Sangfor Cloud Agent Deployment Manual

Product Version	V2.1.3EN
Document Version	01
Released on	Jan. 3, 2024

Disclaimer

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

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

Technical Support

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

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

About This Document

This document describes how to deploy Cloud Agent for SkyOPS.

Intended Audience

This document is intended for:

- System / Network Administrator
- MSP / tenant

Note Icons

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

Change Log

Date	Change Description
Jan. 3, 2024	This is the first release of this document.

Contents

Technical Support 1
Change Log 2
1 Introduction 4
2 Private Cloud Version Requirements 4
3 Cloud Agent Deployment 5
    3.1 Obtain Cloud Agent Package 5
    3.2 Check Configuration Specifications 5
    3.3 Deployment Steps 5
4 Connect to MCS 10
5 Connect to Private Cloud 11
    5.1 Connect to HCI 11
    5.2 Connect to SCP 12
    5.3 Connect to VDC 14
6 Alarms Reporting in SkyOPS 16
7 Cloud Agent Platform Operations 16
    7.1 Disable Data Center on Cloud Agent 17
    7.2 Enable/Disable Cloud Agent 17
    7.3 Enable Agent Automatic Upgrade 18
    7.4 Remove Data Center 19
    7.5 Cloud Agent Management 20
    7.6 Agent Installation 20
8 Notes 20
9 Upgrade 22

1 Introduction

Customers can connect to the Sangfor Cloud Service Center through a cloud agent and upload private cloud alerts to the Sangfor Cloud Service Center. In this way, customers using private cloud can experience cloud O&M services. O&M personnel can quickly view all private cloud alerts in SkyOPS to locate the problems.

In the private cloud scenario, SkyOPS can push alarms to MCS by installing the Cloud Agent component.

1. Addressing the issue of delayed handing of alarm events for private cloud users, all private cloud alarms are collected and forwarded to SCC, allowing us to proactively serve customers by identifying issues before they do.
2. When the SCP and HCI platform with Cloud Agent has software update service license, the tenant of MCS can select Cloud Agents as private cloud probing sites for creating business probe.
3. After the data center connecting the Cloud Agent, data can be reported to AIops for analysis, and disposal recommendations in the alarm event details. The Intelligent Risk Prediction page helps identify risks in advance and mitigate issues. (The SCC AIOps analysis feature will be available in future versions.)

2 Private Cloud Version Requirements

Cloud Agent can connect to the following platform versions:

HCI: 680R1_EN with patch sp-HCI-6.8.0_R1-col-20231012.pkg; 6.9.1_EN

SCP: 6.9.0R1_EN or 6.9.1_EN

VDC: 590_EN or 591_EN

Download link of sp-HCI-6.8.0_R1-col-20231012.pkg

https://download.sangfor.com/Download/aDeploy/HCI/Patches/sp-HCI-6.8.0_R1-col-20231012.zip

If HCI is not connected to SCP, a patch is required to support the connection with the Cloud Agent. However, if HCI is managed by SCP, it is recommended to connect to the Cloud agent through SCP. In this case, HCI's alarms will be pushed to SCP.

3 Cloud Agent Deployment

3.1 Obtain Cloud Agent Package

Sangfor_Skyops_2.1.3_EN(20230925).ova

Sangfor_Skyops_2.1.3_EN(20230925).vma

https://community.sangfor.com/plugin.php?id=service:download&action=view&fid=47#/42/288

3.2 Check Configuration Specifications

It is recommended that the virtual machine use the following recommended configuration when deploying the Cloud Agent. The number of disks must be greater than or equal to 4 (disk 1 is the system disk, disk 2 is used for MySQL, disk 3 is used for MySQL backup, and disk 4 is used for containers)

Item	recommended
CPU	2 cores
Memory	4GB
Disk	Disk 1:80 GB Disk 2: 200GB Disk 3: 400GB Disk 4: 400GB
NIC	2 NICs (eth0 and eth1)

3.3 Deployment Steps

Cloud agent deployment supports dual NIC and Single NIC deployment. The deployment steps include configuring network interfaces, initializing the environment, and configuring DNS services.

If the customer isolates the Intranet and Internet, dual NICs are required. Eth0

is to access the Intranet to connect the management network of SCP/HCI/VDI. Eth1 is to access the Internet to connect MCS.

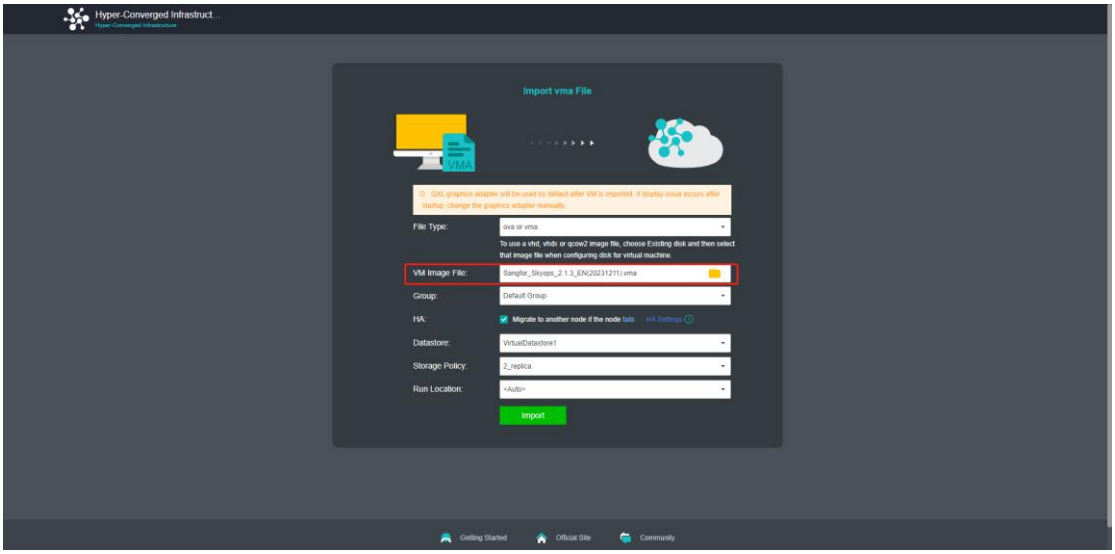
If single NIC can access both the Intranet and Internet. Only need to connect eth0 to SCP/HCI/VDI and MCS.

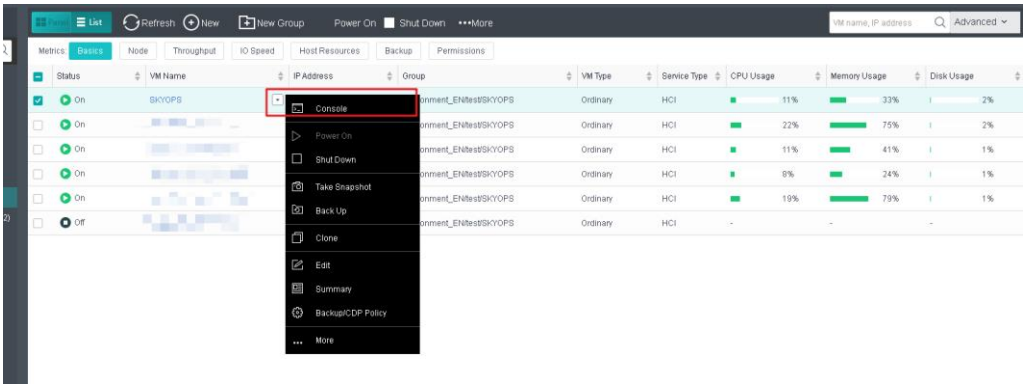
NOTE

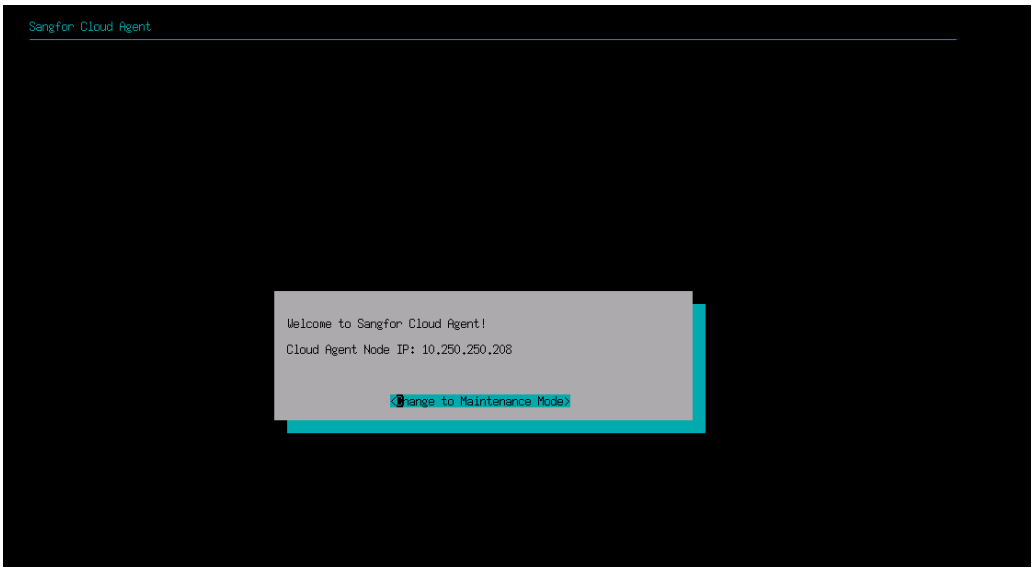
Translation: Modifying network configurations directly on the Cloud Agent virtual machines in SCP and HCI is not supported, including network settings, subnet masks, and gateways. If you need to make changes, please go to the virtual machine: open the console and modify the network configuration in the network settings.

Processor	2 core(s)
Memory	4 GB
Disk 1	80 GB
Disk 2	200 GB
Disk 3	400 GB
Disk 4	400 GB
eth0	Connected To: Switch1
eth1	Connected To: Edge1

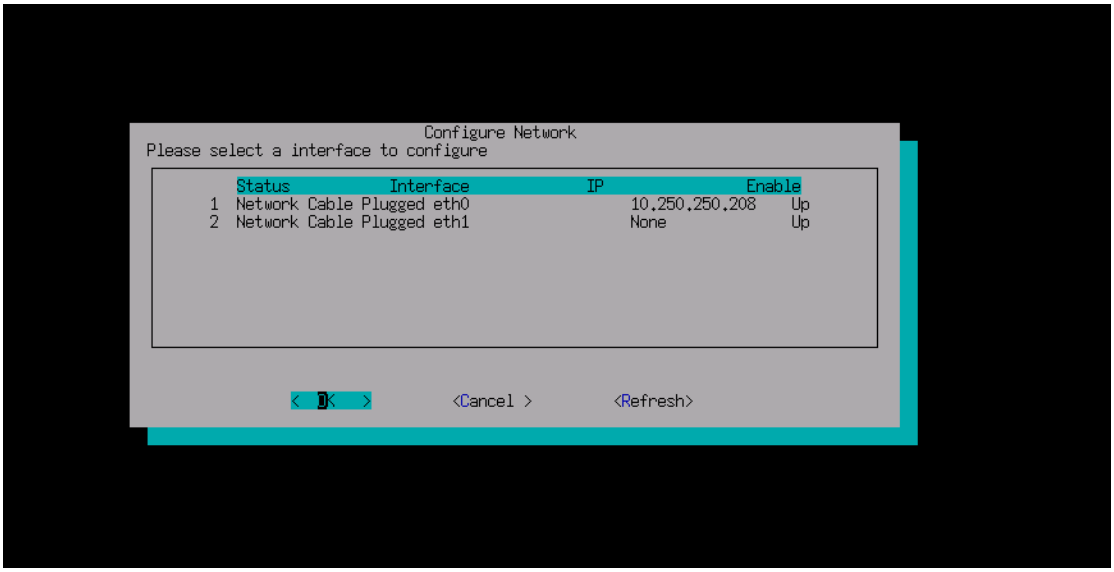
1. Configurate NIC. Import the **vma/ova** obtained in Chapter 3. Power on the Cloud Agent. Click on the VM console and place the VM into Maintenance Mode.

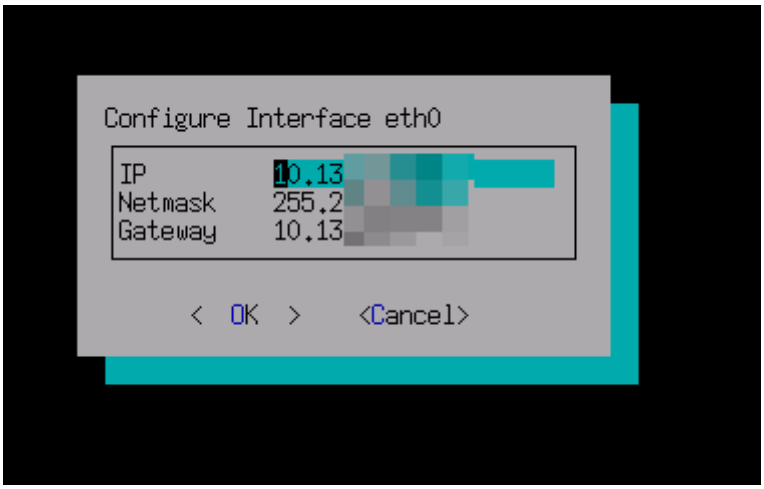






Enter the SSH password (the initial password of Cloud Agent is adminsangfor12#$5) to open the options screen. Select **Configure Network** to enter the network settings screen. Configure network for eth0. The IP address for accessing the internal network is configured here, as shown in the figures below:

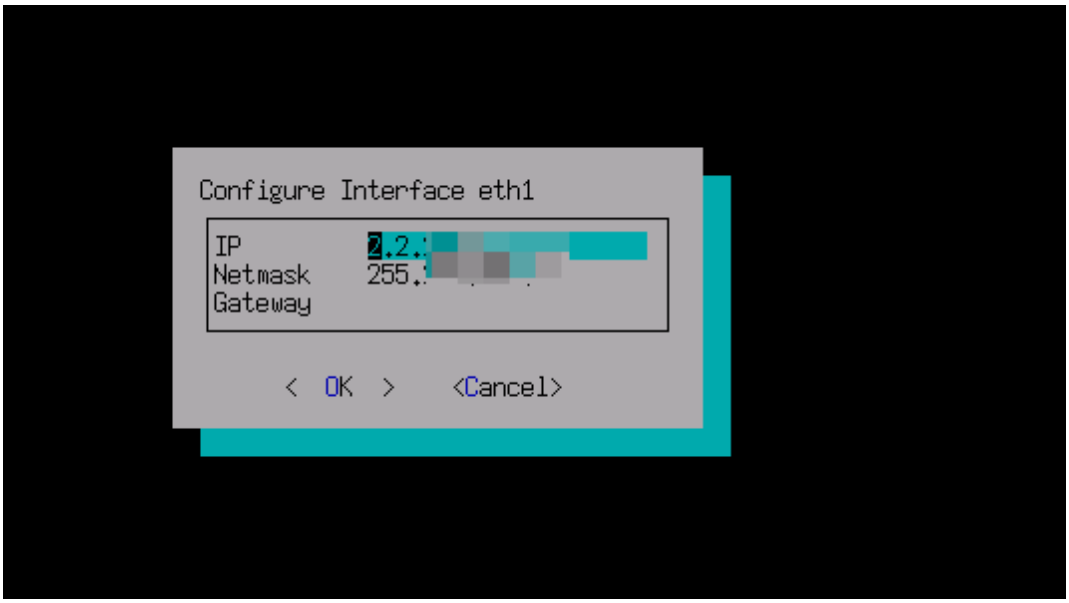




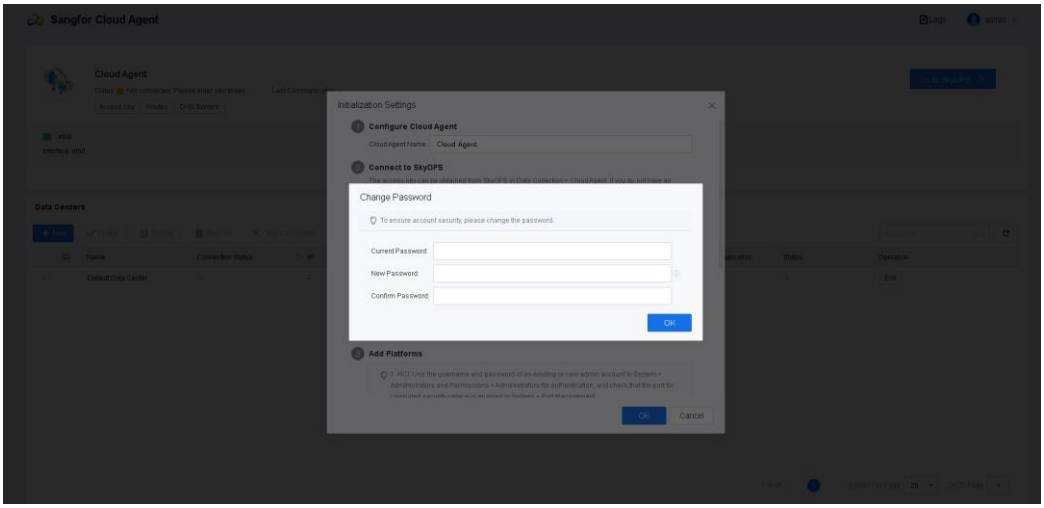
NOTE

If user's Cloud Agent eth0 management interface is directly connected to the public network, there is no need to configure a second network interface. Only configuring the eth0 interface is sufficient.

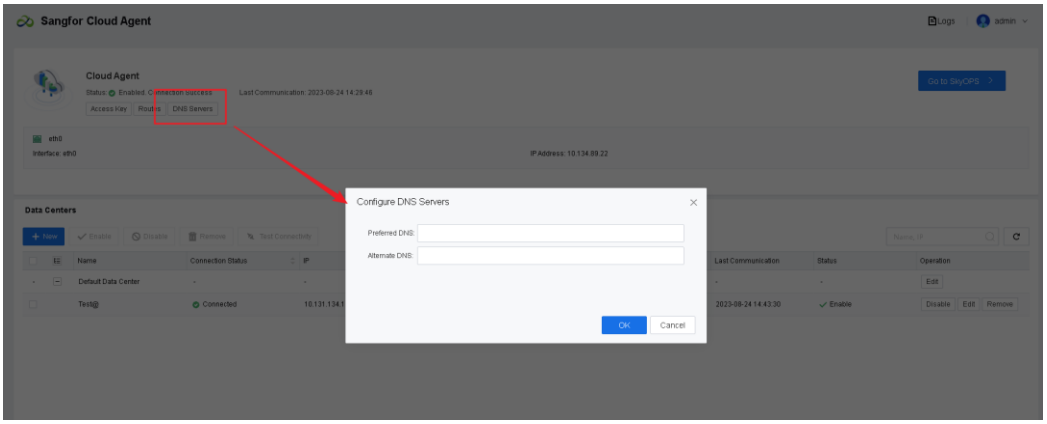
(Ignore this step for single-NIC deployment.) If two NICs need to be configured, repeat the preceding steps to configure network for eth1. The IP address for accessing the external network is configured here, and there is no need to configure a gateway, as shown in the figure below:



2. Access web console, access Cloud Agent web console with the IP of management interface (eth0). E.g., https://IP and default account (admin/admin). Change the default password.



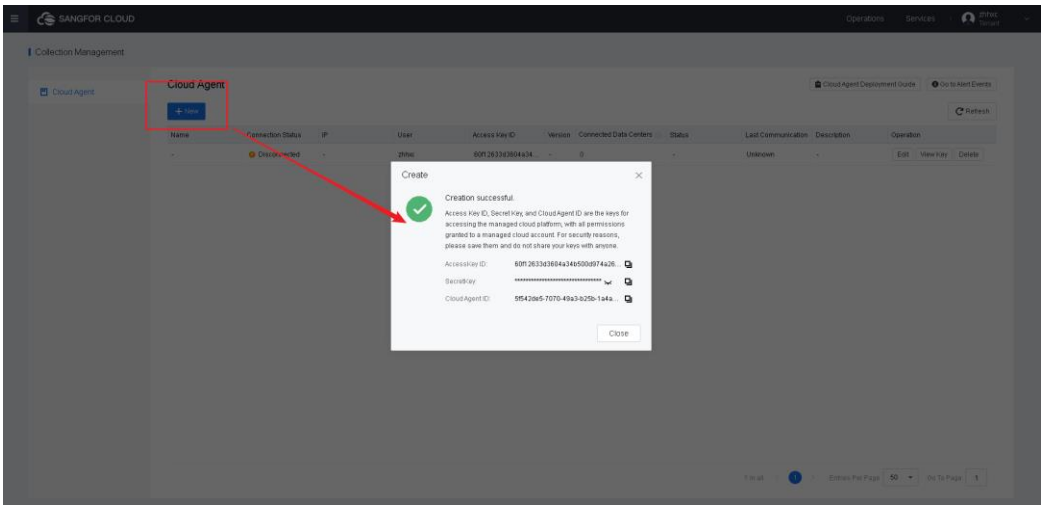
3. Configure DNS IP, configure the DNS IP and Click OK. E.g., Preferred DNS: 8.8.8.8; Alternate DNS: 8.8.4.4. DNS should be configured according to the requirements to ensure proper resolution of MCS's public domain names.



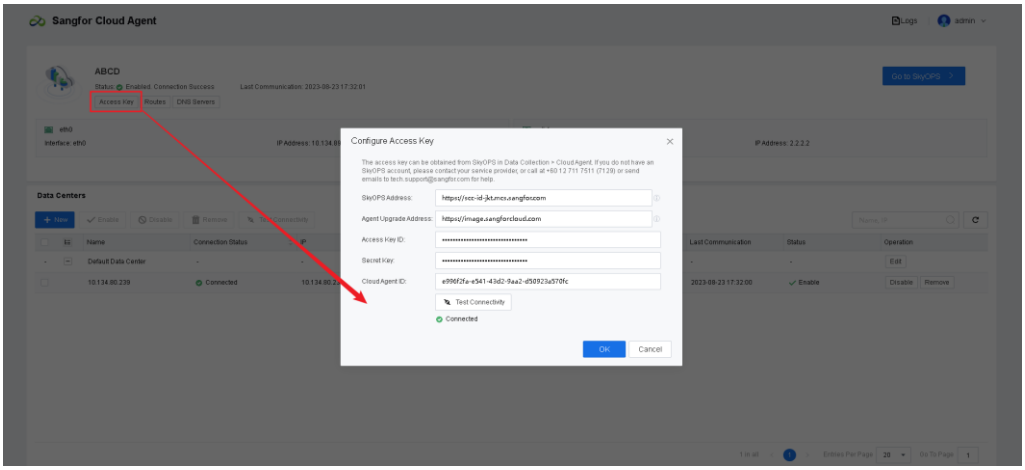
4 Connect to MCS

If private cloud customers want the operations administrator to assist in private cloud platform management, the private cloud environment must be connected to MCS through Cloud Agent. To ensure network security for the private cloud environment, eth1 of Cloud Agent is usually exposed to the public network, while eth0 is used for communicating with SCP and HCI over internal network. When connected to a data center, Cloud Agent will automatically report the cluster information of the data center and the alerts generated by the platform.

1. Make sure that the Sangfor Cloud Agent platform can ping the following two domain names: scc-id-jkt.mcs.sangfor.com (domain name of MCS, Depends on the domain name of your local MCS) and image.sangforcloud.com (domain name of Harbor server).
2. On the MCS, choose **Collection Management > Cloud Agent** to add a Cloud Agent and record the **Access Key ID, Secret Key, Cloud Agent ID**.



3. Click **Access Key** on the Sangfor Cloud Agent to configure access key as configured in step 1 and then click **OK**. Check the status should be normal.



5 Connect to Private Cloud

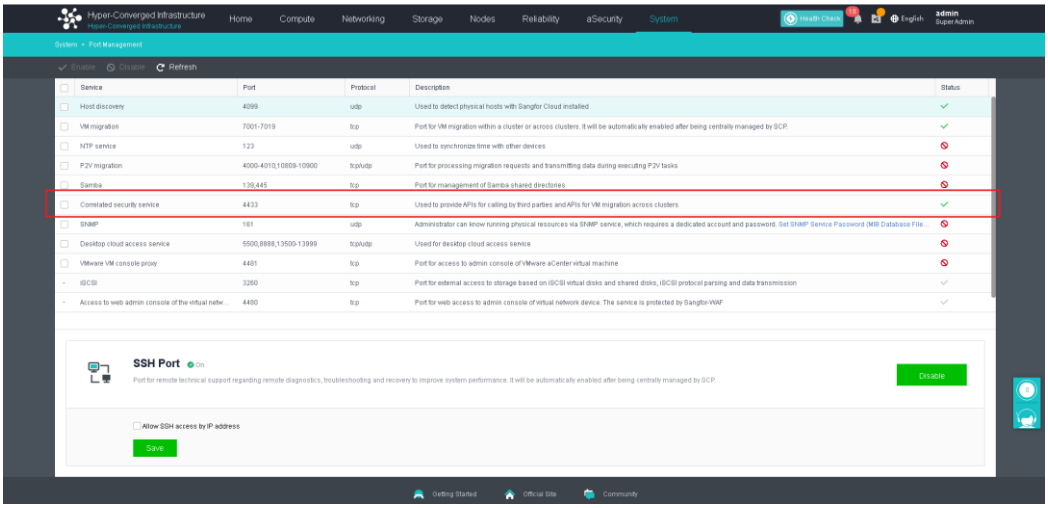
Currently, Sangfor Cloud Agent can be connected to HCI, SCP, and VDC platforms.

The following firmware versions are required by Cloud Agent 2.1.3_EN:

- HCI: 680R1_EN with patch sp-HCI-6.8.0_R1-col-20231012.pkg; 6.9.1_EN
- SCP: 6.9.0R1_EN or 6.9.1_EN
- VDC: 590_EN or 591_EN

5.1 Connect to HCI

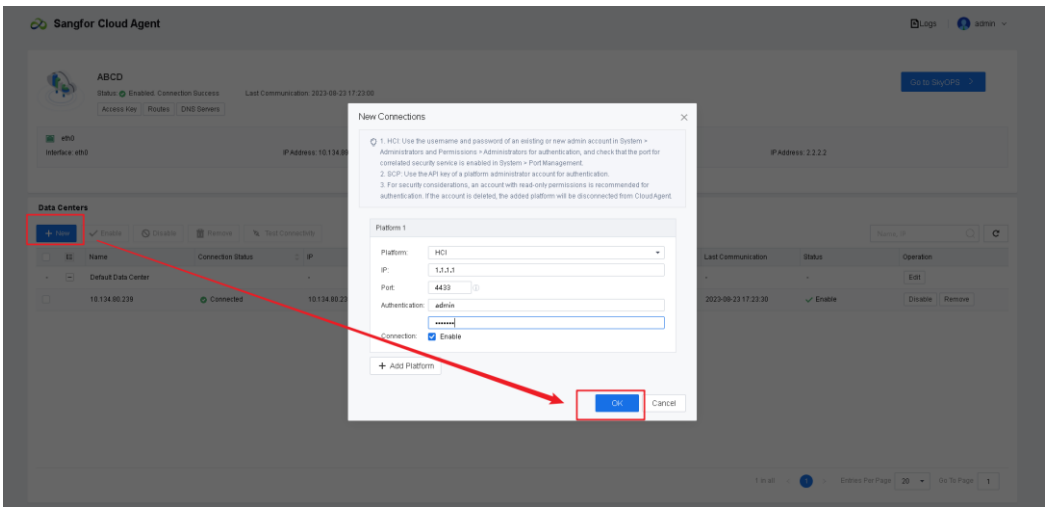
1. Check the **Correlated Security Service** is enabled on the HCI. And Cloud Agent can access port 4433 of HCI.



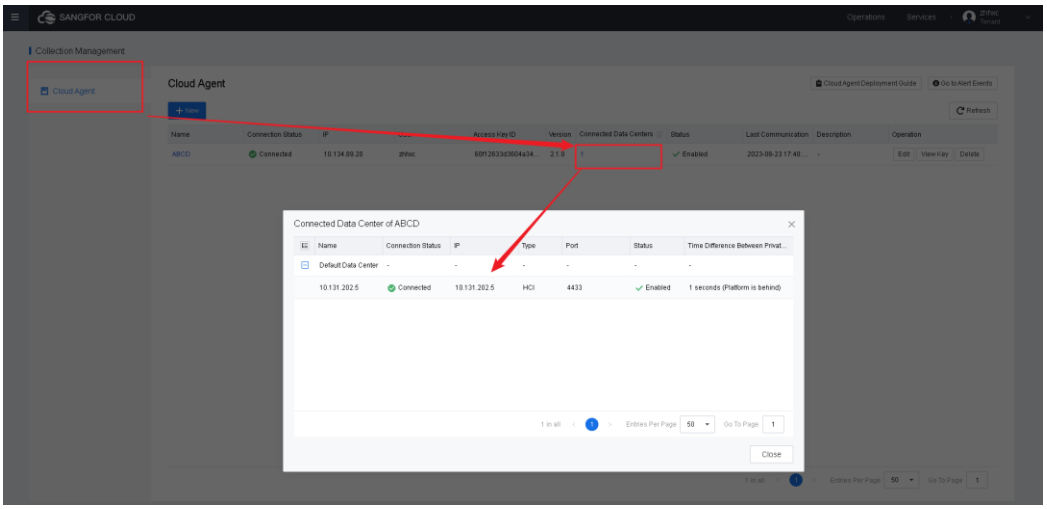
2. Create a new data center on the Cloud Agent. Platform select HCI, IP is HCI

cluster management IP, port is 4433, authentication is HCI admin.

3. Click on **OK** and if the connection is established successfully, the connection status will be **connected**.



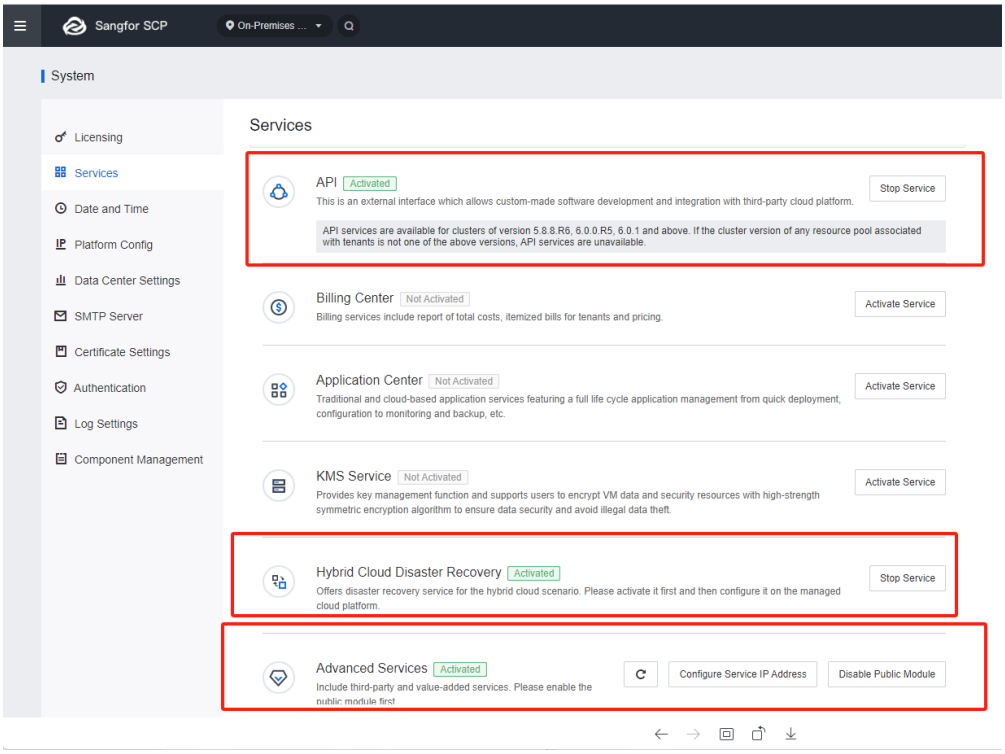
4. Check on the MCS, you can see this agent already connect to HCI.

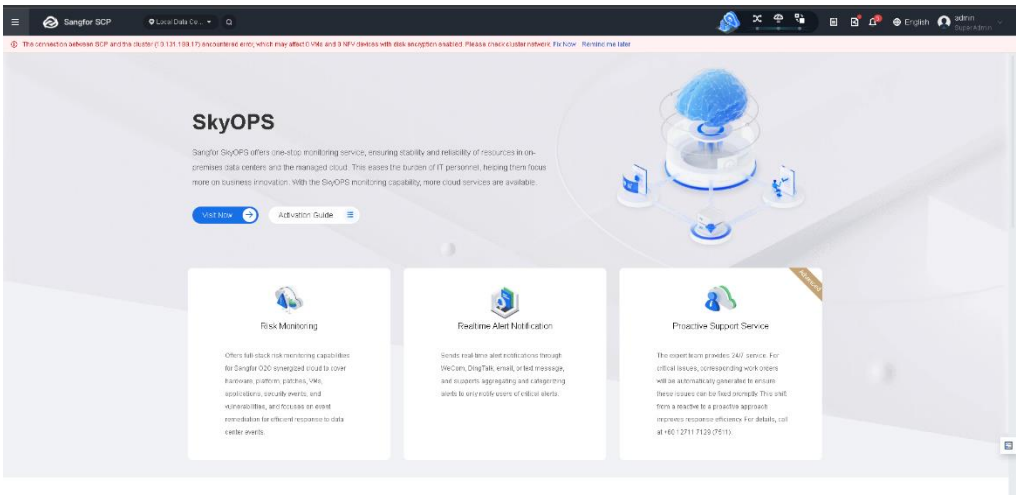


5.2 Connect to SCP

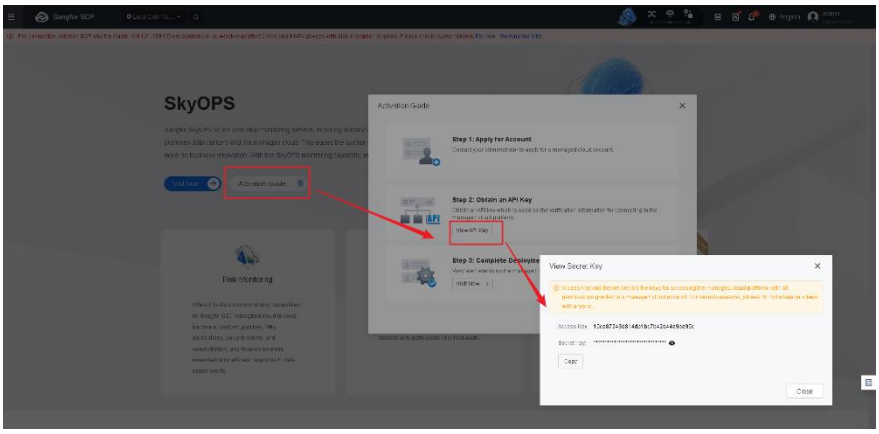
Before connecting Cloud Agent to SCP, make sure the following conditions are met:

1. The SCP version is 690R1_EN or 691_EN.
2. **API services** and **advanced services** are enabled, check on the SCP web consoles > **System** > **Services**.

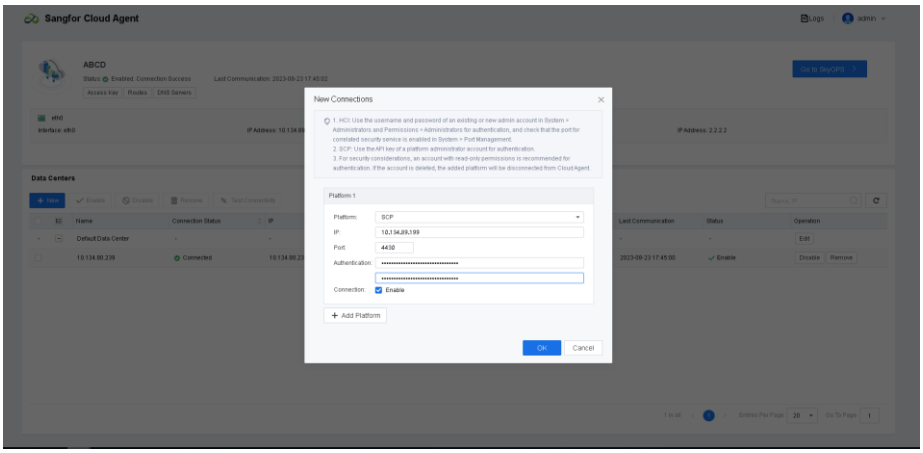




3. Click **Activation Guide** on the SkyOPS page of SCP to obtain the authentication information.



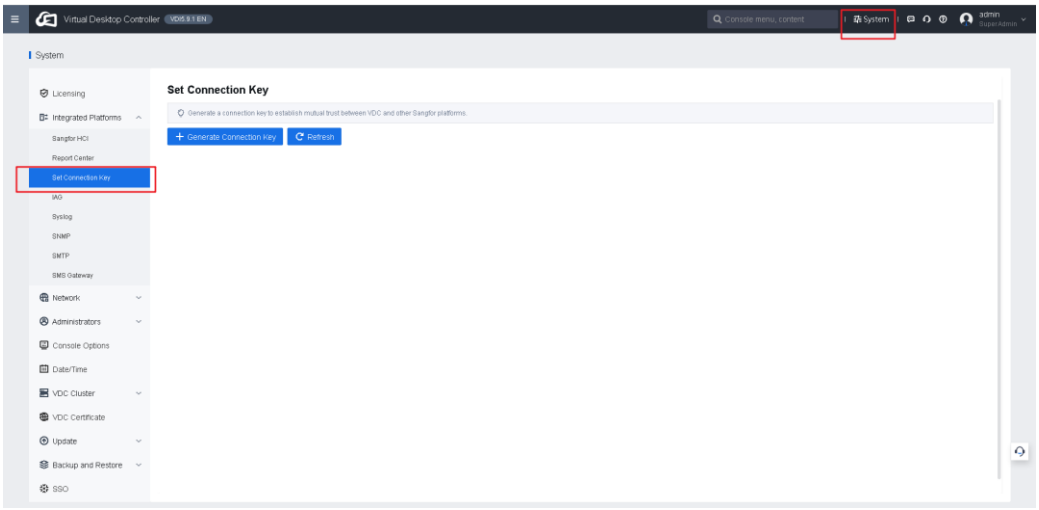
4. Create a new data center on the Cloud Agent and platform select SCP
5. IP is the management IP of SCP
6. The port is 4430 for the single-NIC mode of Cloud Agent, and it is 443 for dual-NIC mode.
7. Enter the authentication information that you have obtained on the SCP.

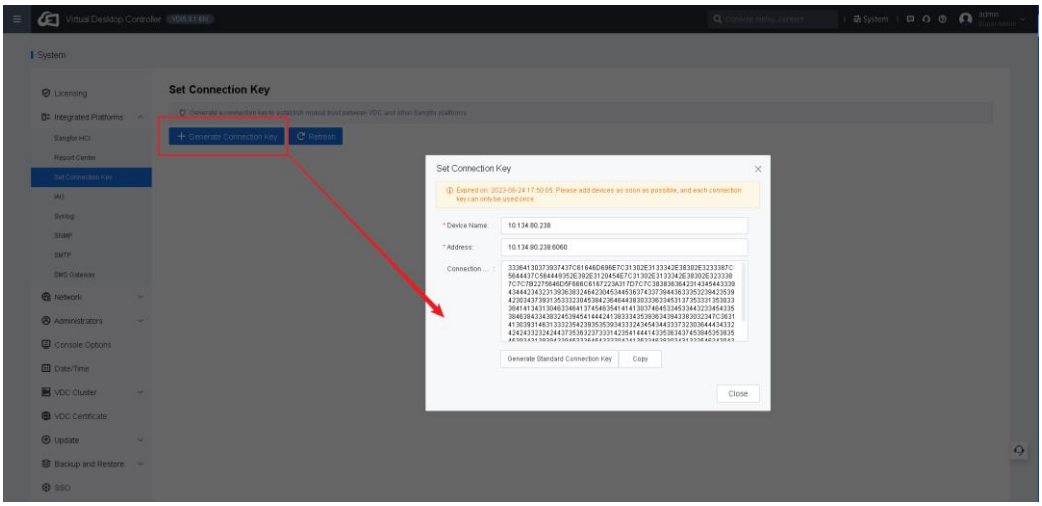


5.3 Connect to VDC

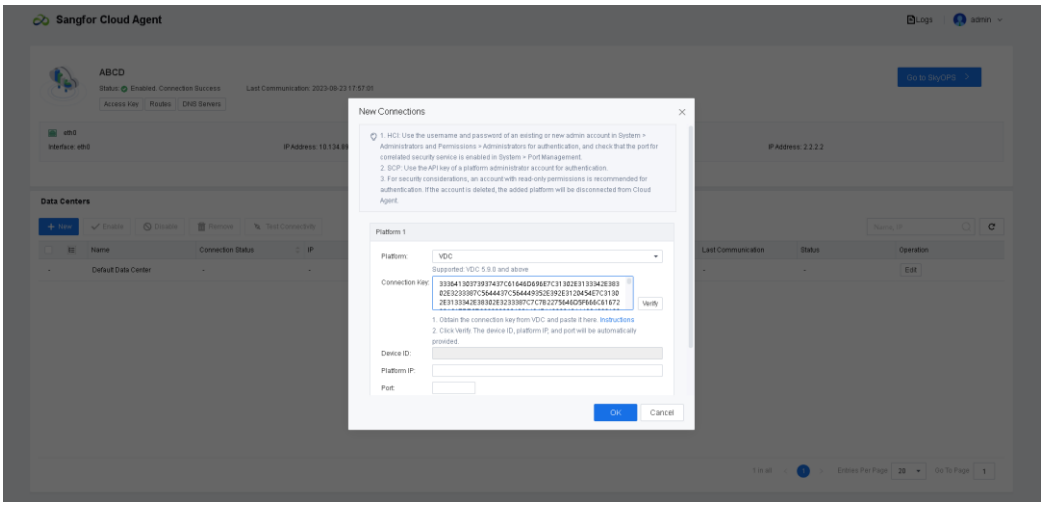
Perform the following operations to connect Cloud Agent to VDC:

Step 1. 1. Log in to VDC and obtain a connection key from **System** > **Integrated Platforms** > **Set Connection Key** > **Generate Connection Key**. Copy the connection key.

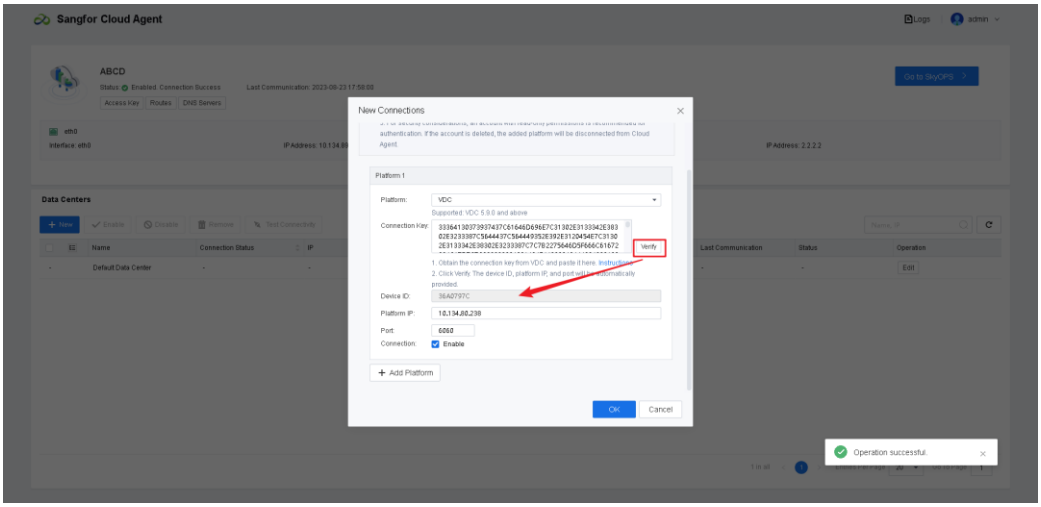




Step 2. 2. Click **New o**n the Sangfor Cloud Agent platform. Paste the connection key obtained from VDC.



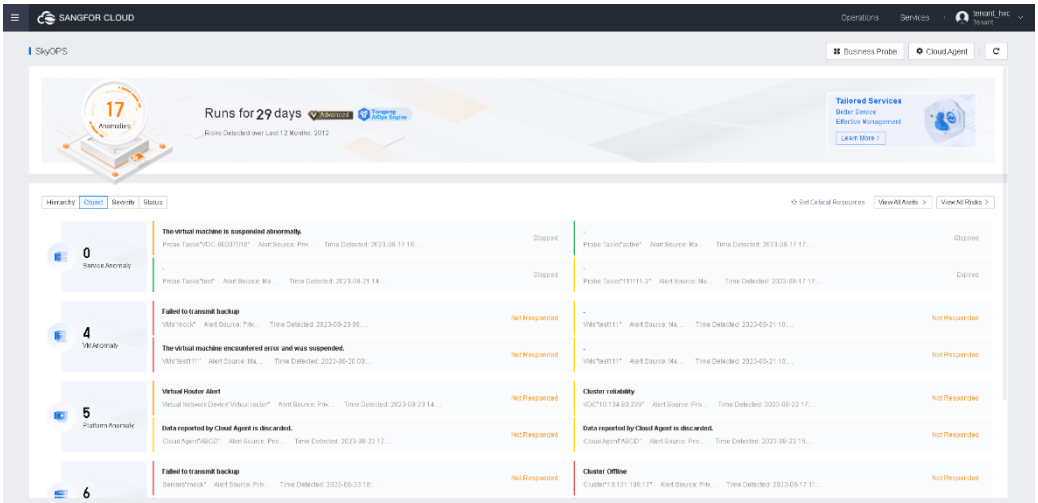
Step 3. 3. Click **Verify**. The device ID, platform IP address, and port are automatically provided. After the connection is established successfully, a record indicating the connection is normal is displayed in the list.

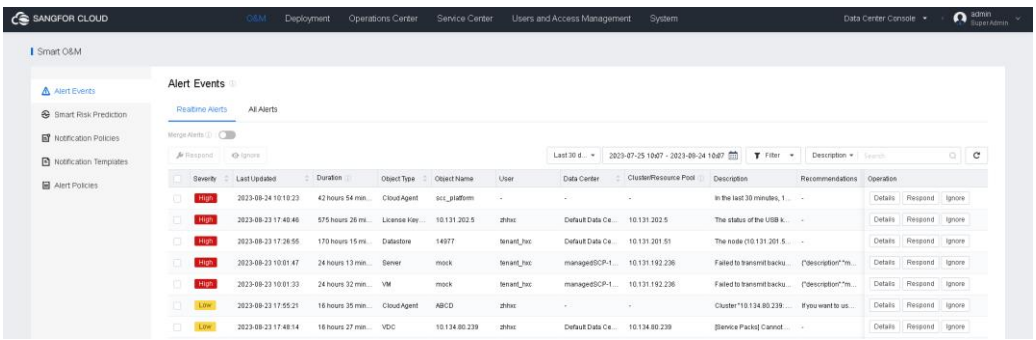


6 Alarms Reporting in SkyOPS

After Cloud Agent is connected to SCP, HCI, or VDC, it will automatically collect unread alerts every 30 seconds and report to Sangfor Cloud.

The MSP admin and Tenants can check the warning logs on the **Smart O&M** > **Alerts** page of Sangfor Cloud.

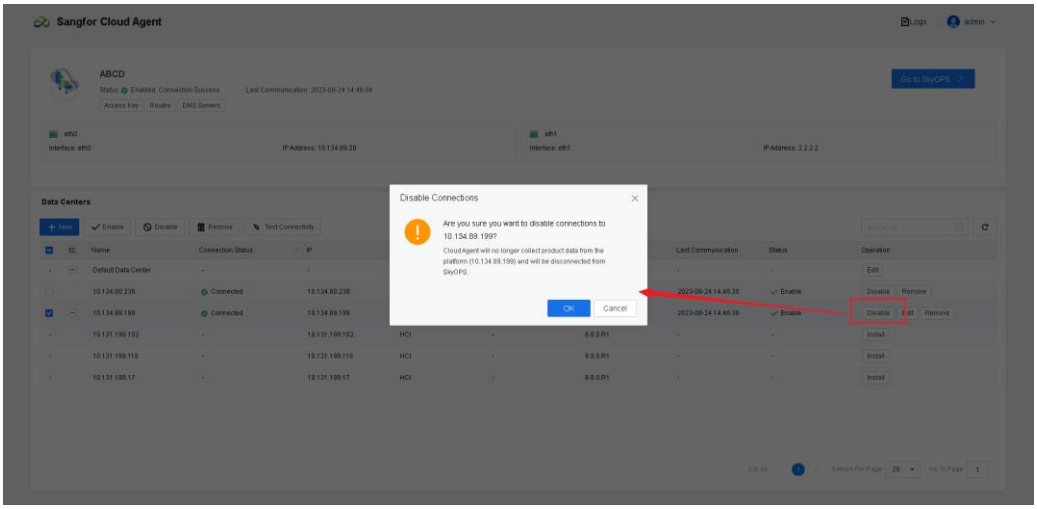


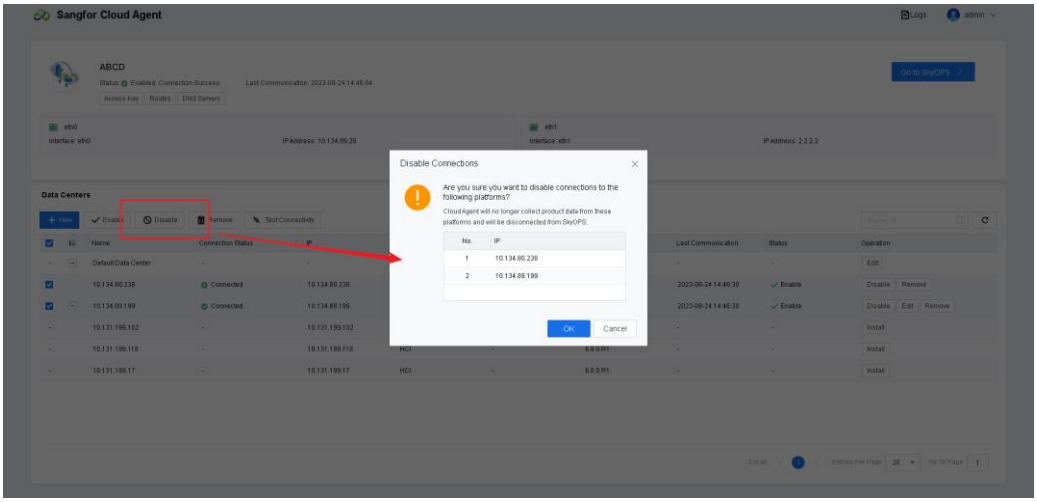


7 Cloud Agent Platform Operations

7.1 Disable Data Center on Cloud Agent

Disable the data center on Cloud Agent. It will stop collecting and uploading logs from this private cloud to MCS.

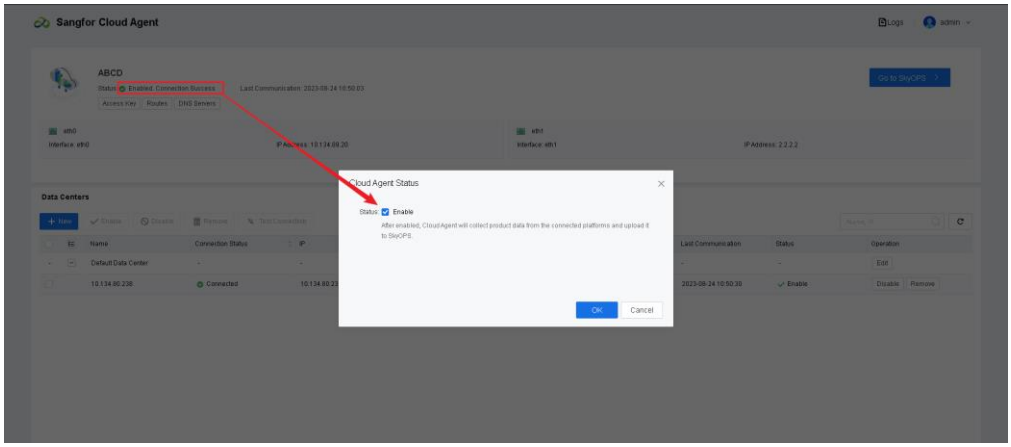




7.2 Enable/Disable Cloud Agent

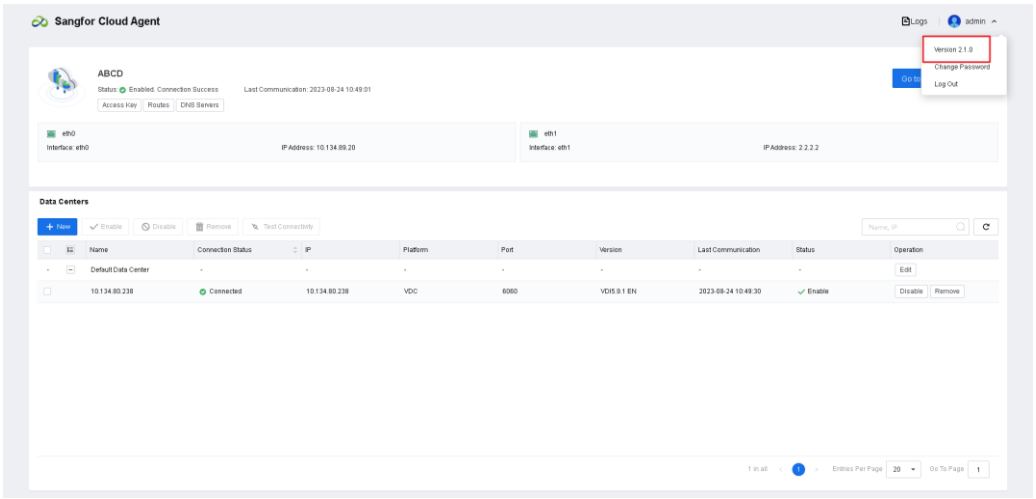
If you disable the Cloud Agent.

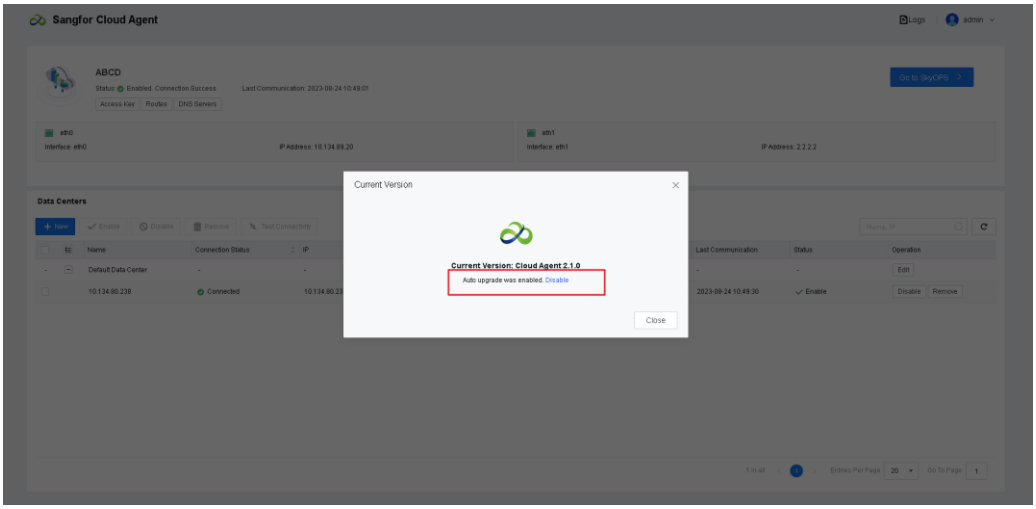
1. It will stop collecting and uploading logs from all private cloud to MCS.
2. Automatic upgrade will be disabled.



7.3 Enable Agent Automatic Upgrade

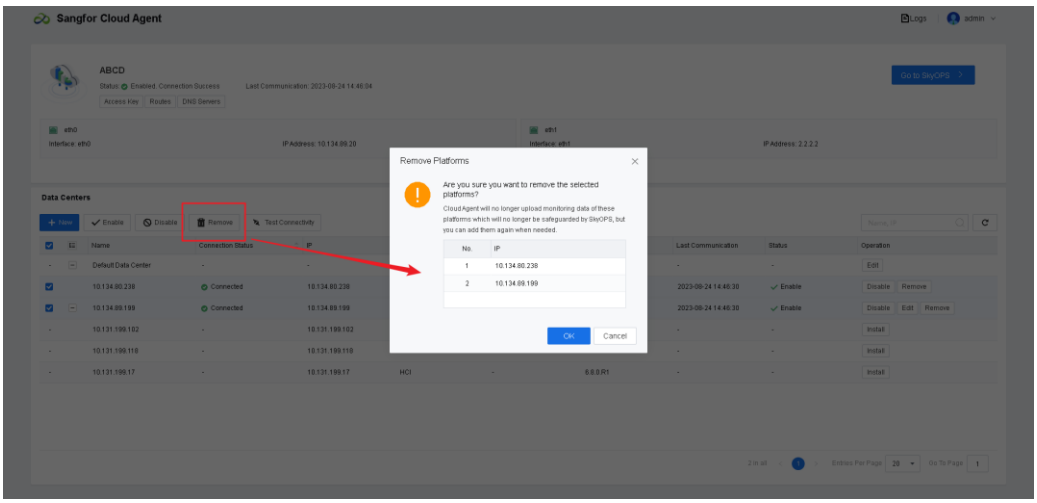
If automatic upgrade is required for Cloud Agent, go to **Sangfor Cloud Agent > Current Version** to enable it. After it is enabled, Cloud Agent will be upgraded using the latest update package with the heartbeat following the release of a new Cloud Agent package. If it is disabled, automatic upgrade will not be performed. It is enabled by default.

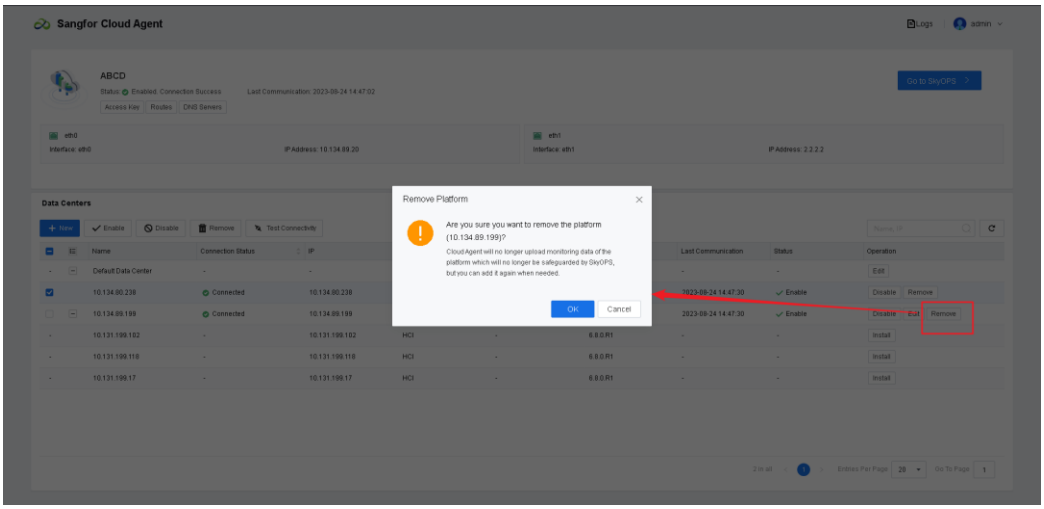




7.4 Remove Data Center

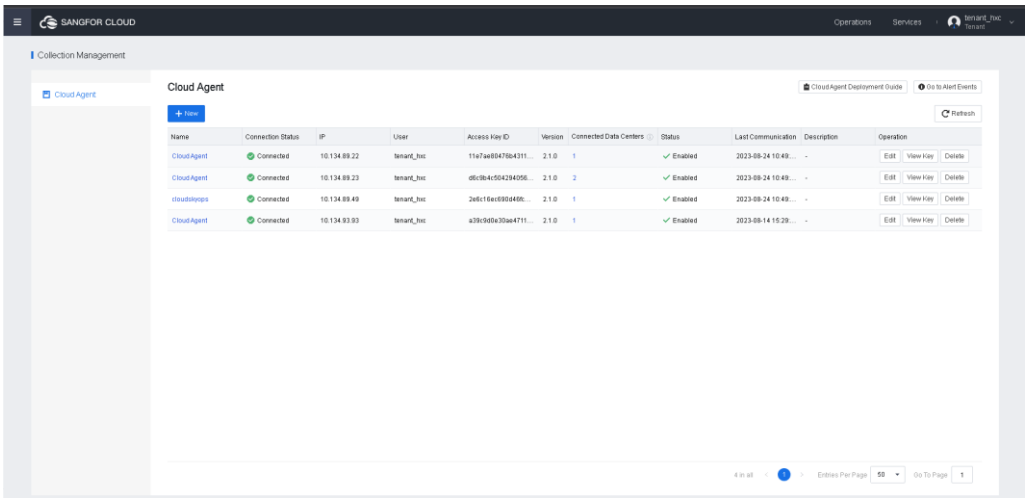
If you remove a data center on Cloud Agent, alerts from the data center will no longer be reported.





7.5 Cloud Agent Management

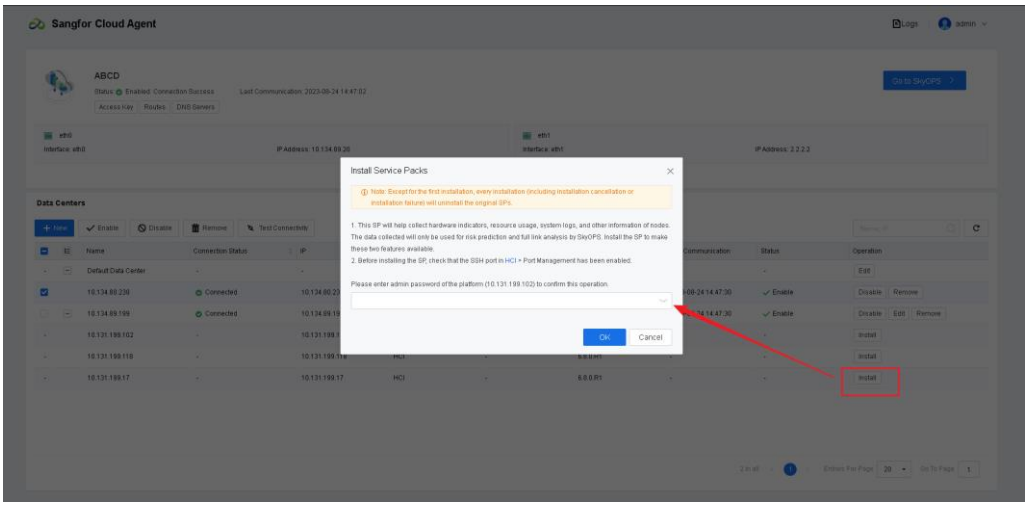
A tenant can go to Sangfor Cloud and choose **Collection Management** > **Cloud Agent** to view the connection status of Cloud Agents.



7.6 Agent Installation

Agent can be installed for the connected HCI platforms on Sangfor Cloud Agent. After successful installation, in **Smart O&M** > **Alerts** of Sangfor Cloud, issue location, full link analysis, and remediation details are displayed. On the **Smart Risk Prediction** page, risks can be viewed and handled in advance (this feature will be available in later versions of Sangfor Cloud).

Applicable versions: HCI 680R1, including the HCI platforms connected to Cloud Agent or managed by SCP platforms that have been connected to Cloud Agent



8 Notes

1. One HCI, SCP, or VDC platform only can connect one Cloud Agent.
2. If a data center is connected to Cloud Agent for the first time, Cloud Agent will obtain unread alerts in the past one month. Cloud Agent send collection request to HCI/SCP/VDI every 30 seconds and collect 50 alerts per time.
3. The Cloud Agent should meet following requirements:
   a) Cloud Agent can connect to Sangfor Cloud.
   b) Manage IP must configure on eth0. Otherwise, redirection from Sangfor Cloud to Cloud Agent may fail.
   c) Can not configure SNAT or DNAT on the Cloud agent.
4. If the Cloud Agent already associated tenant, it required to disable or delete the access key ID or secret key on the existing tenant, remove the Cloud Agent from the Cloud Agent list in Sangfor Cloud. And then associate to a new tenant.
5. If the cloud platform key of Sangfor Cloud tenant co-administrator is configured on Cloud Agent, the tenant co-administrator must have at least permissions for **O&M - Monitoring and Alerts** > **Bulk create alerts** and **SkyOPS** > **Sync Cloud Agent**.
   a) The connection status between Cloud Agent and SkyOPS can be maintained only through the SkyOPS > Sync Cloud Agent interface. An abnormal connection between Cloud Agent and SkyOPS only indicates that data of Cloud Agent and the connected platforms cannot be synchronized to SkyOPS. It does not indicate that HCI alerts cannot be reported to Sangfor Cloud.
   b) If the O&M - Monitoring and Alerts > Bulk create alerts permission is not assigned, alerts from HCI cluster and SCP data center cannot be reported even if the connection to Sangfor Cloud is normal.
6. Before connecting a newly deployed SCP to Cloud Agent, API services and advanced services need to be enabled in System > Services.
7. Default background password of Cloud Agent 2.1.0_EN: Frontend password + sangfor12#$5
8. When you connect Cloud Agent to Sangfor Cloud, make sure that the Sangfor Cloud Agent platform can ping the following two domain names: https://scc-id-jkt.mcs.sangfor.com (domain name of Sangfor Cloud; Cloud Agent needs to be reachable on the network of Sangfor Cloud) and

https://image.sangforcloud.com (domain name of Harbor server; an image needs to be obtained from Harbor server for the automatic upgrade of Cloud Agent).

9. The following scenario do not connect HCI cluster to Cloud Agent, should connect SCP to Cloud Agent
   a) One HCI cluster managed by multiple SCP
   b) HCI cluster already Cluster licensed by SCP, Otherwise, the cluster license may be abnormal, affecting the probe test.
   c) HCI cluster already managed by SCP
10. If the SCP already connected to Cloud Agent, remove HCI from this SCP cannot clear the mark of Cloud Agent automatically. You must manually clear it in the HCI backend: rm -rf /cfs/skyops_config.json. (The HCI can no longer be independently connected to other Cloud Agent if the mark is not cleared.)
11. After the agent is installed for the HCI which is managed by SCP and connected to Cloud Agent, to disable the platform management by SCP, go to the server background and uninstall the agent from nodes using the following command: /sf/data/local/opt/aops/aops-super-agent/aops-agent-service -control uninstall

    If the agent is not uninstalled, spm, spa, and octopus processes will run on the HCI platform. Data will continue to be reported but will not be received by Sangfor Cloud Agent. As a result, data is continuously sent to Sangfor Cloud Agent, and useless processes running on the HCI platform consume resources. There are no other adverse functional impacts.)
12. If the slave node of the HCI cluster has been connected to Sangfor Cloud and installed with the agent, it cannot be installed with the agent after the HCI cluster is connected to Cloud Agent. If the agent needs to be installed, go to the server background and clear the residual agent configuration using the following command: /sf/data/local/opt/aops/aops-super-agent/aops-agent-service -control uninstall
13. SCP platforms that have been connected to Sangfor Cloud and enabled with offline disaster recovery cannot be connected to Cloud Agent.

9 Upgrade

dev upgrade:

Step 4. 1. Access the Cloud Agent background (username: root; port: 22; password: frontend password + suffix of the corresponding version). Upload the dev file to the /sf/data/local/ path:

Step 5. 2. chmod +x xxx.dev file

Step 6. 3. /xxx.dev -icp sangfor.vt@201314

Step 7. 4. reboot

Upgrade through Harbor server: With automatic upgrade enabled on the Sangfor Cloud Agent platform, after a new version is released, automatic upgrade can be performed after 30 minutes.