



SANGFOR

aCloud

aCMP Deployment Guide

Version 5.8.6



Change Log

Date	Change Description
Otc 15, 2018	Edition of aCMP deployment guide

CONTENT

Chapter 1 Introduction of aCMP	4
Chapter 2 Testing Resource	4
2.1 Deployment Requirement.....	4
Chapter 3 aCMP deployment guide.....	5
3.1 aCloud5.8.6 import aCMP image	5
3.2 Congiure aCMP network IP.....	8
3.3 aCMP Authorization	13
3.4 aCloud cluster joins aCMP centralized management	16
3.5 Authorize aCloud clusters through aCMP	19
3.6 NFV Authorization.....	20
3.7 Availibility Zone	22
Chapter 4 aCMP Active and Standby Deployment	24

Chapter 1 Introduction of aCMP

Sangfor enterprise cloud management platform- aCMP, use Sangfor's virtualized resource pool that build through hyper-converged architecture with third party virtualization platform through a streamlined or automated approach to deliver resources as service to business unit or business user, in order to achieve automation and maintenance in the platform.

Sangfor enterprise cloud management platform can achieve to manage third party virtualization platform like VMware, etc. The management platform adopts distributed architecture design which consists of enterprise level cloud architecture cluster. Each node can provide corresponding management services, and any node failure will not cause interruption in the platform. Besides that, aCMP can provide hierarchical and decentralized management for different platform users. Each platform can use manage corresponding resources allocated by the aCMP. For each resources allocated can be deployed with more granular control and management. This greatly meet the enterprise-level cloud platform and build the flexibility of multitenant use of IT resources in the cloud IT architecture.

Chapter 2 Testing Resource

Testing Material Name	Instruction
aCMP installation image	aCMP5.8.6 by importing ova image file to deploy in aCloud. Ova image file download link: http://community.sangfor.com/plugin.php?id=service:download&action=view&fid=47#/12/all
aServer Authorization Key	aCMP authorization needs to be authorized by the aServer authorization KEY
Authorization File	Apply for the corresponding authorization file through authorized KEY ID.

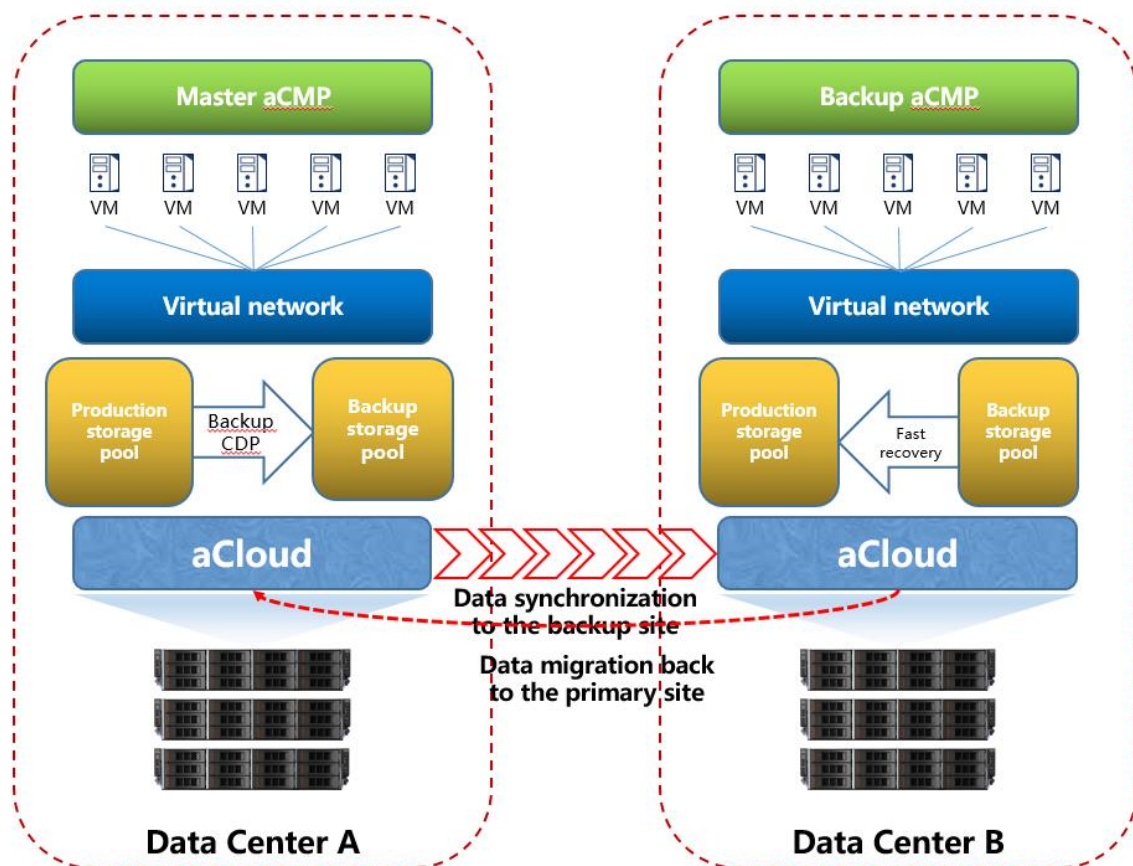
2.1 Deployment Requirement

aCMP5.8.6 only can deploy in aCloud5.8.6, it does not support deploy in third party platform (VMware)

Based on figure below, if aCMP requires simultaneous management of multiple cross-

regional aCloud clusters:

- Both cluster bandwidth must at least has 10Mb/s;
- If customer require remote open virtual machine, each virtual machine needs 2Mb/s;



Chapter 3 aCMP deployment guide

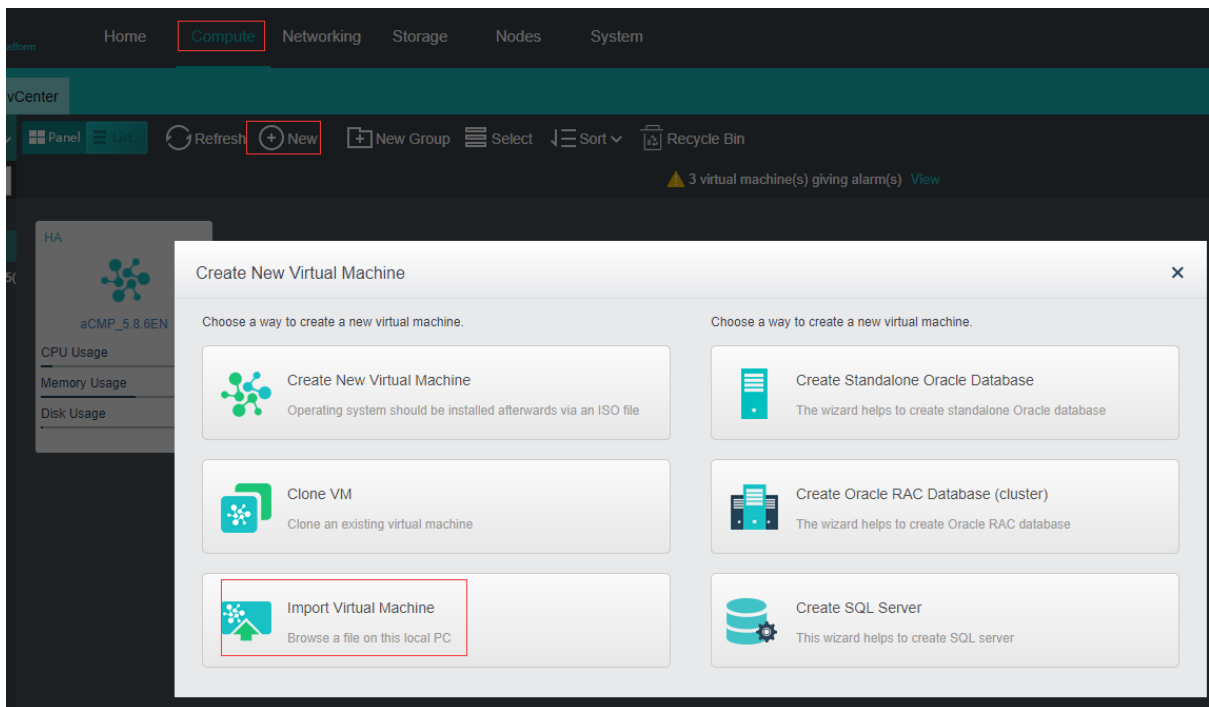
3.1 aCloud5.8.6 import aCMP image

【Steps】

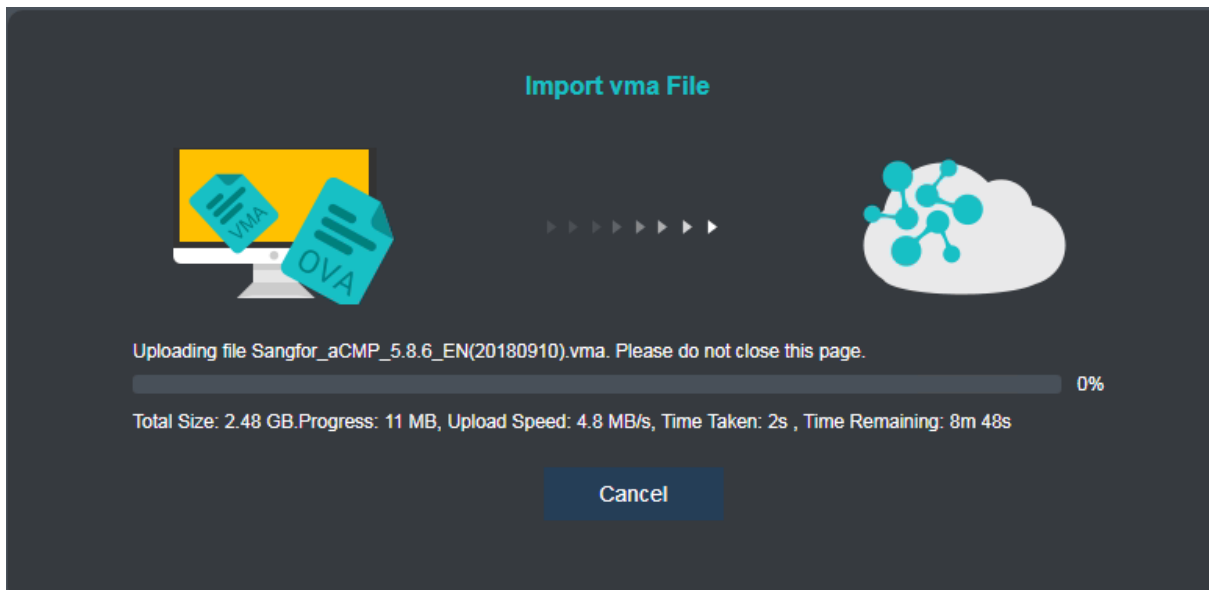
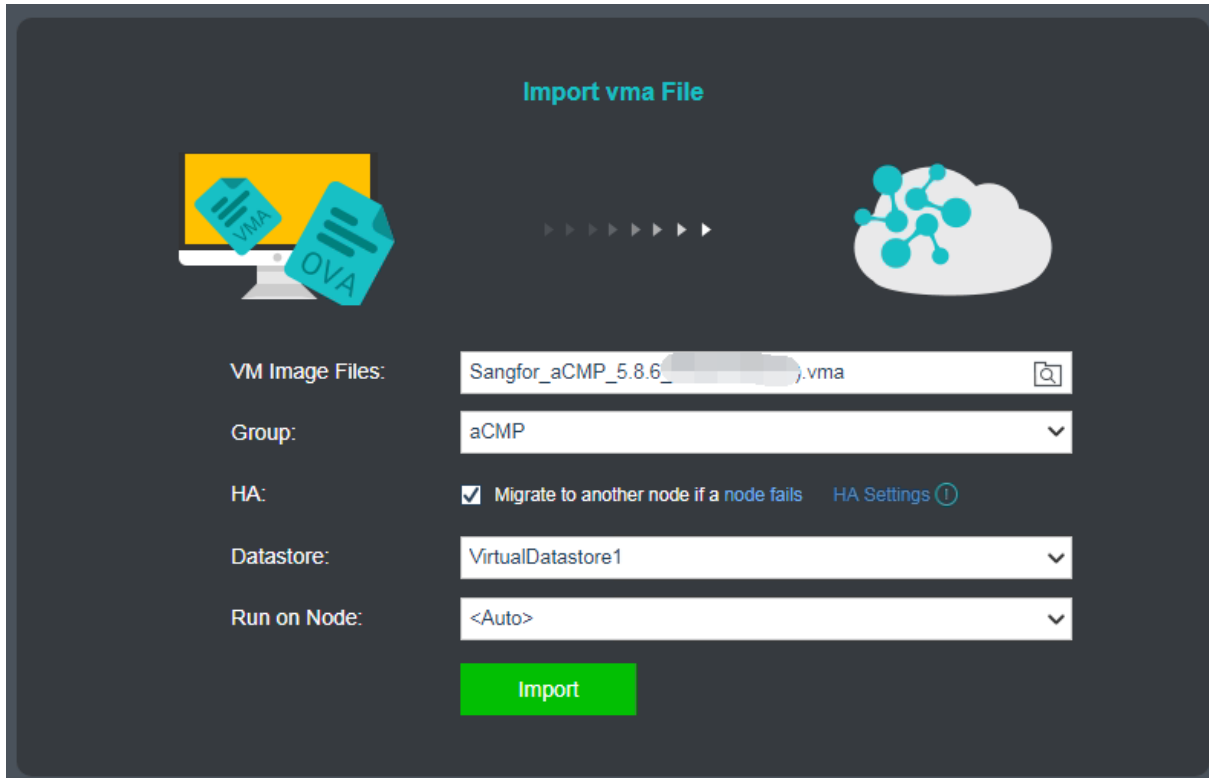
Open aCloud5.8.6 login page:



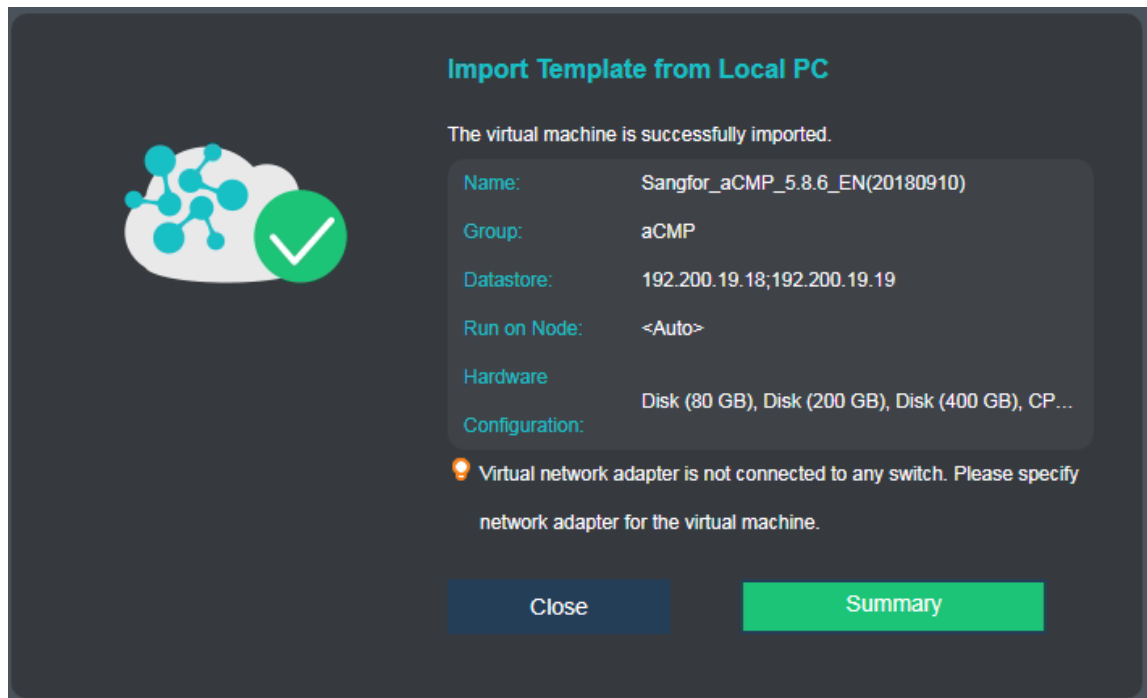
1. Click 『Compute』 → 『New』 → 『import Virtual Machine』



2. Select aCMP virtual machin,select corresponding group, storage location and running location, click **Import** button, then it will show upload interface;



3. After success upload the image file, require to open the aCMP virtual machine to configure network.

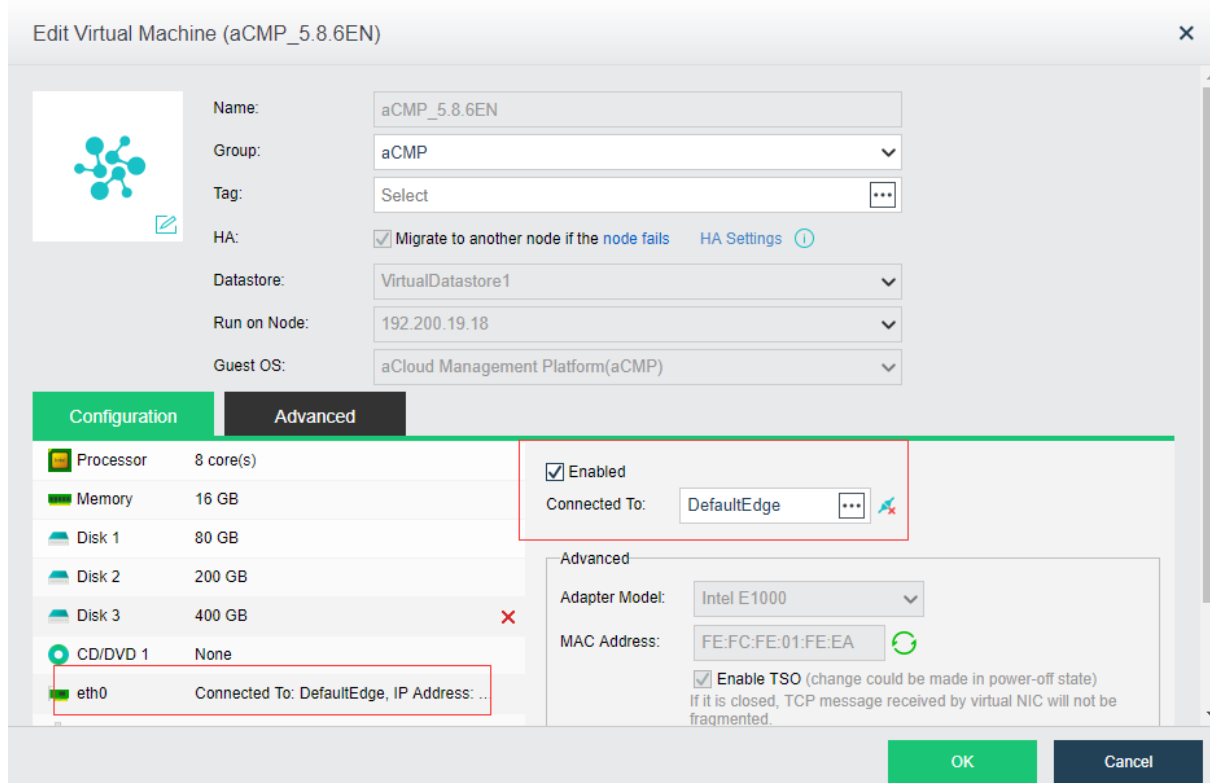


3.2 Congiure aCMP network IP

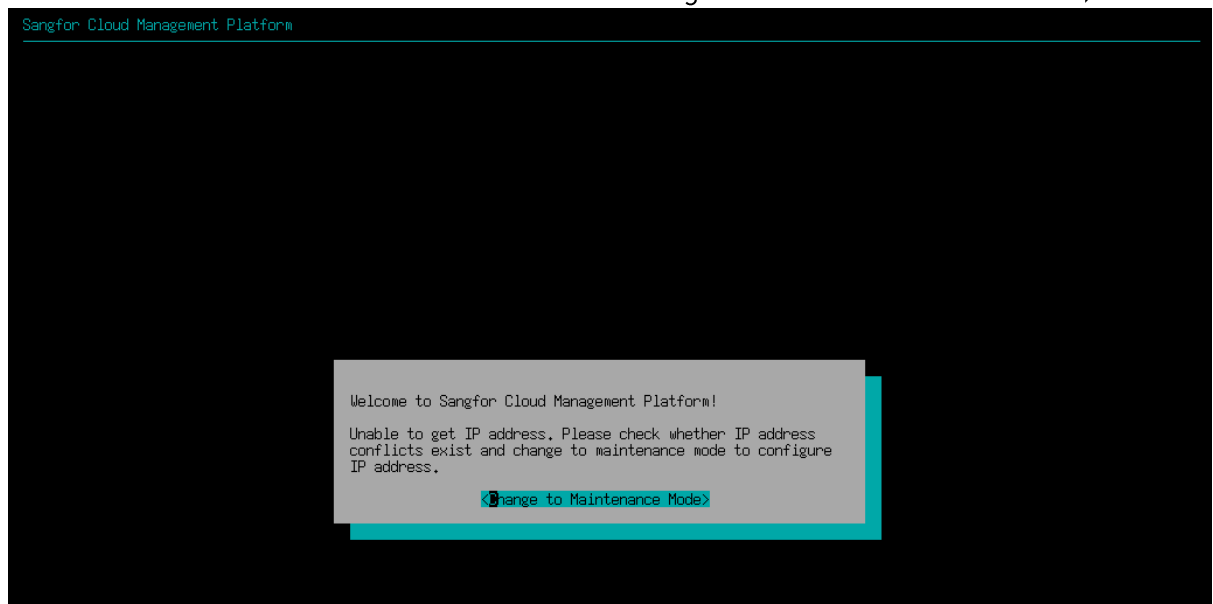
After success import aCMP into HCI, require to configure network configuration in aCMP cloud management platform. So that aCMP can communicate with aCloud cluster network, then aCMP can manage those reachable cluster in the network.

【Steps】

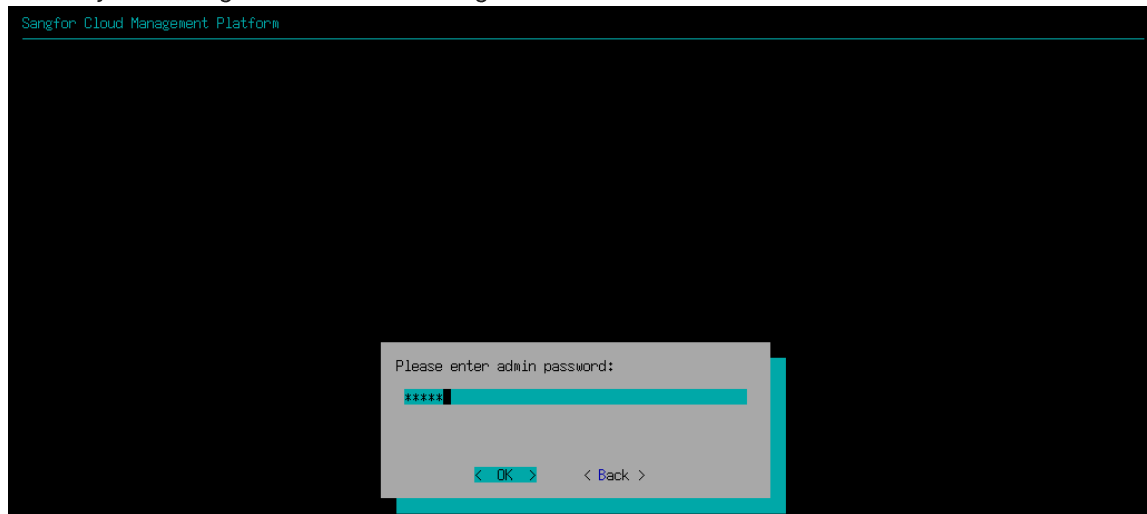
1. Select aCMP virtual machine, click 『more』 → 『setting』 . Configure the network card to make it connect to second/third layer of aCloud. Click button;



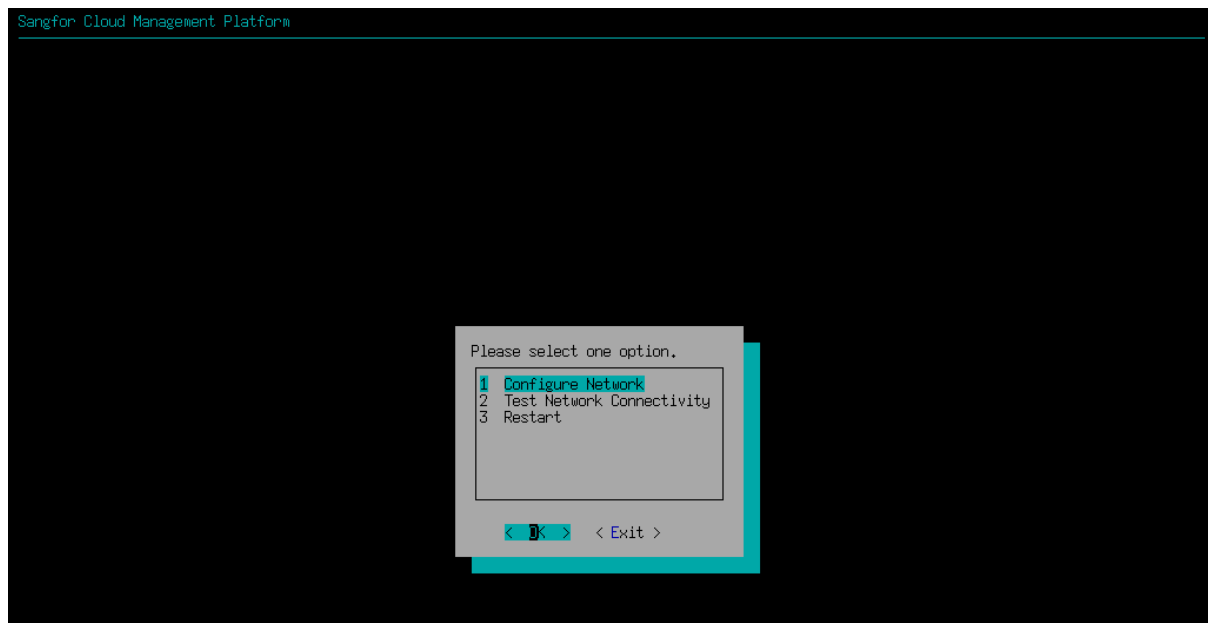
2. Power on the aCMP virtual machine and login to aCMP virtual machine;



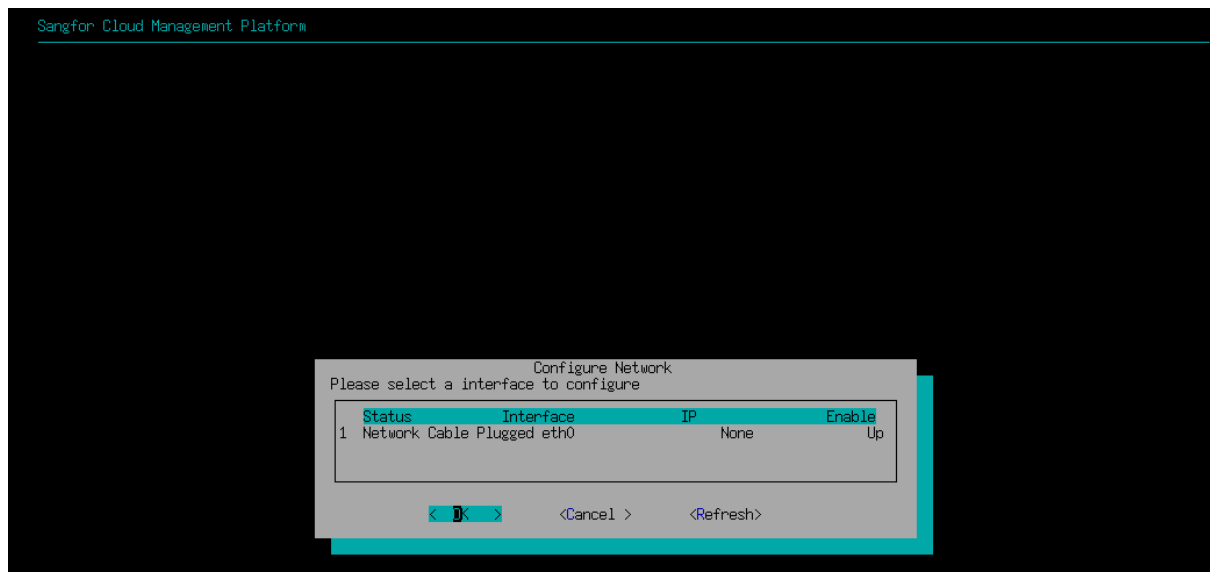
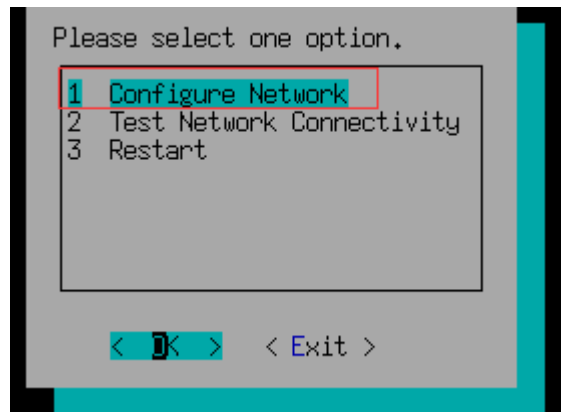
3. Click anywhere on the virtual machine console, type "enter" on the keyboard to enter maintenance mode, then enter the password (the initial password is admin), select the OK option after entering the password. Then type "enter" on the keyboard again to enter configuration interface.



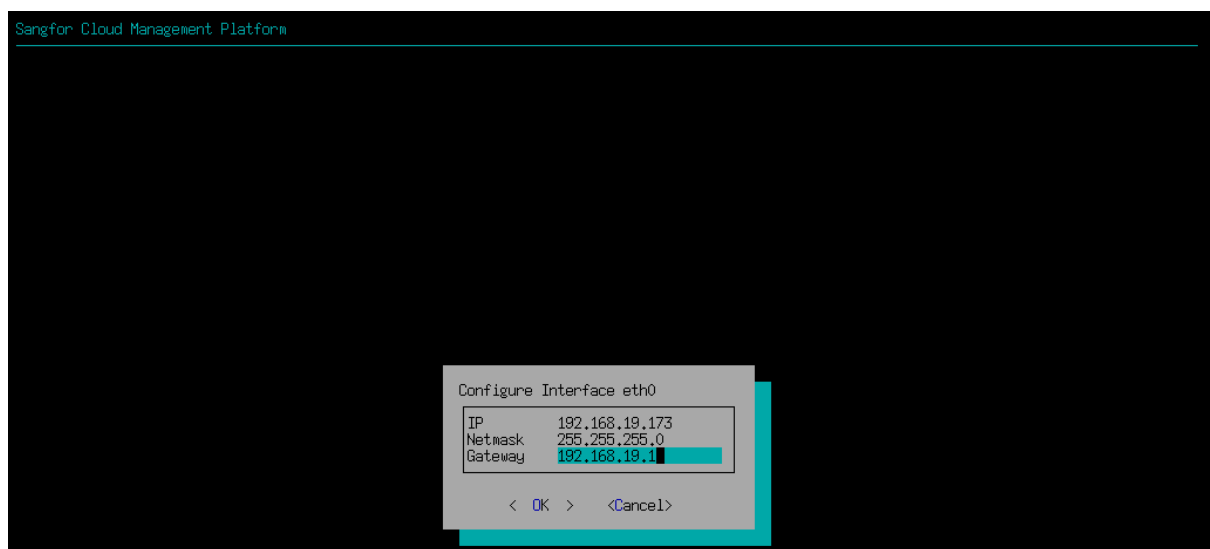
After click OK wil show an interfase as shown below:



4. Use keyboard "↑↓"key to select 『Configure Netwrok』 and press enter key on keyboard;



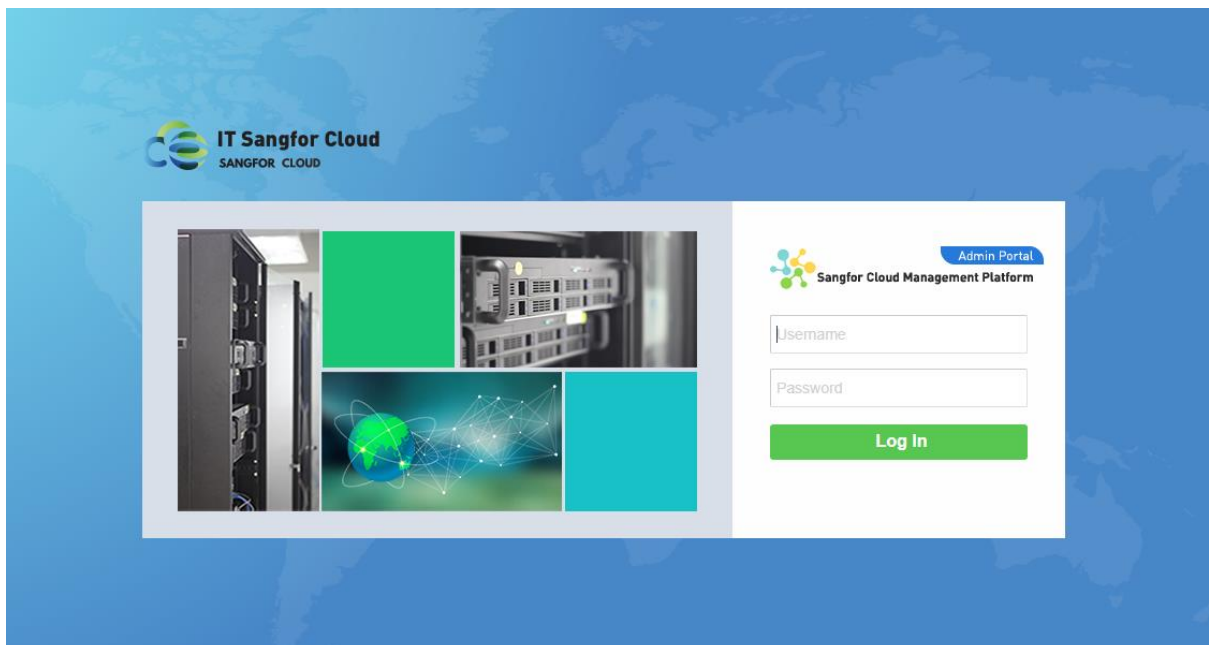
5. Configure IP address, netmask and gateway and press OK.



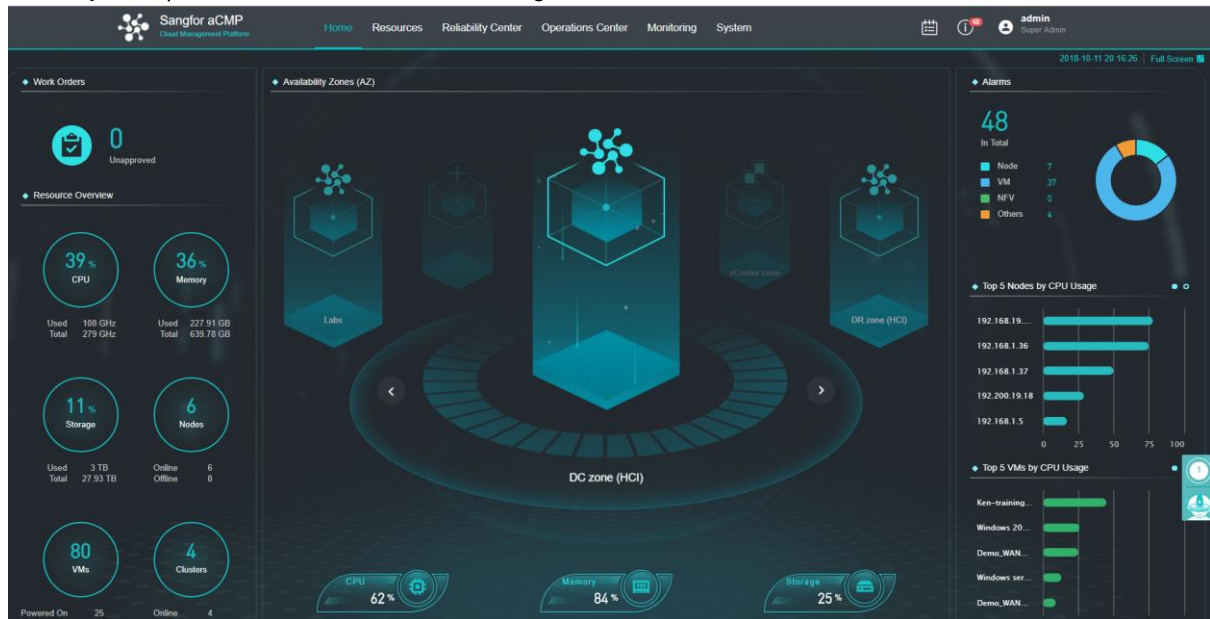
Save settings successfully. Please log in with the new IP address.



6. Open a browser and type in https://IP:4430



7. Default username and password is admin/admin. (To ensure the security please modify the password once success login)

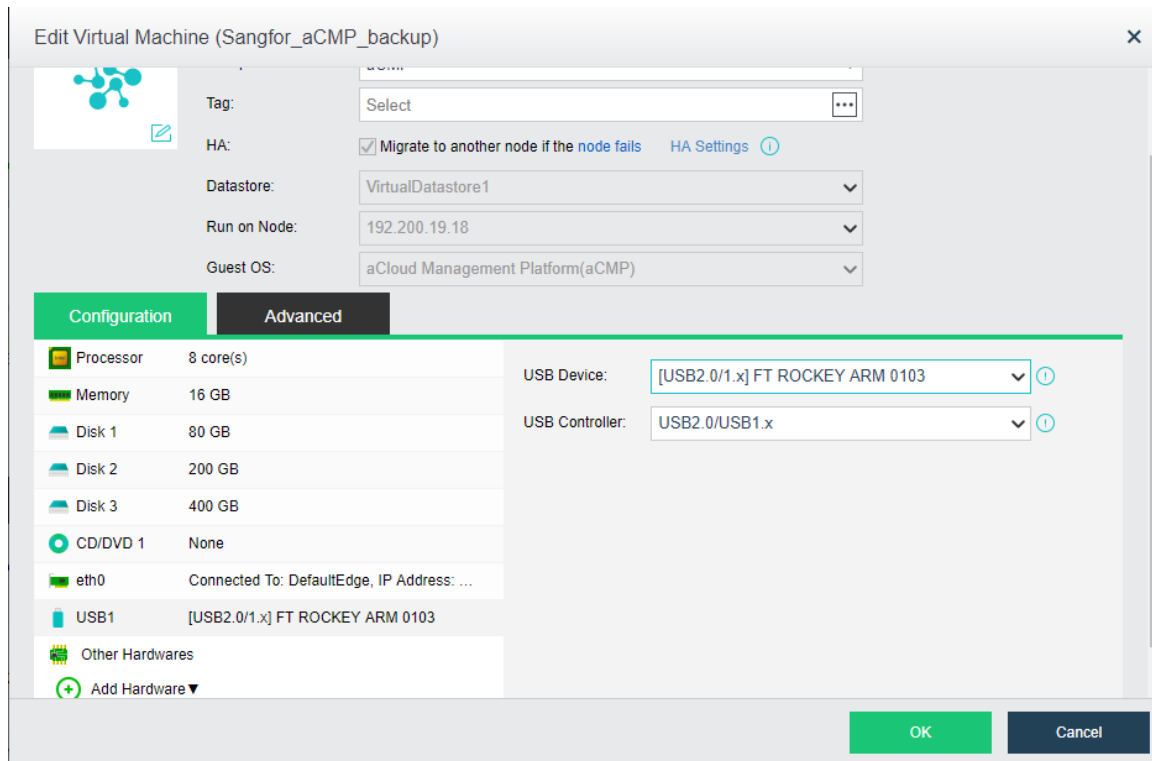


3.3 aCMP Authorization

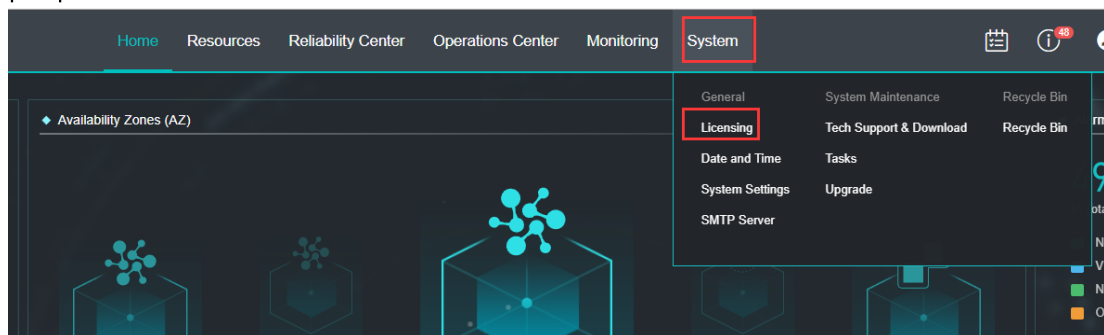
After configuring the network configuration of aCMP, you need to insert the previously prepared USB KEY into the USB interface of the aCloud cluster (any one), and then perform the authorization activation of aCMP as follows:

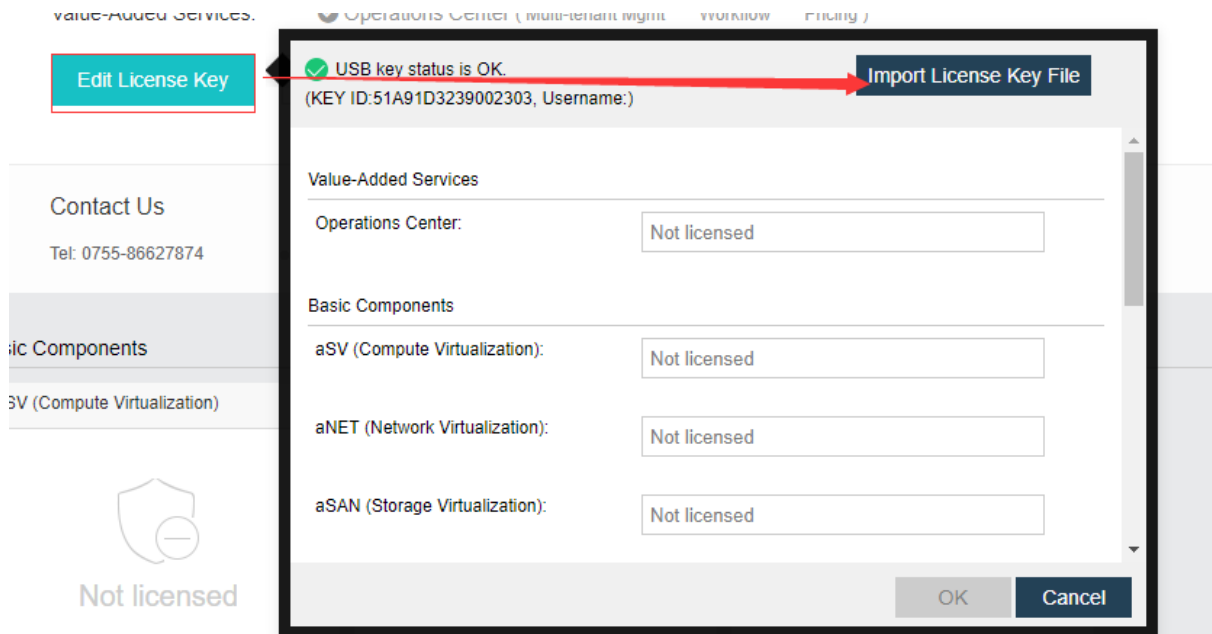
【Steps】

1. Click aCMP virtual machine → 『Configuration』 → Add USB Hardware → Map the USB to the virtual machine;

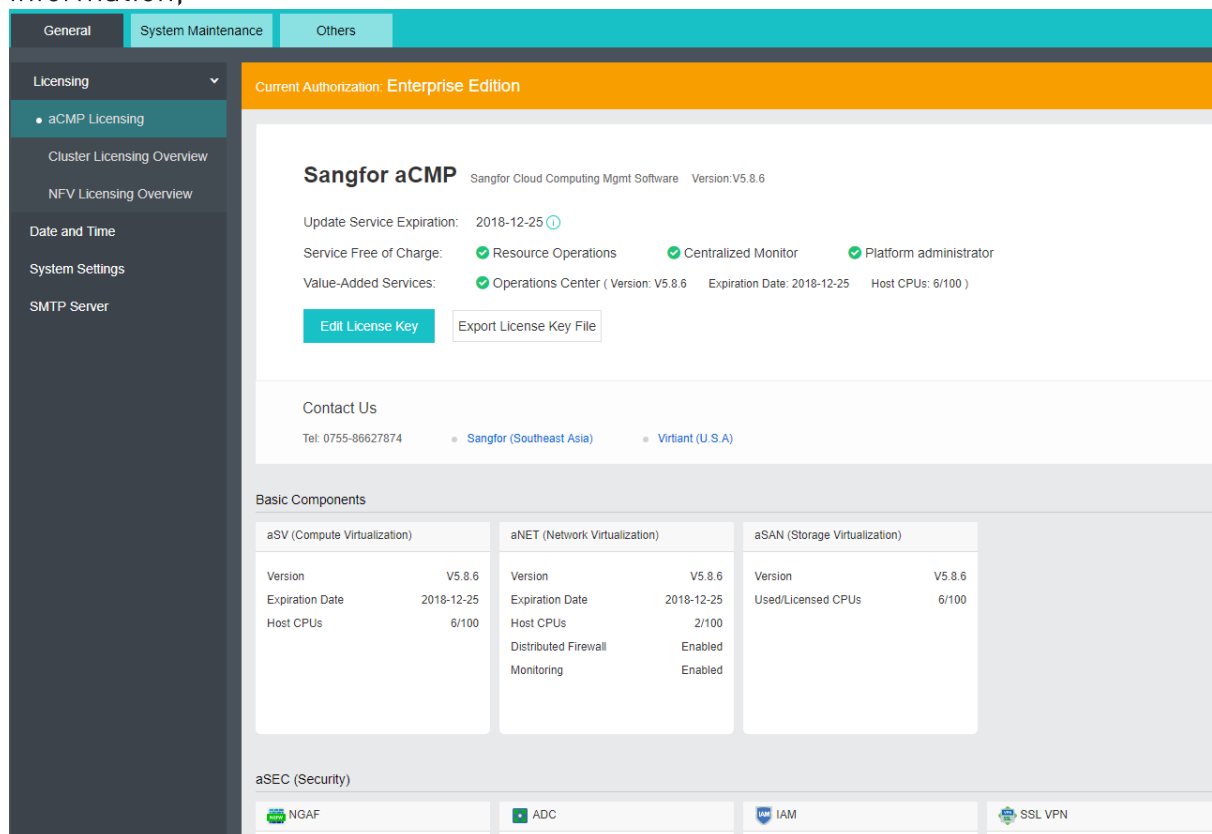


2. Login to aCMP homepage, click 『System』 → 『Licensing』 → 『General』 to enter aCMP authorization page. Then click 『Edit License Key』 and select the prepared authorization file with suffix .lic.





After the import is successful, you can view the corresponding serial number information;



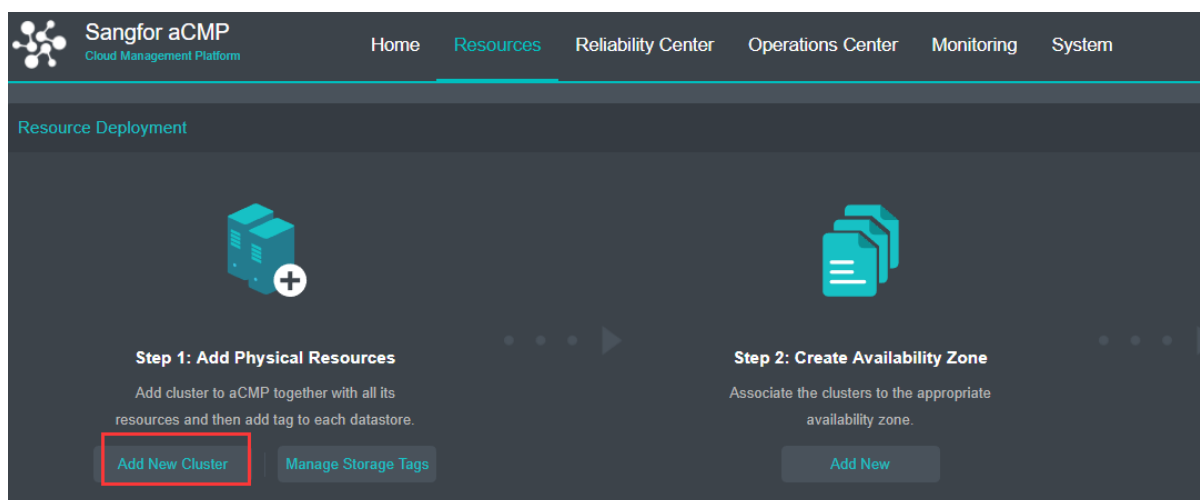
3.4 aCloud cluster joins aCMP centralized management

Version Requirement:

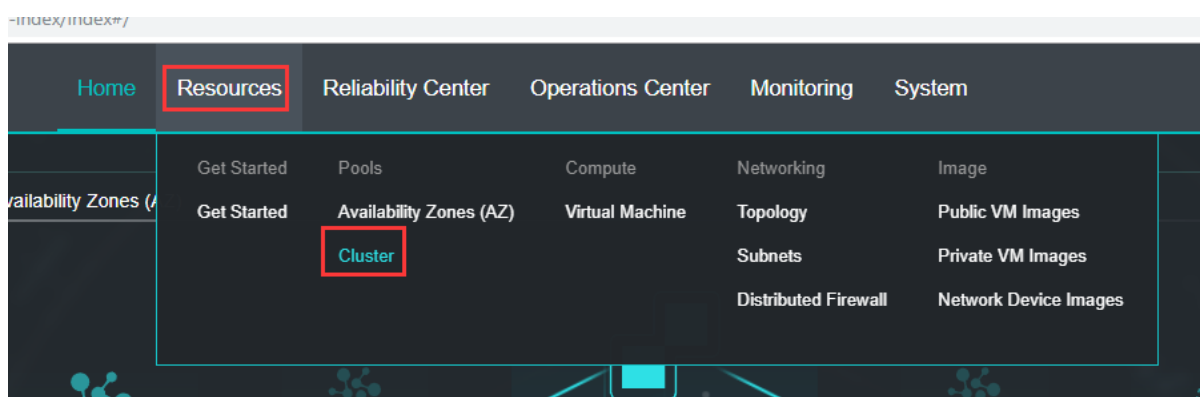
aCMP5.8.6 only support aCloud5.8.6 centralized control, aCloud with version lower than 5.8.6 is not supported to join aCMP5.8.6 centralized control.

【Steps】

1. Login to aCMP platform homepage, select 『Resources』 → 『Get Started』 , then click **Add New Cluster** button as figure shown below:



- Or select 『Resources』 → 『Clusters』 and click **New** button.



2. Enter cluster IP、 username、 password、 cluster name、 description and cluster type accordingly. Then click **Next** button. (Keep the default port number if there is unchange port number)

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. According to the actual situation of the cluster, you can set different tags for different storage volumes. By default the tags include "None", "High Performance", "Good Performance", and "Large Capacity". These tags can be changed according to the actual situation. The tags can change in [Cluster] → [Manage Storage Tag]. After setting complete click **Next** button

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 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. After ensure all information enter correctly, click **OK** button

Pools > Cluster > Add New Cluster

Basics Add Tags Confirm

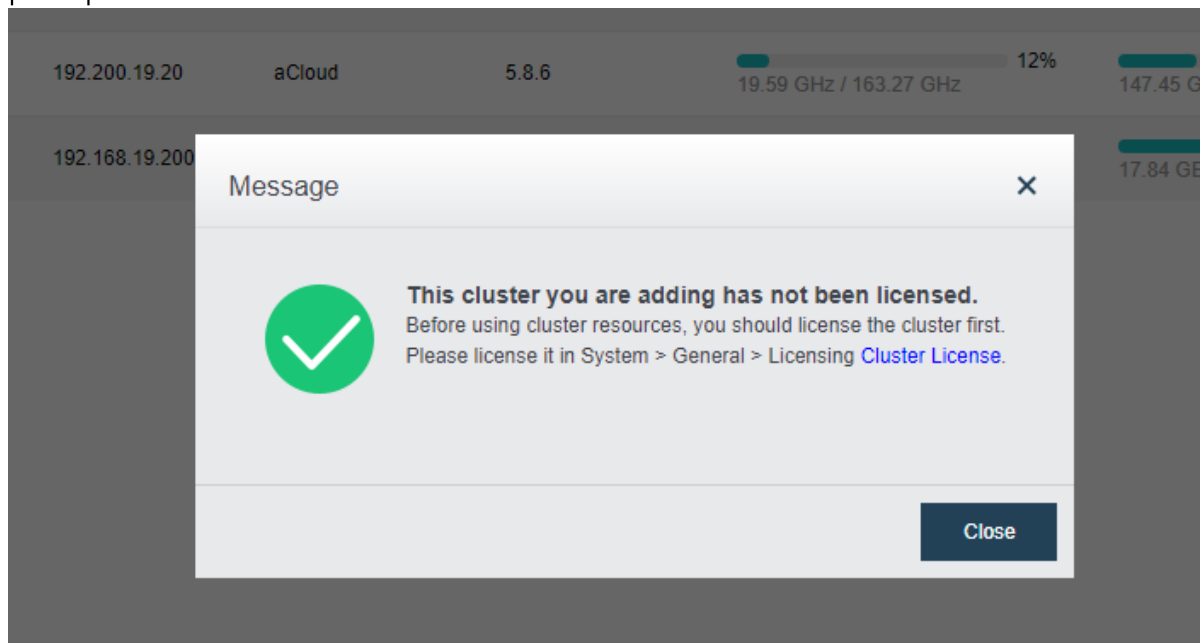
Cluster Name: DR(demo)
 Description:
 Cluster Type: aCloud
 Cluster IP: 192.200.19.20
 Port: 443

Tagging Storage:

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

Back OK Cancel

5. The first time add cluster to the aCMP cloud management platform, aCMP will prompt out for authorization.



3.5 Authorize aCloud clusters through aCMP

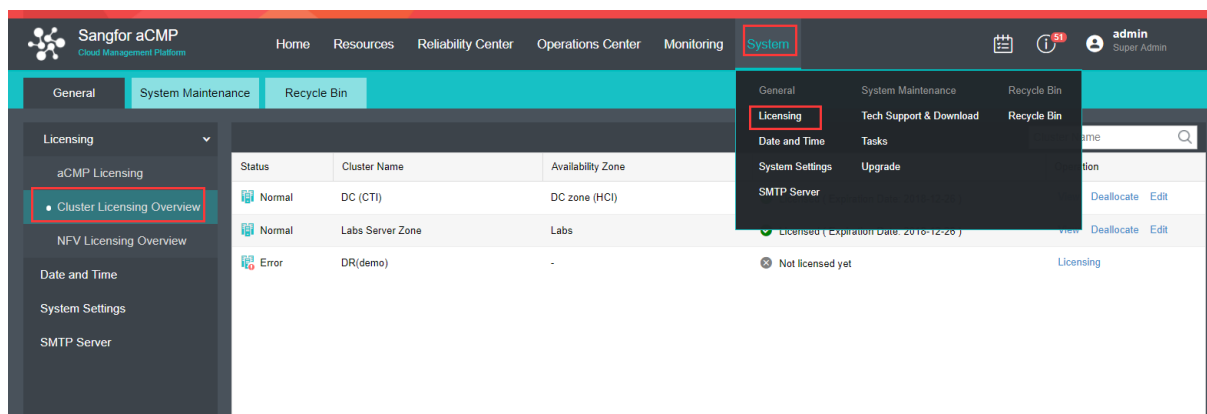
After aCloud cluster success added into aCMP, the aCloud cluster needed to be authorized to ensure the aCloud cluster service is available or perform authorization reclaim, edit and other operations. All the operations are performed in aCMP.

【Pre-requirement】

aCMP must be import authorization and authorization number enough to authorize manged aCloud cluster.

【Steps】

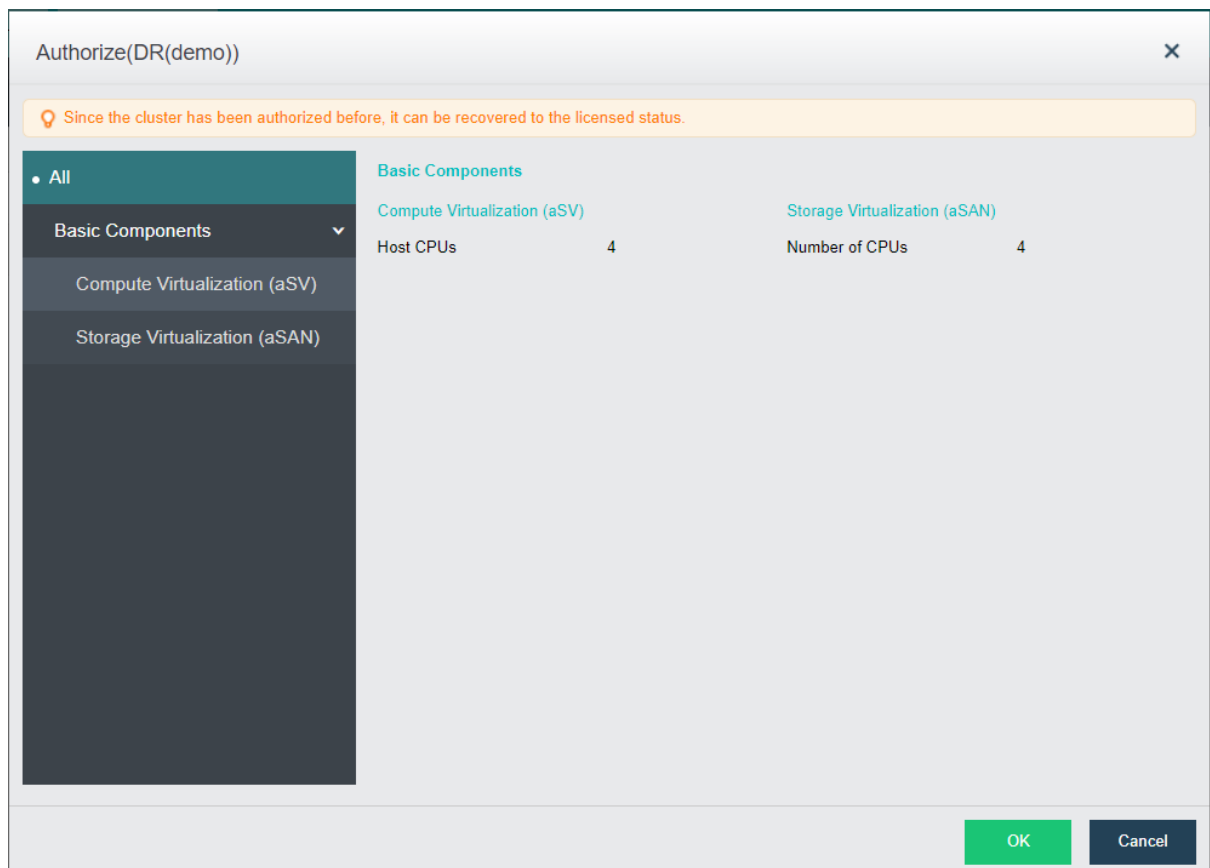
1. Login to aCMP homepage, select 『System』 → 『Licensing』 → 『Cluster Licensing Overview』 to check which cluster has not been authorize. Then click **Licensing** button to authorize the particular cluster.



2. Click on the abnormal cluster [Licensing];

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 assigning the authorization, click the **OK** button to complete the authorization.



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

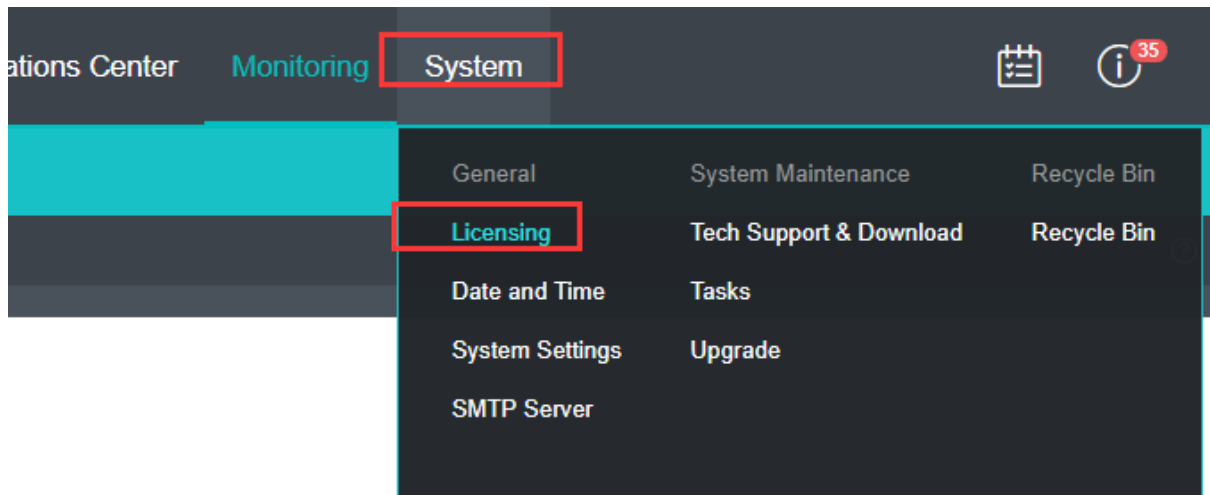
Status	Cluster Name	Availability Zone	Cluster	Operation
Normal	DC (CTI)	DC zone (HCI)	✔ Licensed (Expiration Date: 2018-12-26)	View Deallocate Edit
Normal	DR(demo)	DR zone (HCI)	✔ Licensed (Expiration Date: 2018-12-26)	View Deallocate Edit
Normal	Labs Server Zone	Labz	✔ Licensed (Expiration Date: 2018-12-26)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

3.6 NFV Authorization

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



General System Maintenance Recycle Bin

Licensing

- aCMP Licensing
- Cluster Licensing Overview
- NFV Licensing Overview**
- Date and Time
- System Settings
- SMTP Server

Expand All Collapse All Object name Q Advanced

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
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

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

Expand All Collapse All Object name Q Advanced

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
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

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

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

DC zone (HCI)

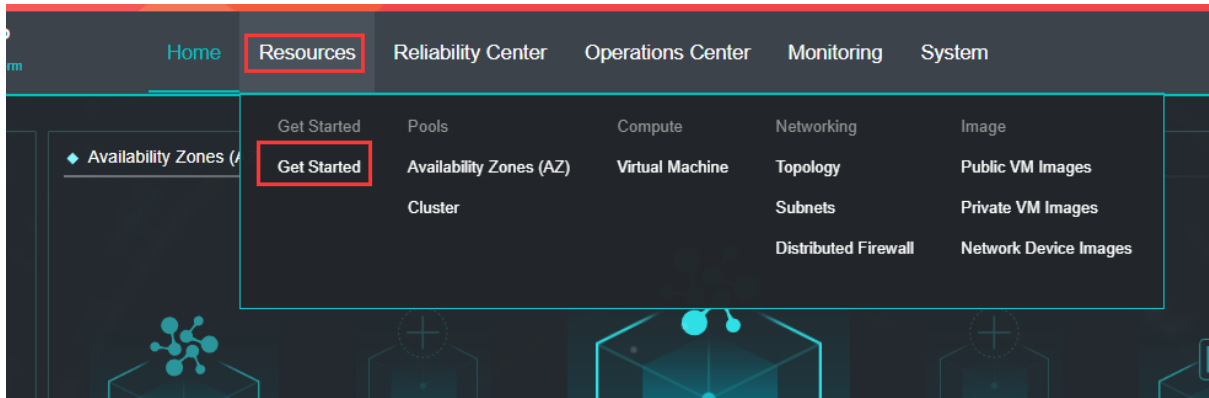
Device Name	Configuration Standard	Resource Type	Status	Expiration Date	View	Deallocate	Shut Down
NGAF4	NGAF	DC (CTI)	Licensed	2018-12-26	View	Deallocate	Shut Down
SC NGAF	NGAF	DC (CTI)	Licensed	2018-12-26	View	Deallocate	Shut Down
IAM4	IAM	DC (CTI)	Licensed	2018-12-26	View	Deallocate	Shut Down
IAM4_ken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

3.7 Availability Zone

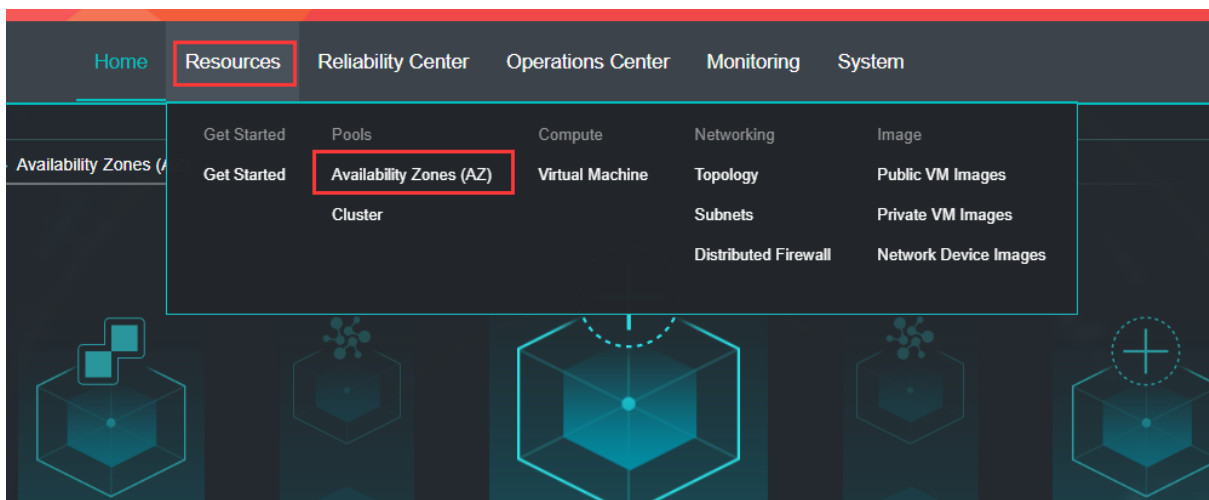
After the cluster is managed, it is necessary to divide the existing different clusters into different Availability Zones. The so-called availability zone concept is targeted at the data center. Generally, the Availability Zone can contain multiple clusters. By dividing the logical concept of the Availability Zone can effectively help the administrator to manage the platform.

【Steps】

1. Click 『Resources』 → 『Get Started』 as shown below:



Or click 『Resources』 → 『Availability Zone』 will prompt out a page and click **New** button to build new zone:



2. Fill in corresponding information and click Next button to proceed.

3. Select targeted cluster that needed to add in to the Availability Zone. (If the target cluster is not found, can add the cluster manually. For the detail please refer to Section 3.4) Click **Ok** to proceed to next step.

Please select a cluster that you want to associate with. No suitable cluster? [Add Cluster](#)

Name	Cluster Type	Description	Cluster IP	CPU Usage	Memory Usage	Storage Usage
Labs Server Zone	aCloud	-	192.168.19.174	41.85 GHz / 50.42 GHz 83%	9.02 GB / 32 GB 28%	5.33 GB / 11.7 TB 0%

Back Next Cancel

4. Ensure all the information is correct and click **OK** button.

Resources > Availability Zones > Create Availability Z...

Basics Associate with Cluster Confirm

Name: sangfor CTI
Resource Type: aCloud
Description:

Cluster:

Name	Cluster Type	Description	Cluster IP
Labs Server Zone	aCloud	-	192.168.19.174

5. The added Availability Zone can be edit and delete.

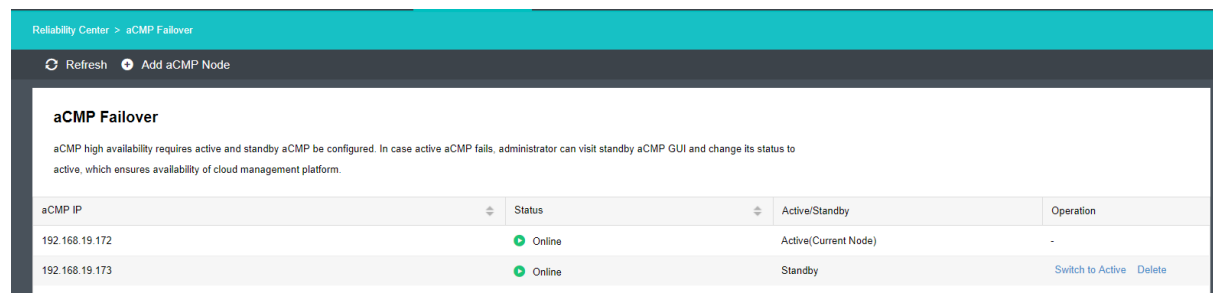
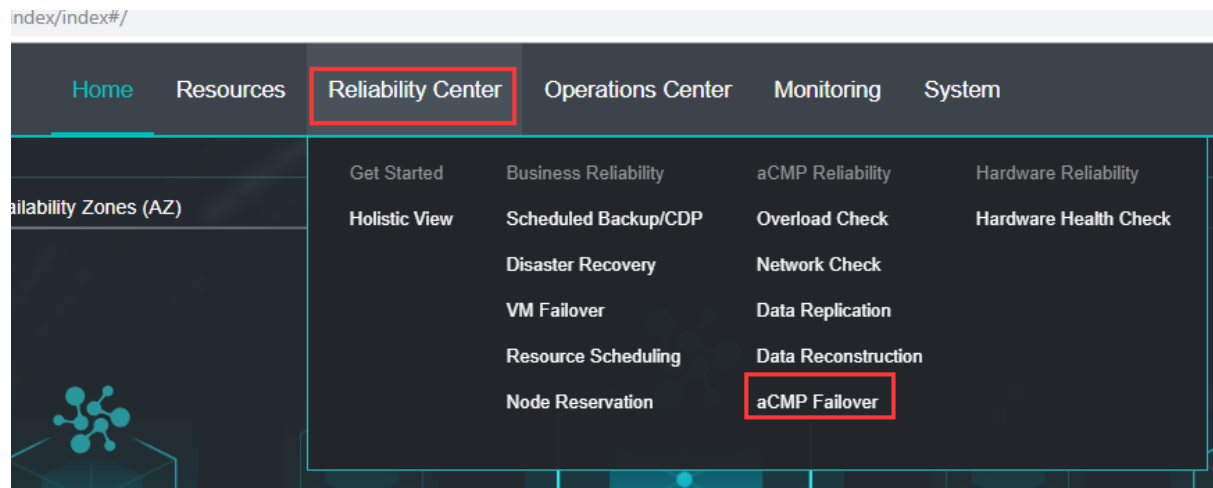
Name	Description	Resource	CPU Usage	Memory Usage	Storage Usage	Operation
DC zone (HCI)	-	aCloud	18.51 GHz / 53.62 GHz 35%	51.09 GB / 64 GB 80%	883.23 GB / 3.59 TB 24%	Edit Delete
DR zone (HCI)	-	aCloud	24.68 GHz / 163.27 GHz 15%	147.62 GB / 512 GB 29%	532.15 GB / 10.84 TB 5%	Edit Delete
sangfor CTI	-	aCloud	38.83 GHz / 50.42 GHz 77%	8.93 GB / 32 GB 28%	0 B / 0 B 0%	Edit Delete
vCenter zone	-	VMware	389 MHz / 11.39 GHz 3%	17.84 GB / 31.78 GB 56%	1.48 TB / 1.81 TB 82%	Edit Delete

Chapter 4 aCMP Active and Standby Deployment

Application scenario: Active aCMP has been deployed and require to build another aCMP as backup in another data center.

Configuration steps:

- 1) Deploy aCMP IP in a remote data center according section 3.1, 3.2 and 3.3 and the IP address is different from the active aCMP.
- 2) Click 『Reliability Center』 → 『aCMP Failover』



- 3) Click **Add aCMP Node** button , type in the backup aCMP's IP address and password, then click **OK** button.

Add aCMP Node [X]

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:

OK **Cancel**

After success added standby aCMP, it is shown in the aCMP Failover page as shown below:

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

Follow the steps above to complete the deployment of the aCMP standby machine.



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

