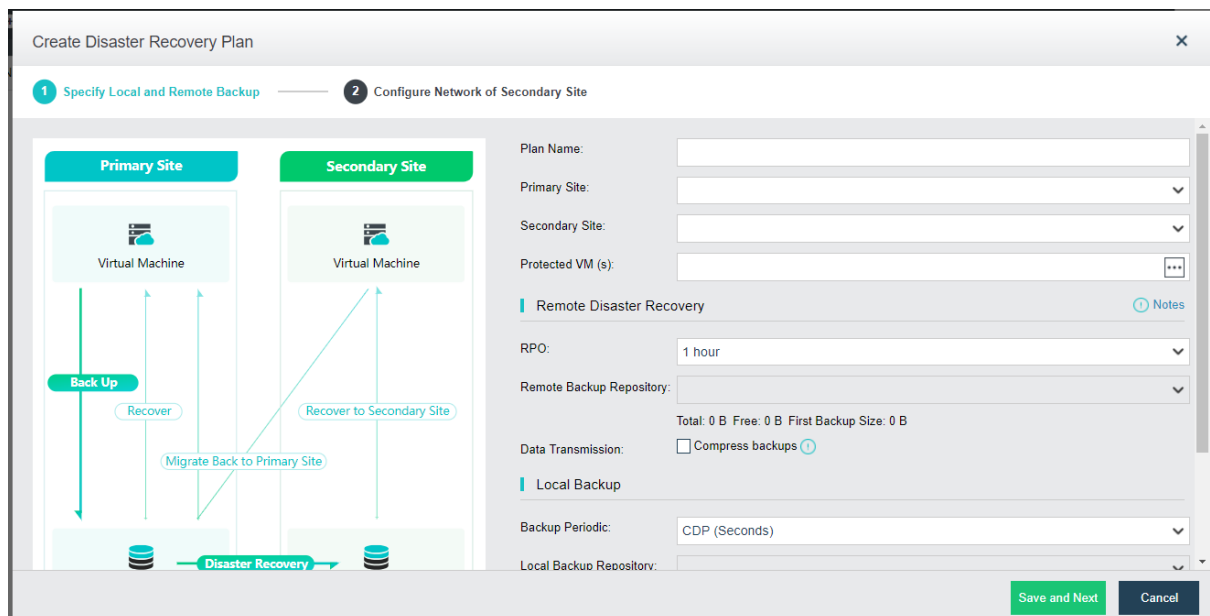
Link compression function: since the speed of transmission process will directly affect RTO, in order to improve transmission efficiency, we can turn on the link compression function to compress the data transmitted. The configuration is as shown in the following figure



4. Select 『Disaster Recovery Plan』 and click **Create DR Plan**;



5. Enter “Configure Data Synchronization Mode” page, fill in the corresponding parameter, then click **Submit** and **Next**. After the creation of disaster recovery plan, click **Configure Network of Secondary Site**;



【Plan Name】 to name the disaster recovery plan

【Primary Site】 to configure the primary site which refers to the aCloud nodes for daily business operations.

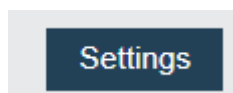
【Secondary Site】 to configure disaster recovery phases which refer to the nodes that need to be switched to after the failure of the primary node and are usually remote.

【Protected VM】 to configure the virtual machine that needs to execute DR plan

【Remote Backup Repository】 to configure the location where DR data are stored.

【RPO】 the full name of RPO is Recovery Point Objective (RPP) where second, minute, hour and day-level recovery configurations are provided.

【Data Transmission】 to configuration whether to enable the compression of disaster recovery data. Note that if the compression is enabled, it will increase CPU consumption on the host, which is not recommended in the case of insufficient CPU resources on the hardware.



Click **Settings** to conduct detailed configuration of remote backup and local backup parameters. See the following figure:

The screenshot shows a 'Settings' dialog box with a close button (X) in the top right corner. It features two tabs: 'Remote Disaster Recovery' (highlighted in green) and 'Local Backup'. The configuration options are as follows:

- RPO:** A dropdown menu set to '30 minutes'.
- Recovery Point File Retention Period:** A dropdown menu set to 'One week'.
- Remote Backup Repository:** A dropdown menu set to 'DataStore'.
- Data Transmission:** A checkbox labeled 'Compress backups' which is currently unchecked. Below it, a note reads: 'Compress backup files before transmission, to improve transmission efficiency and reduce bandwidth consumption, but this will consume more CPU resources.'

At the bottom right, there are two buttons: 'OK' (green) and 'Cancel' (dark blue).

The following configuration interface will appear after clicking Next:

The screenshot shows the 'Create Disaster Recovery Plan' dialog box with a close button (X) in the top right corner. It displays a progress indicator with two steps: '1 Specify Local and Remote Backup' (marked with a green checkmark) and '2 Configure Network of Secondary Site' (marked with a blue circle and '2').

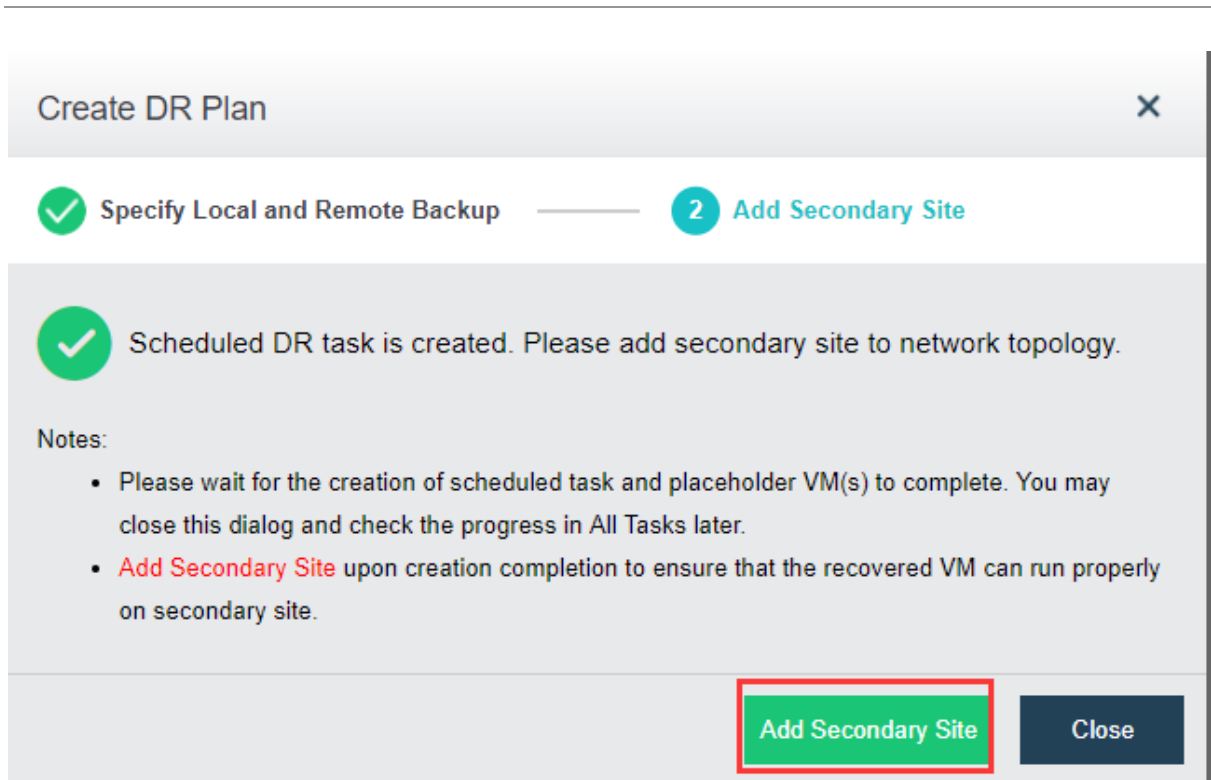
Below the progress indicator, the text reads 'Creating, please wait...(19%)' followed by a green progress bar that is approximately 19% full.

Notes:

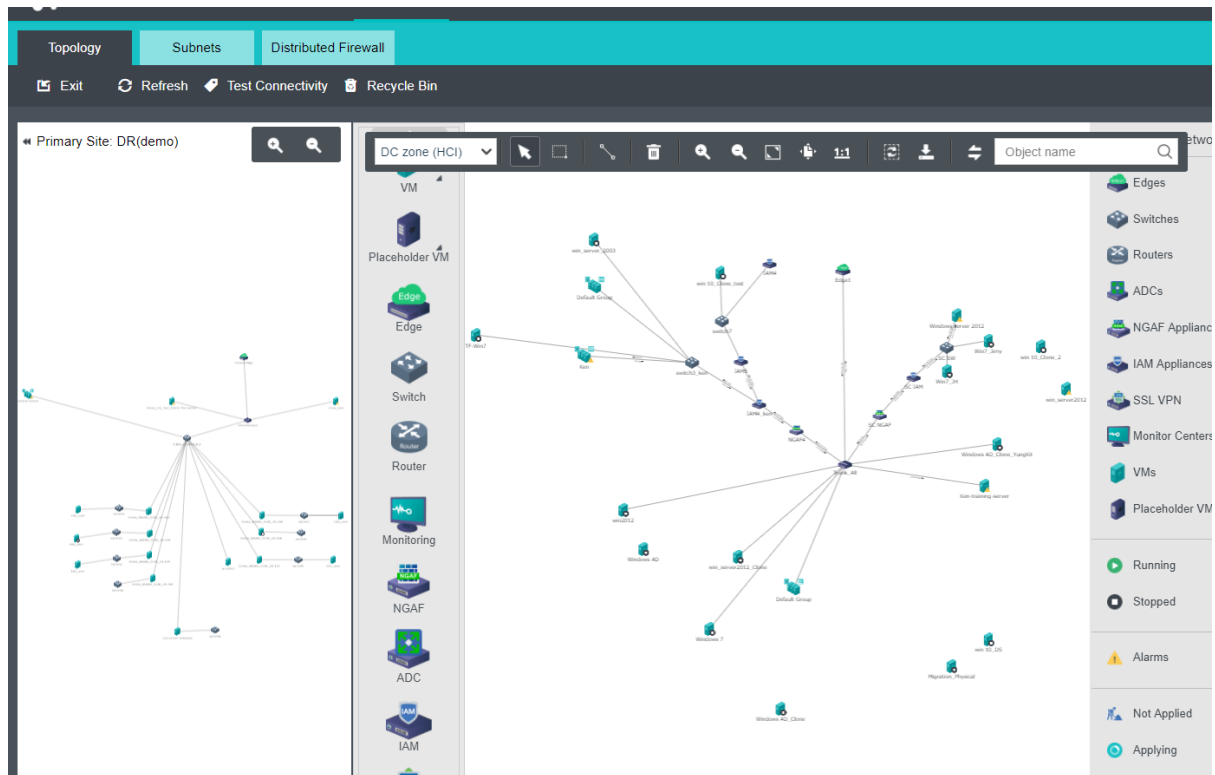
- Placeholder VM (s) will be created at secondary site after disaster recovery plan is created. This process may take a while. You may go to Tasks to view the progress of this task after hiding task progress.
- Configure topology for secondary site upon creation completion to ensure that the recovered VM can run properly on secondary site.

At the bottom, there are two buttons: 'Configure Network of Secondary Site' (disabled, grey) and 'Hide Progress' (dark blue).

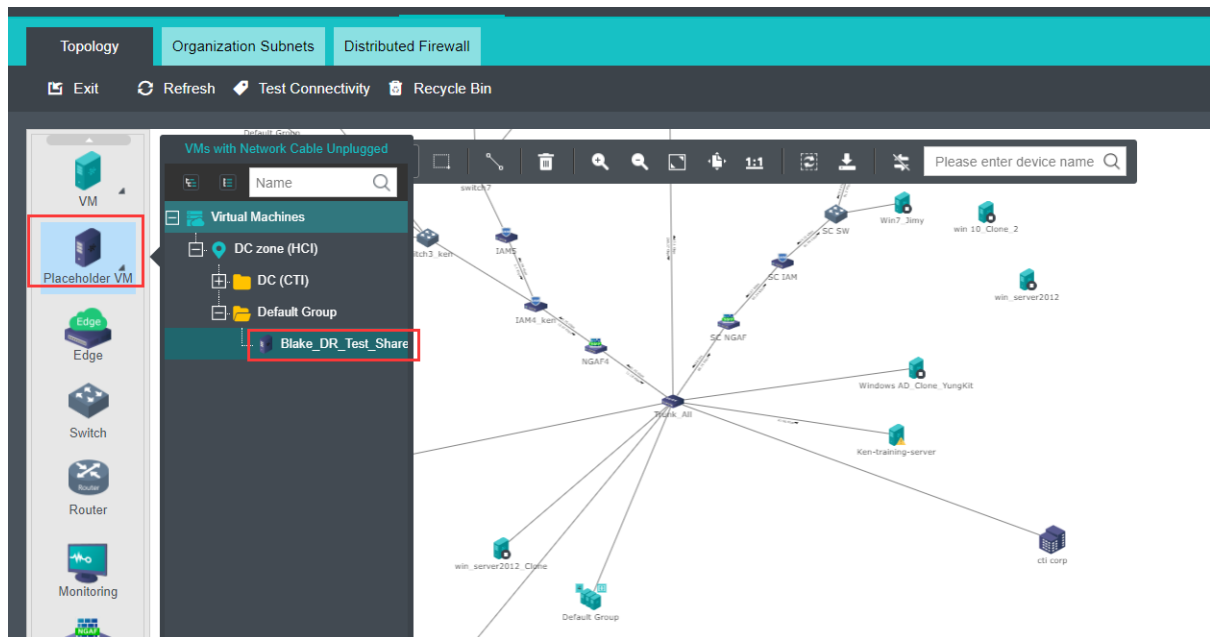
Wait for successful creation. Click Configure Network of Secondary Site. See the following figure:



The following configuration interface be displayed after clicking:



Select the corresponding DR virtual machine, then conduct topology editing in the corresponding disaster recovery area. See the following figure:



: the physical disk, virtual shared disk, external USB device and external optical drive added for the virtual machine do not support disaster recovery.



: please synchronize the system time of the primary site, the secondary site and aCMP to keep it consistent.

- So far, the configuration of disaster recovery plan has been completed, select 『Operation Center』 → 『Remote Disaster Recovery』, click 『Disaster Recovery Plan』; Then you can see all disaster recovery plans; check the disaster recovery plan to be configured; click **Execute DR Plan Now**. You can also edit, configure network and delete existing disaster recovery plans.

DR Plan Name	Primary Site	Secondary Site	Protected VMs	Remote Disas...	Remote Back...	Local Backup	Local Backup ...	Status	Next DR Plan Execution Ti...	Operation
<input type="checkbox"/> DC to DR	DC zone (HCI)	DR zone (HCI)	1	RPO: 30 minut...	VirtualDatasto...	Continuous D...	DataStore	✓	2018-10-11 16:30:00	Edit Configure Network Delete
<input checked="" type="checkbox"/> Blake	DR zone (HCI)	DC zone (HCI)	1	RPO: 30 minut...	DataStore	Continuous D...	VirtualDatasto...	✓	2018-10-11 16:30:00	Edit Configure Network Delete

3.3.3.2 Local File Retrieval

[Function Description]

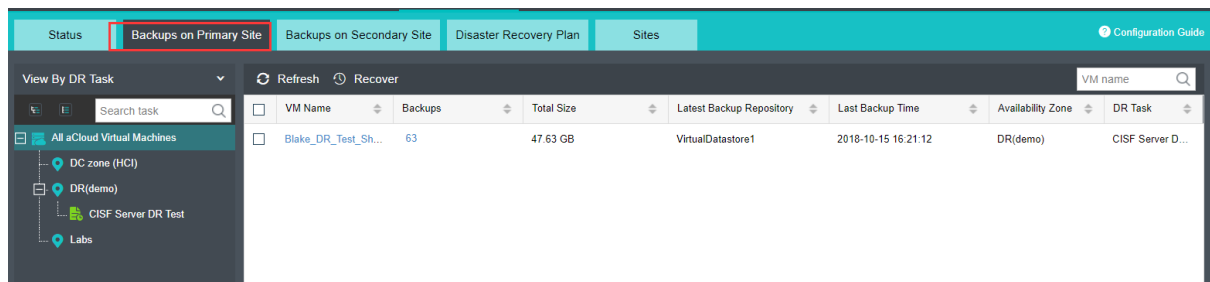
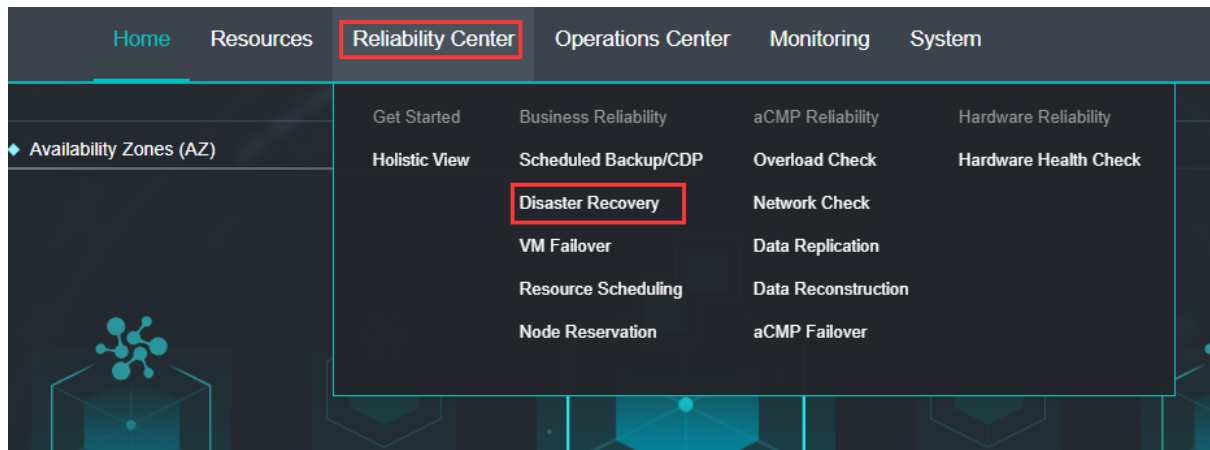
The disaster recovery program of SANGFOR is a “local backup - remote disaster recovery” program. After configuring disaster recovery plan (CDP) for the corresponding virtual machine, if some files are deleted by mistake, such files may be recovered by local file retrieval.

[Prerequisites]

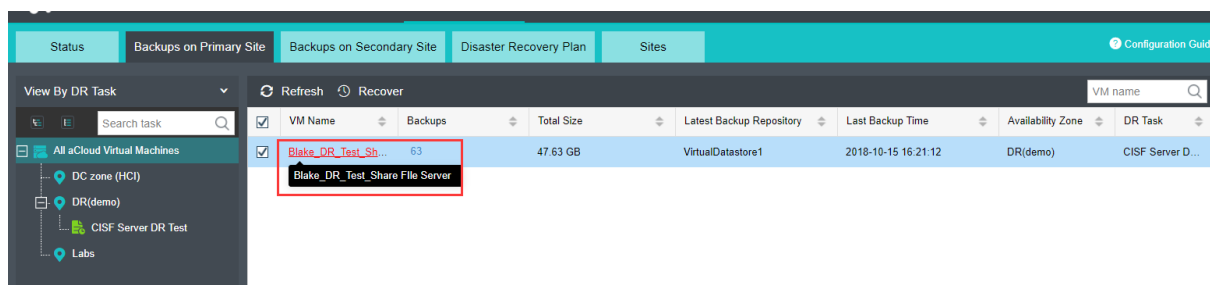
The corresponding virtual machine has been added to the disaster recovery plan and configured with second-level disaster recovery.

[Operating Steps]

1. Log in to the home page of aCMP platform, select 『Reliability Center』 → 『Disaster Recovery』 → 『Backups on Primary Site』 to view all primary site backup data;



2. Click the virtual machine that needs to retrieve a file to enter the Details interface, select 『Backups』;



Virtual Machine > Blake_DR_Test_Share File Server

Summary Snapshots **Backups** Tasks Alarms

Refresh Scan New IO Activity Logs Backup Settings Start CDP Stop CDP

Time Range: Last 2 hour 2018-10-15 15:00 to 2018-10-15 17:00 Search Backup IO Activities

Expand All Collapse All Delete

Time	Type	Used Space	Datastore	Description	Backup Lock	Operation
2018-10-15 16:18:43	Backup	128 MB	VirtualDatastore1	-	Not ena...	Browse Files Recover Clone
2018-10-15 15:12:59	Backup	128 MB	VirtualDatastore1	-	Not ena...	Browse Files Recover Clone
2018-10-15 14:09:55	Backup	128 MB	VirtualDatastore1	-	Not ena...	Browse Files Recover Clone

Disaster Recovery Plan

CISF Server D... Enabled

Automatic Backup

Periodic: Every 1 hr(s)

Size: 47.63 GB

CDP

Status: Powered On

Logs Retentio... : 24 hour(s)

Max IO Activity... : 800 GB

IO Activity Log... : 0 %

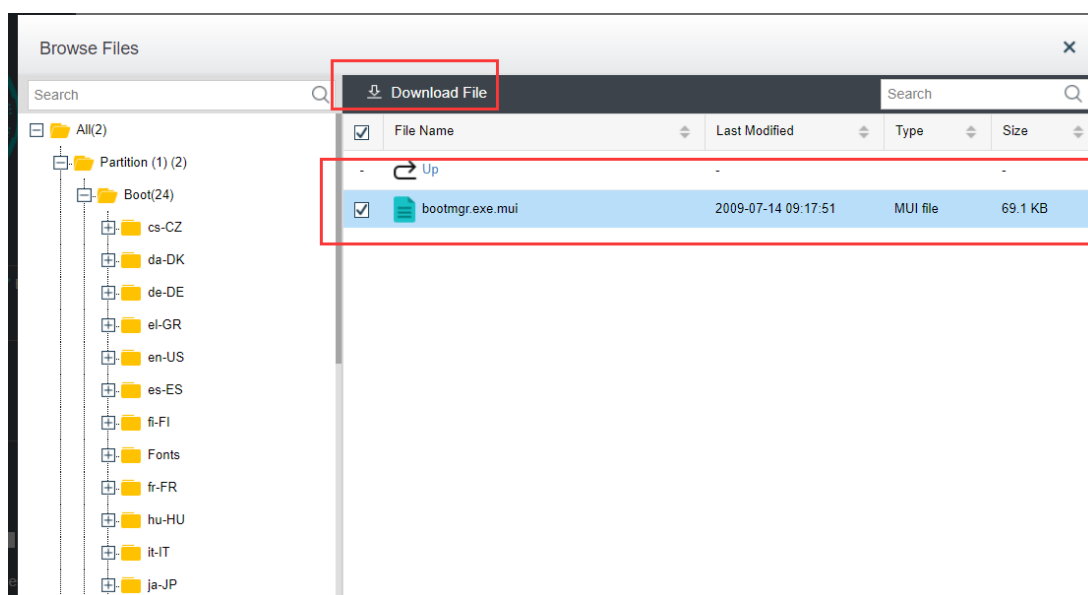
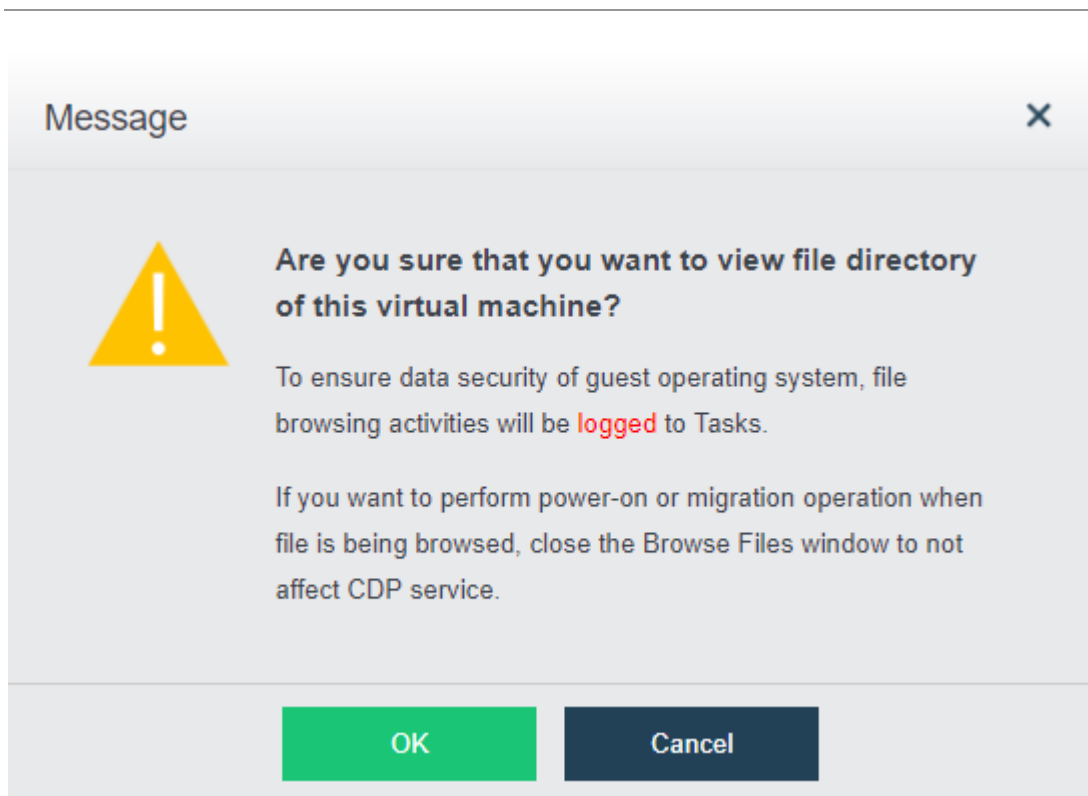
Disaster Recovery Across Sites

RPO: 30 minutes

- Click the **Retrieve File**, Click the **OK** in the pop-up window, and download the corresponding file in the corresponding directory structure for the purpose of recovery;

Expand All Collapse All Delete

Time	Type	Used Space	Datastore	Description	Backup Lock	Operation
2018-10-15 16:18:43	Backup	128 MB	VirtualDatastore1	-	Not ena...	Browse Files Recover Clone
2018-10-15 15:12:59	Backup	128 MB	VirtualDatastore1	-	Not ena...	Browse Files Recover Clone
2018-10-15 14:09:55	Backup	128 MB	VirtualDatastore1	-	Not ena...	Browse Files Recover Clone
2018-10-15 13:07:06	Backup	128 MB	VirtualDatastore1	-	Not ena...	Browse Files Recover Clone
2018-10-15 12:03:51	Backup	128 MB	VirtualDatastore1	-	Not ena...	Browse Files Recover Clone
2018-10-15 11:01:05	Backup	128 MB	VirtualDatastore1	-	Not ena...	Browse Files Recover Clone



3.3.3.3 Data Recovery on Primary Site

[Function Description]

If an abnormality occurs in a virtual machine or a plurality of virtual machines at the primary site, you may choose to restore the virtual machine backups or CDP data directly at the primary site, which reduces the recovery time and the risk of business outage window.

[Prerequisites]

The corresponding virtual machine has been added to the disaster recovery plan and has generated complete backup data.

[Operating Steps]

1. Log in to the home page of the aCMP platform and select the 『Operations Center』 → 『Disaster Recovery』 → 『Backups on Primary Site』 to view all disaster recovery hosts;

The screenshot shows the Sangfor aCMP Cloud Management Platform interface. The top navigation bar includes 'Home', 'Resources', 'Reliability Center' (highlighted with a red box), 'Operations Center', 'Monitoring', and 'System'. A dropdown menu is open under 'Reliability Center', with 'Disaster Recovery' highlighted by a red box. Below this, the 'Backups on Primary Site' tab is selected. The interface displays a table of backup data with columns: VM Name, Backups, Total Size, Latest Backup Repository, Last Backup Time, Availability Zone, and DR Task. A red box highlights the 'Recover' button and the first row of the table.

VM Name	Backups	Total Size	Latest Backup Repository	Last Backup Time	Availability Zone	DR Task
Blake_DR_Test_Sh...	64	47.75 GB	VirtualDatastore1	2018-10-15 18:24:16	DR(demo)	CISF Server D...

2. Click the **Recover**, select the recovery method and destination location, and click the **OK**;

Recover VM



- 1 Choose Method — 2 Destination Location

Recovery Method:

Create New Virtual Machine (recommended)

1. A new virtual machine will be recovered from this backup, while the existing one will not be affected.
2. Upon completion of VM recovery and data verification, you may manually make the new virtual machine run business services.
3. You need to connect the VM to the network manually to avoid the IP address conflict. Connect the new virtual machine to the network manually to avoid IP address conflict, re-authorize the virtual machine if guest OS or software authorization is bound with hardware ID as the new virtual machine has a different hardware ID.

Overwrite Existing Virtual Machine

1. The original virtual machine will be powered off and be deleted. Contact Sangfor technical support to recover the virtual machine within 30 days or else the virtual machine will be automatically cleaned up.
2. VM hardware configuration keeps unchanged. Therefore, guest OS or software does not need to be reauthorized.
3. Network of recovered virtual machine is unchanged.
4. Recover virtual machine from backup and snapshot of the virtual machine will lost after recovery.

Next

Cancel

Recover VM



- ✓ Choose Method — 2 Destination Location

VM Name	Recover to Backup	New VM Name	Recover to Group	Destination Data...	Recover to the C...	Operation
Blake_DR_T...	2018-10-15 16:18:43	Blake_DR_Test_...	Default group	VirtualDatastore1	<Auto>	Select Desti...

Back

OK

Cancel

Name:

Destination Location:

Group:

Storage:

Run on Node:

Datastore:

[Restore Defaults](#)

3. You can see that the virtual machine recovery is being executed in Tasks;

Status	Action	Object	Start Time	End Time	Admin	Operation
<div style="width: 55%;"><div style="width: 55%;"></div></div> 55%	Create VM from ...	Blake_DR_Test_...	2018-10-15 18:35:28	-	admin (192.168.19.206)	View Cancel
<div style="width: 5%;"><div style="width: 5%;"></div></div> 5%	Create CDP bac...	Blake_DR_Test_...	2018-10-15 18:34:23	-	Sangfor Cloud Manag...	View Cancel
Completed	Auto-clean up I...	Blake_DR_Test_...	2018-10-15 18:25:24	2018-10-15 18:25:35	Sangfor Cloud Manag...	View
Completed	Create CDP bac...	Blake_DR_Test_...	2018-10-15 18:25:12	2018-10-15 18:25:23	Sangfor Cloud Manag...	View
Completed	Auto-clean up I...	Blake_DR_Test_...	2018-10-15 18:24:26	2018-10-15 18:24:43	Sangfor Cloud Manag...	View
Completed	Auto-clean up I...	Blake_DR_Test_...	2018-10-15 18:24:07	2018-10-15 18:24:25	Sangfor Cloud Manag...	View

3.3.3.4 Planned Data Recovery to Secondary Site

[Function Description]

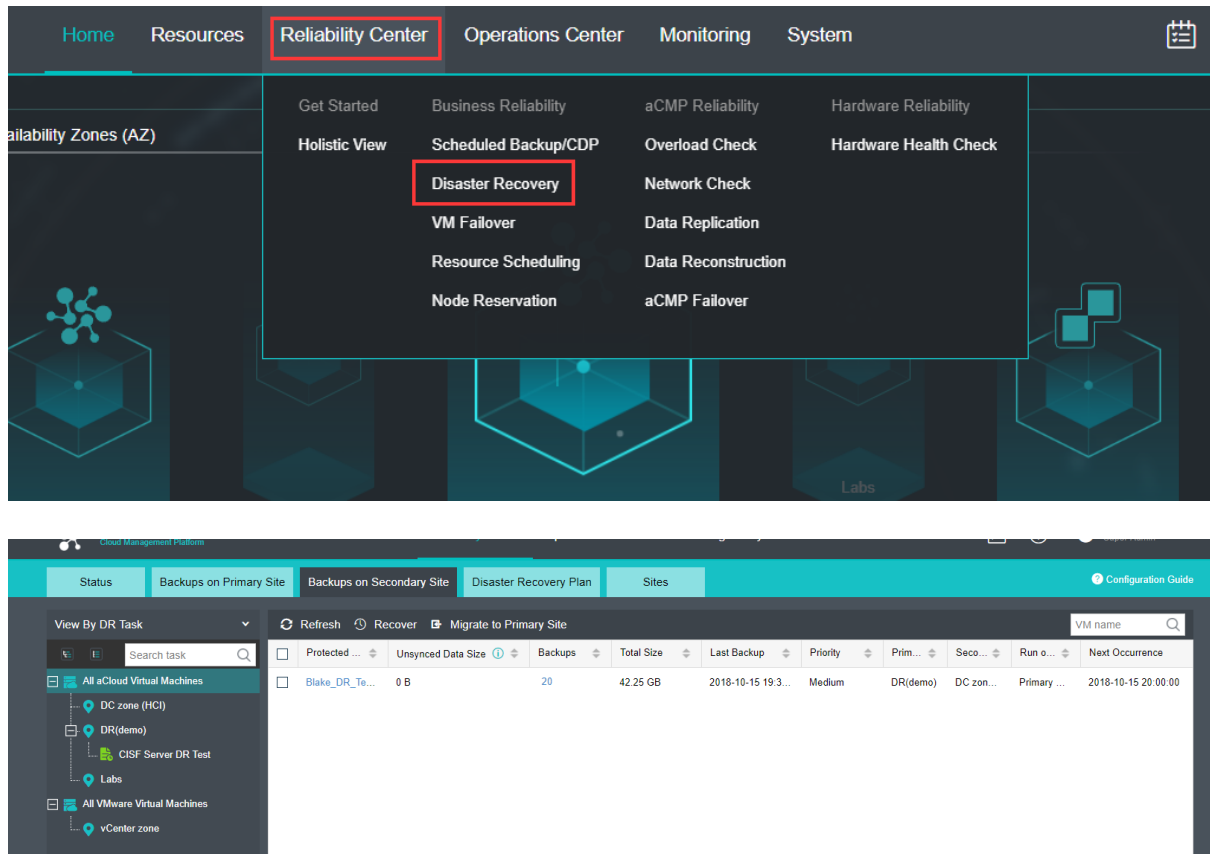
If an abnormality occurs in a virtual machine or a plurality of virtual machines at the primary site, or a planned recovery is needed for the disaster recovery data of a secondary site due to the need for disaster recovery drills, you may choose the function of planned data recovery to the secondary sites.

[Prerequisites]

The corresponding virtual machine has been added to the disaster recovery plan and has generated complete backup data.

[Operating Steps]

1. Log in to the home page of the aCMP platform and select the 『Operations Center』 → 『Disaster Recovery』 → 『Backups on Secondary Site』 to view the disaster recovery data at the secondary site, as shown in the figure below:



2. Select the virtual machine to be recovered, click the **Recover**, select whether to use reserved resources for cloud virtual machine recover and select the destination datastore in the pop-up window, click the **Recover**, and you will need to enter the user password to confirm this operation;

Recover
✕

Recovery Method:

Planned Recovery (for online primary site)

The virtual machine at primary site will be shut down immediately and newest data be synced to secondary site. Upon data sync completion, the placeholder VM at secondary site will be automatically powered on. **Business are shortly interrupted during the recovery.** If error occurs during the process, the recovery will be canceled.

Recovery after Disaster

The placeholder VM at secondary site will be powered on immediately, **and data have not been synchronized to secondary site will lose.** If the virtual machine at primary site is online, the recovered VM at secondary site may encounter IP address conflict. Please make sure that VM network configuration at primary and secondary sites will not cause IP address conflict.

Use reserved resources for VM recovery ([Resource Reservation](#))

Objects:

VM Name	Destination Site	Destination Datastore	DR Task
Blake_DR_Test_Share File Server	DC zone (HCI)	DataStore	CISF Server DR Test

Recover
Cancel

Alert
✕

Are you sure that you want to perform recovery?

Enter password (**admin**) to confirm this operation

.....|

OK
Cancel



: If you select Planned Recovery, this method will immediately shut down the virtual machine at the primary site, synchronize the latest data to the secondary site, and automatically pull the disaster recovery standby at the secondary site after the data synchronization is completed. Short interruption may happen to business during this process. Recovery will be canceled if any error occurs.

3. You can see that the virtual machine recovery is being executed in Tasks;

Tasks						
All		Disaster Recovery 1				
Status	Action	Object	Start Time	End Time	Admin	Operation
30%	Shut down virtua...	Blake_DR_Test_...	2018-10-15 19:53:04	-	Sangfor Cloud Manag...	View Cancel
Completed	Log in	admin	2018-10-15 19:43:16	2018-10-15 19:43:16	admin (192.168.19.206)	View
Completed	Create CDP bac...	Blake_DR_Test_...	2018-10-15 19:37:51	2018-10-15 19:41:02	Sangfor Cloud Manag...	View
Completed	Auto-clean up I...	Blake_DR_Test_...	2018-10-15 19:26:37	2018-10-15 19:26:47	Sangfor Cloud Manag...	View
Completed	Create CDP bac...	Blake_DR_Test_...	2018-10-15 19:26:25	2018-10-15 19:26:32	Sangfor Cloud Manag...	View
Completed	Auto-clean up I...	Blake_DR_Test_...	2018-10-15 19:25:24	2018-10-15 19:25:42	Sangfor Cloud Manag...	View

3.3.3.5 Recovery to Secondary Site After Disaster

[Function Description]

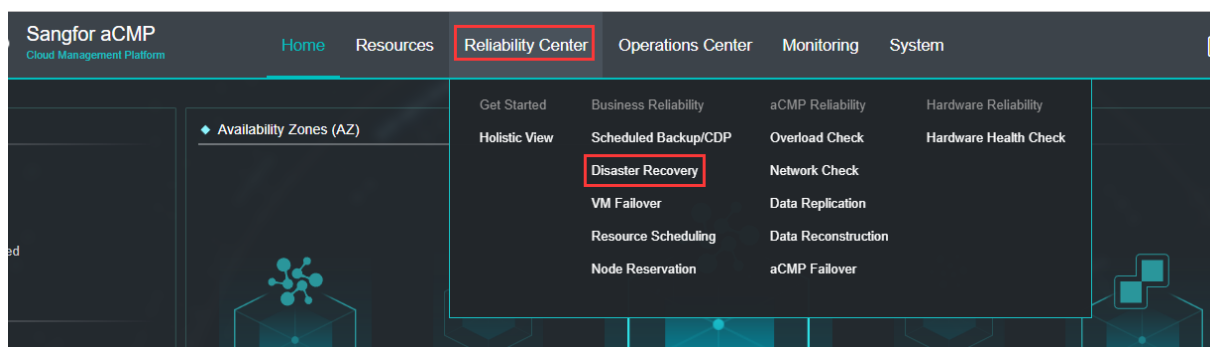
If a disaster occurs at the primary site and the cluster is unavailable, and all virtual machines are powered off or unavailable at this time, you may log in to the standby aCMP cloud management platform through the secondary site to perform the recovery after disaster. You may choose to recover the virtual machines to the secondary site.

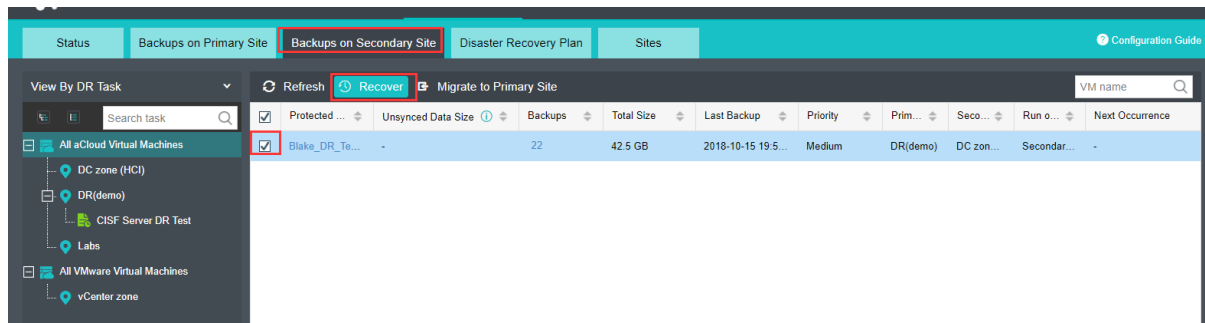
[Prerequisites]

The corresponding virtual machine has been added to the disaster recovery plan and has generated complete backup data at the secondary site.

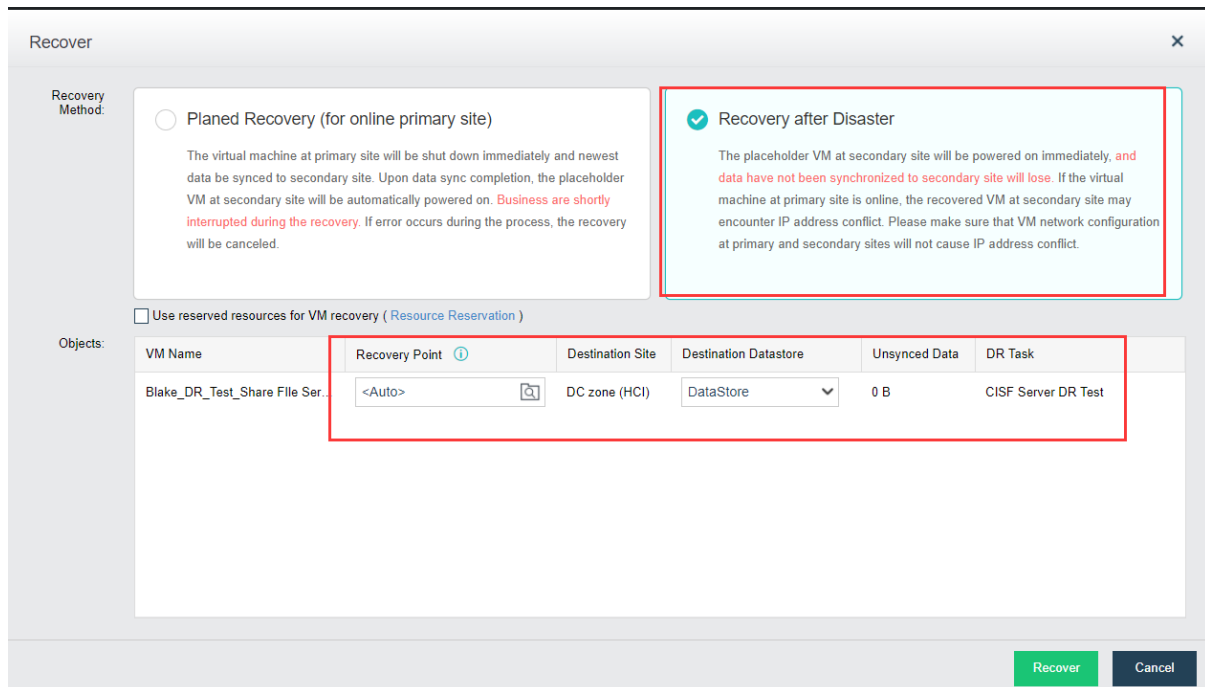
[Operating Steps]

1. Log in to the home page of the aCMP platform and select the 『Operations Center』 → 『Disaster Recovery』 → 『Backups on Secondary Site』 to view the disaster recovery data at the secondary site;





2. Select the virtual machine to be recovered, click **Recover**, select the Recovery after Disaster, select whether to use reserved resources for virtual machine recovery and select the destination data store and recovery point in the pop-up window, click **Recover**, and you will need to enter the user password to confirm this operation;



: If you select Recovery after Disaster, this method will immediately pull the disaster recovery standby at the secondary site, and the data not synchronized to the standby site will be lost. If the virtual machine at the primary site is online, the disaster recovery standby pulled at the secondary site may encounter IP address conflict. Please make sure that the network configurations at the primary and secondary sites will not cause IP address conflict.

3. You can see that the virtual machine recovery is being executed in Tasks;

Tasks						
All		Disaster Recovery				
Status	Action	Object	Start Time	End Time	Admin	Operation
<div style="width: 75%;"><div style="background-color: #0070c0; height: 10px;"></div></div> 75%	Recover VM upo...	Blake_DR_Test_...	2018-10-16 17:37:29	-	admin (192.168.19.206)	View Cancel
✔ Completed	Update VM type	Blake_DR_Test_...	2018-10-16 17:37:31	2018-10-16 17:37:37	admin (192.168.19.206)	View
✔ Completed	Recovery after d...	CISF Server DR...	2018-10-16 17:37:29	2018-10-16 17:37:30	admin (192.168.19.206)	View
✔ Completed	Update baseline...	Blake_DR_Test_...	2018-10-16 17:22:56	2018-10-16 17:23:06	admin (192.168.19.206)	View
✔ Completed	Backup transmis...	Blake_DR_Test_...	2018-10-16 17:22:17	2018-10-16 17:22:56	admin (192.168.19.206)	View
✔ Completed	Start CDP client	Blake_DR_Test_...	2018-10-16 17:21:59	2018-10-16 17:22:17	admin (192.168.19.206)	View

3.3.3.6 Migrate to Primary Site

[Function Description]

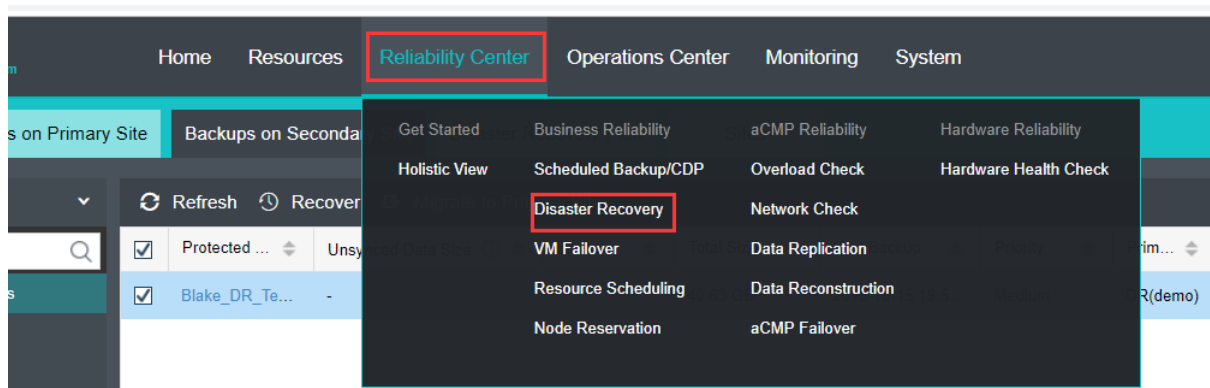
After the primary site returns to normal, you may choose to migrate the virtual machines that are recovered to the secondary site to the primary site.

[Prerequisites]

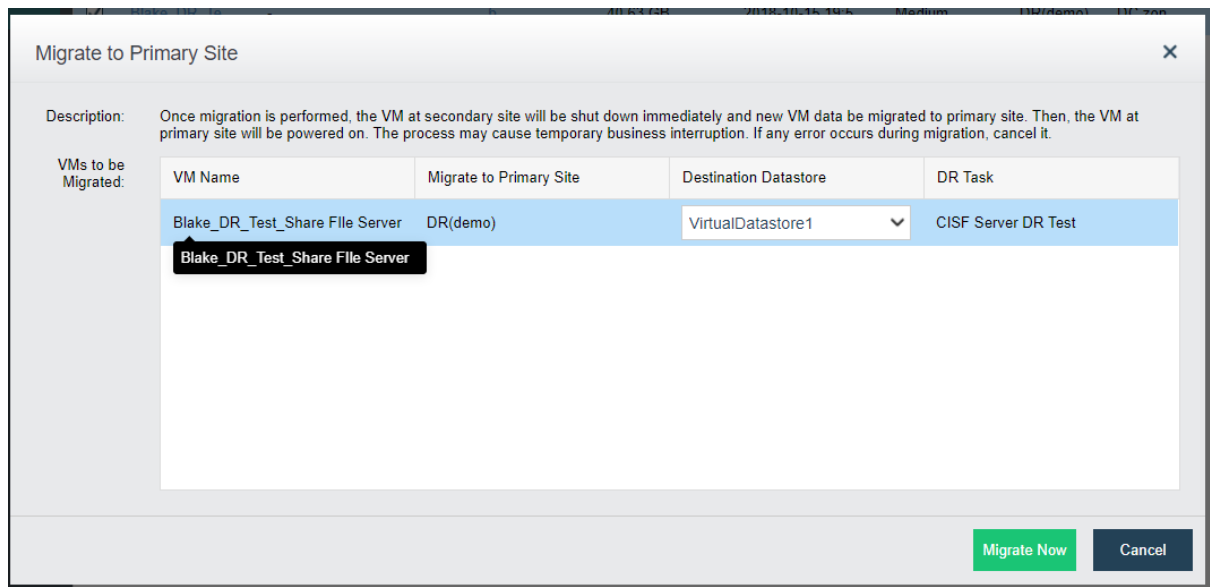
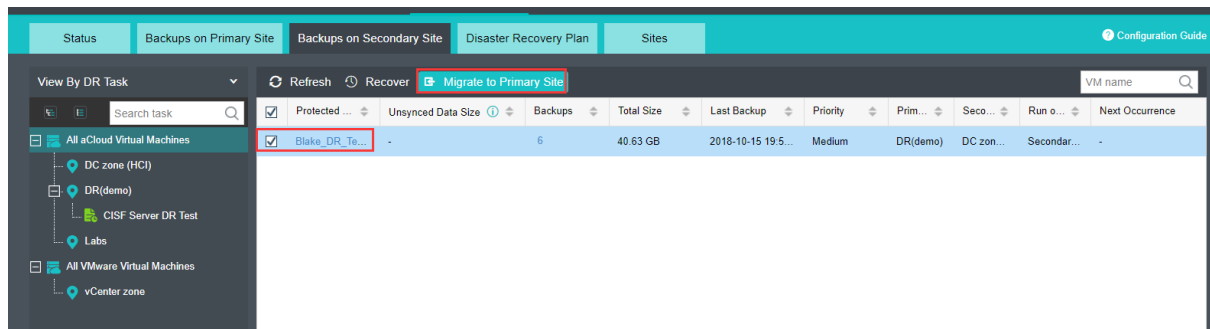
The virtual machine has been recovered to the secondary site and the primary site has returned to normal before the migration.

[Operating Steps]

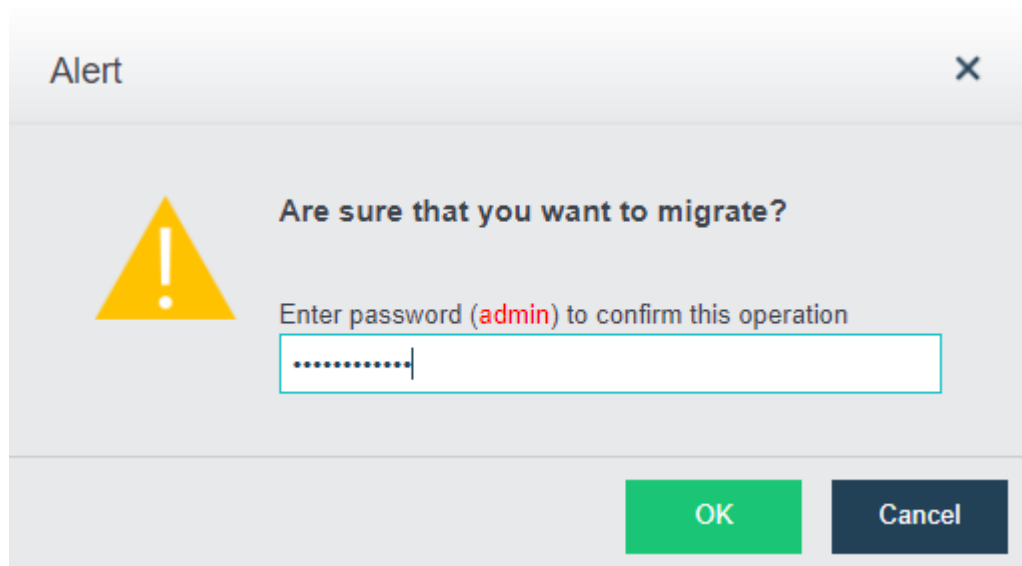
1. Log in to the home page of the aCMP platform and select the 『Operations Center』 → 『Disaster Recovery』 → 『Backups on Secondary Site』 to view the disaster recovery data at the secondary site;



2. Select the virtual machine to be migrated, click **Migrate to Primary Site**, select the destination datastore for the migration, and click **Migrate Now**;



3. Enter the password and click OK;



4. You can see that the virtual machine migration is being executed in Tasks.

Tasks						
All		Disaster Recovery 1				
Status	Action	Object	Start Time	End Time	Admin	Operation
30%	Shut down virtua...	Blake_DR_Test_...	2018-10-16 16:36:11	-	Sangfor Cloud Manag...	View Cancel
✓ Completed	Log in	admin	2018-10-16 16:30:49	2018-10-16 16:30:49	admin (192.168.19.206)	View
✓ Completed	Log out	sangfor	2018-10-16 16:30:39	2018-10-16 16:30:39	sangfor (192.168.19.2...	View
✓ Completed	Log in	sangfor	2018-10-16 16:28:37	2018-10-16 16:28:37	sangfor (192.168.19.2...	View
✓ Completed	Log in	admin	2018-10-16 16:24:19	2018-10-16 16:24:19	admin (192.168.19.206)	View
✓ Completed	Log out	sangfor	2018-10-16 16:24:09	2018-10-16 16:24:09	sangfor (192.168.19.2...	View
✓ Completed	Log in	sangfor	2018-10-16 16:22:53	2018-10-16 16:22:53	sangfor (192.168.19.2...	View
✓ Completed	Log in	admin	2018-10-16 16:16:02	2018-10-16 16:16:02	admin (192.168.19.206)	View

3.3.4 aCMP Reliability

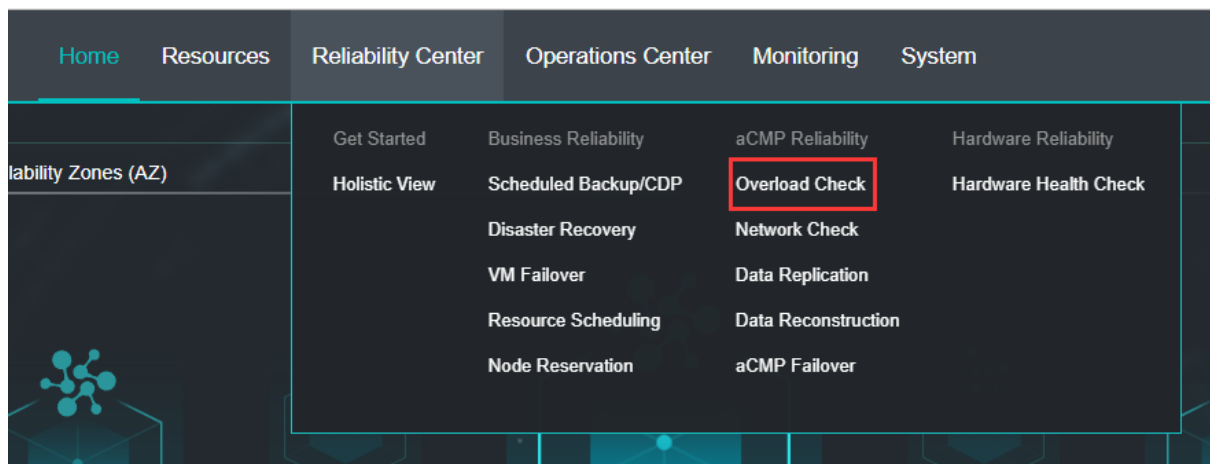
3.3.4.1 Overload Check

[Function Description]

This function checks whether the hardware CPU, memory and storage resource usage and network port traffic status are overloaded.

[Operating Steps]

1. Log in to the home page of the aCMP platform and select 『Reliability Center』 → 『Overload Check』 to view the CPU, memory and storage resource usage as well as network port status;



Reliability Center > Overload Check

Availability Zone

- DC zone (HCI)
- Labs
- DR(demo)

Overload Check

It checks network throughput and whether CPU, memory and storage usage are overloaded. Start Now Latest Check: 2018-10-12 16:50:55


CPU		Memory	Storage	Interface
Node	CPU Usage	CPU Overcommitment		
192.168.1.36	47.6 %	125.00 %		
192.168.1.37	51.3 %	75.00 %		
Cluster	Running vCPU Overcommitment	Virtual CPU Overcommitment (All)		
DC (CTI)	100.00 %	700.00 %		

[Entity Description >>](#)

[Solutions >>](#)


2. You may click **Start Now** to get the latest status, click the Entity Description to view the corresponding detected items and detection thresholds, and click the Solutions to view the corresponding suggested solutions.


Confirm

 **To not affect cluster performance, we recommend cluster health check be performed when the running business system is not busy. Are you sure that you want to perform health check now?**

OK Cancel

[Entity Description >>](#)

CPU Usage:
Check whether host CPU usage is normal.
More than (including) 90%: 

CPU Overcommitment:
Check CPU configuration on each virtual machine.
Above 500%: 

[Solutions >>](#)

CPU Usage:
If the usage is not normal, troubleshoot the issue as follows:
1. Power off unnecessary virtual machines running on that node if CPU usage of a certain node is too high.
2. Add more nodes into the cluster if CPU usage of all nodes are too high.
3. If CPU usage of certain host is too high, migrate some virtual machines to another host with lower CPU usage to relieve workloads of the overloaded host.

CPU Overcommitment:
High CPU overcommitment may make available host CPU resource insufficient, even affect business performance.

3.3.4.2 Network Check

[Function Description]

This function checks and detects the redundancy and connectivity status of the host management interface, data communication interface, and virtual storage interface.

[Operating Steps]

1. Log in to the home page of the aCMP platform and select 『Reliability Center』
→ 『Network Check』 to view the CPU, memory and storage resource usage as well as network port status;

Reliability Center > Network Check

Availability Zone

- DC zone (HCI)
- Labs
- DR(demo)

Network Check

It checks redundancy and connectivity of management interfaces, business interfaces, overlay network interfaces and storage network interfaces of nodes.

Start Now

Latest Check: 2018-10-15 09:59:27

Node	MTU	Netmask	IP Conflict	Port Multiplexing	Prot Redundancy
192.168.1.36 eth2	1500	255.255.255.0	Normal	Error	Not configured
192.168.1.37 eth0	1500	255.255.255.0	Normal	Error	Not configured

Entity Description >>

Solutions >>

3. You may click **Start Now** to get the latest status, click the Entity Description to view the corresponding detected items and detection thresholds, and click the Solutions to view the corresponding suggested solutions.

Entity Description >>

MTU:

Check whether MTU of management interfaces on all nodes are the same.
MTU of management interfaces should be identical: ❌

Netmask Consistency:

Check whether netmask of the management interfaces of all the nodes are the same.
Netmasks are inconsistent: ❌

IP Address Conflict:

Check whether IP address of the Management interface conflicts with any interface or device.
IP address conflict exists: ❌

Reuse of Management Interface:

Check whether management interface uses the same interface with edge or overlay network interface.
Management interface is reused: ❌

Aggregate Interface:

Check whether management interface is an aggregate interface.
It is not an aggregate interface: ⚠️

Solutions >>

MTU:

If MTU of management interfaces are not the same, it may make clustered node unable to communicate with each other and perform operations like backup, etc. Please configure the same MTU for management interfaces of all hosts.

Netmask Consistency:

If netmasks of management interfaces are not the same, it may make clustered nodes unable to communicate with each other and perform operations like backup, etc. Please configure the same netmask for management interfaces of all hosts.

IP Address Conflict:

If management interface address conflicts with any interface or device, it may cause network error. Please configure another IP address for the management interface.

Reuse of Management Interface:

Please set another interface as management interface and make sure that it does not use the same interface with overlay network interface or edge.

Aggregate Interface:

If the interface is not an aggregate interface, single point of failure may occur, which will affect business continuity.

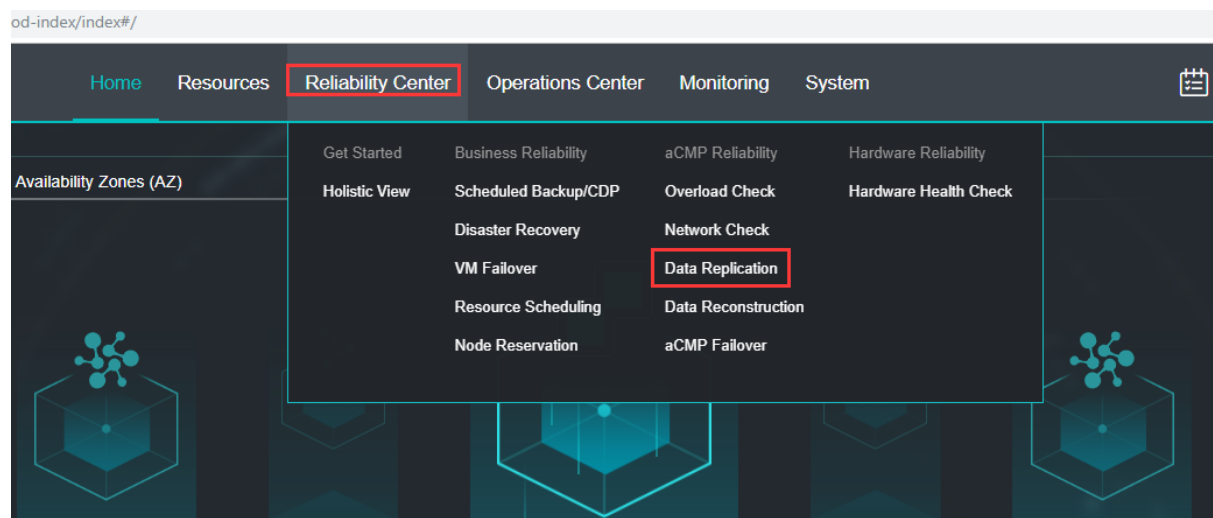
3.3.4.3 Data Replication

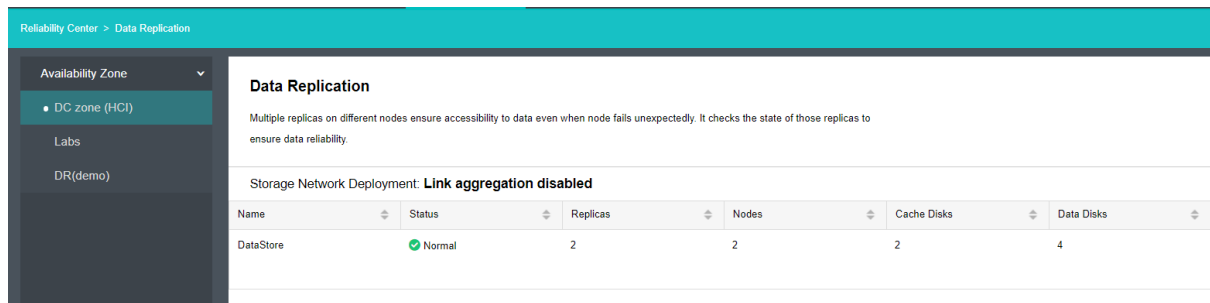
[Function Description]

This function checks and detects the redundancy and connectivity status of the host management interface, data communication interface, and virtual storage interface.

[Operating Steps]

1. Log in to the home page of the aCMP platform and select 『Reliability Center』 → 『Data Replication』 to enter the data-replication-viewing interface, where you can view such statuses as virtual storage replications, virtual storage deployment method, disk and host distribution;





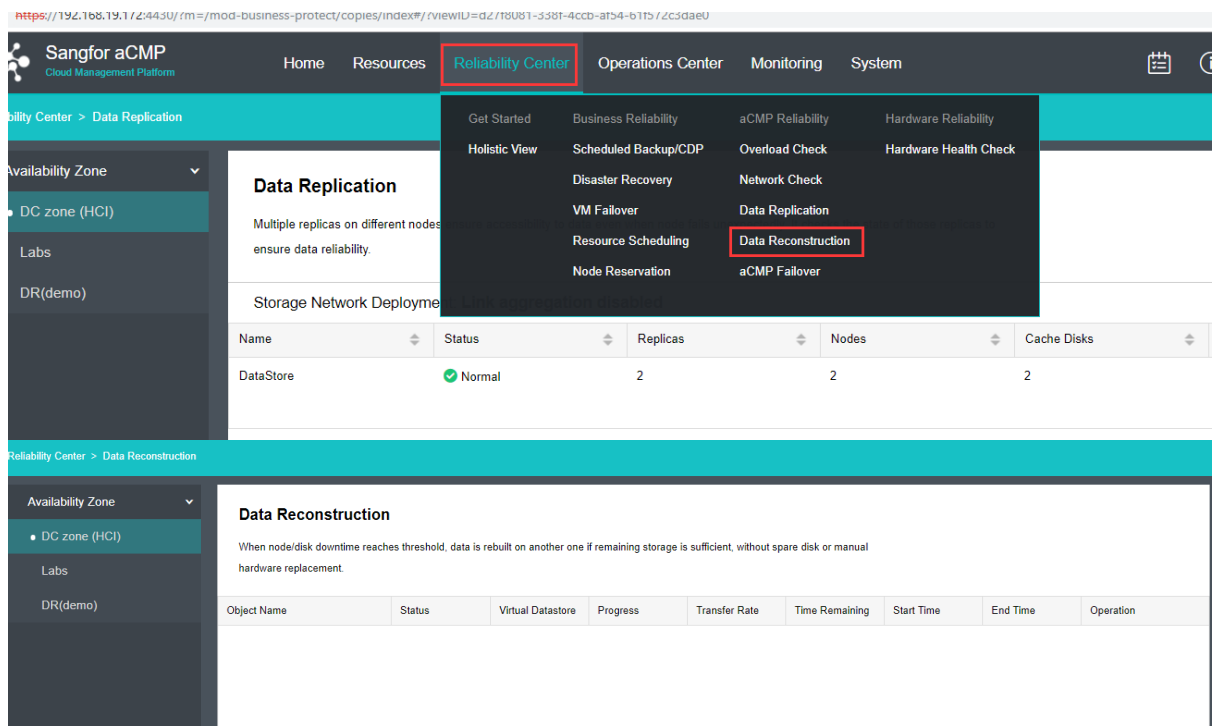
3.3.4.3 Data Reconstruction

[Function description]

When the host or hard disk fails and times out, this function is used to automatically rebuild the replications to other hard disks/hosts in the cluster and recover the validity of data replications without hot spare or manual intervention to replace the disk/host.

[Operating steps]

1. Log in to the home page of the aCMP platform and select 『Reliability Center』 → 『Data Reconstruction』 to enter the view interface of data reconstruction and to view such status;



3.3.5 Hardware Reliability

3.3.5.1 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 so as to identify possible usability problems in advance.

[Operating steps]

1. Log in to the home page of the aCMP platform and select 『Reliability Center』 → 『Hardware Health Check』 to view hardware status in the hardware health check interface;

index/index#/

Home Resources **Reliability Center** Operations Center Monitoring System

Reliability Zones (AZ)

Get Started Business Reliability aCMP Reliability Hardware Reliability

Holistic View Scheduled Backup/CDP Overload Check **Hardware Health Check**

Disaster Recovery Network Check

VM Failover Data Replication

Resource Scheduling Data Reconstruction

Node Reservation aCMP Failover

Reliability Center > Hardware Health Check

Availability Zone

- DC zone (HCI)
- Labs
- DR(demo)

Hardware Health Check

Start Now Latest Check: 2018-10-15 10:24:18

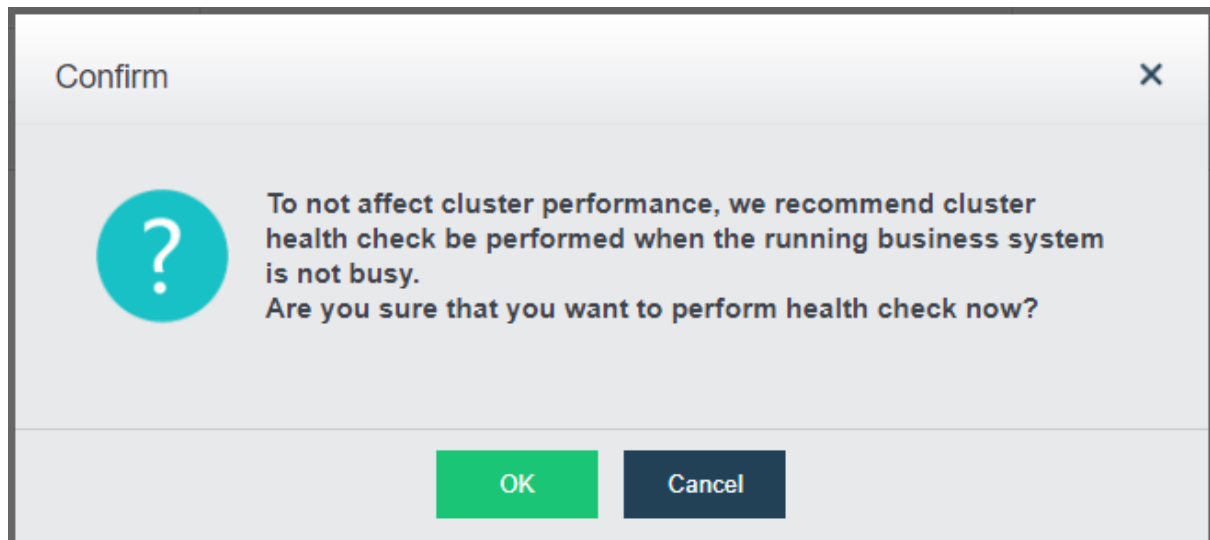
It checks the status of CPU, memory, SSD, HDD, NIC, RAID card and external storage to discover the issues which may affect business availability.

	CPU	Memory	SSD	HDD	NIC	RAID Card	External Storage
Node	CPU Model	CPU Temperature	CPU Clock Speed				
192.168.1.36	Intel(R) Xeon(R) CPU E3-1230 v3 @ 3.30GHz	61.6 °C	3.3 GHz				
192.168.1.37	Intel(R) Xeon(R) CPU E3-1231 v3 @ 3.40GHz	63 °C	3.4 GHz				

Entity Description >>

Solutions >>

2. You may click Start Now to get the latest status, click the Entity Description to view the corresponding detected items and detection thresholds, and click the Solutions to view the corresponding suggested solutions.



Entity Description >>

CPU Model:
Display CPU model.

CPU Temperature:
Check whether temperature of CPU stays above 80°C for 10 minutes.
Over 80°C for 10 minutes: ⚠

CPU Clock Speed:
Check CPU clock speed every one hour, whether clock speed drop occurs. Logs will be reserved for 30 days.
CPU Clock Speed: ⚠

Solutions >>

CPU Temperature:
If the temperature of CPU keeps high for a long time, such problems as node failure, automatic restart, etc, will occur. Troubleshoot the issue as follows:
1. Check whether the cooling fan of the host is working properly.
2. Contact your hardware supplier to replace CPU or the host.

CPU Clock Speed:
Configuration error or hardware failure may cause CPU clock speed change which may have impacts on computing performance. To resolve the issue, you can try the following steps:
1. Check whether physical host is connected with dual power supplies. If not, please connect it with dual power supplies.
2. Enabling power saving mode may changes its clock speed. Please make sure that power saving mode is disabled.

3.3 Operations Center

Sangfor aCMP user management has multi-level management authority control, including platform administrators, organization administrators and organization members by default. Sangfor aCMP can manage specific resources by creating roles according to users' resource management requirements of different scenarios, thus greatly improving the management accuracy.

For example, if a company has an R&D department and a sales department that share a hyper-converged environment, then the platform administrator can create two organization administrators to respectively help manage the two departments. This is not only beneficial to inter-department management, but also greatly reduces the O&M strength for platform administrators.

3.3.1 Users

3.3.1.1 Roles

[Function description]

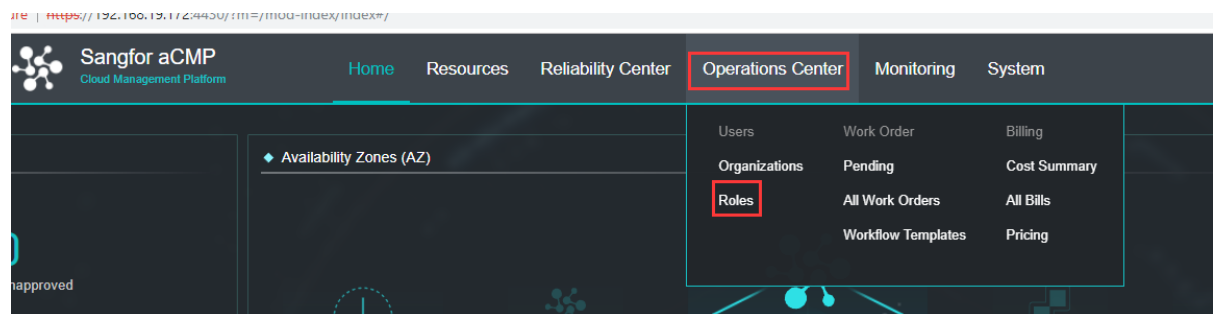
Sangfor aCMP associates administrators with different resources through roles. Serving as hubs for administrators and resources, roles can associate resource dimensions such as virtual machines and networks to administrators, but they cannot achieve fine-grained management of availability zones or specific virtual machines.

[Prerequisites]

Sangfor aCMP management resources are ready and the roles are planned

[Operating Steps]

1. Log in to the home page of the aCMP platform and select 『Operations Center』 → 『Roles』 to enter the role management interface. By default, the system will create three roles, namely, super administrator, organization administrator and organization member, which can be viewed only instead of being edited, and then click **New**;



<input type="checkbox"/>	Role Name	Type	Organization	Description	Operation
<input type="checkbox"/>	Super Admin	Platform Administrator	-	Default administrative role with all permissions on this platform	View
<input type="checkbox"/>	Asset Manager	Organization Administrator	-	Default administrative role with all permissions on self-service portal for organizations, indicating or...	View
<input type="checkbox"/>	User	Member	-	Default user role, indicating user of virtual machine	View

2. Enter the relevant information and click Next;

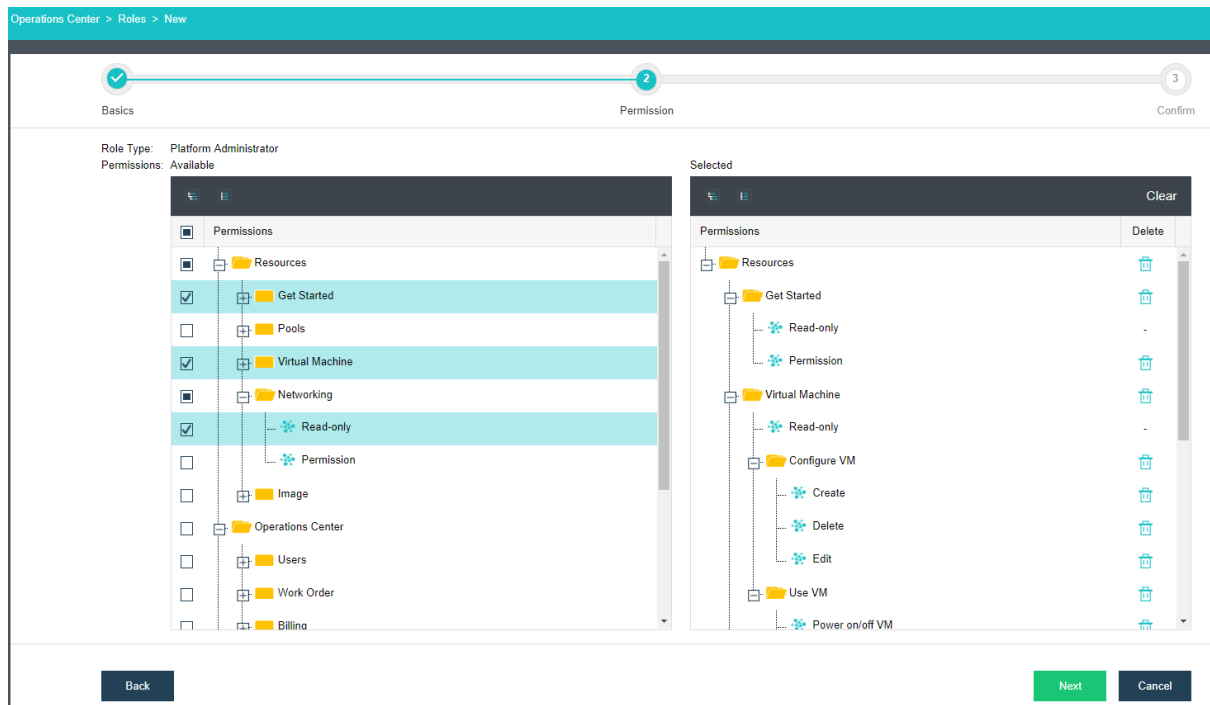
Operations Center > Roles > New

1 Basics 2 Permission 3 Confirm

Name:

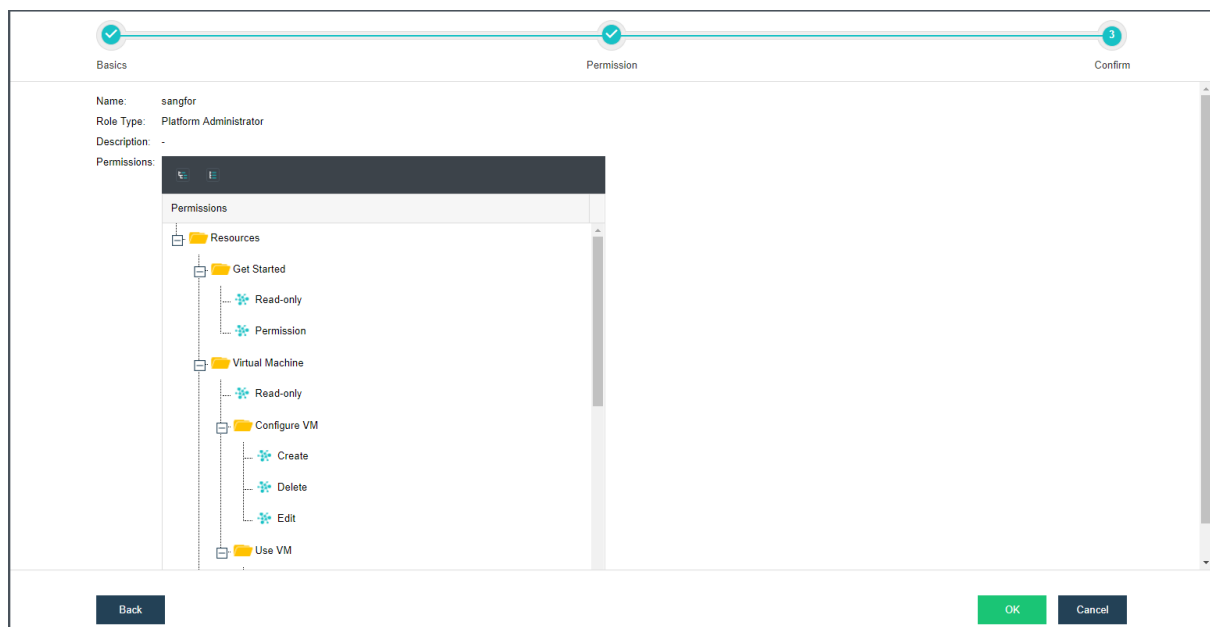
Description:

3. Here you can assign specific resources to the role. It should be noted that the assignation is made by default according to the function module. After selecting the corresponding resources, click Next;



: "Read-only" here means that resources can only be used purely and cannot be modified. For example, if a "virtual machine" is read-only, it means that it can only be used and cannot be deleted after shutdown. "Permission" and other configurations mean that resources can be managed.

4. Finally confirm the information and click the OK;



5. On the "Roles" page, you can view, edit and delete the roles created, and you can also tick multiple roles for batch deletion.

Role Name	Type	Organization	Description	Operation
Super Admin	Platform Administrator	-	Default administrative role with all permissions on this platform	View
Asset Manager	Organization Administrator	-	Default administrative role with all permissions on self-service portal for organizations, indicating or...	View
User	Member	-	Default user role, indicating user of virtual machine	View
sangfor	Platform Administrator	admin	-	View Edit Delete

3.3.1.2 Create Organizations and Organization Administrators

[Function Description]

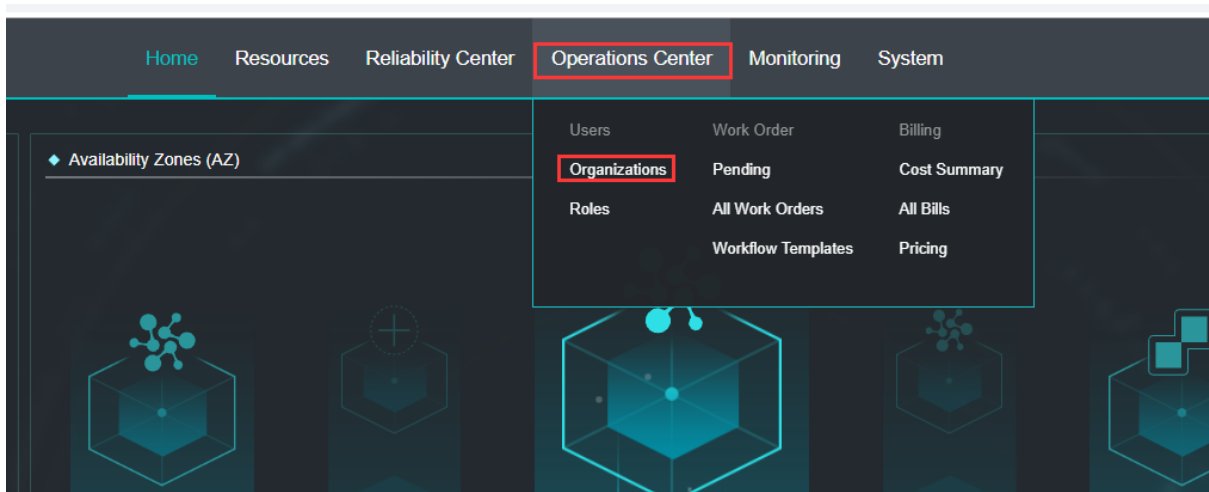
Organization is the unit used by the aCMP to allocate resources. As the secondary administrator of the platform, the organization administrator is responsible for user management tasks in each area and is an essential part of the aCMP platform O&M management. Sangfor can realize fine-grained resource management by associating organization administrators with roles.

[Prerequisites]

Sangfor aCMP management resources are ready and relevant organizational structures are planned.

[Operating Steps]

1. Log in to the home page of the aCMP platform, select 『Operations Center』 → 『Organizations』 , and click New;



Username	Role	Organization	Real Name	Mobile Number	Email	Operation
admin	Super Admin	-	admin	-	-	Edit Change Password
sangfor	Asset Manager	Blake	blake	60123398519	blake.chen@sangfor....	Edit Reset Password Delete

2. Enter the name of an organization. At the same time, you can create the organization administrator or choose not to create it temporarily and add it later. Click Next for the next configuration after this configuration:

Operations Center > Organization Administrator > Ne...

1 Basics — 2 Resources — 3 Confirm

Name:

Description:

Asset Manager Create now Create later

Username:

Real Name:

Mobile Number:

Email:

Password:

Retype Password:

3. Click **Add** to enter the resource configuration interface;

Operations Center > Organization Administrator > Ne...

✓ Basics — 2 Resources — 3 Confirm

Select an availability zone so that resources in that availability zone are accessible to the organization.

4. Select the availability zone that provides resources and click **Next**;

Add New
✕

1 Select Availability Zone
 2 Networking
 3 Allocate Resources
 4 Confirm

	Availability Zone	Resource	CPU Usage	Memory Usage	High Performance ...	Good Performance ...	Large Capacity Usage
<input type="radio"/>	DC zone (HCI)	aCloud	<div style="display: flex; align-items: center;"><div style="width: 54%; height: 10px; background-color: #0070c0;"></div> 54% 28.94 GHz / 53.62 ...</div>	<div style="display: flex; align-items: center;"><div style="width: 86%; height: 10px; background-color: #0070c0;"></div> 86% 55.21 GB / 64 GB</div>	-	<div style="display: flex; align-items: center;"><div style="width: 28%; height: 10px; background-color: #0070c0;"></div> 28% 1015.6 GB / 3.59 TB</div>	-
<input type="radio"/>	vCenter zone	VMware	<div style="display: flex; align-items: center;"><div style="width: 14%; height: 10px; background-color: #0070c0;"></div> 14% 1.64 GHz / 11.39 GHz</div>	<div style="display: flex; align-items: center;"><div style="width: 57%; height: 10px; background-color: #0070c0;"></div> 57% 18.06 GB / 31.78 GB</div>	-	<div style="display: flex; align-items: center;"><div style="width: 82%; height: 10px; background-color: #0070c0;"></div> 82% 1.48 TB / 1.81 TB</div>	-
<input type="radio"/>	Labs	aCloud	<div style="display: flex; align-items: center;"><div style="width: 76%; height: 10px; background-color: #0070c0;"></div> 76% 38.32 GHz / 50.42 ...</div>	<div style="display: flex; align-items: center;"><div style="width: 29%; height: 10px; background-color: #0070c0;"></div> 29% 9.2 GB / 32 GB</div>	-	-	-
<input checked="" type="radio"/>	DR(demo)	aCloud	<div style="display: flex; align-items: center;"><div style="width: 12%; height: 10px; background-color: #0070c0;"></div> 12% 19.02 GHz / 163.27 ...</div>	<div style="display: flex; align-items: center;"><div style="width: 32%; height: 10px; background-color: #0070c0;"></div> 32% 164.11 GB / 512 GB</div>	-	<div style="display: flex; align-items: center;"><div style="width: 6%; height: 10px; background-color: #0070c0;"></div> 6% 679.92 GB / 10.84 TB</div>	-

Next
Cancel

5. Assign network for organization subnet, where you can select "Router", "Physical Egress" and "NFC Network Device" for network devices. After the selection, click Next;


Add New
✕

✓ Select Availability Zone
 2 Networking
 3 Allocate Resources
 4 Confirm

Subnet:

Connected To:

A typical network is often created for small-sized organization. A switch is generated and connected to it by default.



To use more typical networks for the organization, go to Network > Topology.

Back
Next
Cancel

6. Allocate resources and click Next;

Add New
✕

✔ Select Availability Zone — ✔ Networking — 3 Allocate Resources — 4 Confirm

Resources in Current Availability Zone ■ Total ■ Allocated

vCPU : 20 core(s)
72 core(s)

Memory : 100 GB
512 GB

Good Perform... 2 GB
10.84 TB

Resource Allocated to Current Organization

CPU : core(s)

Memory: GB

Good Performa... GB

Back
Next
Cancel



:"Total Authorized Allotments" means the sum of resource quotas allocated to all organizations, which can exceed the total amount of resources.

7. Finally confirm the information and click OK;

Add New
✕

✔ Select Availability Zone — ✔ Networking — ✔ Allocate Resources — 4 Confirm

Availability Zone: DR(demo)

Network Interface: DR test Net

DefaultEdge DefaultGroup

Allocated:

CPU 10 core(s)

Memory 50GB

Storage

High Performance 0GB

Good Performance 500GB

Large Capacity 0GB

Back
OK
Cancel

8. After the addition, you can view the added availability zones and their quotas, where you can also edit and delete the zones, or add other availability zone operations. Please click **Next** after the addition is completed;

Progress: Basics (checked) — Resources (checked) — **3 Confirm**

<input checked="" type="checkbox"/>	Availability Zone	Resource	CPU Quota	MemoryQuota	High PerformanceQu...	Good PerformanceQ...	Large CapacityQuota	Operation
<input checked="" type="checkbox"/>	DR(demo)	aCloud	10 core(s)	50GB	0GB	500GB	0GB	Edit Delete

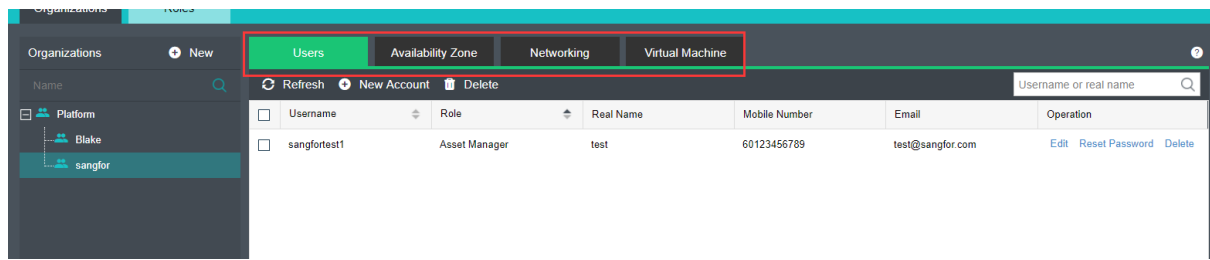
9. Confirm the information and click OK;

Progress: Basics (checked) — Resources (checked) — **3 Confirm**

Name: sangfor
Description: -
Asset Manager: sangfortest1
Availability Zone: DR(demo)

Availability Zone	Resource	CPU Quota	MemoryQuota	High Performan...	Good Performa...	Large Capacity...
DR(demo)	aCloud	10 core(s)	50GB	0GB	500GB	0GB

10. After an organization is created, you can add users and view such information as availability zone, network and virtual machines.



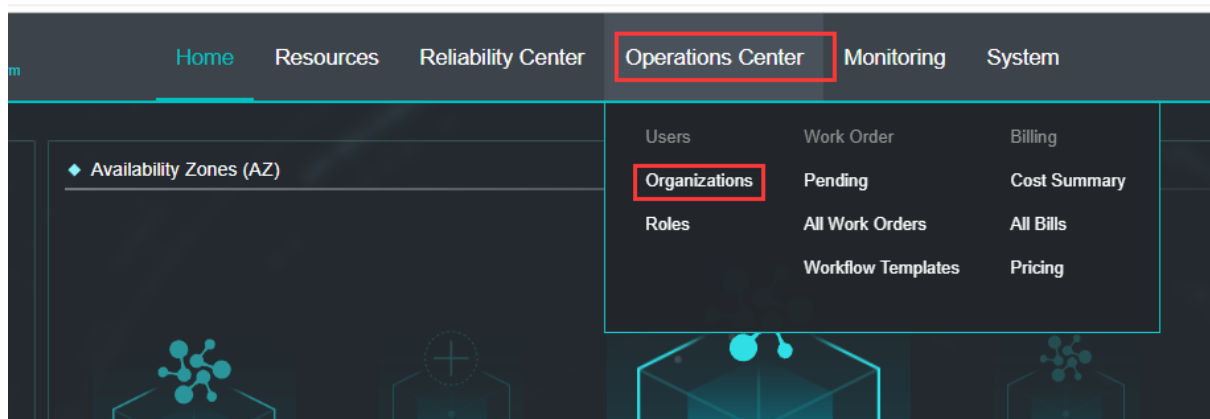
3.3.1.3 Create Users

[Function Description]

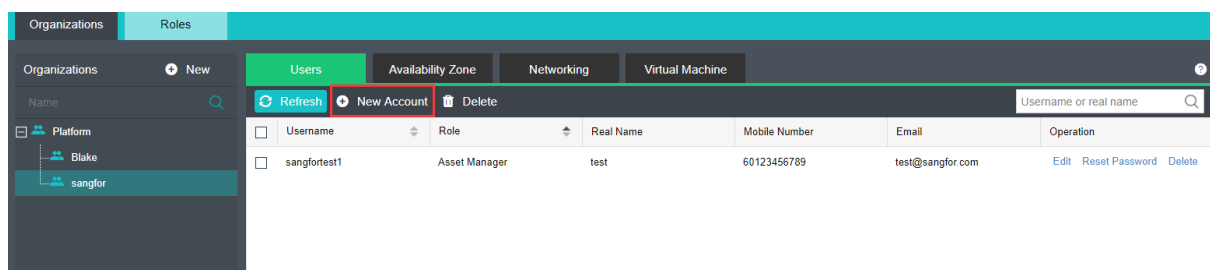
An organization user is a user of the virtual machines in the aCMP, which needs to be created by a super administrator or an organization administrator.

[Operating Steps]

1. Log in to the home page of the aCMP platform and select 『Operations Center』 → 『Organizations』 ;



2. Click the 『Platform』 → 『New Account』 or select the corresponding organization → 『New Account』 to enter the user creation interface;



3. Fill in the user-related information, pay attention to the "Role" and "Organization" as you need to choose according to the actual situation. The "Role" is set according to 3.3.1.1, then click OK.

Operations Center > Organizations > New Account

Username:

Role:

Organization:

Real Name:

Mobile Number:

Email:

Password:

Retype Password:

4. You can see that the user is created and you can edit, modify its password and delete the user.

Organizations Roles

Organizations + New

Platform

Blake

sangfor

Users Availability Zone Networking Virtual Machine

Refresh + New Account Delete Username or real name

Username	Role	Real Name	Mobile Number	Email	Operation
<input type="checkbox"/> sangfortest1	Asset Manager	test	60123456789	test@sangfor.com	Edit Reset Password Delete
<input checked="" type="checkbox"/> test	User	test	60123456789	test1@sangfor.com	Edit Reset Password Delete

3.3.2 Work Order

3.3.2.1 Create Approval Workflow

[Function Description]

The aCMP users need to apply for different system virtual machines and can independently apply for work orders. The administrator can set approval workflows for work orders based on actual conditions and can set approval personnel as needed.

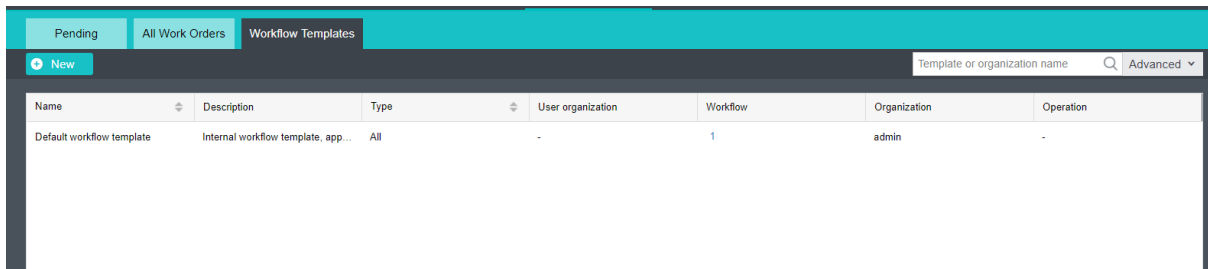
[Prerequisites]

The corresponding approver account is created

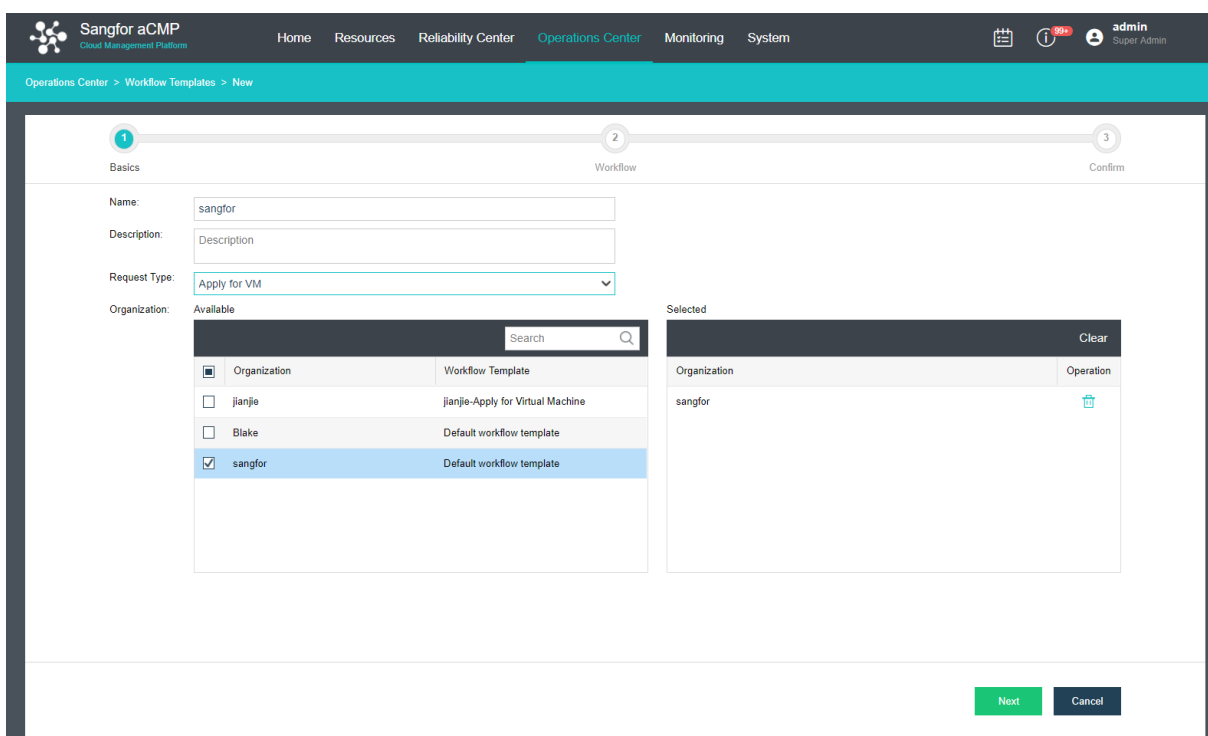
[Operating Steps]

1. Log in to the home page of the aCMP platform and select 『Operations Center』 → 『Workflow Templates』 to enter the interface for workflow approval. The

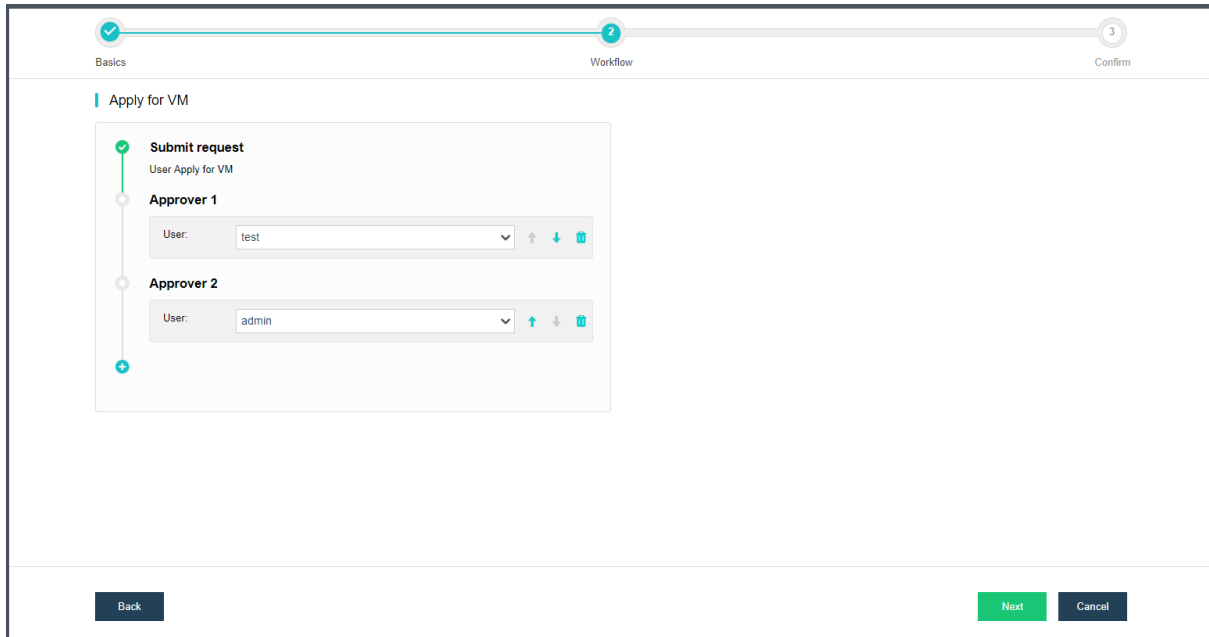
system creates a default workflow by default. Before any changes are made, all work orders are approved by the super administrator by default. Click the **New**;



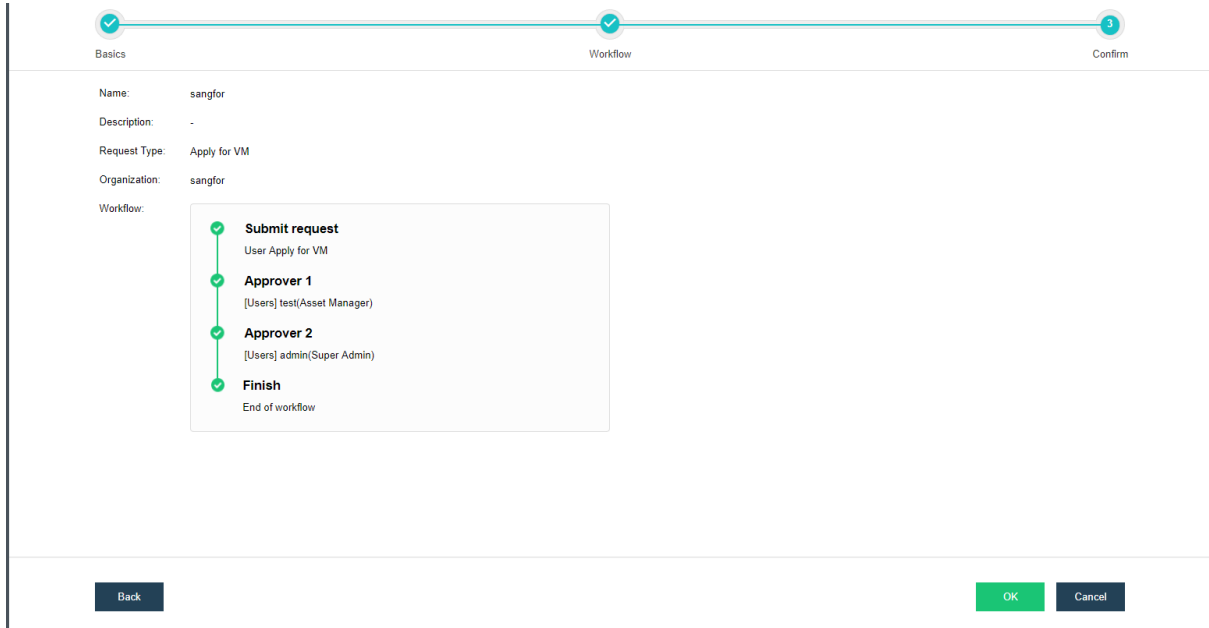
2. Fill in the relevant information, select "Request Type" and "Organization", and click Next;



3. Select the approver. If multi-level approval is needed, please click \oplus and select relevant users. If not, please delete them or adjust the position of each approver by clicking " $\downarrow \uparrow$ ". Click Next after the setting;



4. Click OK after the setting.



5. After this, you can view the workflows created in the approval workflow where you can also edit and delete the existing ones.

Workflow Templates							
Name	Description	Type	User organization	Workflow	Organization	Operation	
Default workflow template	Internal workflow template, app...	All	-	1	admin	-	
sangfor	-	Apply for VM	1	2	admin	Edit Delete	
jianjie-Update Virtual Machine	Customized by organization	Change VM configurations	1	1	jianjie	Edit Delete	
jianjie-Apply for Virtual Machine	Customized by organization	Apply for VM	1	1	jianjie	Edit Delete	

3.3.2.2 Create Work Orders

[Function Description]

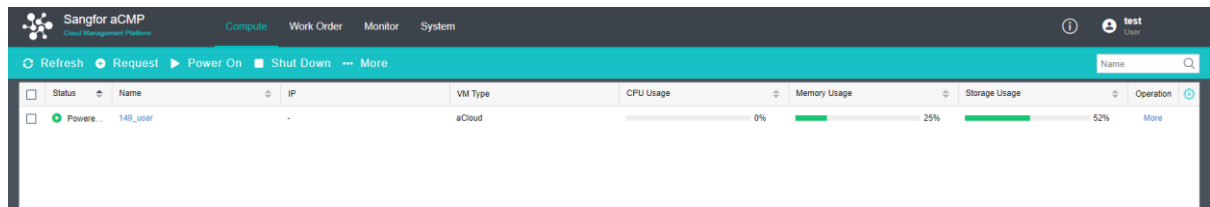
Cloud management users need to apply for different system virtual machines and can apply for work orders independently. After the proposed work orders are approved, the corresponding virtual machines can be automatically generated and distributed to cloud management users.

[Note]

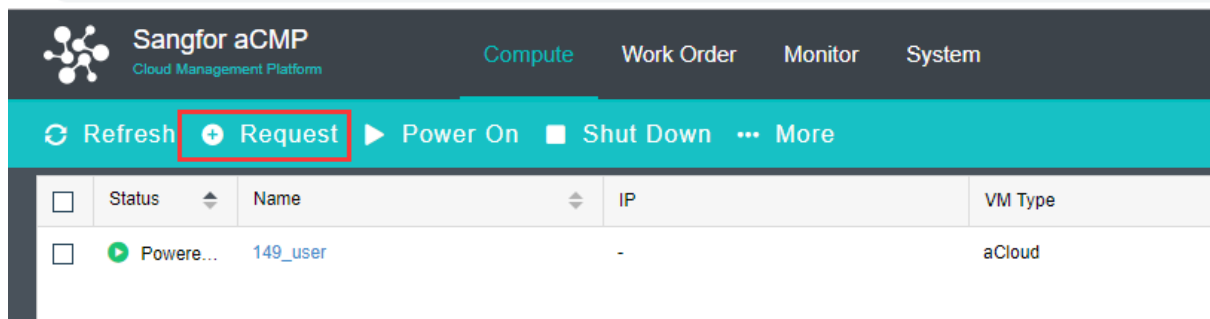
Acmp management users cannot apply for ISO and can only apply for virtual machines

[Operating Steps]

1. When logging in to the aCMP user login interface, cloud management users need to log in to the port without the 4430, and they can view the existing resources of cloud management users after logging in successfully;



2. You can do some basic operations on existing virtual machines. If you need to apply for a new virtual machine, please click ⊕ **Request**, as shown in the figure below:



Availability Zone DR(demo)

Availability zone network should be isolated from each other.

Image 144_user

Networking NIC 1: DR test Net-switch to edge

+ Add NIC (9 NICs can also be added)

Specifications CPU: 2 core(s) Memory: 4 GB

Storage Storage Tag: Good Pe... Disk 1: 40 GB

+ Add Disk (14 more disks can be added)

VMs 1

Basics Name: FTP server Description: Description

Purpose FTP server

Applying Configuration Availability Zone: DR(demo) Image: 144_user CPU: 2 core(s) Memory: 4 GB Disk 1: 40 GB

Apply Now Cancel



: Here "Networking" - "NIC1" refers to the egress switch to which the virtual machine is connected.

3. Select the corresponding image, the number of network cards and disks as well as the number of virtual machines applied, and click **Apply Now**, then you can view the submission status in the "Work Order";

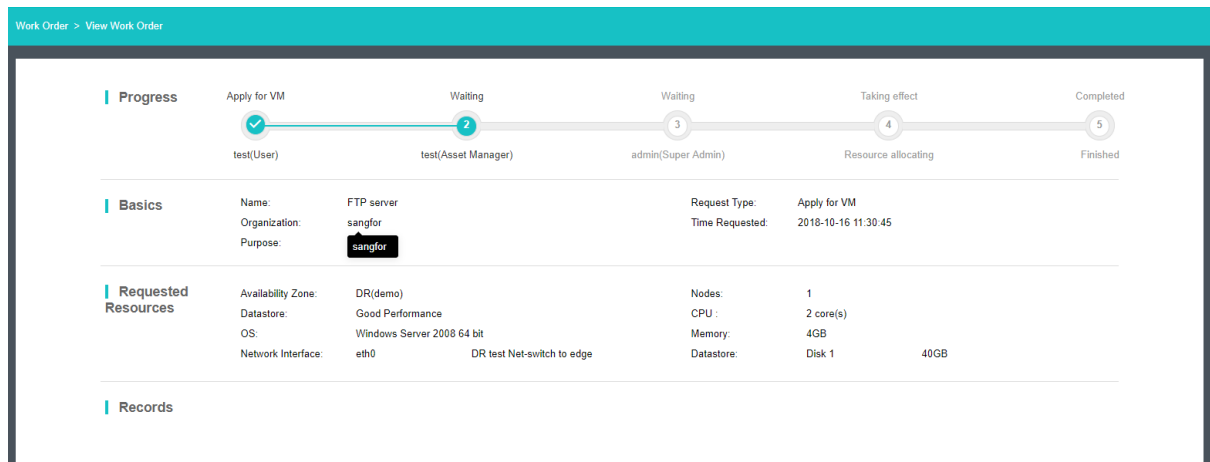
Sangfor aCMP Cloud Management Platform

Compute **Work Order** Monitor System

Refresh Work order number

Order Number	Status	Current Processor	Request Type	Time Requested	Operation
20181016000003	Waiting	test(Asset Manager)	Apply for VM	2018-10-16 11:30:45	View

Click View to view specific information of work orders, as shown below:



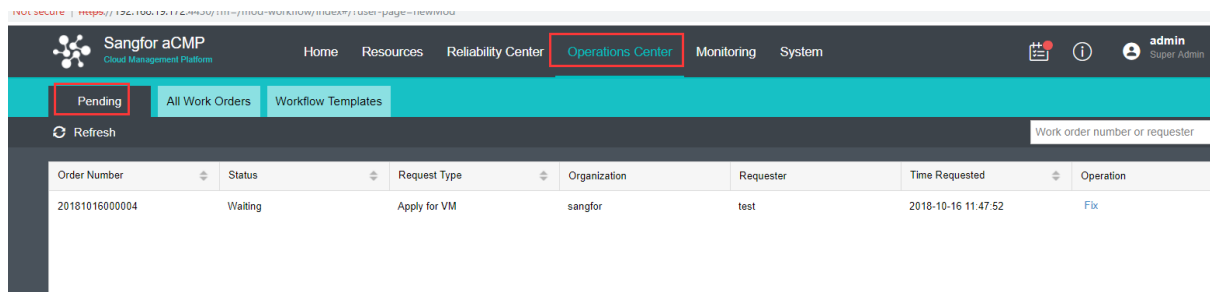
3.3.2.3 Approve/Review Work Orders

[Function Description]

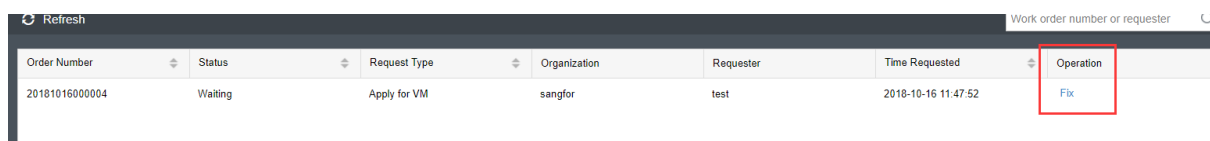
If added to the approval workflow as approvers, the organization administrator and super administrator can, via reviewing and approving the applications, approve and reject work orders and modify the virtual machine configurations requested by the applicant.

[Operating Steps]

1. After logging in to the aCMP administrator interface, the organization administrator/super administrator can click the 『Operations Center』 → 『Pending』 to view all pending work orders;



2. Click Fix and fill in the approval comment in the pop-up approval interface. You can also manually add disks. Click **All** if you need to re-modify the configuration. Click **Add Disk** to generate extra disks for the virtual machine. Click X on the right of the new disk if you need to delete the new disk. Approval comment must be filled in. Click **Approve**.



Basics	Name: FTP Server Organization: sangfor Purpose: FTP server	Request Type: Apply for VM Time Requested: 2018-10-16 11:47:52
Requested Resources	Availability Zone: DR(demo) Datastore: Good Performance OS: Windows Server 2008 64 bit Network Interface: eth0 DR test Net-switch to edge	Nodes: 1 CPU: 2 core(s) Memory: 4GB Datastore: Disk 1 40GB
Progress	<p>Apply for VM (test\User) [Completed]</p> <p>Waiting (admin(Super Admin)) [Active]</p> <p>Taking effect (Resource allocating) [Pending]</p> <p>Completed (Finished) [Completed]</p>	
Records		

Resource Scaling	<input type="button" value="Add Disk"/>	<input checked="" type="button" value="All"/>	Comment
Item	Allocate		
Nodes:	<input type="text" value="1"/>		<input type="text" value="OK"/>
CPU:	<input type="text" value="2"/>	core(s)	
Memory:	<input type="text" value="4"/>	GB	
			<input type="button" value="Reject"/> <input type="button" value="Approve"/> <input type="button" value="Cancel"/>

Click All for configuration:

Edit
✕

Basics
Resources
Configuration
Advanced

CPU: core(s)

[Show More](#)

Memory:

GB

[Show More](#)

Datastore:

Disk Capacity: GB

Pre-allocation ⓘ

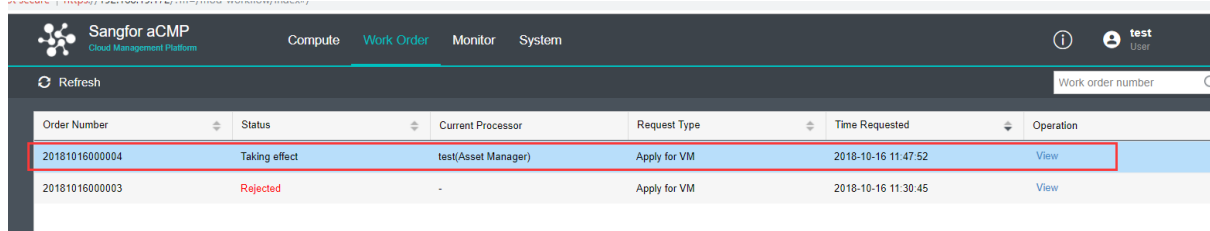
(14 more disks can be added)

If the approval workflow includes multiple levels of administrators, each level of administrator needs to join the approval;

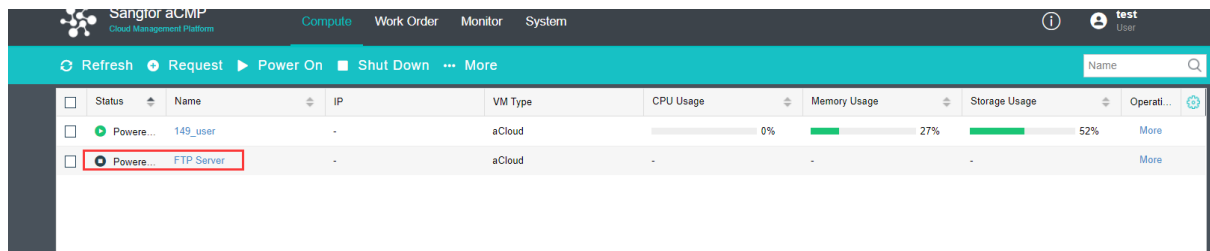


: Configurable items may be different for different administrators in configuring advanced options.

- After the approval is successful, you can log in to the cloud management terminal user to view the distributed virtual machine;



Order Number	Status	Current Processor	Request Type	Time Requested	Operation
20181016000004	Taking effect	test/Asset Manager)	Apply for VM	2018-10-16 11:47:52	View
20181016000003	Rejected	-	Apply for VM	2018-10-16 11:30:45	View



Status	Name	IP	VM Type	CPU Usage	Memory Usage	Storage Usage	Operati...
Power...	149_user	-	aCloud	0%	27%	52%	More
Power...	FTP Server	-	aCloud	-	-	-	More



:As it takes a certain period of time to distribute the resources after the approval, the user needs to wait for some time before seeing the distributed virtual machine in the cloud management terminal.

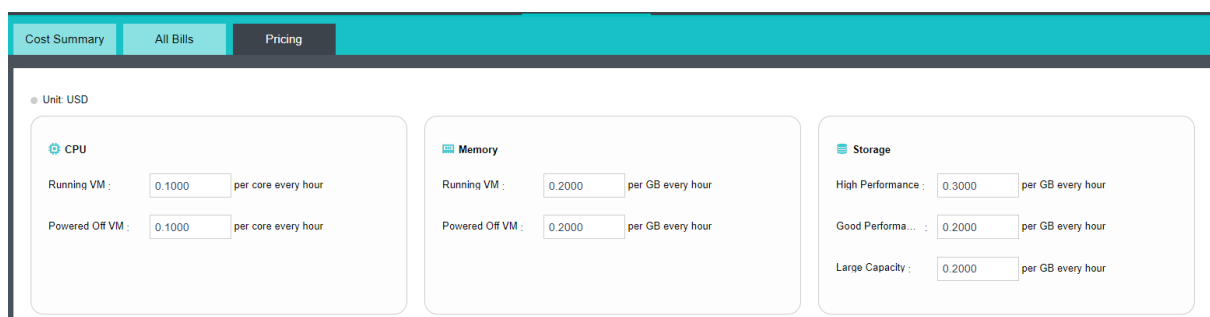
3.3.3 Billing

[Function Description]

Administrators can independently control and set the unit prices of platform resources. The aCMP counts the tenant resource usage every 10 minutes, calculates the billing based on usage and price, and updates the resource usage billing every 1 hour on the interface. The IT department's services are quantified through statistics on resource usage.

[Operating Steps]

- Log in to the home page of the aCMP platform and select 『Operations Center』 → 『Billing』 to enter the Pricing interface;



Unit: USD

Resource	Unit Price	Unit
CPU	Running VM : 0.1000	per core every hour
	Powered Off VM : 0.1000	per core every hour
Memory	Running VM : 0.2000	per GB every hour
	Powered Off VM : 0.2000	per GB every hour
Storage	High Performance : 0.3000	per GB every hour
	Good Performance : 0.2000	per GB every hour
	Large Capacity : 0.2000	per GB every hour

- Fill in the unit price and amount you need to set, and click **Save**.

Cost Summary All Bills Pricing

Unit: USD

CPU

Running VM : per core every hour

Powered Off VM : per core every hour

Memory

Running VM : per GB every hour

Powered Off VM : per GB every hour

Storage

High Performance : per GB every hour

Good Performa... : per GB every hour

Large Capacity : per GB every hour

3. Select 『Operations Center』 → 『Cost Summary』 to set the time period for statistics. You can view the cost summary of different organizations in the selected period;

Cost Summary All Bills Pricing

Period: 2018-10-15 - 2018-10-17 Unit: USD Export Report

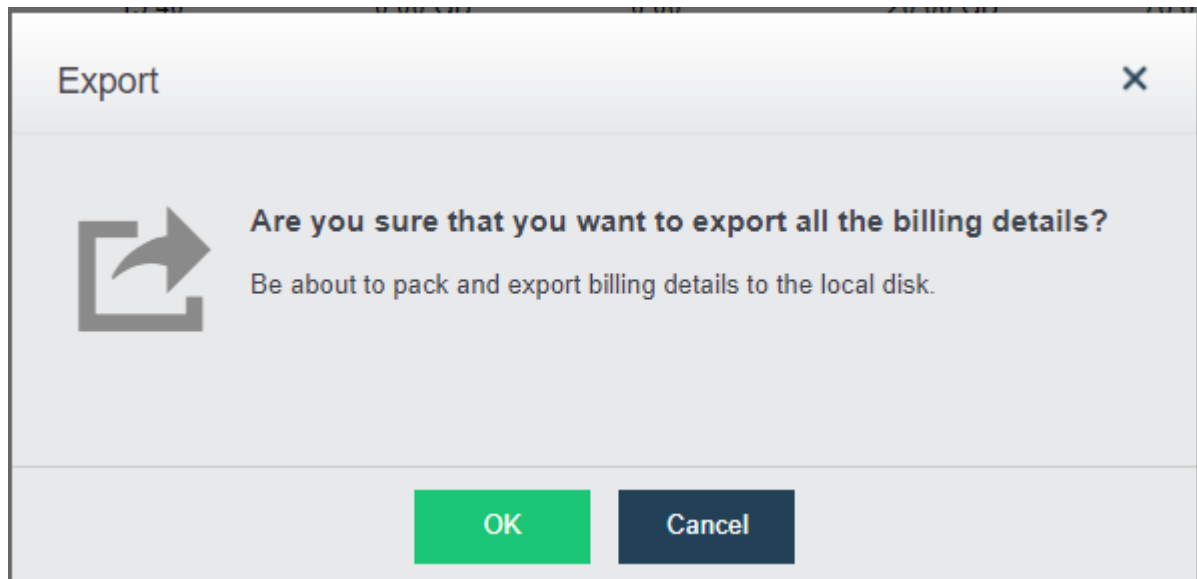
Organization	Virtual CPU	Virtual Memory	Storage	Total
jianje	15.33	30.80	153.33	199.47
sangfor	0.33	30.80	13.33	14.53

4. Select 『Operations Center』 → 『All Bills』 to set the query time period. You can view all bills of different organizations in the current period, and report export (as excel files) is supported.

Cost Summary All Bills Pricing

Period: 2018-10-02 - 2018-10-16 Organization: jianje Total Costs: 199.47 USD Unit: USD Export Report

VM Name	CPU	CPU Costs	Memory	Mem Costs	High Perfor...	High Perfor...	Good Perfor...	Good Perfor...	Large Capa...	Large Capa...	Total
ALL	10.00 core(s)	15.33	12.00 GB	30.80	0.00 GB	0.00	60.00 GB	153.33	0.00 GB	0.00	199.47
Debian Template	4.00 core(s)	7.67	4.00 GB	15.40	0.00 GB	0.00	20.00 GB	76.67	0.00 GB	0.00	99.73
webservers	4.00 core(s)	7.67	4.00 GB	15.40	0.00 GB	0.00	20.00 GB	76.67	0.00 GB	0.00	99.73
test	2.00 core(s)	0.00	4.00 GB	0.00	0.00 GB	0.00	20.00 GB	0.00	0.00 GB	0.00	0.00



3.4 Monitoring Center

By integrating the Sangfor Monitoring aMC, Sangfor aCMP cloud management platform can add important virtual machines to the monitoring center for monitoring, so that administrators can discover the possible abnormalities and failures of the platform or virtual machines in the first time.

Note: The monitoring center template was not implemented in aCMP 5.8.6 _ EN version, so the module manual contents are temporarily vacant and aMC functions will be implemented in subsequent versions. Please ignore the aMC function in current version.

3.5 Network Administration

It can perform unified network management on the managed clusters. Based on different availability zones and organizations, the super administrator can view the corresponding network topology, and the organization administrator can also view the network structure of relevant organizations. Meanwhile, tenants are supported to configure their own distributed firewall policies. The firewall policy of each tenant only takes effect in the tenant's domain and does not conflict with the super administrator's configuration policy.

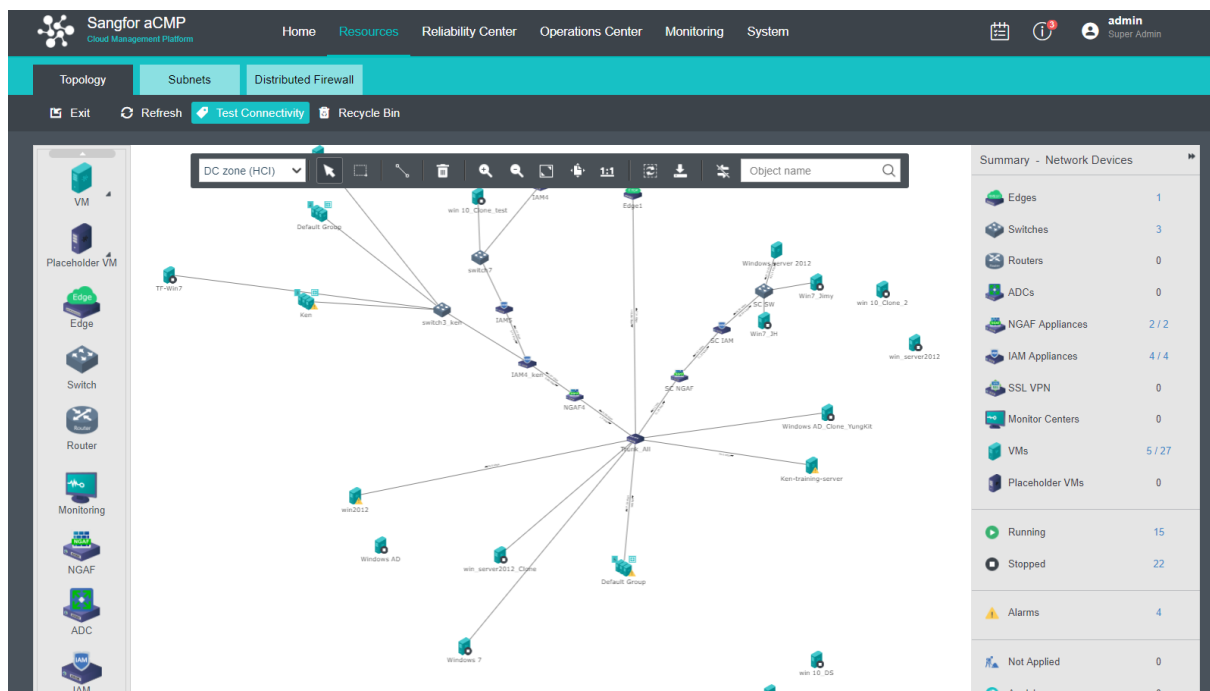
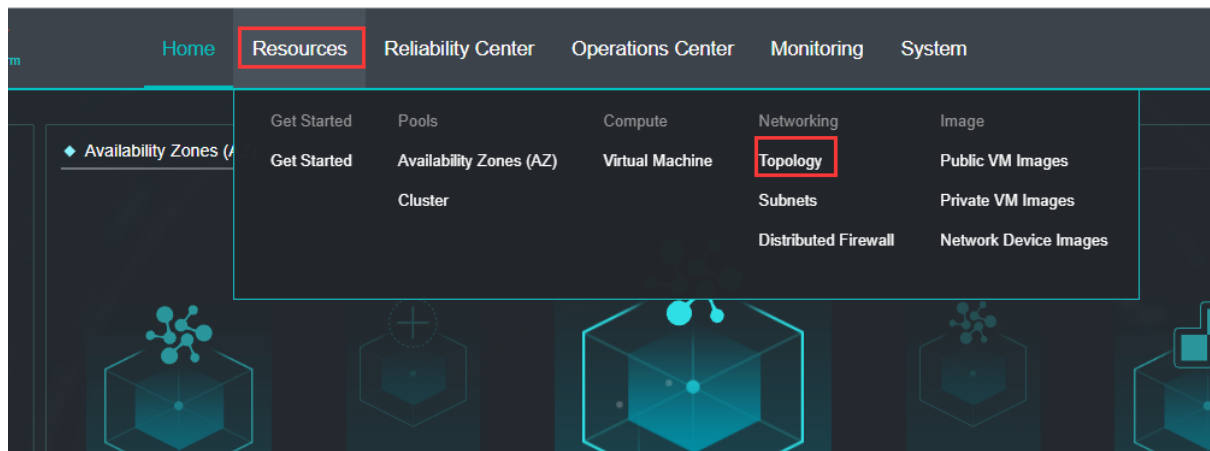
3.5.1 Network Topology

[Function Description]

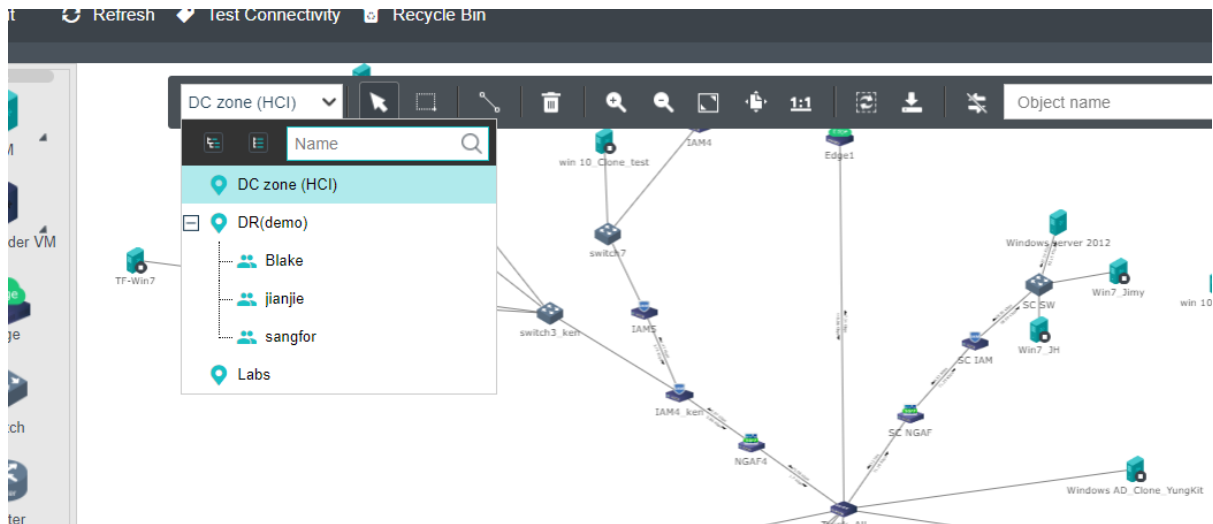
The super administrator can view the network status of the aCMP platform, and can view and adjust the corresponding network structure in the availability zone or organization as a dimension.

[Operating Steps]

1. Log in to the aCMP administrator interface, and click 『Resources』 → 『Topology』 to enter the topology interface;



2. Select the corresponding availability zones or organizations. You can view the corresponding network topology;



3. Click 『Subnets』 to enter the list showing all subnets, and click **New** to distribute new network for the organization.

Name	Availability Zone	Organization	Connected To	Operation
DR test Net	DR(demo)	sangfor	DefaultEdge	Edit Delete

Create Subnet

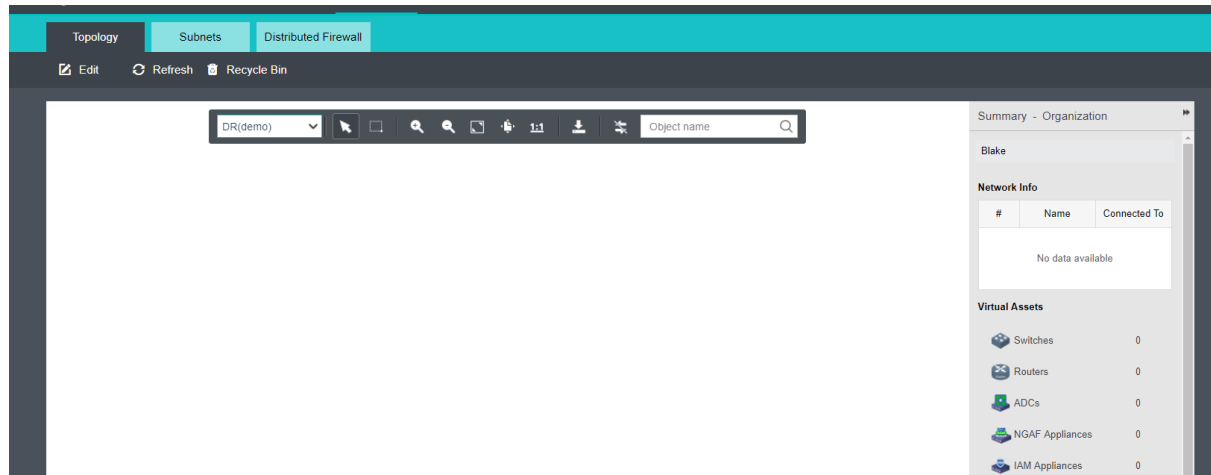
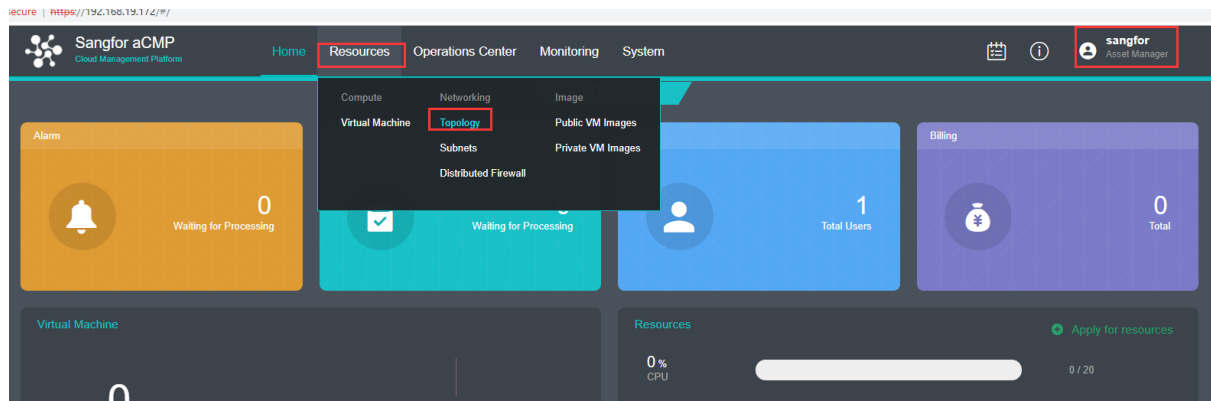
Availability Zone:

Organization:

Subnet:

Connected To:

4. The organization administrator can view the network that it manages, and can do some network operations, such as adding switches and routers. The organization administrator can also login with the its account password and click 『Resources』 → 『Topology』 to view the corresponding information;



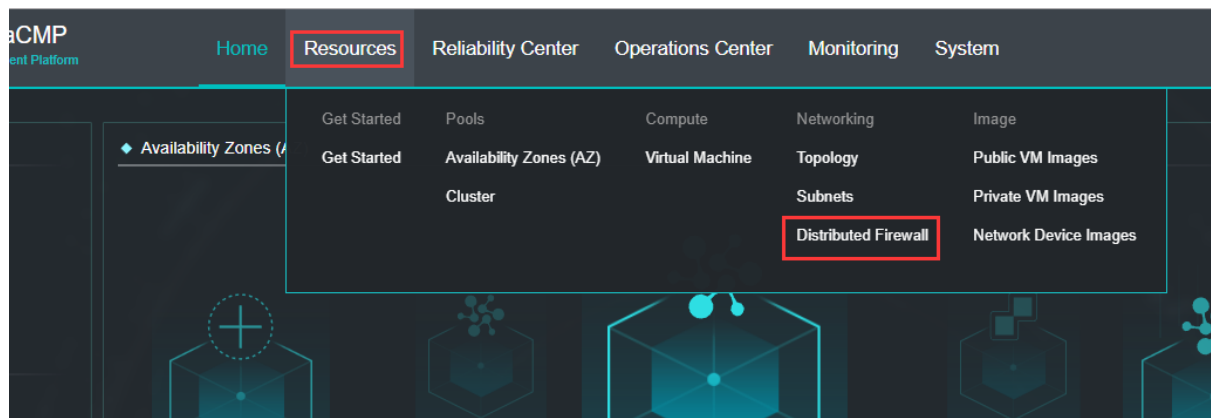
3.5.2 Distributed Firewalls

[Function Description]

The organization administrator can set firewall rules for the networks in the effective domain, and the super administrator can set firewall rules for the entire platform network, which do not conflict with each other.

[Operating Steps]

1. Log in to the aCMP administrator interface, and click 『Resources』 → 『Distributed Firewalls』 to enter the firewall edit page and to view the existing firewall rules;



Priority	Name	Applicable Scope	Source	Destination	Service	Action	Status	Edit
1	Allow all operations by a...	Public Zones	192.168.19.172	All	[all] All(All protocols & ports)	Allow	✓	
-	Default Policy	Public Zones	All	All	[all] All(All protocols & ports)	Allow	✓	-

2. Click ⊕ **New**, select availability zone and applicable scope, set match clauses, select the services and policy actions to be valid, and click OK after all is confirmed;

Add New Rule ✕

Enabled

Name:

Availability Zone: DC zone (HCI) ▼

Applicable Scope: Public Zones ▼

- Match Clause

Source

Any IP address

Specified IP address

IP Group ▼ Select ⋮

Specify VM

Virtual MacI ▼ Select ⋮

➔

Destination

Any IP address

Specified IP address

IP Group ▼ Select ⋮

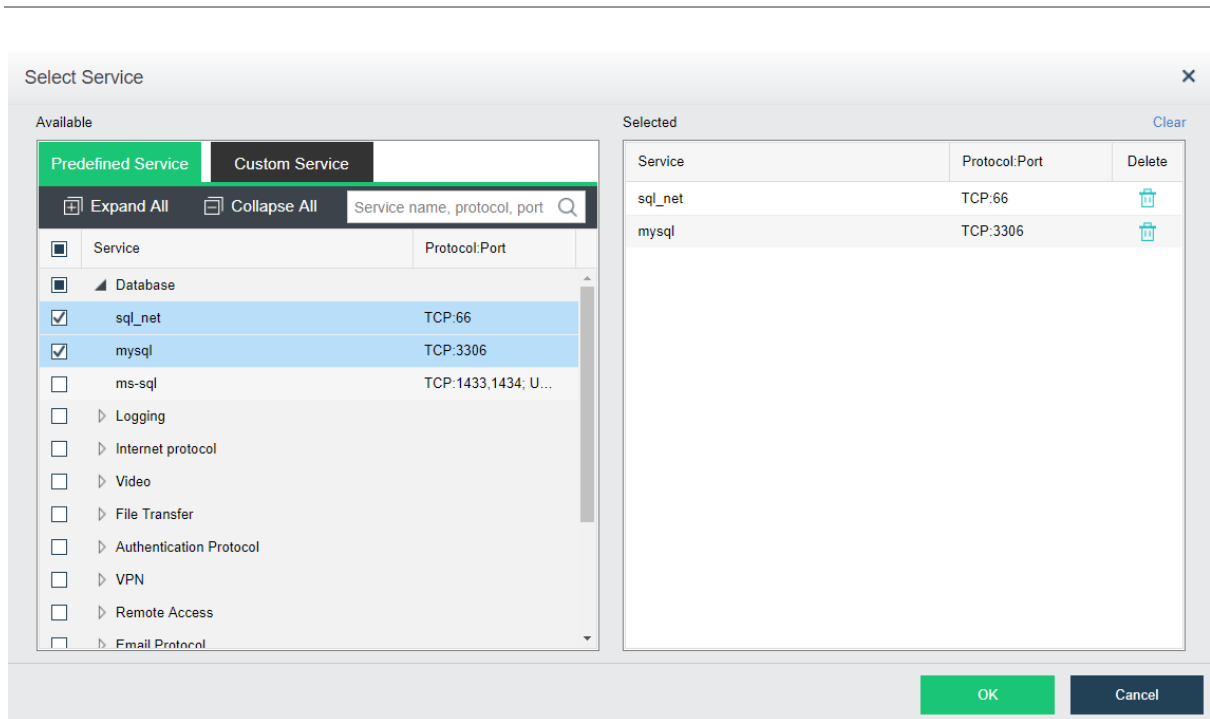
Specify VM

Virtual MacI ▼ Select ⋮

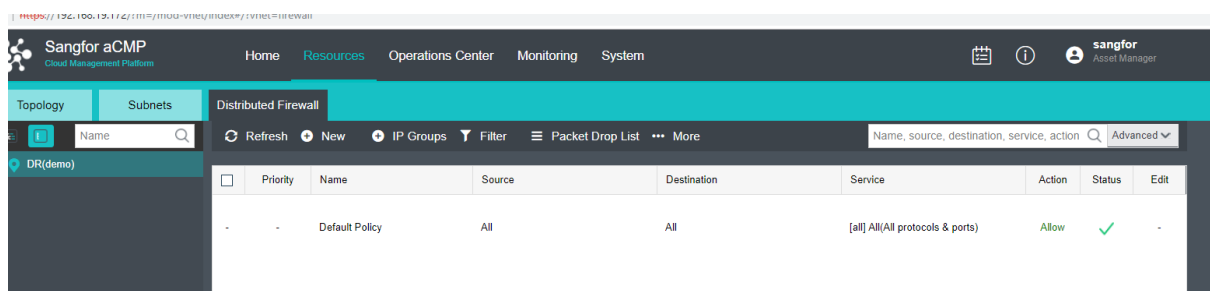
Service: Select ⋮

Action: Allow Reject

OK
Cancel



3. Similarly, you can set the firewall policies in the organization subnet by logging in with the organization administrator's account.



Chapter4 FAQ

1. Cluster is managed by multiple aCMPs simultaneously: When a cluster is managed by multiple aCMPs simultaneously, only one aCMP can be authorized successfully.

Solution: Cancel the management from the excess aCMP, and it will return to normal after a few minutes, or turn off the excess aCMPs, and it will return to normal in 30 minutes.

2. IP address conflict in cluster: Because authorization information may be rejected on the wrong cluster, this problem may occur when multiple aCloud clusters are configured with the same IP address.

Solution: It will recover immediately after IP address conflicts are resolved.

-
3. aCloud is forcibly removed from the management: Log in to the aCloud front-end, click "Manage" and view the "License" icon status. If aCloud has been removed from the management, and aCMP shows that it is in the state of the management, then this is the cause.

Solution: Delete the cluster on aCMP and re-manage it.



Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

The information in this document is subject to change without notice.

To obtain the latest version, contact the international service center of SANGFOR Technologies Inc

