Sangfor Managed Cloud Service

SkyOPS User Guide

Product Version	V2.2.32
Document Version	V1
Released on	Oct. 07, 2023

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 the Operation and maintenances user guide of MCS.

Intended Audience

This document is intended for:

- tenant

Note Icons

English Icon	Description
⚠DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
⚠WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
⚠CAUTION	Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.
⚠NOTICE	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.
📖NOTE	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
Oct. 07, 2023	This is the first release of this document.

Contents

SkyOPS

Monitoring: The MCS platform can detect anomalies and load on hosts and virtual machines. It also supports adding monitoring charts to track specific metrics of certain virtual machines and can display them in tabular form on the page.

Probe: Users can create probe tasks to perform real-time probe operations to ensure the services work. Once services become unavailable, users will receive alerts to take prompt action.

SkyOPS: 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.

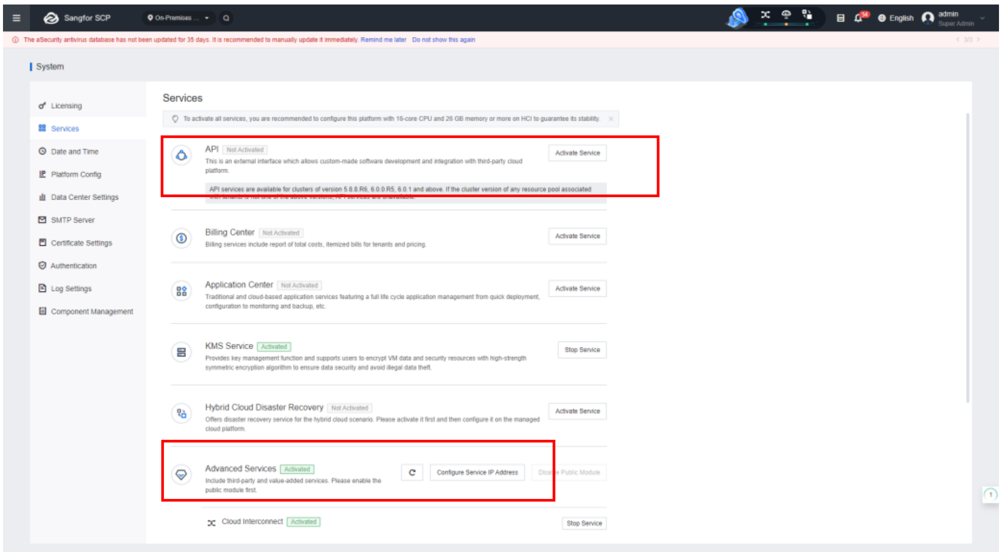
1.1 Private Cloud Resource Connected to Cloud Agent

1.1.1 Prerequisites

1. The local office has deployed the cloud agent virtual machine and can log in to configure it. A cloud agent is an agent probe deployed in a private cloud for on-premise and Managed Cloud data exchange.
2. The cloud agent, local SCP, and MCS are reachable.

1.1.2 Private Cloud SCP connected to Cloud Agents

1. The private cloud SCP **API** and **Advanced Services** must be activated before connecting to cloud agents.



The aSecurity antivirus database has not been updated for 35 days. It is recommended to manually update it immediately. Remind me later Do not show this again

Services

To activate all services, you are recommended to configure this platform with 16-core CPU and 26 GB memory or more on HCI to guarantee its stability.

API Not Activated — Activate Service
This is an external interface which allows custom-made software development and integration with third-party cloud platform.
API services are available for clusters of version 5.8.8.R6, 6.0.0.R5, 6.0.1 and above. If the cluster version of any resource pool associated with tenants is not one of the above versions, API services are unavailable.

Billing Center Not Activated — Activate Service
Billing services include report of total costs, itemized bills for tenants and pricing.

Application Center Not Activated — Activate Service
Traditional and cloud-based application services featuring a full life cycle application management from quick deployment, configuration to monitoring and backup, etc.

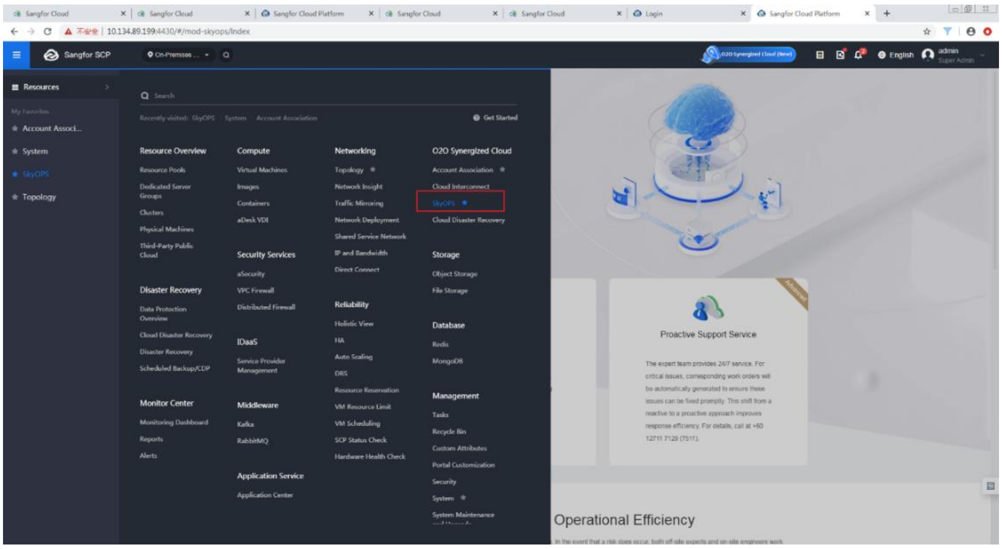
KMS Service Activated — Stop Service
Provides key management function and supports users to encrypt VM data and security resources with high-strength symmetric encryption algorithm to ensure data security and avoid illegal data theft.

Hybrid Cloud Disaster Recovery Not Activated — Activate Service
Offers disaster recovery service for the hybrid cloud scenario. Please activate it first and then configure it on the managed cloud platform.

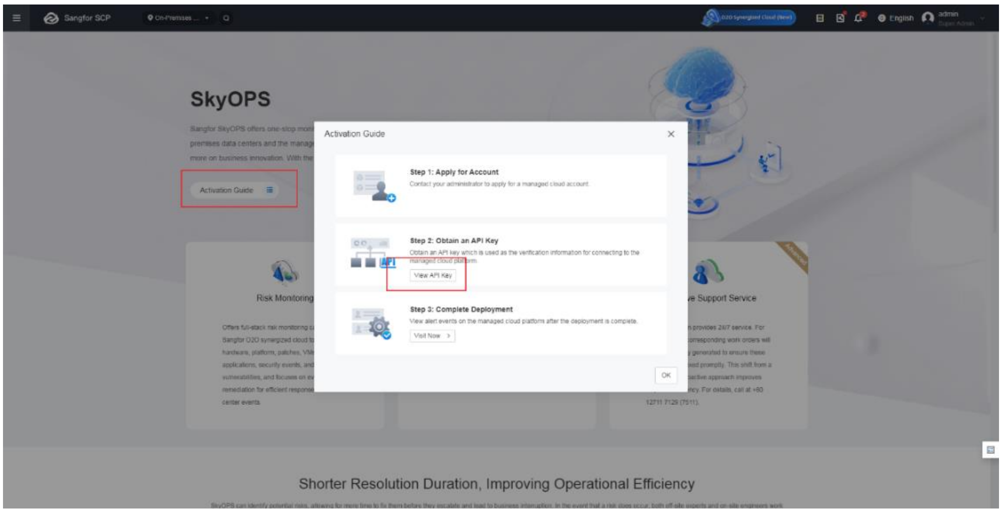
Advanced Services Activated — Configure Service IP Address — Disable Public Module
Include third-party and value-added services. Please enable the public module first.

Cloud Interconnect Activated — Stop Service

2. Obtain AKSK information in the SkyOPS.



The expert team provides 24/7 service. For critical issues, corresponding work orders will be automatically generated to ensure these issues can be fixed promptly. This shift from a reactive to a proactive approach improves response efficiency. For details, call at +60 12711 7129 (7511).



Activation Guide

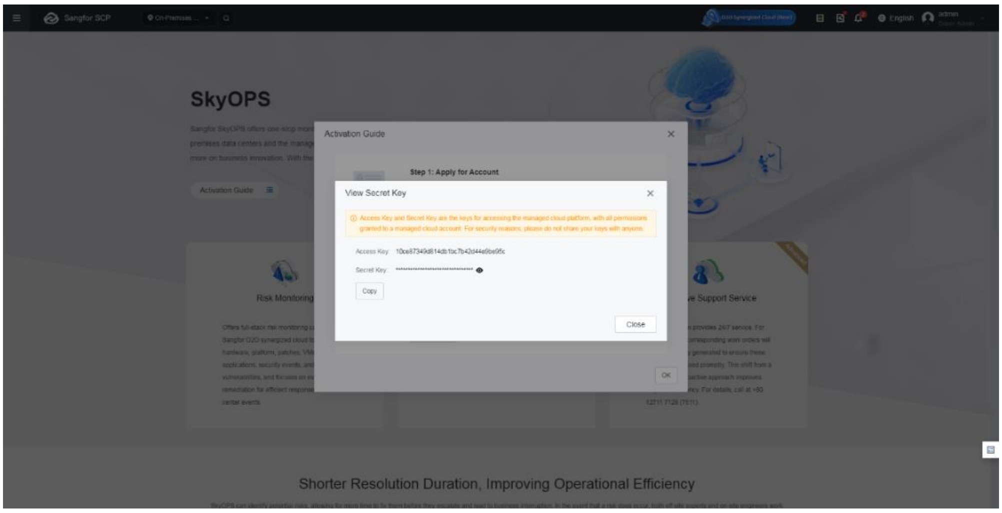
Step 1: Apply for Account
Contact your administrator to apply for a managed cloud account.

Step 2: Obtain an API Key
Obtain an API key which is used as the verification information for connecting to the managed cloud platform.
View API Key

Step 3: Complete Deployment
View alert events on the managed cloud platform after the deployment is complete.
Visit Now >

OK

Shorter Resolution Duration, Improving Operational Efficiency



View Secret Key

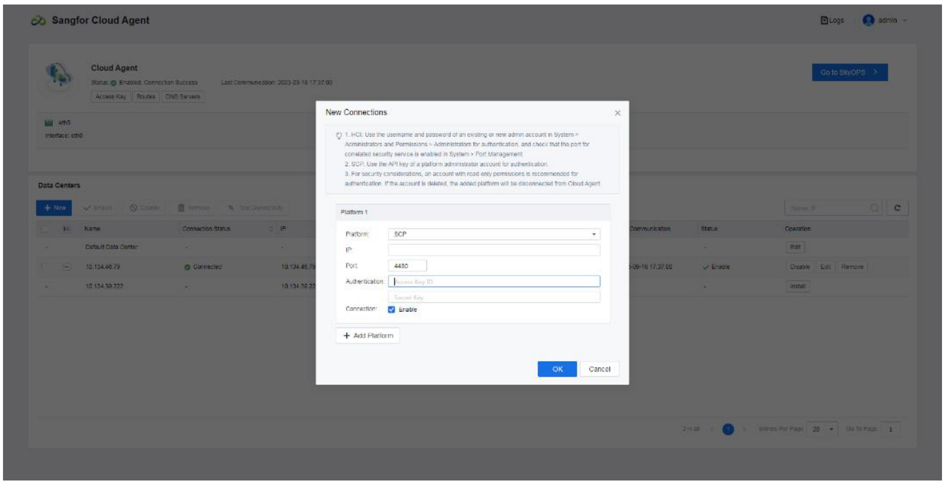
ⓘ Access Key and Secret Key are the keys for accessing the managed cloud platform, with all permissions granted to a managed cloud account. For security reasons, please do not share your keys with anyone.

Access Key: 10ce87349d814db1bc7b42d44e9be95c

Secret Key: ******************************

SkyOPS
Activation Guide
Step 1: Apply for Account
Copy
Close
OK
Risk Monitoring
Shorter Resolution Duration, Improving Operational Efficiency

3. Connect the SCP to cloud agents.



New Connections

1. HCI: Use the username and password of an existing or new admin account in System > Administrators and Permissions > Administrators for authentication, and check that the port for correlated security service is enabled in System > Port Management.
2. SCP: Use the API key of a platform administrator account for authentication.
3. For security considerations, an account with read-only permissions is recommended for authentication. If the account is deleted, the added platform will be disconnected from Cloud Agent.

Platform 1

Platform: SCP

IP:

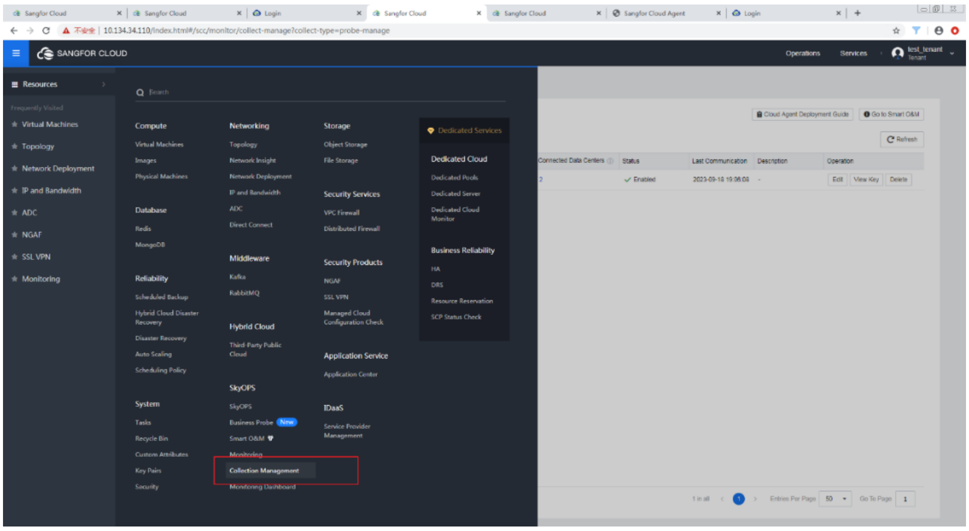
Port: 4430

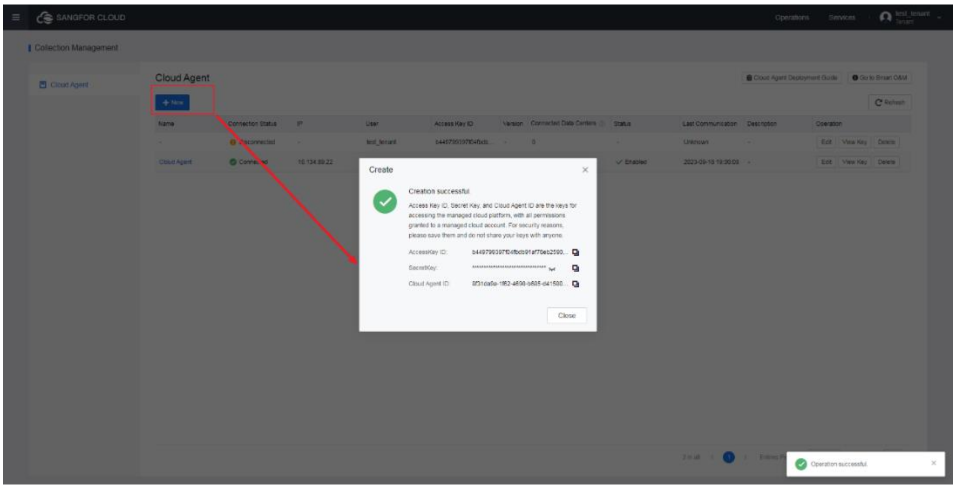
Authentication: Access Key ID / Secret Key

Connection: ☑ Enable

1.1.3 Cloud Agent Connected to MCS

1. Obtain cloud agent information from the managed cloud tenant, then input the Cloud Agent ID to connect to the Sangfor Cloud Service Center.





Create

Creation successful

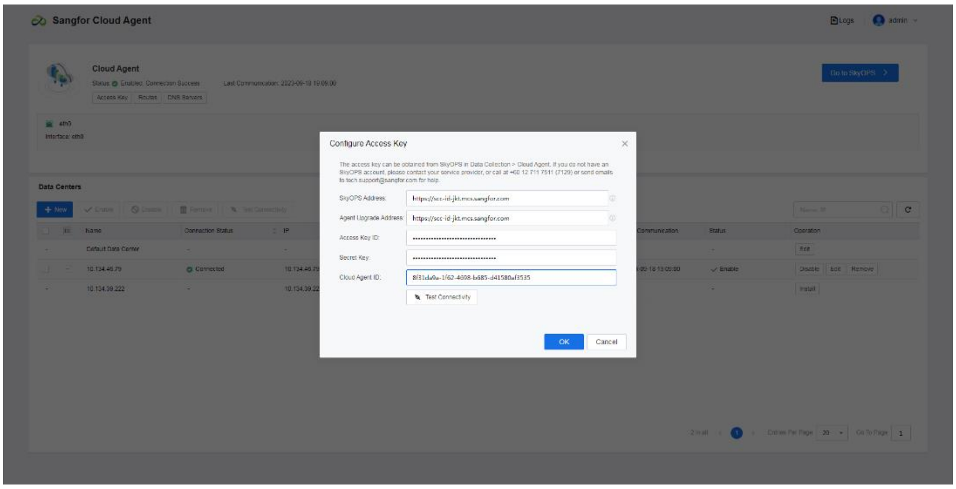
Access Key ID, Secret Key, and Cloud Agent ID are the keys for accessing the managed cloud platform, with all permissions granted to a managed cloud account. For security reasons, please save them and do not share your keys with anyone.

AccessKey ID: b449799397f04fbdb91af78eb2590...

SecretKey: ********************************

Cloud Agent ID: 8f31da9a-1f62-4690-b685-d41580...

Close



Configure Access Key

The access key can be obtained from SkyOPS in Data Collection > Cloud Agent. If you do not have an SkyOPS account, please contact your service provider, or call at +60 12 711 7511 (7129) or send emails to tech support@sangfor.com for help.

SkyOPS Address: https://scc-id-jkt.mcs.sangfor.com

Agent Upgrade Address: https://scc-id-jkt.mcs.sangfor.com

Access Key ID: ********************************

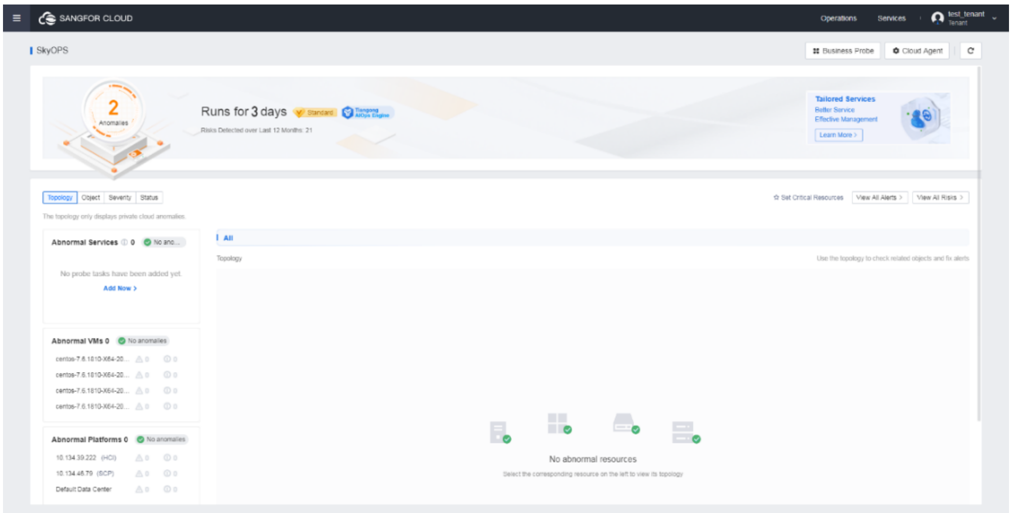
Secret Key: ********************************

Cloud Agent ID: 8f31da9a-1f62-4698-b685-d41580af3535

Test Connectivity

OK Cancel

2. After successfully connecting, users will be directed to the SkyOPS page on their next login.



The topology only displays private cloud anomalies.

No probe tasks have been added yet.

Use the topology to check related objects and fix alerts

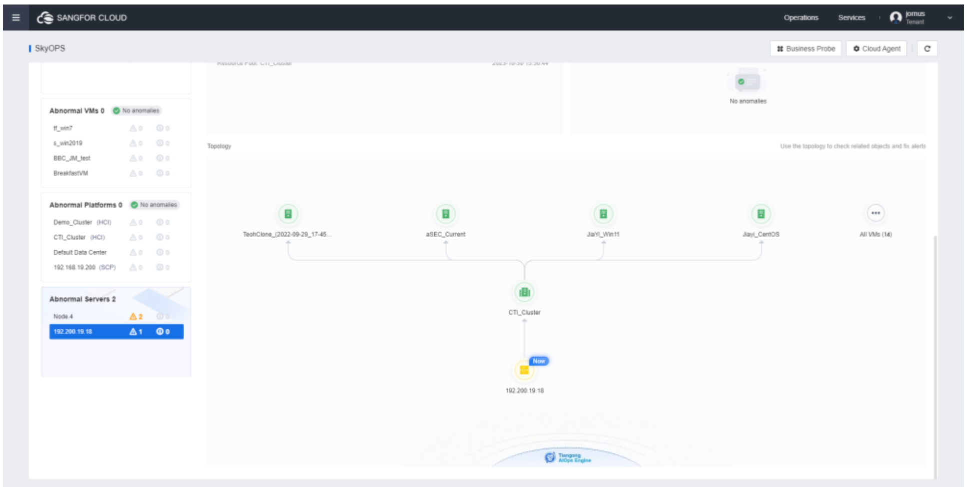
No abnormal resources

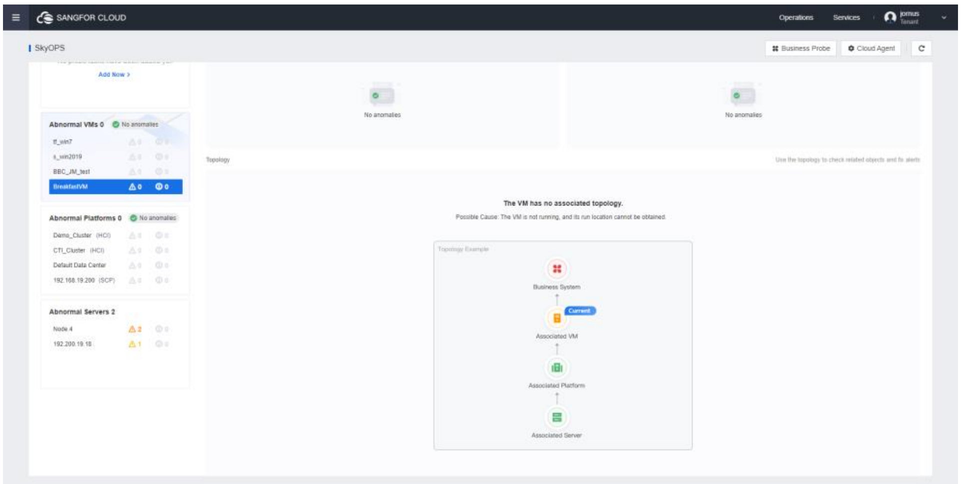
Select the corresponding resource on the left to view its topology

1.2 Viewing SkyOPS

1.2.1 Viewing Private Cloud Resource Hierarchy

1. The tenant SkyOPS has a new feature: the business service topology map. It can display the hierarchy of resources under the cloud agent and the association of tenants' LAN probe tasks. The topology will not display the node's topology if it has no association.

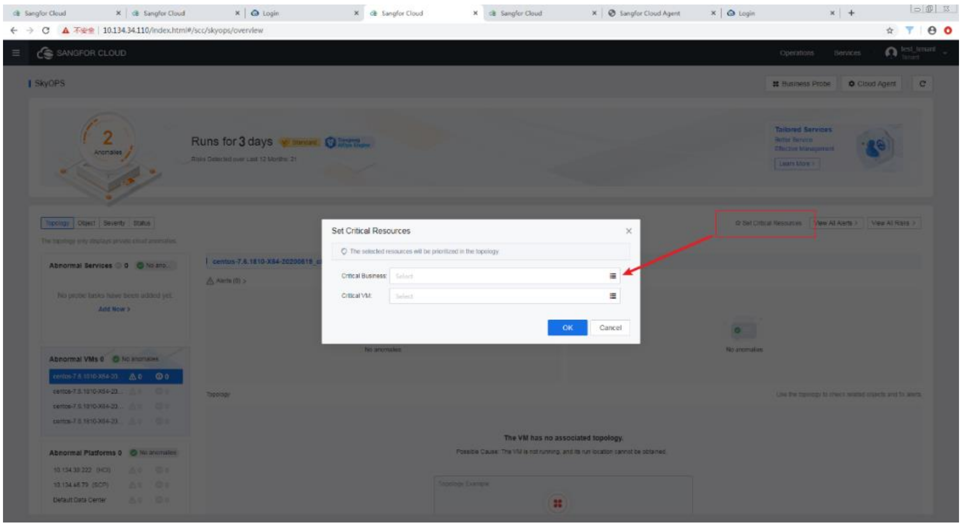




The VM has no associated topology.

Possible Cause: The VM is not running, and its run location cannot be obtained.

2. Tenants can set the **Critical business services, Databases**, and **VMs** to be prioritized in the topology in SkyOPS.



Set Critical Resources

The selected resources will be prioritized in the topology

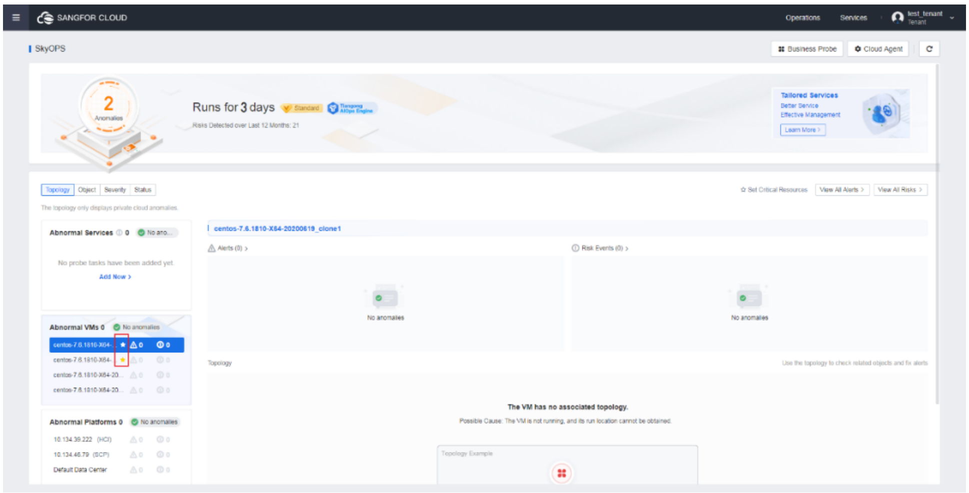
Critical Business: Select

Critical VM: Select

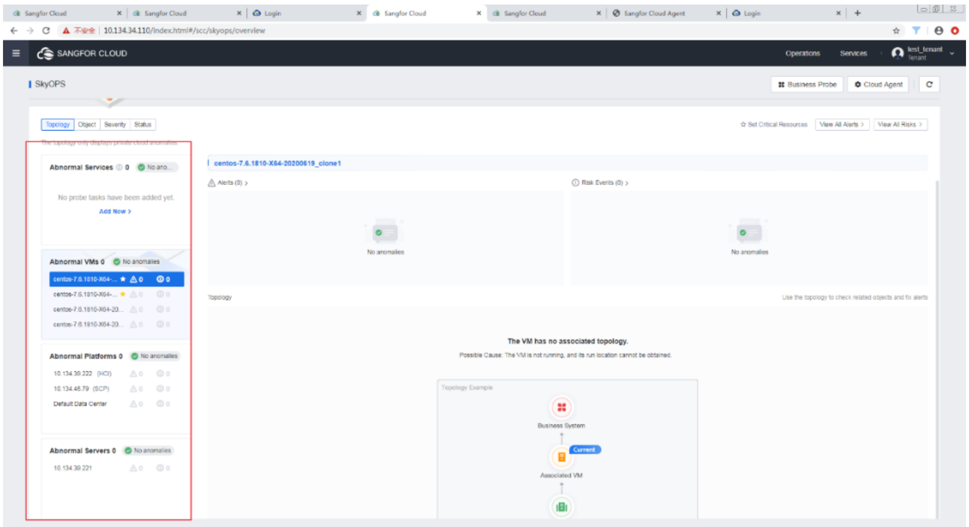
OK Cancel

The VM has no associated topology.

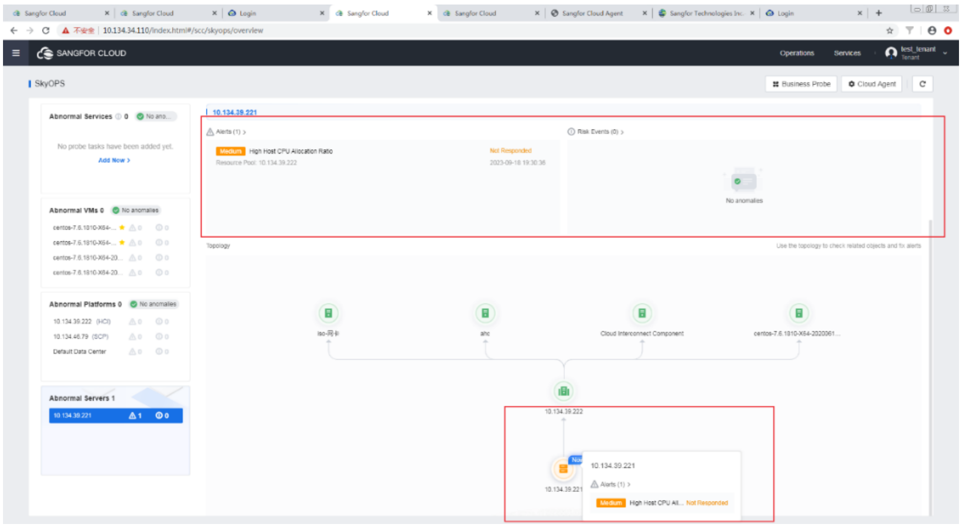
Possible Cause: The VM is not running, and its run location cannot be obtained.



3. The tenant SkyOPS displays abnormal resources on the left. When no anomalies exist, four resource information items are shown by default. It will show all abnormal resources if there are any.

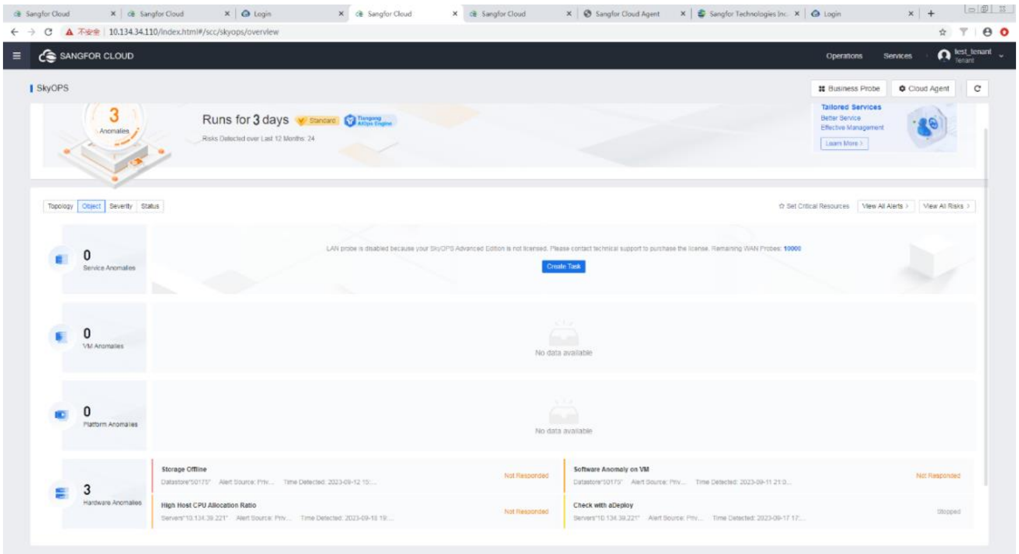


4. Tenants can view the 20 most recent alerts and risk events. The business service topology shows the three most recent alerts and risk events of associated resources.



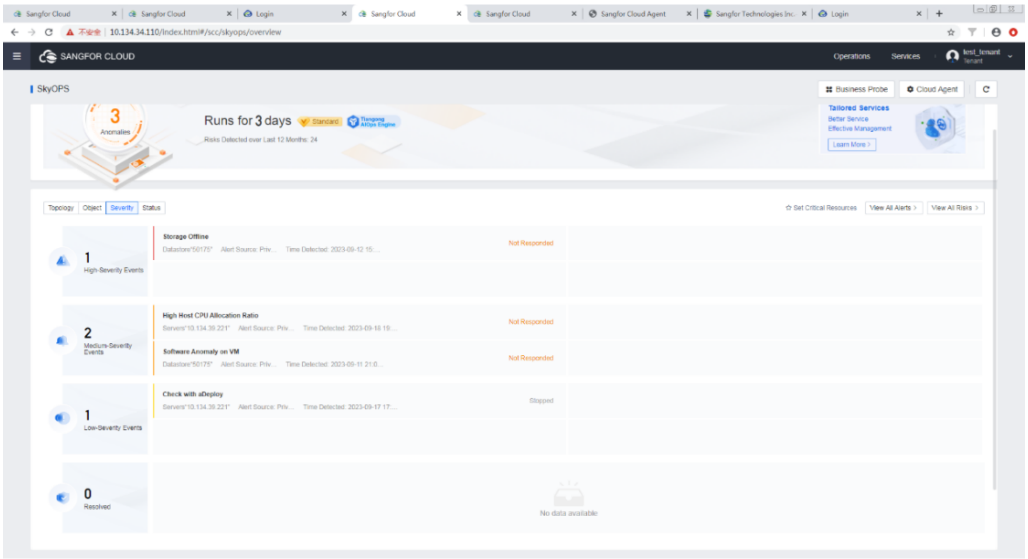
1.2.2 Viewing Private Cloud Alert Events by Object

In SkyOPS, tenants can view different alert events reported on the private cloud, including service anomalies, VM anomalies, platform anomalies, and hardware anomalies.



1.2.3 Viewing Private Cloud Alert Events by Severity

In SkyOPS, tenants can view alert events with different severities reported on the private cloud, including high-severity events, medium-severity events, low-severity events, and resolved events.



1 High-Severity Events

- Storage Offline — Datastore"50175" Alert Source: Priv... Time Detected: 2023-09-12 15:... — Not Responded

2 Medium-Severity Events

- High Host CPU Allocation Ratio — Servers"10.134.39.221" Alert Source: Priv... Time Detected: 2023-09-18 19:... — Not Responded
- Software Anomaly on VM — Datastore"50175" Alert Source: Priv... Time Detected: 2023-09-11 21:0... — Not Responded

1 Low-Severity Events

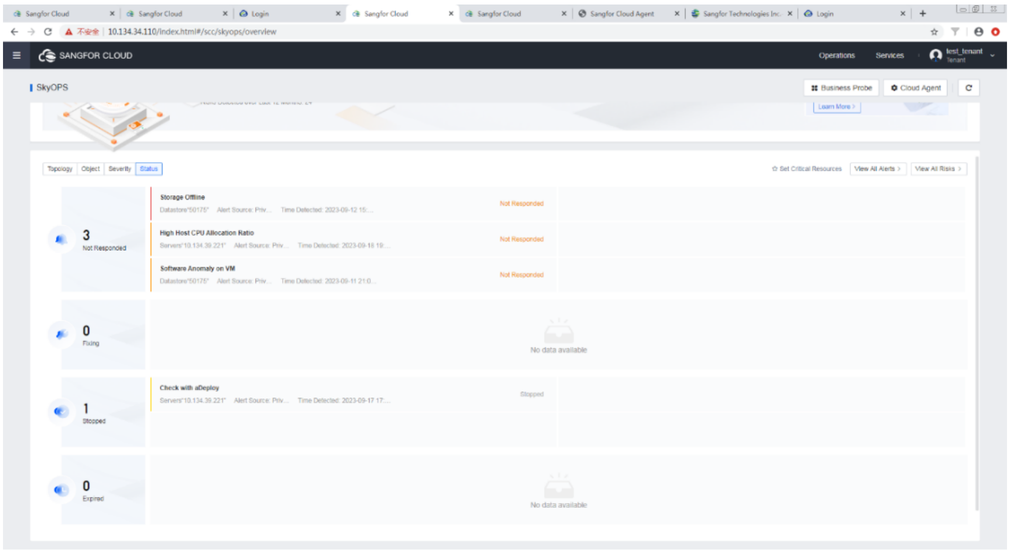
- Check with aDeploy — Servers"10.134.39.221" Alert Source: Priv... Time Detected: 2023-09-17 17:... — Stopped

0 Resolved

No data available

1.2.4 Viewing Private Cloud Alert Events by Status

In SkyOPS, tenants can view the status of alert events reported on the private cloud, including Not Responded, Fixing, Stopped, and Expired.



3 Not Responded

- Storage Offline — Datastore"50175" Alert Source: Priv... Time Detected: 2023-09-12 15:... — Not Responded
- High Host CPU Allocation Ratio — Servers"10.134.39.221" Alert Source: Priv... Time Detected: 2023-09-18 19:... — Not Responded
- Software Anomaly on VM — Datastore"50175" Alert Source: Priv... Time Detected: 2023-09-11 21:0... — Not Responded

0 Fixing

No data available

1 Stopped

- Check with aDeploy — Servers"10.134.39.221" Alert Source: Priv... Time Detected: 2023-09-17 17:... — Stopped

0 Expired

No data available

1.3 Business Probe

1.3.1 Introduction

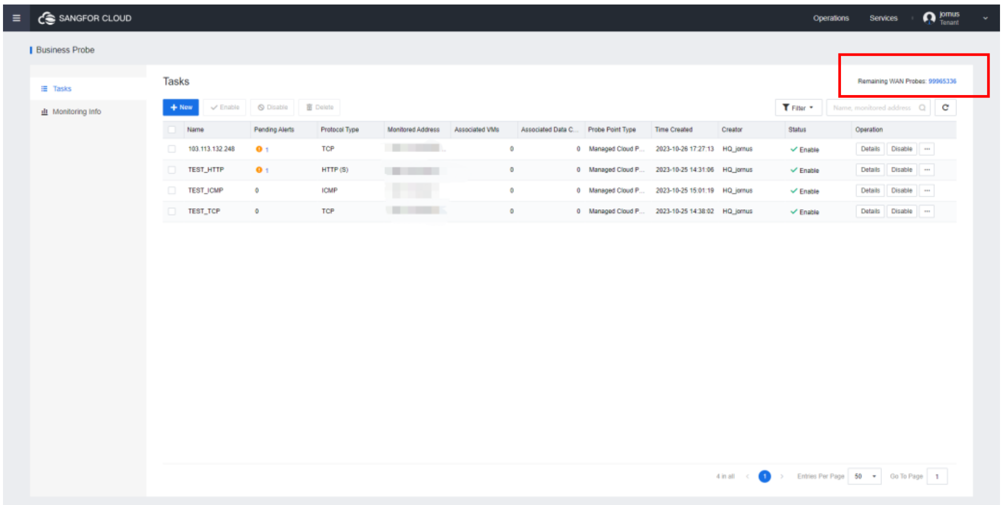
Create a business probe task to conduct a real-time probe of your business to ensure the service is available. When the service is unavailable, you can receive an alarm notification as soon as possible and handle it on time. We support business probes of MCS tenant services and private cloud tenant services.

In the MCS scenario, creating a business probe task can monitor the availability of public network services in real time, including the manage service cloud and private cloud, ensuring the business's operation. By regularly probing public network services, tenants can promptly detect service failures or abnormalities and repair them to avoid business interruption or impact on user experience. The business probe task can also help tenants understand the performance and stability of public network services and provide data support for service optimization and improvement.

1.3.2 Obtain Business Probe Service

1.3.2.1 MCS Tenant Obtain Business Probe Service

This function requires authorization from the administrator first. The tenant can create an MCS business probe task on the business probe page. The **Remaining WAN probe** in the top right corner shows the remaining authorization.



Remaining WAN Probes: 99965336

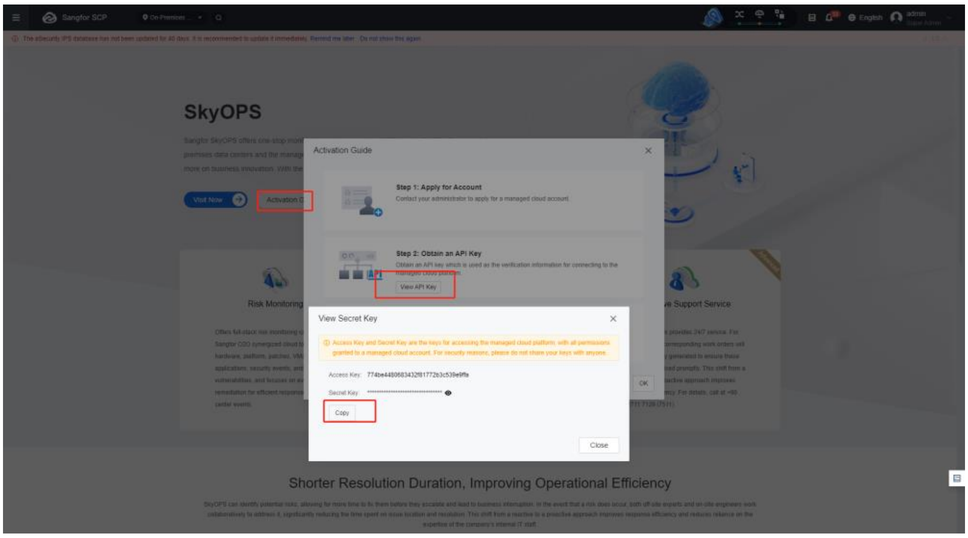
Name	Pending Alerts	Protocol Type	Monitored Address	Associated VMs	Associated Data C...	Probe Point Type	Time Created	Creator	Status	Operation
103.113.132.248	● 1	TCP	[redacted]	0	0	Managed Cloud P...	2023-10-26 17:27:13	HQ_jomus	✓ Enable	Details Disable ···
TEST_HTTP	● 1	HTTP (S)	[redacted]	0	0	Managed Cloud P...	2023-10-25 14:31:06	HQ_jomus	✓ Enable	Details Disable ···
TEST_ICMP	0	ICMP	[redacted]	0	0	Managed Cloud P...	2023-10-25 15:01:19	HQ_jomus	✓ Enable	Details Disable ···
TEST_TCP	0	TCP	[redacted]	0	0	Managed Cloud P...	2023-10-25 14:38:02	HQ_jomus	✓ Enable	Details Disable ···

1.3.2.2 Private Cloud Tenant Obtain Business Probe Service

In the private cloud scenario, a virtual machine is deployed on the local SCP as a cloud agent, and one cloud agent is a probe point.

1. Administrator log in to SCP and navigate to **Resource > O2O Synergized Cloud > SkyOPS**.

2. Click **Activation Guide > View API Key** to obtain the **Access Key** and **Secret Key**.


Sangfor SCP
SkyOPS
Visit Now
Activation G
Activation Guide
Step 1: Apply for Account
Step 2: Obtain an API Key
View API Key
Risk Monitoring
View Secret Key
Copy
Close
OK
Shorter Resolution Duration, Improving Operational Efficiency

Contact your administrator to apply for a managed cloud account.

Obtain an API key which is used as the verification information for connecting to the managed cloud platform.

Access Key and Secret Key are the keys for accessing the managed cloud platform, with all permissions granted to a managed cloud account. For security reasons, please do not share your keys with anyone.

Access Key: 774be4480683432f81772b3c539e9ffa

Secret Key: ********************************

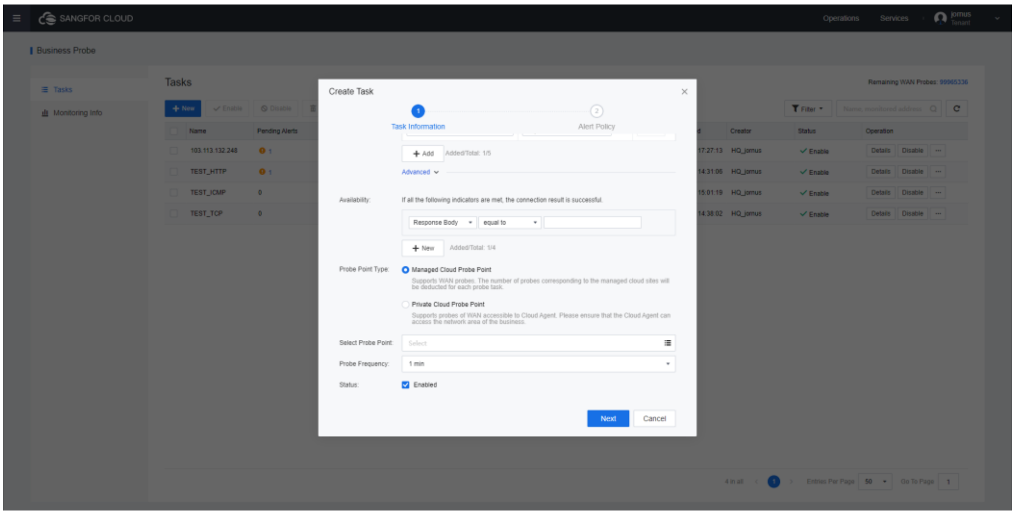
3. Provide the obtained keys to the MCS team, and they will connect the SCP of the private cloud to MCS. After successfully connecting, **Visit Now** will appear on this page, and you can start using the business probe function.

1.3.3 Probe Point Configuration

Private cloud, managed cloud, and hybrid cloud tenants can regularly run probes on WAN or LAN services for real-time monitoring, ensuring task feasibility.

1.3.3.1 Managed Cloud Probe Point

Please contact the Managed Cloud team for deployment for the Managed Cloud Probe Point. Under normal circumstances, it has already been deployed. As shown in the figure below:



Added/Total: 1/5

Availability: If all the following indicators are met, the connection result is successful.

Response Body | equal to

Added/Total: 1/4

Probe Point Type: ● Managed Cloud Probe Point

Supports WAN probes. The number of probes corresponding to the managed cloud sites will be deducted for each probe task.

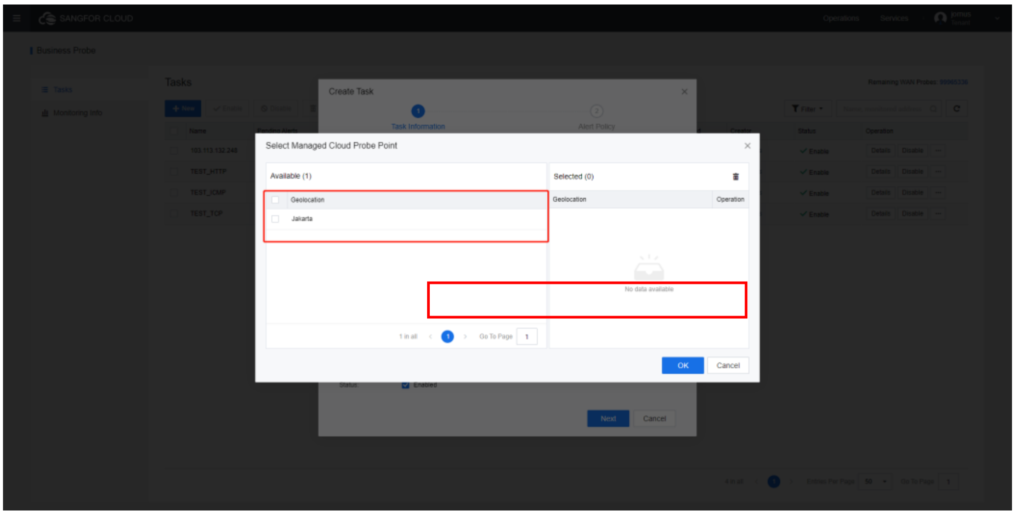
○ Private Cloud Probe Point

Supports probes of WAN accessible to Cloud Agent. Please ensure that the Cloud Agent can access the network area of the business.

Select Probe Point: Select

Probe Frequency: 1 min

Status: ☑ Enabled



Available (1)

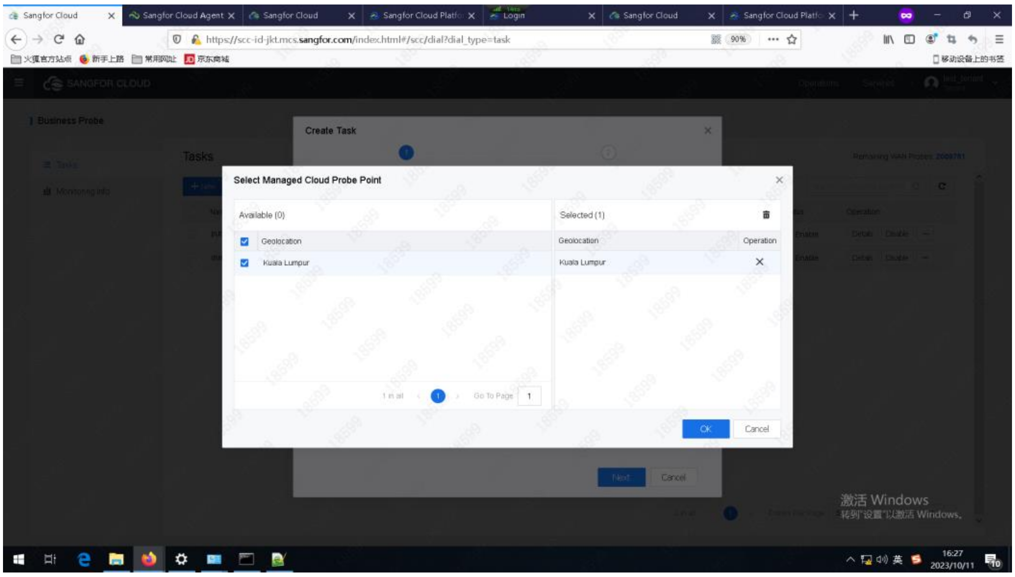
□	Geolocation
□	Jakarta

1 in all 1 Go To Page 1

Selected (0)

Geolocation	Operation

No data available



https://scc-id-jkt.mcs.sangfor.com/index.html#/scc/dial?dial_type=task

Available (0)

☑	Geolocation
☑	Kuala Lumpur

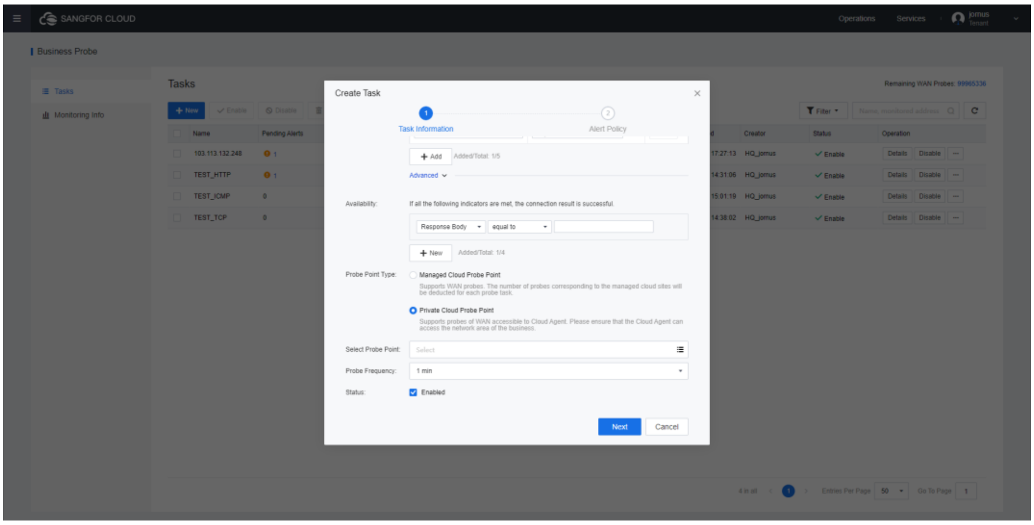
1 in all 1 Go To Page 1

Selected (1)

Geolocation	Operation
Kuala Lumpur	×

1.3.3.2 Private Cloud Probe Point

Please contact the local office to assist with deployment. One cloud agent is a probe point, as shown in the figure below.



Create Task

1 Task Information — 2 Alert Policy

Added/Total: 1/5

Availability: If all the following indicators are met, the connection result is successful.

Response Body | equal to

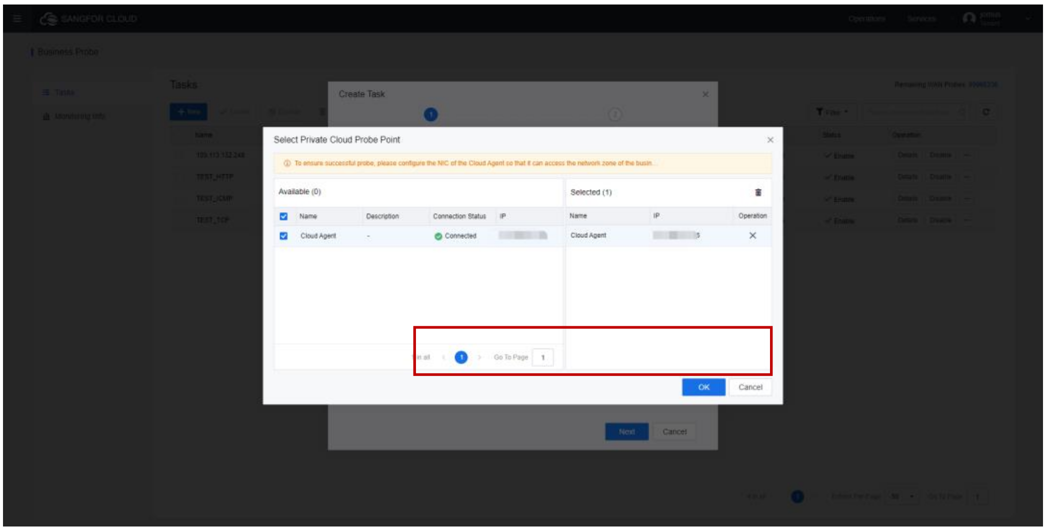
Added/Total: 1/4

Probe Point Type:
- ○ Managed Cloud Probe Point — Supports WAN probes. The number of probes corresponding to the managed cloud sites will be deducted for each probe task.
- ● Private Cloud Probe Point — Supports probes of WAN accessible to Cloud Agent. Please ensure that the Cloud Agent can access the network area of the business.

Select Probe Point: Select

Probe Frequency: 1 min

Status: ☑ Enabled



Select Private Cloud Probe Point

ⓘ To ensure successful probe, please configure the NIC of the Cloud Agent so that it can access the network zone of the busin...

Available (0)

☑	Name	Description	Connection Status	IP
☑	Cloud Agent	-	Connected	[redacted]

Selected (1)

Name	IP	Operation
Cloud Agent	[redacted]	✕

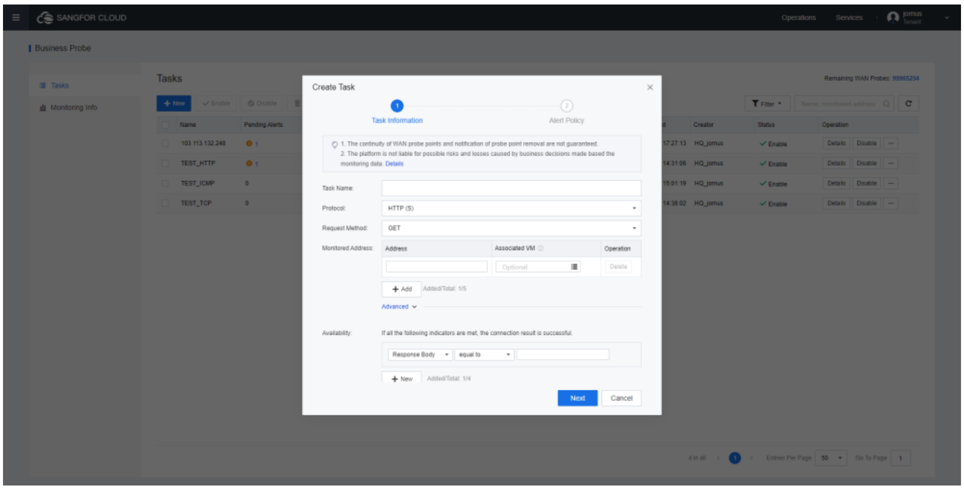
1.3.4 Creating Probe Task

Tenants can create probe tasks to monitor the availability of WAN services in real-time, ensuring the operation of services. By running probes on WAN services regularly, the tenants can detect service faults or anomalies promptly and adopt remedial measures to prevent service interruptions or a negative impact on user experience.

1.3.4.1 Task Information

1. Navigate to **SkyOPS > Business Probe > Tasks** to create a probe task.

2. Click **New**, and **Availability** indicators are available in the drop-down list.



Create Task

1 Task Information — 2 Alert Policy

1. The continuity of WAN probe points and notification of probe point removal are not guaranteed.
2. The platform is not liable for possible risks and losses caused by business decisions made based the monitoring data. Details

Task Name:

Protocol: HTTP (S)

Request Method: GET

Monitored Address:

Address	Associated VM	Operation
	Optional	Delete

+ Add Added/Total: 1/5

Advanced

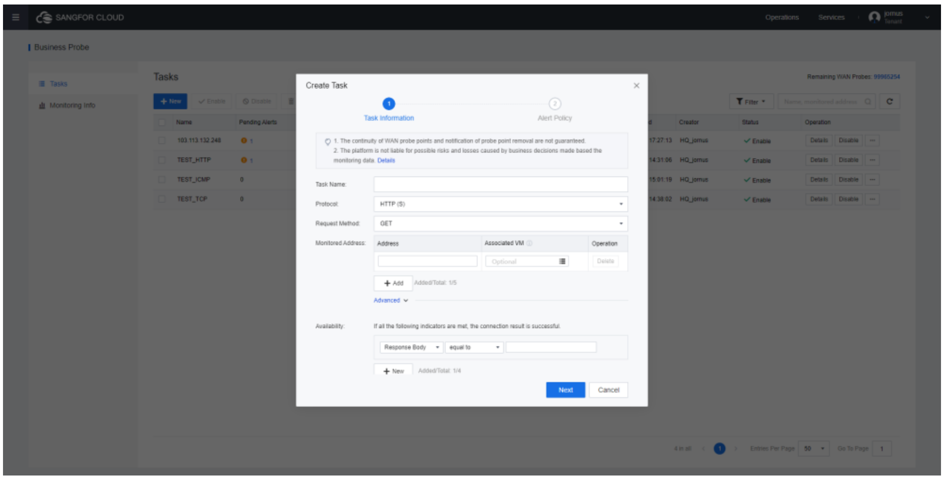
Availability: If all the following indicators are met, the connection result is successful.

Response Body ▾ equal to ▾

+ New Added/Total: 1/4

Next Cancel

3. Indicators for HTTP probe tasks: **Response Time**, **Status Code**, **Response Header**, and **Response Body**. Indicators for TCP probe tasks: **Response Time**. Indicators for ICMP probe tasks: **Packet Loss Rate** and **Response Time**.



Create Task

1 Task Information — 2 Alert Policy

1. The continuity of WAN probe points and notification of probe point removal are not guaranteed.
2. The platform is not liable for possible risks and losses caused by business decisions made based the monitoring data. Details

Task Name:

Protocol: HTTP (S)

Request Method: GET

Monitored Address:

Address	Associated VM	Operation
	Optional	Delete

+ Add Added/Total: 1/5

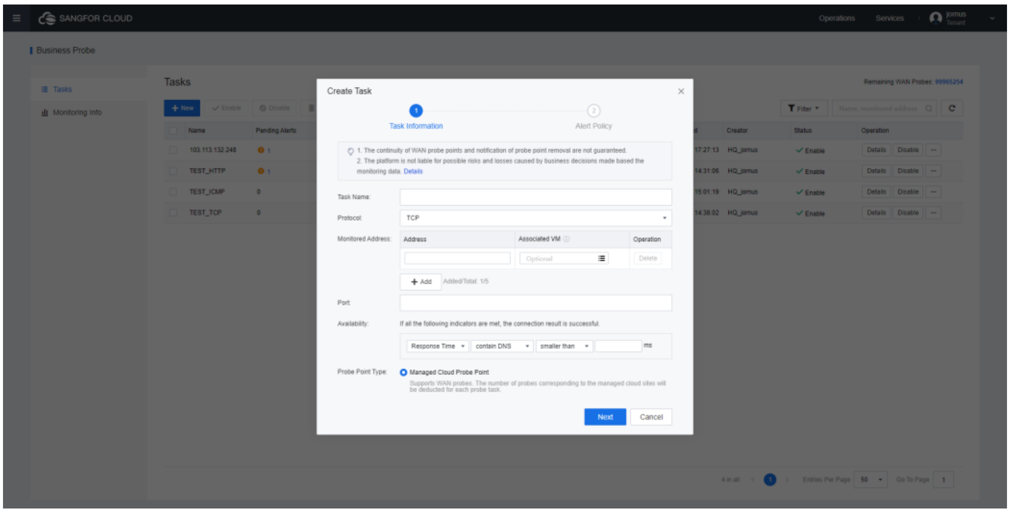
Advanced

Availability: If all the following indicators are met, the connection result is successful.

Response Body ▾ equal to ▾

+ New Added/Total: 1/4

Next Cancel



1. The continuity of WAN probe points and notification of probe point removal are not guaranteed.
2. The platform is not liable for possible risks and losses caused by business decisions made based the monitoring data. Details

Task Name:

Protocol: TCP

Monitored Address: Address | Associated VM | Operation — Optional — Delete

+ Add Added/Total: 1/5

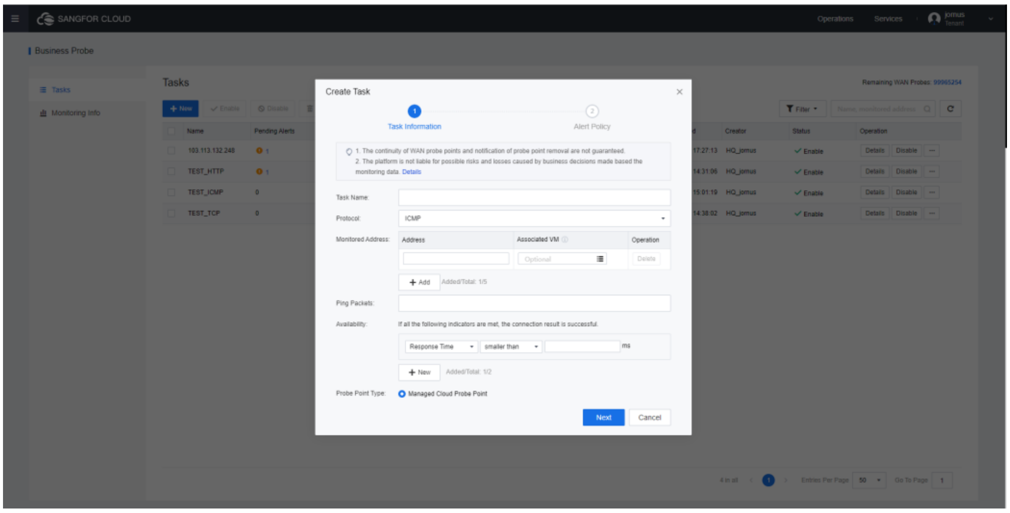
Port:

Availability: If all the following indicators are met, the connection result is successful.

Response Time · contain DNS · smaller than · ms

Probe Point Type: ● Managed Cloud Probe Point

Supports WAN probes. The number of probes corresponding to the managed cloud sites will be deducted for each probe task.



1. The continuity of WAN probe points and notification of probe point removal are not guaranteed.
2. The platform is not liable for possible risks and losses caused by business decisions made based the monitoring data. Details

Task Name:

Protocol: ICMP

Monitored Address: Address | Associated VM | Operation — Optional — Delete

+ Add Added/Total: 1/5

Ping Packets:

Availability: If all the following indicators are met, the connection result is successful.

Response Time · smaller than · ms

+ New Added/Total: 1/2

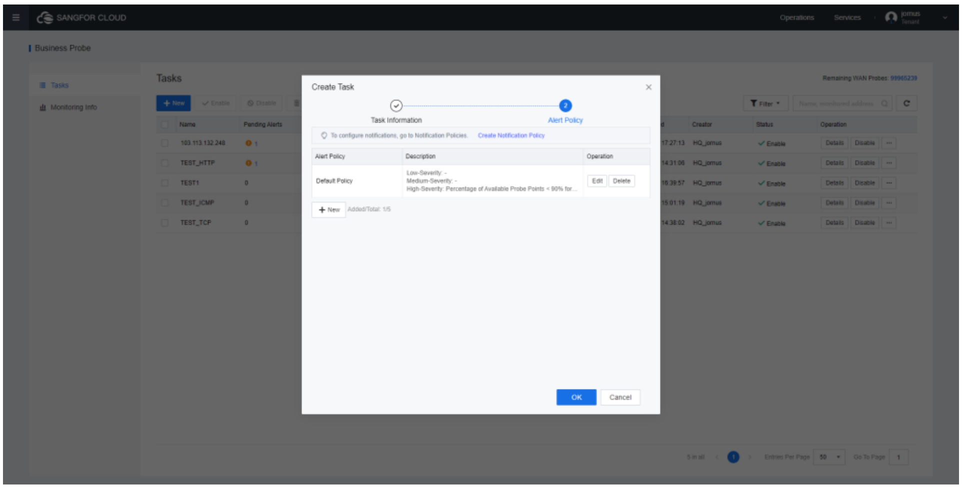
Probe Point Type: ● Managed Cloud Probe Point

4. Select the indicators and specify the condition and value.
5. The combination of indicators is not restricted by default.
6. Four indicators can be added at most. At least one indicator is required.
7. For HTTP probe tasks, click **Advanced** to configure **Request**, **Request Body, Certificate, Proxy**, and **Privacy**.

1.3.4.2 Creating Alert Policies for Business Probe

Tenants can create alert policies for business probes to promptly respond to service faults or anomalies, thus ensuring the operation of services. Alerts or notifications will be triggered automatically in case of service faults or anomalies to inform related personnel to take immediate action. It can significantly shorten fault response time and reduce the risk of service interruptions or impact on user experience.

1. After the probe task has been created, click **Next** to set the alert policy.



Create Task

Task Information — Alert Policy

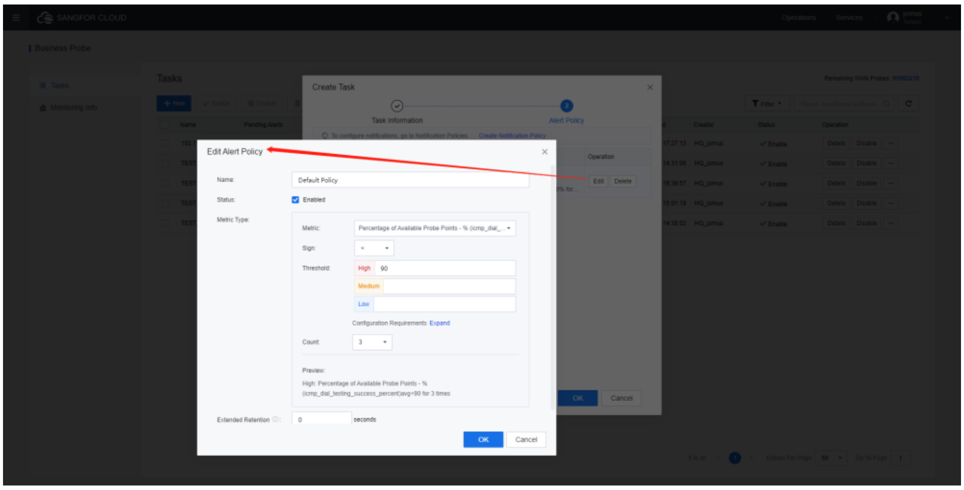
To configure notifications, go to Notification Policies. Create Notification Policy

Alert Policy	Description	Operation
Default Policy	Low-Severity: - Medium-Severity: - High-Severity: Percentage of Available Probe Points < 90% for...	Edit Delete

Added/Total: 1/5

2. A default policy is provided; the **Metric** is **Percentage of Available Probe Points**.

3. Select the required metric from the drop-down list. Available metrics include **Percentage of Available Probe Points, Available Probe Points, Unavailable Probe Points, Round-Trip Time,** and **Packet Loss Rate**. The table below describes these metrics in detail.



Edit Alert Policy

Name: Default Policy

Status: ☑ Enabled

Metric Type:

Metric: Percentage of Available Probe Points - % (icmp_dial_...

Sign: <

Threshold: High 90; Medium; Low

Configuration Requirements Expand

Count: 3

Preview:

High: Percentage of Available Probe Points - % (icmp_dial_testing_success_percent)avg<90 for 3 times

Extended Retention: 0 seconds

Metric	Sign	Threshold	Extended	Probe Task Type

			Retention	
Percentage of Available Probe Points	=, <, >, ≥, ≤, ≠	Low: x, for consecutive x counts Medium: x, for consecutive x counts High: x, for consecutive x counts Percentage Count: 1, 2, 3, 4, 5, 10, 15, 20	Same as that for probe tasks	HTTP, TCP, ICMP
Available Probe Points	Same as above	Same as above	Same as above	HTTP, TCP, ICMP
Unavailable Probe Points	Same as above	Same as above	Same as above	HTTP, TCP, ICMP
Response Time	Same as above	Low: x, for consecutive x counts Medium: x, for consecutive x counts High: x, for consecutive x counts ms Count: 1, 2, 3, 4, 5, 10, 15, 20	Same as above	HTTP, TCP
Round-Trip Time	Same as above	Low: x, for consecutive x counts Medium: x, for consecutive x counts High: x, for consecutive x counts ms Count: 1, 2, 3, 4, 5, 10, 15, 20	Same as above	ICMP

Packet Loss Rate	Same as above	Low: x, for consecutive x counts Medium: x, for consecutive x counts High: x, for consecutive x counts Percentage Count: 1, 2, 3, 4, 5, 10, 15, 20	Same as above	ICMP

4. A maximum of five alert policies can be set.

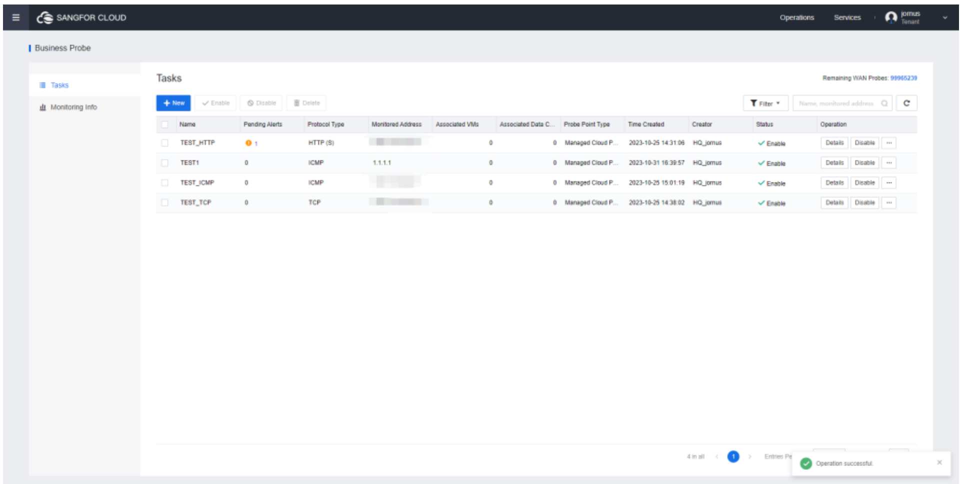
1.3.5 Viewing Business Probe Tasks

1.3.5.1 View Business Probe Tasks List

Tenants can view the business probe task list to understand the status and results of all tasks. It allows the service faults or anomalies to be detected on time, and prompt remedial measures could be taken to ensure the operation of services. By reviewing the business probe task list, information such as probe time and results for each task can be obtained to assess whether the service is operating. Suppose any anomalies or failures occur in the business probe tasks. In that case, prompt remedial measures can be taken to prevent service interruptions or impact on user experience.

1.3.5.1.1 General Scenario

1. Tenants log in to the MCS portal and navigate to **Resource > SkyOPS > Business Probe**.



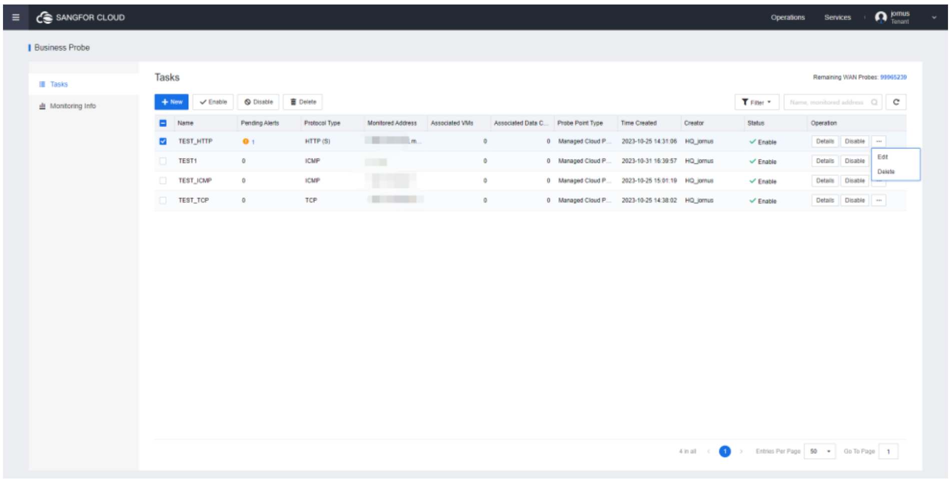
Remaining WAN Probes: 99965239

Name	Pending Alerts	Protocol Type	Monitored Address	Associated VMs	Associated Data C...	Probe Point Type	Time Created	Creator	Status	Operation
TEST_HTTP	1	HTTP (S)	[redacted]	0	0	Managed Cloud P...	2023-10-25 14:31:06	HQ_jomus	✓ Enable	Details Disable ···
TEST1	0	ICMP	1.1.1.1	0	0	Managed Cloud P...	2023-10-31 16:39:57	HQ_jomus	✓ Enable	Details Disable ···
TEST_ICMP	0	ICMP	[redacted]	0	0	Managed Cloud P...	2023-10-25 15:01:19	HQ_jomus	✓ Enable	Details Disable ···
TEST_TCP	0	TCP	[redacted]	0	0	Managed Cloud P...	2023-10-25 14:38:02	HQ_jomus	✓ Enable	Details Disable ···

4 in all 1 Entries Pe

Operation successful.

2. Tenants can view the business probe task list: name, pending alerts, protocol type, monitored address, probe point type, availability, last response time, status, time created, creator, operations (details, edit, disable/enable, delete).



Remaining WAN Probes: 99965239

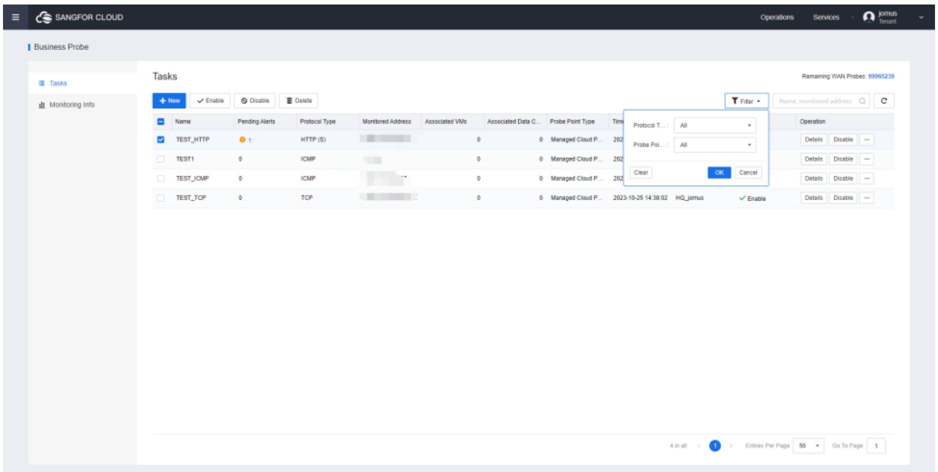
☐	Name	Pending Alerts	Protocol Type	Monitored Address	Associated VMs	Associated Data C...	Probe Point Type	Time Created	Creator	Status	Operation
☑	TEST_HTTP	1	HTTP (S)	[redacted]	0	0	Managed Cloud P...	2023-10-25 14:31:06	HQ_jomus	✓ Enable	Details Disable ···
☐	TEST1	0	ICMP	[redacted]	0	0	Managed Cloud P...	2023-10-31 16:39:57	HQ_jomus	✓ Enable	Details Disable ···
☐	TEST_ICMP	0	ICMP	[redacted]	0	0	Managed Cloud P...	2023-10-25 15:01:19	HQ_jomus	✓ Enable	Details Disable ···
☐	TEST_TCP	0	TCP	[redacted]	0	0	Managed Cloud P...	2023-10-25 14:38:02	HQ_jomus	✓ Enable	Details Disable ···

4 in all 1 Entries Per Page 50 Go To Page 1

3. Filter the task list by:

- Protocol type: HTTP(S), TCP, ICMP

- Probe point type: managed cloud, private cloud



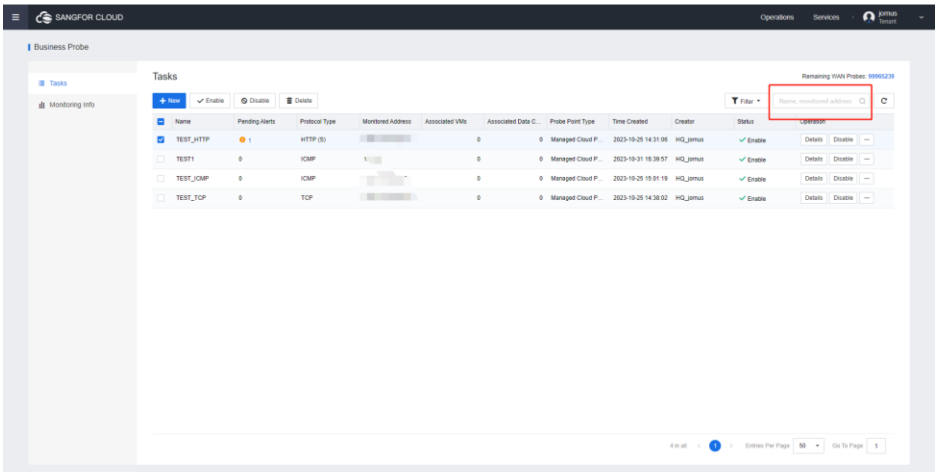
Tasks

Remaining WAN Probes: 99965239

☐	Name	Pending Alerts	Protocol Type	Monitored Address	Associated VMs	Associated Data C...	Probe Point Type	Time			Operation
☑	TEST_HTTP	1	HTTP (S)	[redacted]	0	0	Managed Cloud P...	202			Details Disable ···
☐	TEST1	0	ICMP	[redacted]	0	0	Managed Cloud P...	202			Details Disable ···
☐	TEST_ICMP	0	ICMP	[redacted]	0	0	Managed Cloud P...	202			Details Disable ···
☐	TEST_TCP	0	TCP	[redacted]	0	0	Managed Cloud P...	2023-10-25 14:38:02	HQ_jomus	✓ Enable	Details Disable ···

4 in all 1 Entries Per Page 50 Go To Page 1

4. A fuzzy search by name or monitored address is supported.



Tasks

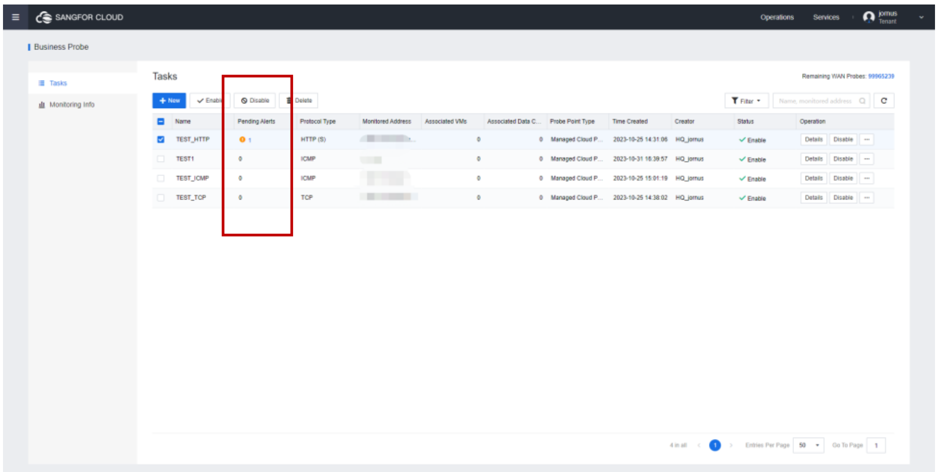
Remaining WAN Probes: 99965239

☐	Name	Pending Alerts	Protocol Type	Monitored Address	Associated VMs	Associated Data C...	Probe Point Type	Time Created	Creator	Status	Operation
☑	TEST_HTTP	1	HTTP (S)	[redacted]	0	0	Managed Cloud P...	2023-10-25 14:31:06	HQ_jomus	✓ Enable	Details Disable ···
☐	TEST1	0	ICMP	[redacted]	0	0	Managed Cloud P...	2023-10-31 16:39:57	HQ_jomus	✓ Enable	Details Disable ···
☐	TEST_ICMP	0	ICMP	[redacted]	0	0	Managed Cloud P...	2023-10-25 15:01:19	HQ_jomus	✓ Enable	Details Disable ···
☐	TEST_TCP	0	TCP	[redacted]	0	0	Managed Cloud P...	2023-10-25 14:38:02	HQ_jomus	✓ Enable	Details Disable ···

4 in all 1 Entries Per Page 50 Go To Page 1

5. You can refresh the list.

6. **Pending alerts** are sorted by alert count from high to low by default.



Tasks

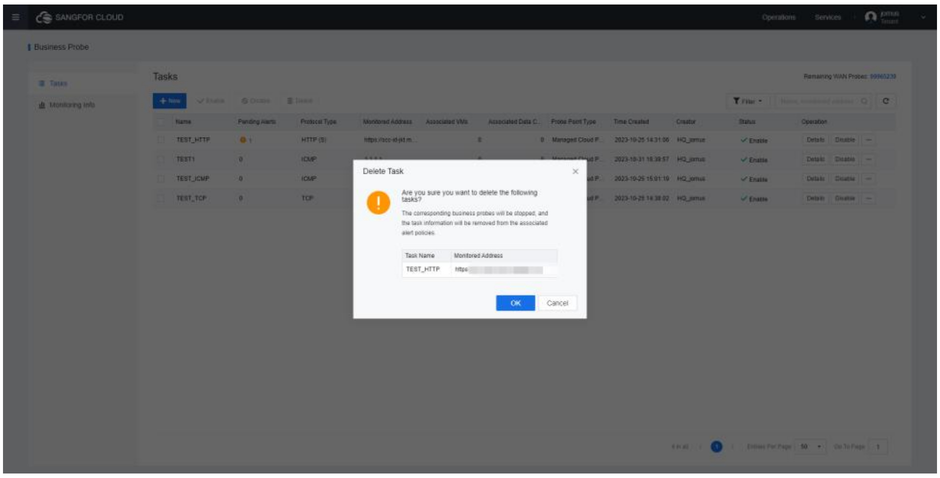
Remaining WAN Probes: 99965239

☐	Name	Pending Alerts	Protocol Type	Monitored Address	Associated VMs	Associated Data C...	Probe Point Type	Time Created	Creator	Status	Operation
☑	TEST_HTTP	1	HTTP (S)	[redacted]	0	0	Managed Cloud P...	2023-10-25 14:31:06	HQ_jomus	✓ Enable	Details Disable ···
☐	TEST1	0	ICMP	[redacted]	0	0	Managed Cloud P...	2023-10-31 16:39:57	HQ_jomus	✓ Enable	Details Disable ···
☐	TEST_ICMP	0	ICMP	[redacted]	0	0	Managed Cloud P...	2023-10-25 15:01:19	HQ_jomus	✓ Enable	Details Disable ···
☐	TEST_TCP	0	TCP	[redacted]	0	0	Managed Cloud P...	2023-10-25 14:38:02	HQ_jomus	✓ Enable	Details Disable ···

4 in all 1 Entries Per Page 50 Go To Page 1

7. The tenant user can delete tasks individually or in bulk. The Delete Task confirmation message will prompt: **Are you sure you want to delete the**

following tasks? The corresponding address will no longer be monitored, and task information will be removed from the associated alert policies. After deletion, the list will refresh, and the deleted tasks will no longer exist. The task information will be removed from the associated alert policies.



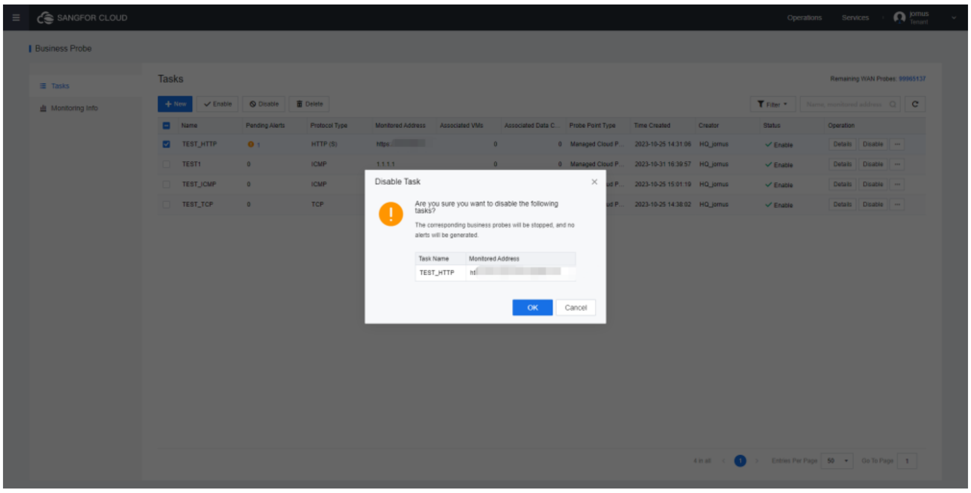
Delete Task

Are you sure you want to delete the following tasks?

The corresponding business probes will be stopped, and the task information will be removed from the associated alert policies.

Task Name	Monitored Address
TEST_HTTP	https [redacted]

8. The tenant user can disable tasks individually or in bulk. The Disable Task with the confirmation message will prompt: **Are you sure you want to disable the following tasks?** The corresponding address will no longer be monitored, and no alerts will be generated. After disabled, the task's status in the list will change to **Disable**.



Disable Task

Are you sure you want to disable the following tasks?

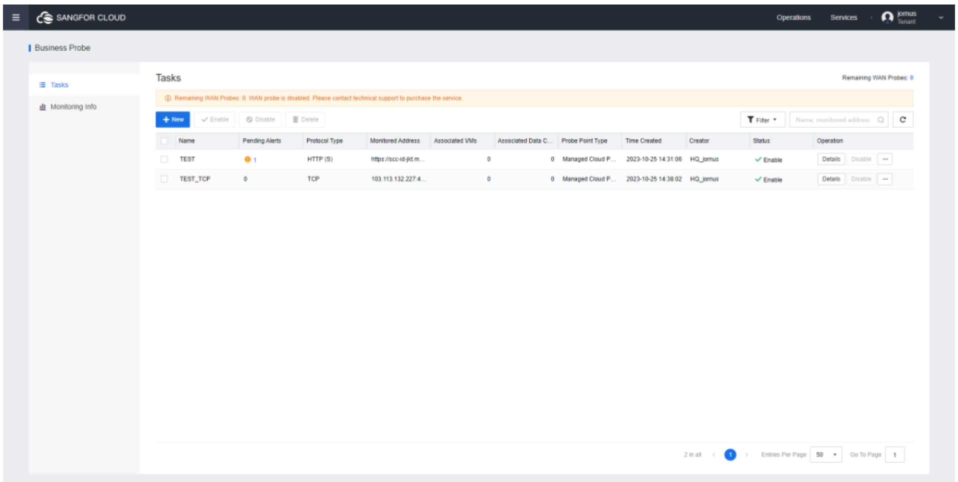
The corresponding business probes will be stopped, and no alerts will be generated.

Task Name	Monitored Address
TEST_HTTP	ht [redacted]

1.3.5.1.2 Tenant WAN Probes Limit Reached

1. The customer has a Sangfor Cloud Service Center tenant user account. If the user's WAN probes have reached the limit, log in to the MCS portal and go to **SkyOPS > Business Probe**.

2. In the task list, a message above the table shows **Remaining WAN Probes: 0. WAN probe is disabled. Please contact technical support to purchase the service**. The WAN probe's function has been automatically disabled. Please contact the administrator for renewal. Related operations on the page are greyed out and disabled. You can only view the details of created tasks and choose to delete them.



Tasks

Remaining WAN Probes: 0

Remaining WAN Probes: 0. WAN probe is disabled. Please contact technical support to purchase the service.

Name	Pending Alerts	Protocol Type	Monitored Address	Associated VMs	Associated Data C...	Probe Point Type	Time Created	Creator	Status	Operation
TEST	1	HTTP (S)	https://scc-id-jkt.m...	0	0	Managed Cloud P...	2023-10-25 14:31:06	HQ_jomus	✓ Enable	Details Disable ···
TEST_TCP	0	TCP	103.113.132.227:4...	0	0	Managed Cloud P...	2023-10-25 14:38:02	HQ_jomus	✓ Enable	Details Disable ···

2 in all < 1 > Entries Per Page 50 Go To Page 1

1.3.5.1.3 Private Cloud Customer Software Upgrade Service Expired

1. The customer has an MCS tenant user account. If the software upgrade service has expired, log in to the MCS and go to **SkyOPS > Business Probe.**

2. Tenants can view business probe task details. In the task list, a message above the table reads **Remaining WAN Probes: 0. WAN probe is disabled. Please contact technical support to purchase the service**. Related operations on the list page are greyed out and disabled. You can only view the details of created tasks and choose to delete them.

1.3.5.2 Viewing Business Probe Task Details

Tenants can view the details of a business probe task to verify task execution progress and whether the service is running. By viewing the details, the tenant can obtain specific execution information on each task, including the probe operation time and result, as well as records and trend charts. Suppose any anomalies or failures occur in a business probe task. In that case, view task details to identify the cause of the fault and remediate promptly to prevent service interruptions or impact on user experience.

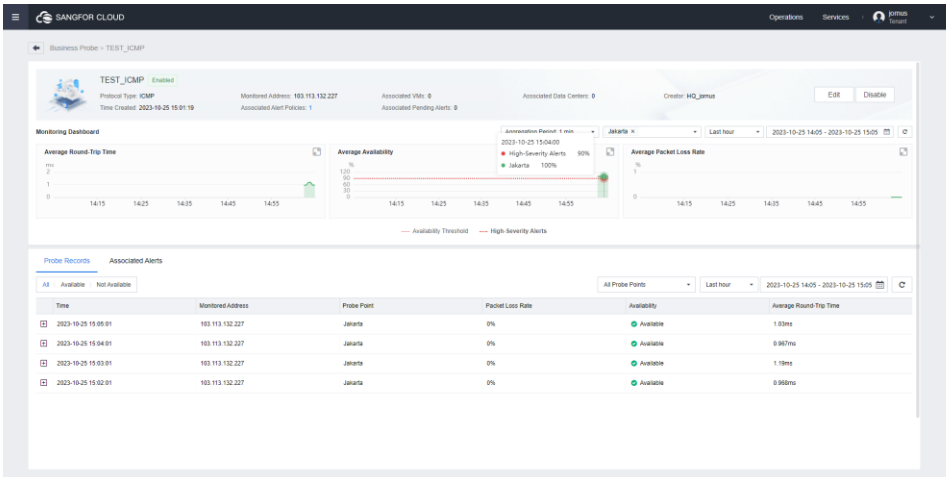
The customer has a MCS user account. Log in to the MCS and go to **SkyOPS > Business Probe**. A task named Task 1 already exists. When the tenant user views the details of Task1, the following information is displayed by default on the page::

1. Basic information: name, protocol type, monitored address, time created, creator, associated alert policies, status, and associated pending alerts.
2. **Response Time** trend chart, **Average Availability** trend chart, and probe records of **Not Available**.
3. Hover the mouse over the number of the **Associated Alert Policies** to view the name of the associated alert policies.
4. Above the trend charts, the tenants can select the Aggregation Period (The aggregation period selection options are the same as the probe frequency; the aggregation period value must be greater than the probe frequency value.) and Time Range. The default time range is Last Hour. Other options include last hour, last 6 hours, last 12 hours, last day, last 7 days, and custom range (not exceeding 7 days).
5. Above the probe records table, the tenant can select probe points (All Probe Points by default) and Time Range. The default time range is the Last Hour. Other options include last hour, last 6 hours, last 12 hours, last day, last 7 days, and custom range (not exceeding 7 days). The table shows 50 probe records by default. Click Show More to show additional records. The table information includes time, monitored address, probe point, availability, and response time.
6. Tenants can select **Last Hour** for the time range, select **Not Available** on the **Probe Records** tab, and then click the **+** next to a probe record to view the detailed information.
7. The detailed information includes DNS time, SSL authentication time, data download time, first packet receiving time, TCP connection time, and information on the response header and body.
8. The HTTP probe task response header, response body, and error information exceeding 15 MB will be truncated.
9. For HTTP probe tasks, detailed response information is shown when the

tenant has selected **Do not save response content.** Otherwise, detailed response information will not be displayed upon expansion.

10. Tenants can check associated alerts on the **Associated Alerts** tab.

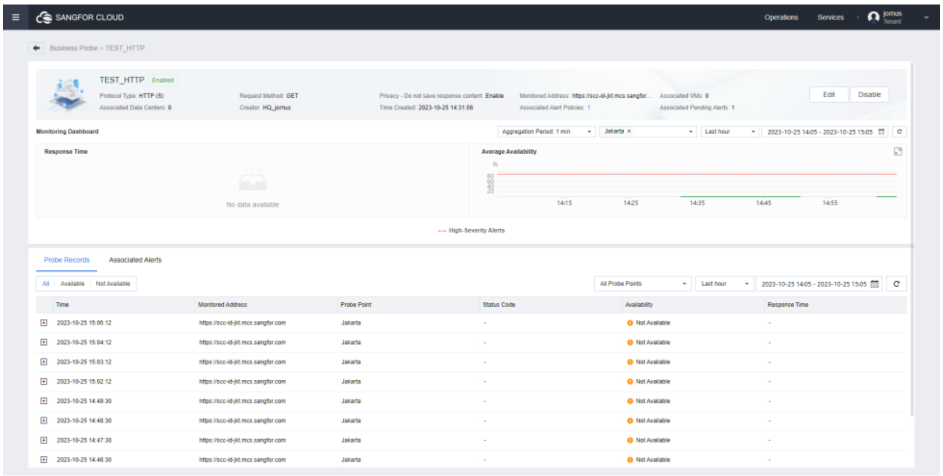
11. Alerts generated in the last 7 days are displayed by default. The administrator can also choose to display alerts generated in the last 1 hour, last 6 hours, last 24 hours, last 2 days, or last 30 days. The alert status can be **Not Responded** or **In Progress**. The table displays severity, occurrence time, object type, object name, description, status, and operations. In the table, alerts are displayed first by severity in the order of High > Medium > Low and then by status in the order of Not Responded > In Progress > Expired > Stopped.



TEST_ICMP Enabled

Protocol Type: ICMP
Time Created: 2023-10-25 15:01:19
Monitored Address: 103.113.132.227
Associated Alert Policies: 1
Associated VMs: 0
Associated Pending Alerts: 0
Associated Data Centers: 0
Creator: HQ_jomus

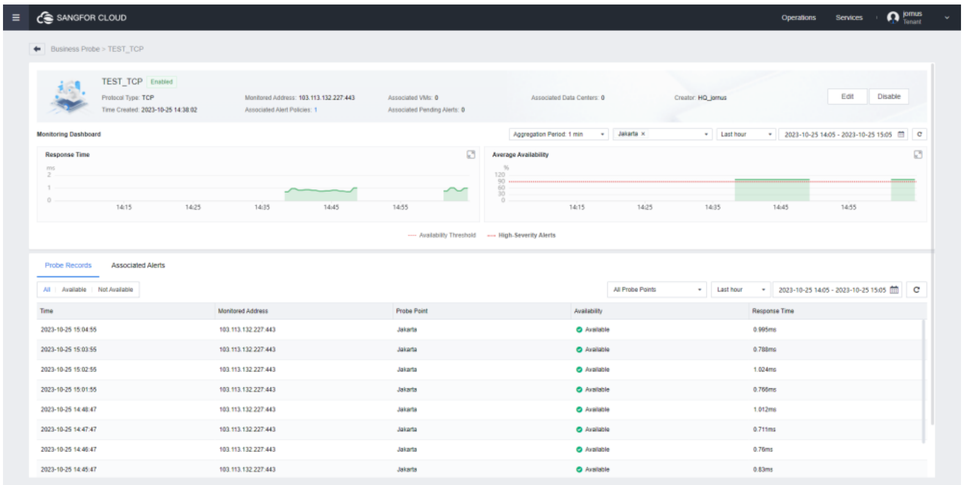
	Time	Monitored Address	Probe Point	Packet Loss Rate	Availability	Average Round-Trip Time
⊞	2023-10-25 15:05:01	103.113.132.227	Jakarta	0%	Available	1.03ms
⊞	2023-10-25 15:04:01	103.113.132.227	Jakarta	0%	Available	0.967ms
⊞	2023-10-25 15:03:01	103.113.132.227	Jakarta	0%	Available	1.19ms
⊞	2023-10-25 15:02:01	103.113.132.227	Jakarta	0%	Available	0.968ms



TEST_HTTP Enabled

Protocol Type: HTTP (S)
Associated Data Centers: 0
Request Method: GET
Creator: HQ_jomus
Privacy - Do not save response content: Enable
Time Created: 2023-10-25 14:31:06
Monitored Address: https://scc-id-jkt.mcs.sangfor...
Associated Alert Policies: 1
Associated VMs: 0
Associated Pending Alerts: 1

	Time	Monitored Address	Probe Point	Status Code	Availability	Response Time
⊞	2023-10-25 15:05:12	https://scc-id-jkt.mcs.sangfor.com	Jakarta	-	Not Available	-
⊞	2023-10-25 15:04:12	https://scc-id-jkt.mcs.sangfor.com	Jakarta	-	Not Available	-
⊞	2023-10-25 15:03:12	https://scc-id-jkt.mcs.sangfor.com	Jakarta	-	Not Available	-
⊞	2023-10-25 15:02:12	https://scc-id-jkt.mcs.sangfor.com	Jakarta	-	Not Available	-
⊞	2023-10-25 14:49:30	https://scc-id-jkt.mcs.sangfor.com	Jakarta	-	Not Available	-
⊞	2023-10-25 14:48:30	https://scc-id-jkt.mcs.sangfor.com	Jakarta	-	Not Available	-
⊞	2023-10-25 14:47:30	https://scc-id-jkt.mcs.sangfor.com	Jakarta	-	Not Available	-
⊞	2023-10-25 14:46:30	https://scc-id-jkt.mcs.sangfor.com	Jakarta	-	Not Available	-



TEST_TCP Enabled

Protocol Type: TCP
Time Created: 2023-10-25 14:38:02
Monitored Address: 103.113.132.227:443
Associated Alert Policies: 1
Associated VMs: 0
Associated Pending Alerts: 0
Associated Data Centers: 0
Creator: HQ_jomus

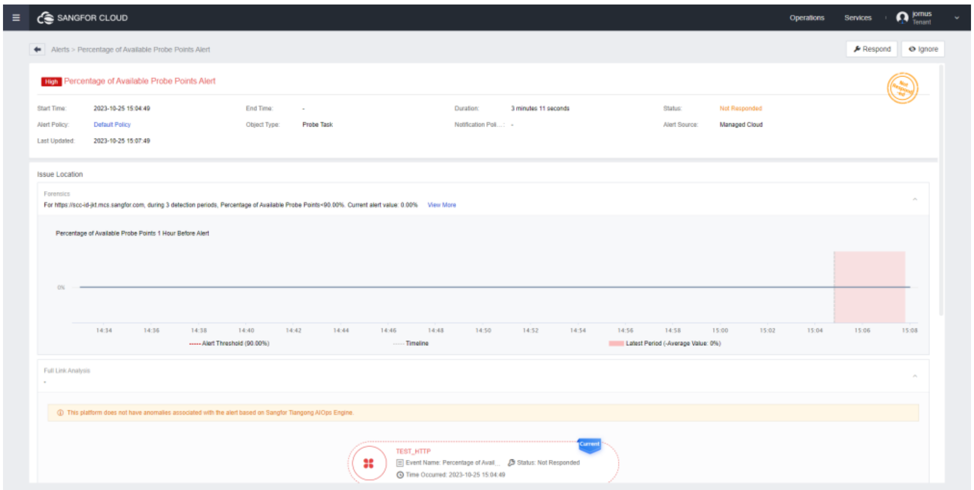
Aggregation Period: 1 min | Jakarta × | Last hour | 2023-10-25 14:05 - 2023-10-25 15:05

Time	Monitored Address	Probe Point	Availability	Response Time
2023-10-25 15:04:55	103.113.132.227:443	Jakarta	✓ Available	0.995ms
2023-10-25 15:03:55	103.113.132.227:443	Jakarta	✓ Available	0.788ms
2023-10-25 15:02:55	103.113.132.227:443	Jakarta	✓ Available	1.024ms
2023-10-25 15:01:55	103.113.132.227:443	Jakarta	✓ Available	0.766ms
2023-10-25 14:48:47	103.113.132.227:443	Jakarta	✓ Available	1.012ms
2023-10-25 14:47:47	103.113.132.227:443	Jakarta	✓ Available	0.711ms
2023-10-25 14:46:47	103.113.132.227:443	Jakarta	✓ Available	0.76ms
2023-10-25 14:45:47	103.113.132.227:443	Jakarta	✓ Available	0.83ms

1.3.5.3 Viewing Associated Business Probe Task Alerts

Tenants can view the associated alerts of a business probe task to respond to faults or anomalies promptly, ensuring service operation. By checking the associated alerts, tenants can better understand the alert policies for a task and obtain information such as alert severity and method. If a business probe task encounters anomalies or failures, the associated alert policies will trigger alerts automatically, notifying relevant personnel to remediate. It can significantly shorten fault response time and reduce the risk of service interruptions or impact on user experience.

1. The customer has an MCS tenant user account and an existing business probe task with a monitored address **url1** that triggered an alert.
2. The tenant user can go to **SkyOPS > Smart O&M > Alert Events** to view the alert.
3. The tenant user views the details of the alert:



High Percentage of Available Probe Points Alert

Start Time: 2023-10-25 15:04:49
Alert Policy: Default Policy
Last Updated: 2023-10-25 15:07:49
End Time: -
Object Type: Probe Task
Duration: 3 minutes 11 seconds
Notification Poli...: -
Status: Not Responded
Alert Source: Managed Cloud

For https://scc-id-jkt.mcs.sangfor.com, during 3 detection periods, Percentage of Available Probe Points<90.00%. Current alert value: 0.00%

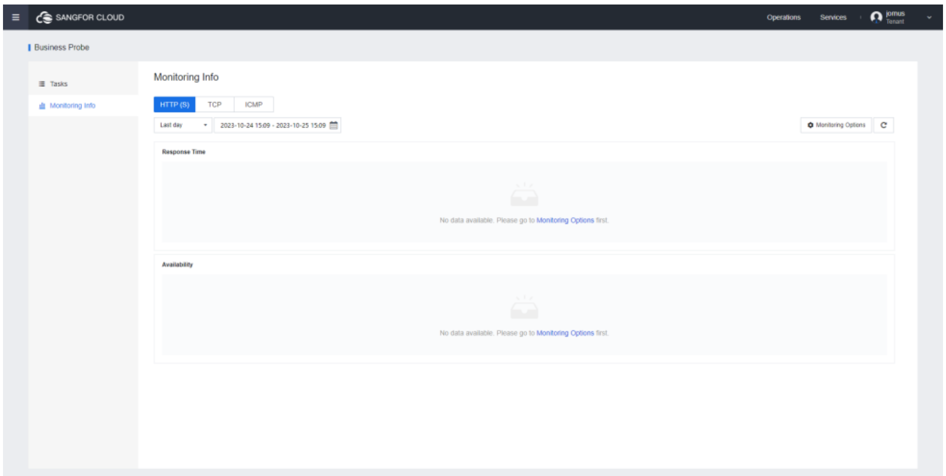
This platform does not have anomalies associated with the alert based on Sangfor Tiangong AIOps Engine.

TEST_HTTP
Event Name: Percentage of Avail... Status: Not Responded
Time Occurred: 2023-10-25 15:04:49

1.3.5.4 Creating Monitoring Dashboard

The main purpose of creating a monitoring dashboard for probe tasks is to monitor the availability of WAN services in real-time to ensure the operation of services. By creating a dashboard, the states and results of multiple probe tasks can be displayed on one page, quickly understanding how services operate. Tenants can view the execution status of business probe tasks in real-time through the monitoring dashboard. If anomalies or failures are detected, prompt remedial measures can be taken to prevent service interruptions or impact on user experience.

1. Navigate to **SkyOPS > Business Probe > Monitoring Info.** HTTP(s)**,** TCP, and ICMP monitoring info are supported.

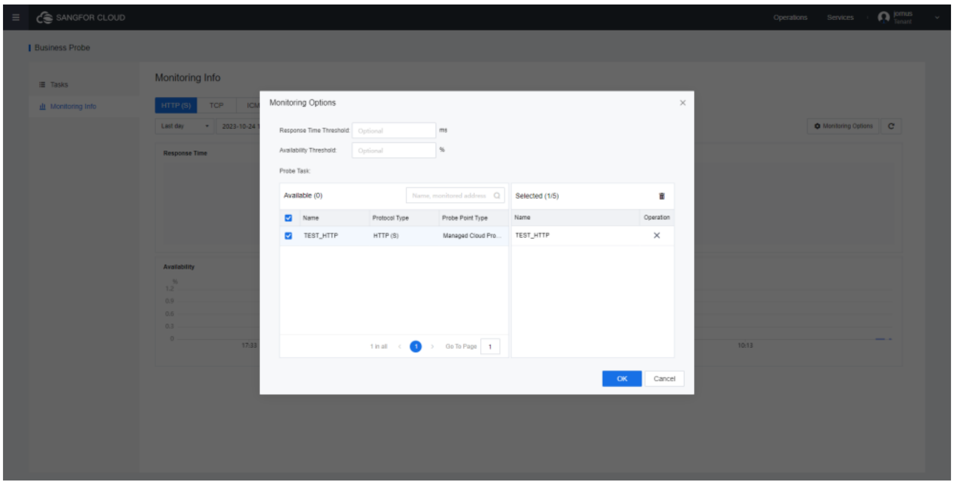


Last day ▾ 2023-10-24 15:09 - 2023-10-25 15:09

No data available. Please go to Monitoring Options first.

No data available. Please go to Monitoring Options first.

2. Click **Monitoring Options** to go to the monitoring options page. A maximum of five probe tasks can be selected.



Response Time Threshold: Optional ms

Availability Threshold: Optional %

Probe Task:

Available (0)

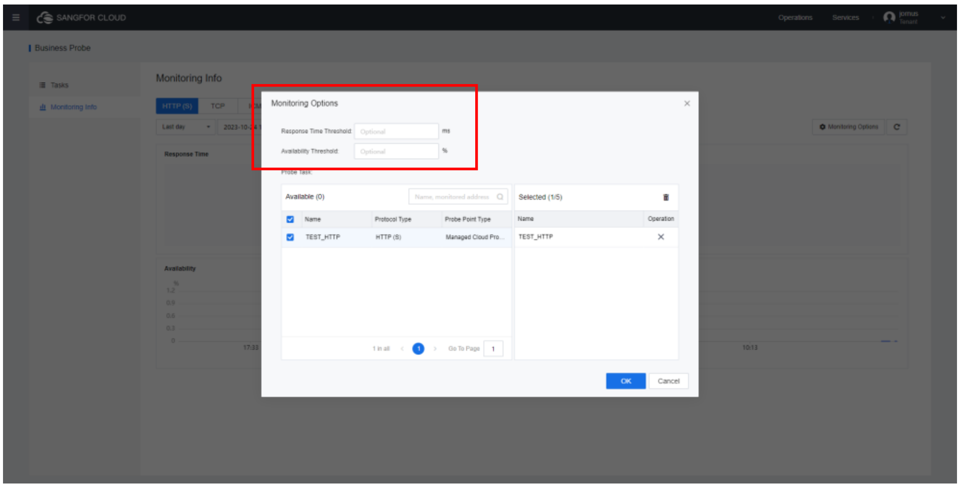
☑	Name	Protocol Type	Probe Point Type
☑	TEST_HTTP	HTTP (S)	Managed Cloud Pro...

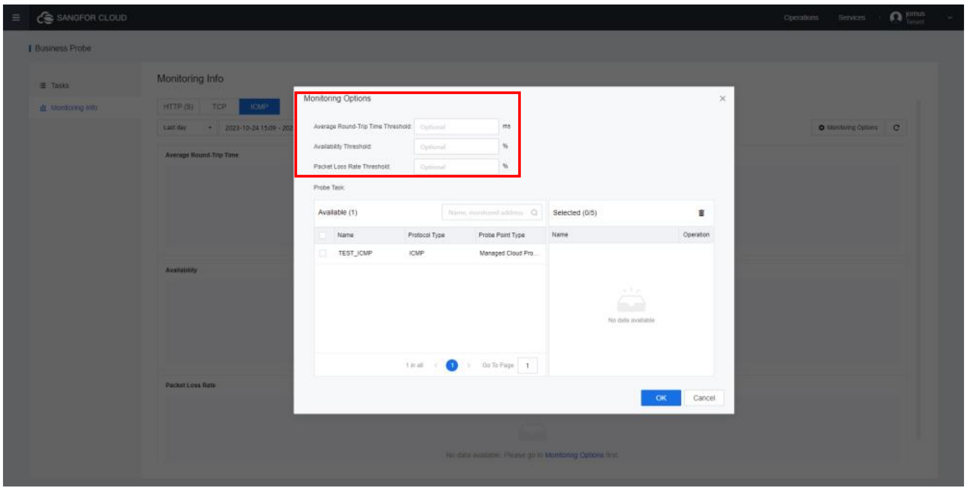
1 in all ‹ 1 › Go To Page 1

Selected (1/5)

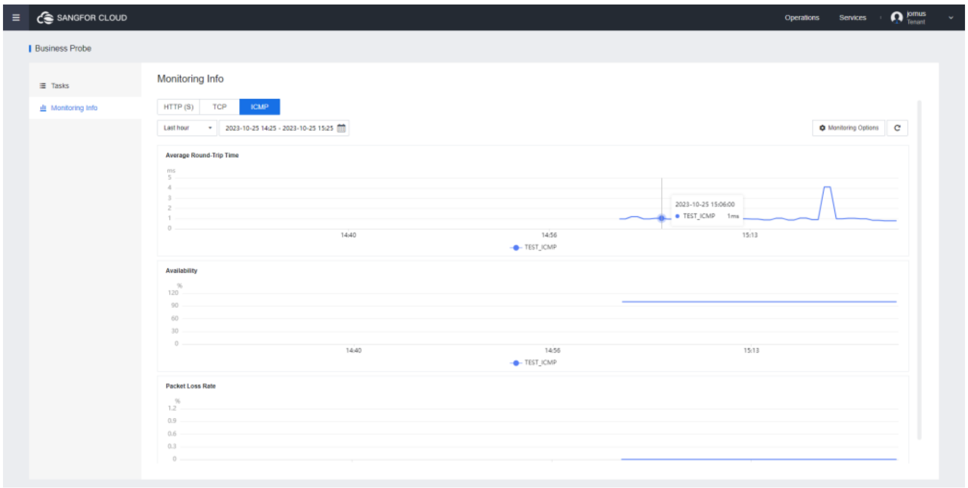
Name	Operation
TEST_HTTP	×

3. The **Response Time Threshold** and **Availability Thresholds** can be set on the monitoring dashboards for HTTP and TCP probe tasks. The average round-trip time, availability, and packet loss rate thresholds can be set on the monitoring dashboard for ICMP probe tasks.



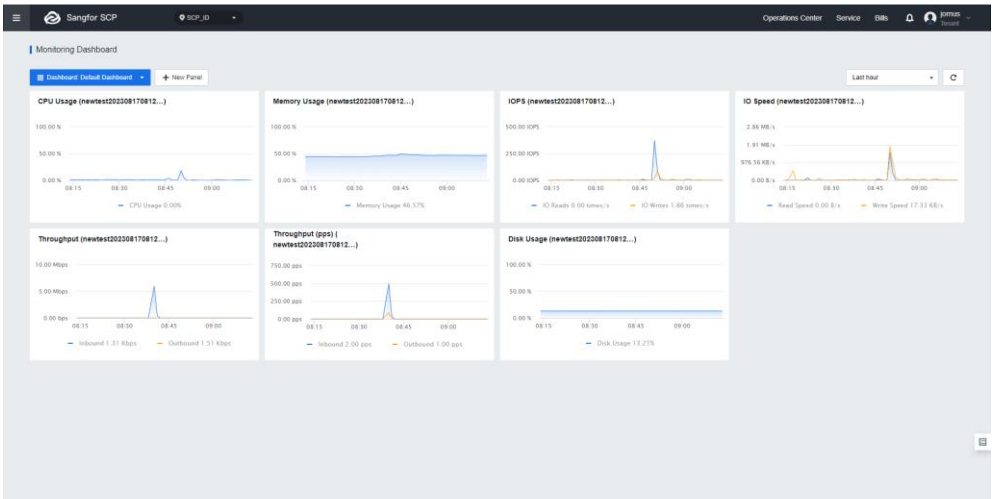


4. On the **Monitoring Info** page, the HTTP(S) and TCP tabs display trend charts of Response Time and Availability, and the thresholds are in dashed lines. Filtering by time range is supported.

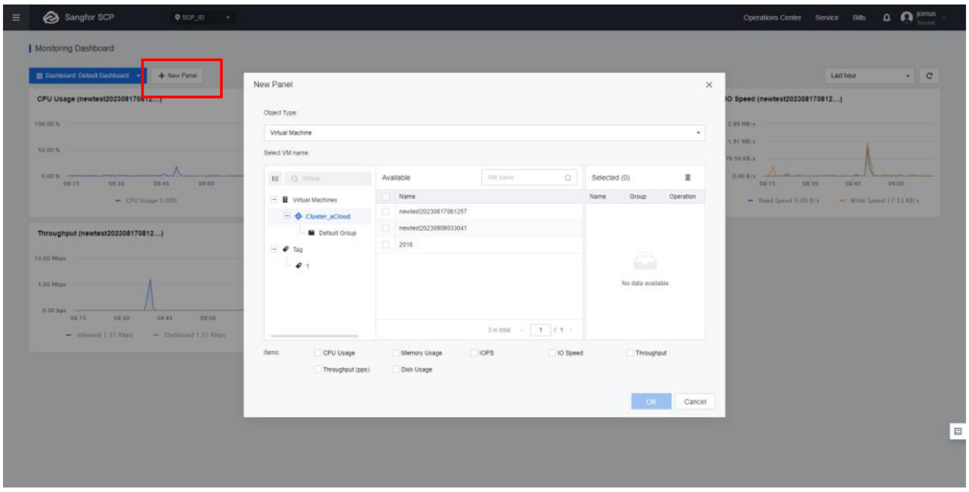


1.4 Monitoring Dashboard

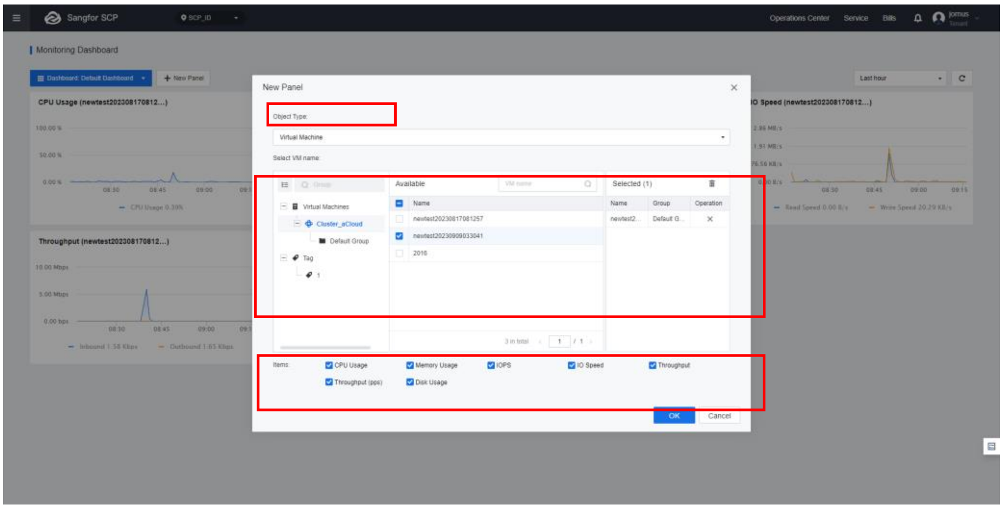
1. Log in to the MCS portal and navigate to **SkyOps > Monitoring Dashboard**. On this page, there are default monitoring dashboard.



2. You can customize and add panels that meet your requirements by clicking **New Panel**.



3. Select the **Object Type**, **VM**, and **Items** to create the dashboard. The available **Object Type** are **Virtual Machine, Elastic IP**, or **Shared Bandwidth**.



New Panel

Object Type: Virtual Machine

Select VM name:

Virtual Machines / Cluster_aCloud / Default Group; Tag / 1

Available

☐	Name
☐	newtest20230817081257
☑	newtest20230909033041
☐	2016

3 in total 1 / 1

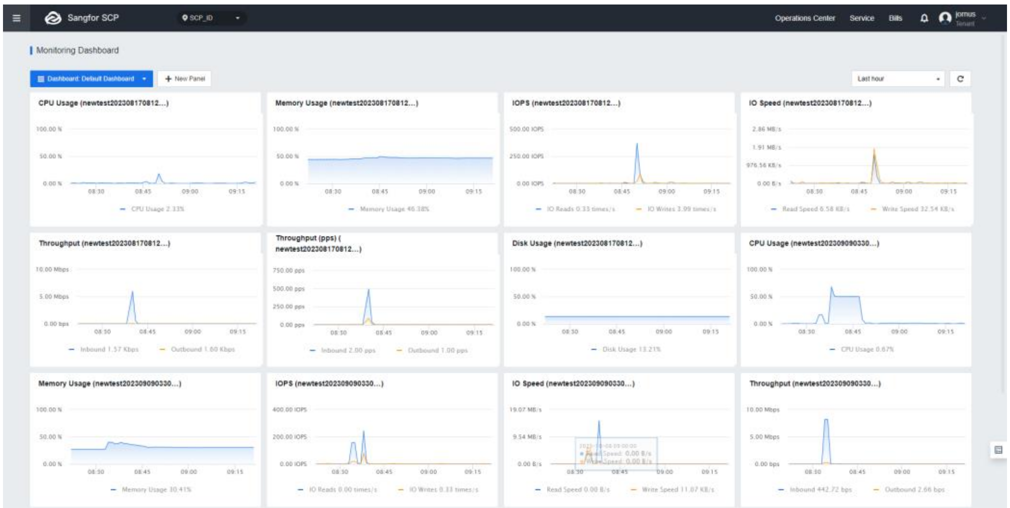
Selected (1)

Name	Group	Operation
newtest2...	Default G...	×

Items: ☑ CPU Usage ☑ Memory Usage ☑ IOPS ☑ IO Speed ☑ Throughput ☑ Throughput (pps) ☑ Disk Usage

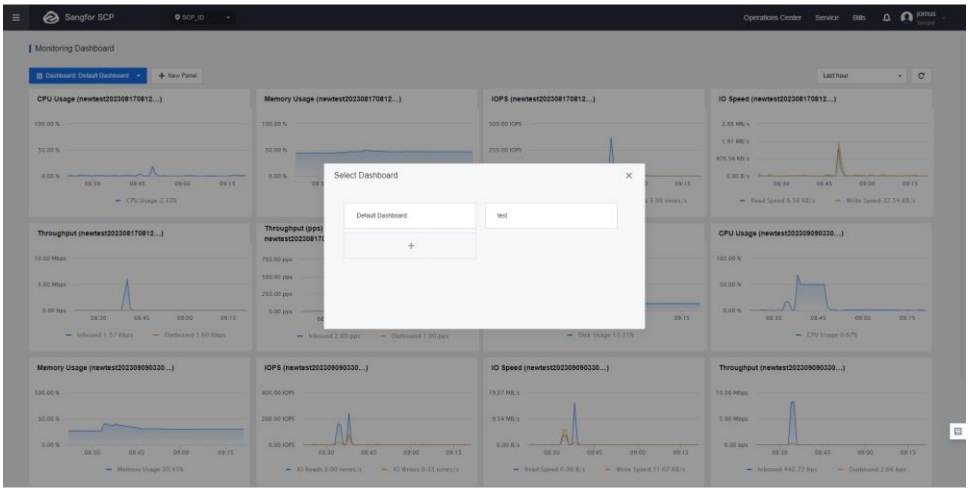
Sangfor SCP
SCP_ID
Operations Center
Service
Bills
Monitoring Dashboard
Dashboard: Default Dashboard
New Panel
Last hour
CPU Usage (newtest202308170812...)
Throughput (newtest202308170812...)
IO Speed (newtest202308170812...)
OK
Cancel

4. Click **OK**, and the customize panel will be auto-generated. The tenant can manually drag and drop to change the panel position or add a new panel by clicking **+New Panel**.

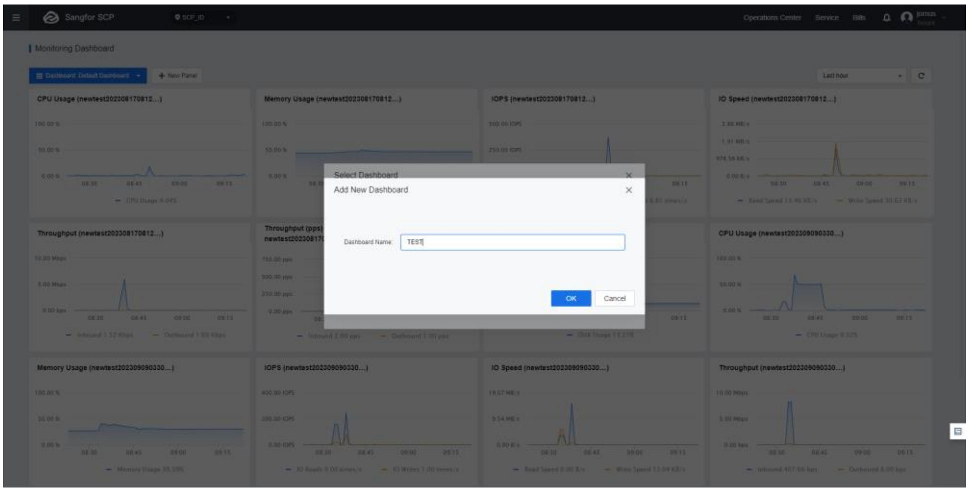


Sangfor SCP
SCP_ID
Operations Center
Service
Bills
Monitoring Dashboard
Dashboard: Default Dashboard
+ New Panel
Last hour
CPU Usage (newtest202308170812...)
Memory Usage (newtest202308170812...)
IOPS (newtest202308170812...)
IO Speed (newtest202308170812...)
Throughput (newtest202308170812...)
Throughput (pps) (newtest202308170812...)
Disk Usage (newtest202308170812...)
CPU Usage (newtest202309090330...)
Memory Usage (newtest202309090330...)
IOPS (newtest202309090330...)
IO Speed (newtest202309090330...)
Throughput (newtest202309090330...)
08:30
08:45
09:00
09:15

5. By clicking **Dashboard**, it supports switching between multiple dashboards if they exist.

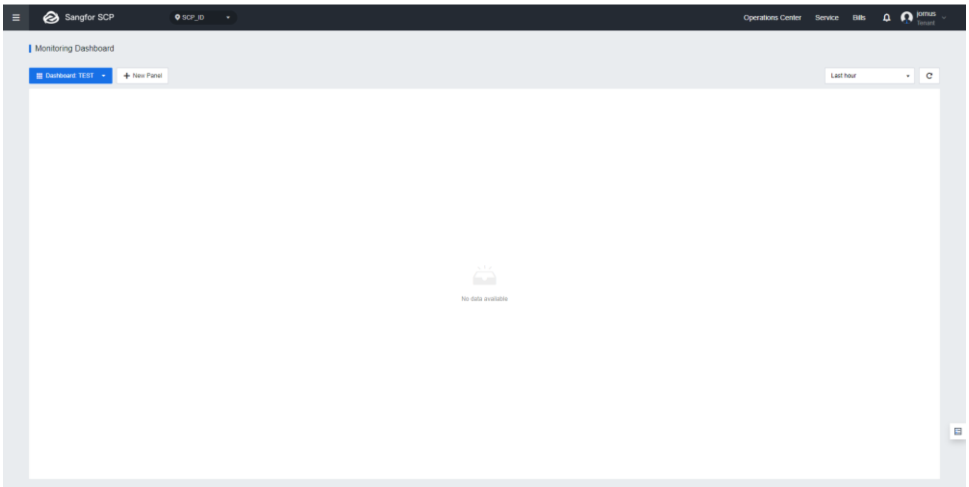


6. Click **+** to create a new dashboard to monitor the VM in different groups better.

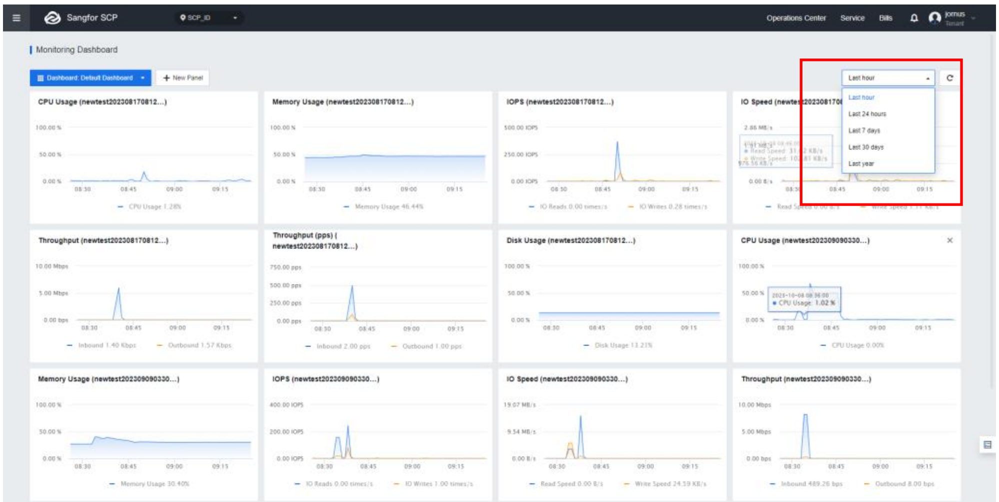


Dashboard Name: TEST

7. Then, you can set up panels for the newly added dashboard.



8. You can use the dropdown menu in the upper right corner to select different dates and times to view the data.


Sangfor SCP
Operations Center
Service
Bills
jomus
Tenant
Monitoring Dashboard
Dashboard: Default Dashboard
New Panel
Last hour
Last hour
Last 24 hours
Last 7 days
Last 30 days
Last year
CPU Usage (newtest202308170812...)
Memory Usage (newtest202308170812...)
IOPS (newtest202308170812...)
IO Speed (newtest20230817...
Throughput (newtest202308170812...)
Throughput (pps) (newtest202308170812...)
Disk Usage (newtest202308170812...)
CPU Usage (newtest202309090330...)
Memory Usage (newtest202309090330...)
IOPS (newtest202309090330...)
IO Speed (newtest202309090330...)
Throughput (newtest202309090330...)
08:30
08:45
09:00
09:15

1.4.1 Monitoring

1.4.1.1 Server

On this page, if any dedicated server (Dedicated resources pool/Dedicated server group) is associated with the tenant, the tenant can monitor the dedicated server. Otherwise, it will remain empty.

1.4.1.2 Virtual Machines

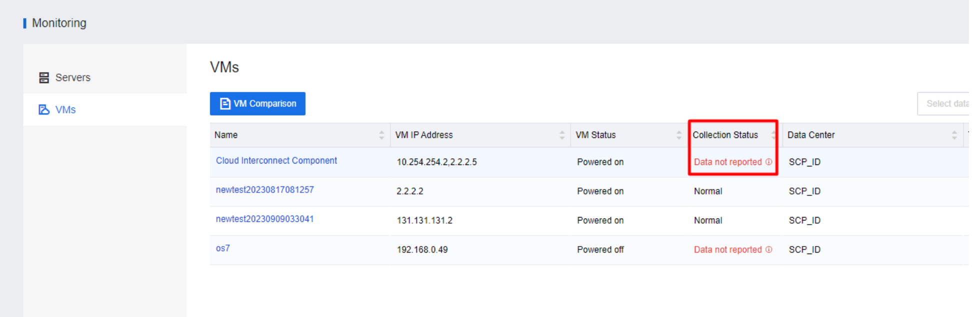
The cloud agent is deployed on the virtual machine to collect and report the monitoring information to the MCS. The Virtual Machine resource usage, traffic usage, and alarm status are shown in graphs.

For virtual machine monitoring, it supports two types of installation methods: **Auto** and **Manual.**

To use the agent auto installation, make sure:

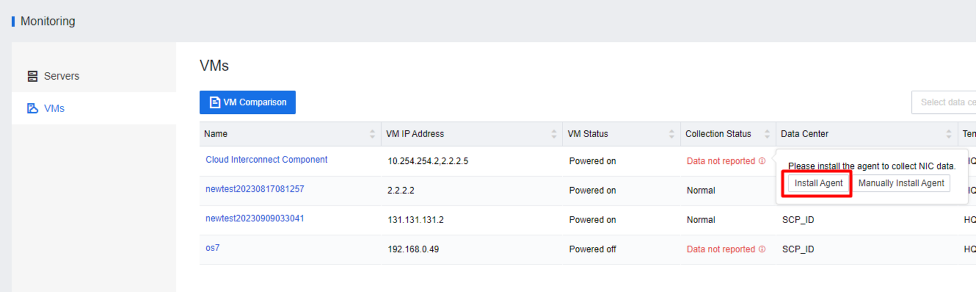
- HCI version is 6.3.0 and above.
- The administrator has already enabled the Shared Service Network for the tenants.
- VM and MCS time difference is less than 5 minutes.

1. Go to **SkyOPS > Monitoring**, and click the **Data not reported** of the selected VM.



Name	VM IP Address	VM Status	Collection Status	Data Center
Cloud Interconnect Component	10.254.254.2,2.2.2.5	Powered on	Data not reported	SCP_ID
newtest20230817081257	2.2.2.2	Powered on	Normal	SCP_ID
newtest20230909033041	131.131.131.2	Powered on	Normal	SCP_ID
os7	192.168.0.49	Powered off	Data not reported	SCP_ID

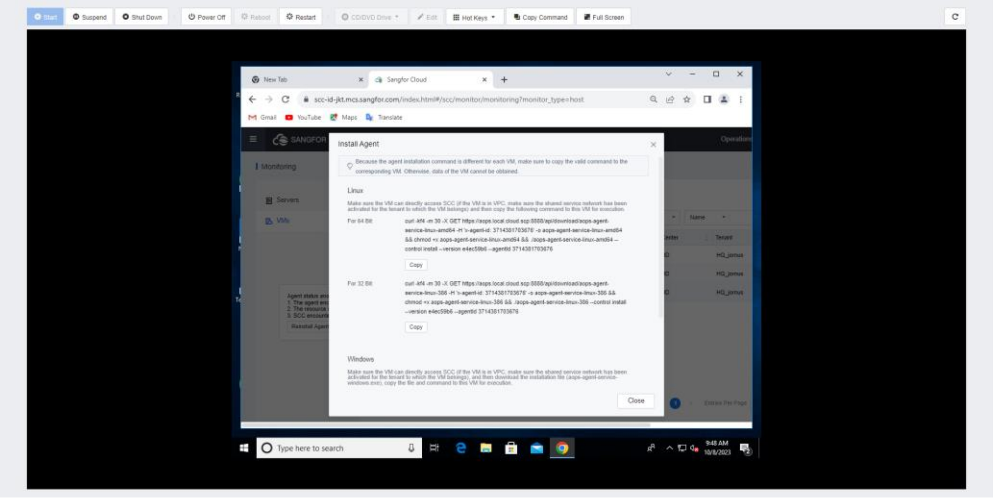
2. Select **Install Agent,** which refers to the auto-installation method.



Please install the agent to collect NIC data.

Name	VM IP Address	VM Status	Collection Status	Data Center	Ten
Cloud Interconnect Component	10.254.254.2,2.2.2.5	Powered on	Data not reported		HC
newtest20230817081257	2.2.2.2	Powered on	Normal		HC
newtest20230909033041	131.131.131.2	Powered on	Normal	SCP_ID	HC
os7	192.168.0.49	Powered off	Data not reported	SCP_ID	HC

3. If the auto-installation fails, then select **Manually Install Agent**. Login to the MCS platform on your virtual machine to download the agent plugin.



Install Agent

Because the agent installation command is different for each VM, make sure to copy the valid command to the corresponding VM. Otherwise, data of the VM cannot be obtained.

Linux

Make sure the VM can directly access SCC (if the VM is in VPC, make sure the shared service network has been activated for the tenant to which the VM belongs) and then copy the following command to this VM for execution.

For 64 Bit

```
curl -kfN -m 30 -X GET https://aops.local.cloud.scp:8888/api/download/aops-agent-service-linux-amd64 -H 'x-agent-id: 3714381703676' -o aops-agent-service-linux-amd64 && chmod +x aops-agent-service-linux-amd64 && ./aops-agent-service-linux-amd64 --control install --version e4ec59b6 --agentid 3714381703676
```

Copy

For 32 Bit

```
curl -kfN -m 30 -X GET https://aops.local.cloud.scp:8888/api/download/aops-agent-service-linux-386 -H 'x-agent-id: 3714381703676' -o aops-agent-service-linux-386 && chmod +x aops-agent-service-linux-386 && ./aops-agent-service-linux-386 --control install --version e4ec59b6 --agentid 3714381703676
```

Copy

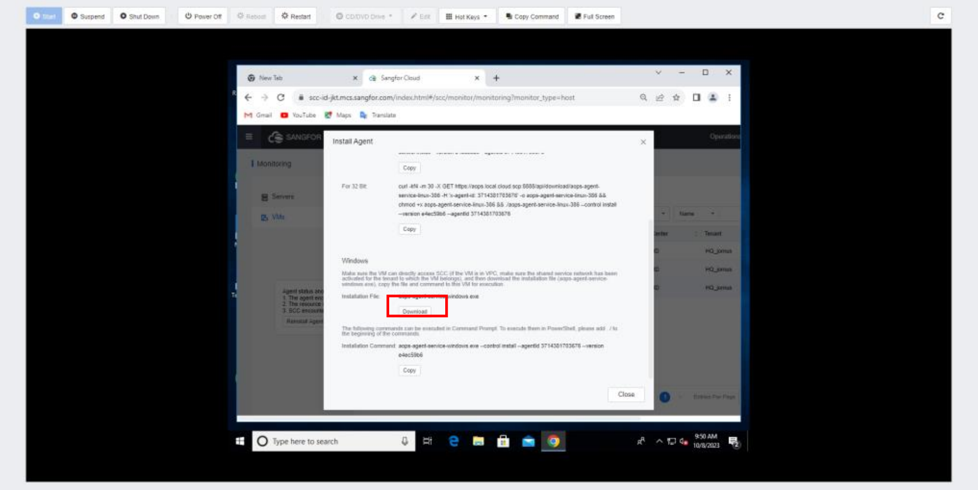
Windows

Make sure the VM can directly access SCC (if the VM is in VPC, make sure the shared service network has been activated for the tenant to which the VM belongs), and then download the installation file (aops-agent-service-windows.exe), copy the file and command to this VM for execution.

Close

Windows virtual machine

1. Click **Download**, then place the file in the C drive directory.



Install Agent

For 32 Bit: curl -kfsl -m 30 -X GET https://aops.local.cloud.scp:8888/api/download/aops-agent-service-linux-386 -H 'x-agent-id: 3714381703676' -o aops-agent-service-linux-386 && chmod +x aops-agent-service-linux-386 && ./aops-agent-service-linux-386 --control install --version e4ec59b6 --agentId 3714381703676

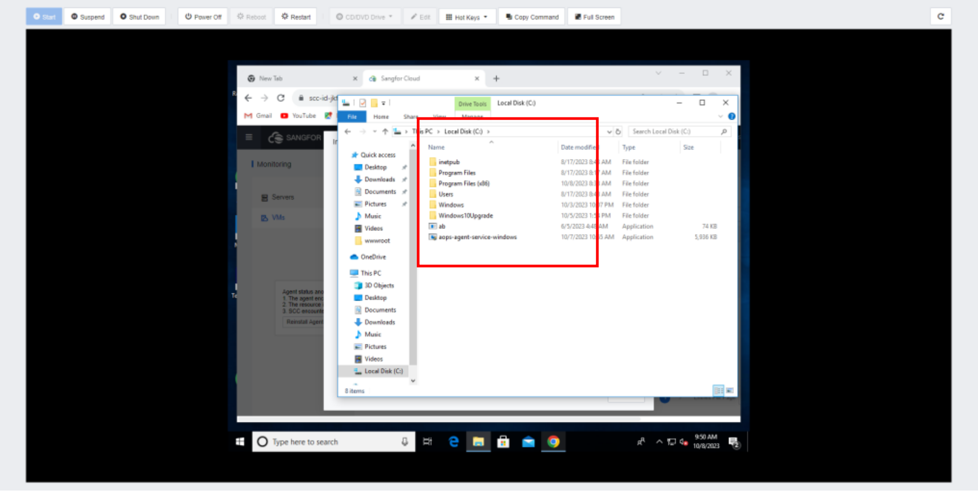
Windows

Make sure the VM can directly access SCC (if the VM is in VPC, make sure the shared service network has been activated for the tenant to which the VM belongs), and then download the installation file (aops-agent-service-windows.exe), copy the file and command to this VM for execution.

Installation File: aops-agent-service-windows.exe

The following commands can be executed in Command Prompt. To execute them in PowerShell, please add ./ to the beginning of the commands.

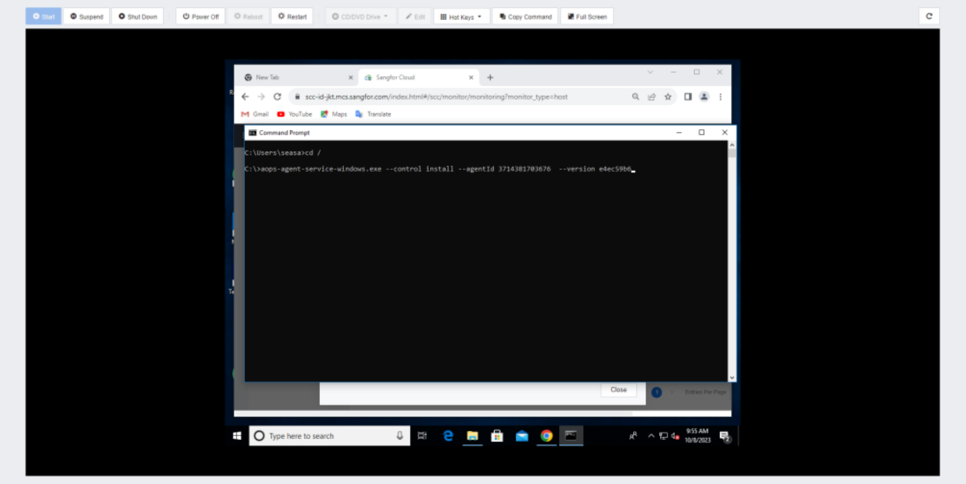
Installation Command: aops-agent-service-windows.exe --control install --agentId 3714381703676 --version e4ec59b6



This PC > Local Disk (C:) >

Name	Date modified	Type	Size
inetpub	8/17/2023 8:4 AM	File folder	
Program Files	8/17/2023 8:1 AM	File folder	
Program Files (x86)	10/8/2023 8:3 AM	File folder	
Users	8/17/2023 8:4 AM	File folder	
Windows	10/3/2023 10:7 PM	File folder	
Windows10Upgrade	10/5/2023 1:5 PM	File folder	
ab	6/5/2023 4:48 AM	Application	74 KB
aops-agent-service-windows	10/7/2023 10:5 AM	Application	5,936 KB

2. Navigate the command prompt (CMD) in the VM, use the **cd** command to navigate to the root directory ("/"), copy the directory from the SCP page, and execute it.



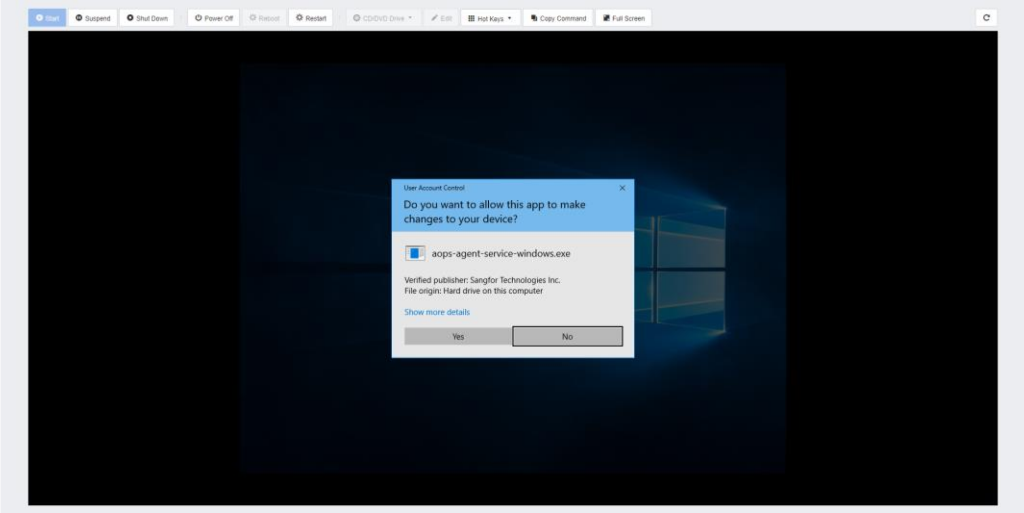
```
C:\Users\seasa>cd /

C:\>aops-agent-service-windows.exe --control install --agentId 3714381703676  --version e4ec59b6
```

3. Click **Yes** on the pop-up page to confirm the operation.

NOTE

After installing the agent, it will collect virtual machine data and report it to MCS.



User Account Control

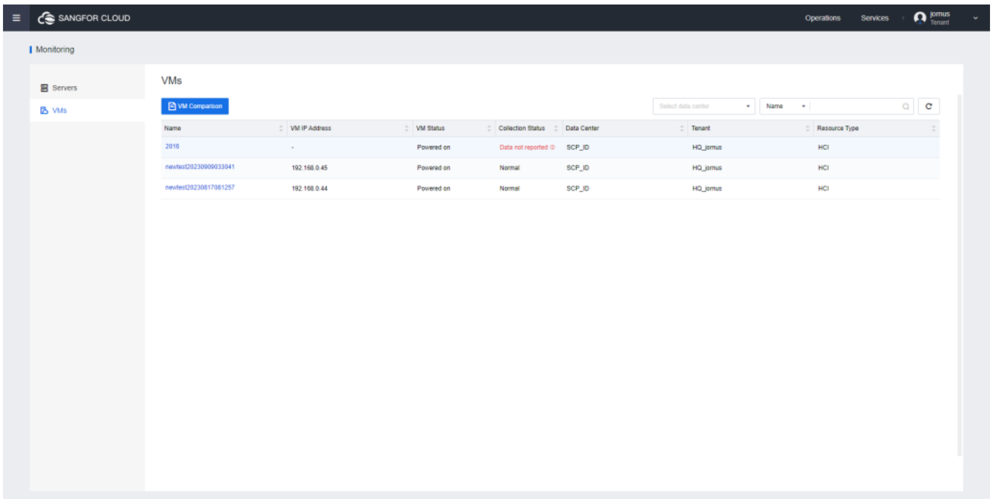
Do you want to allow this app to make changes to your device?

aops-agent-service-windows.exe

Verified publisher: Sangfor Technologies Inc.
File origin: Hard drive on this computer

4. Wait for the successful execution result.

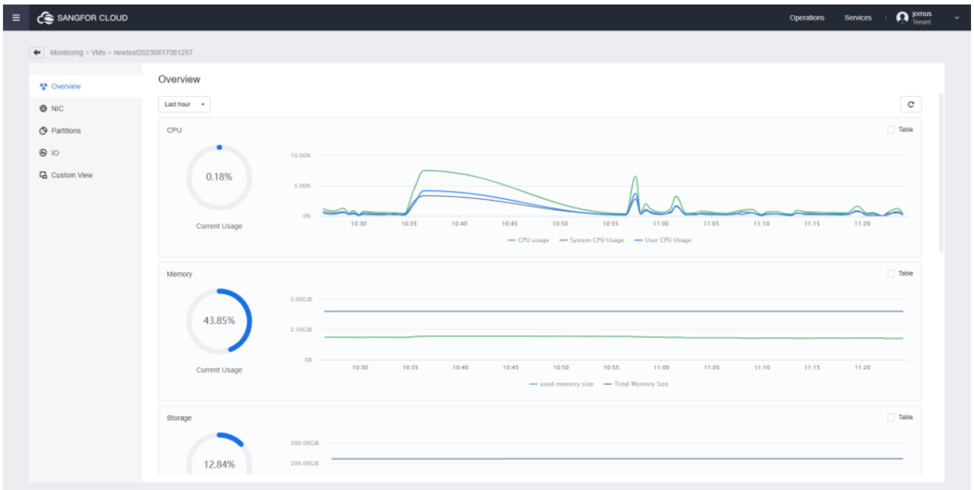
5. After a moment, you will soon see the **Collection Status** change to **Normal**.



VMs

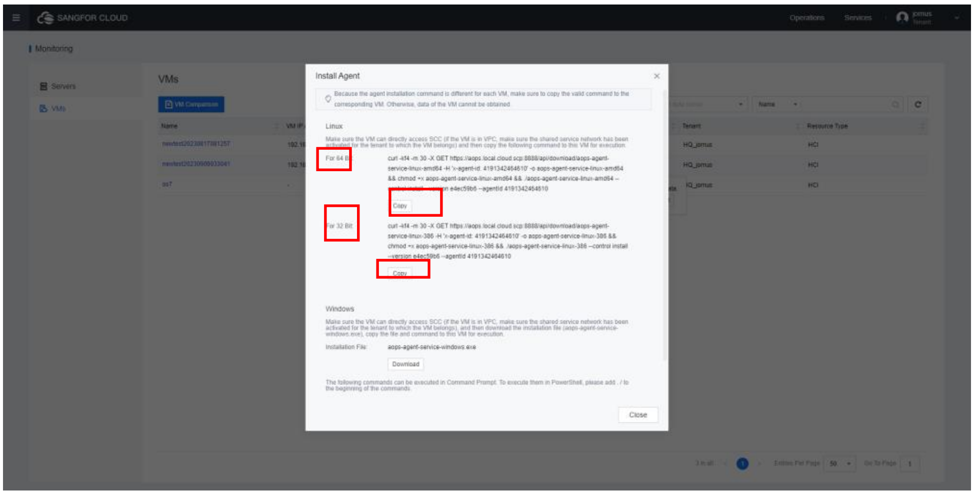
Name	VM IP Address	VM Status	Collection Status	Data Center	Tenant	Resource Type
2016	-	Powered on	Data not reported	SCP_ID	HQ_jomus	HCI
newtest20230909033041	192.168.0.45	Powered on	Normal	SCP_ID	HQ_jomus	HCI
newtest20230817081257	192.168.0.44	Powered on	Normal	SCP_ID	HQ_jomus	HCI

6. Click the virtual machine name, and the tenant can obtain the VM's actual information in real-time.



Linux virtual machine

1. Copy the command on the page, then execute the command in your Linux virtual machine and wait for the execution result.



Install Agent

Because the agent installation command is different for each VM, make sure to copy the valid command to the corresponding VM. Otherwise, data of the VM cannot be obtained.

Linux

Make sure the VM can directly access SCC (if the VM is in VPC, make sure the shared service network has been activated for the tenant to which the VM belongs) and then copy the following command to this VM for execution.

For 64 Bit

```
curl -kf4 -m 30 -X GET https://aops.local.cloud.scp:8888/api/download/aops-agent-service-linux-amd64 -H 'x-agent-id: 4191342464610' -o aops-agent-service-linux-amd64 && chmod +x aops-agent-service-linux-amd64 && ./aops-agent-service-linux-amd64 --control install --version e4ec59b6 --agentId 4191342464610
```

Copy

For 32 Bit

```
curl -kf4 -m 30 -X GET https://aops.local.cloud.scp:8888/api/download/aops-agent-service-linux-386 -H 'x-agent-id: 4191342464610' -o aops-agent-service-linux-386 && chmod +x aops-agent-service-linux-386 && ./aops-agent-service-linux-386 --control install --version e4ec59b6 --agentId 4191342464610
```

Copy

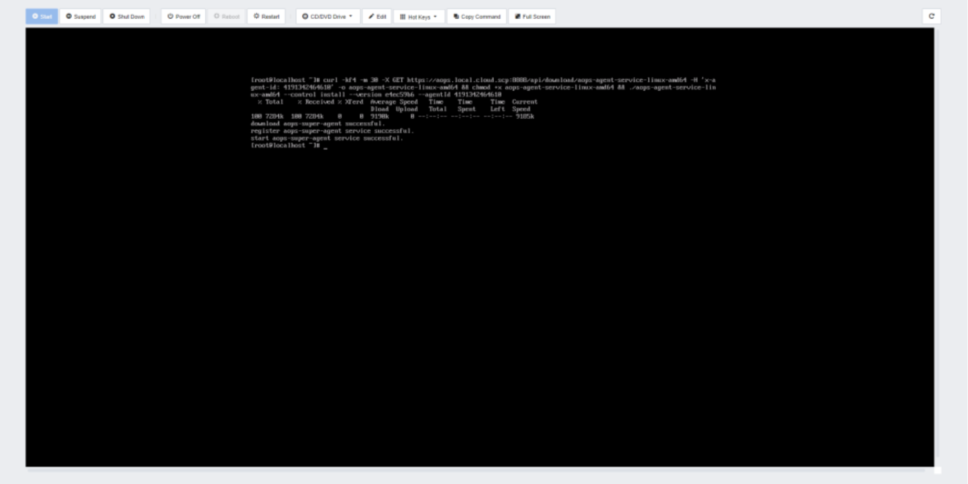
Windows

Make sure the VM can directly access SCC (if the VM is in VPC, make sure the shared service network has been activated for the tenant to which the VM belongs), and then download the installation file (aops-agent-service-windows.exe), copy the file and command to this VM for execution.

Installation File: aops-agent-service-windows.exe

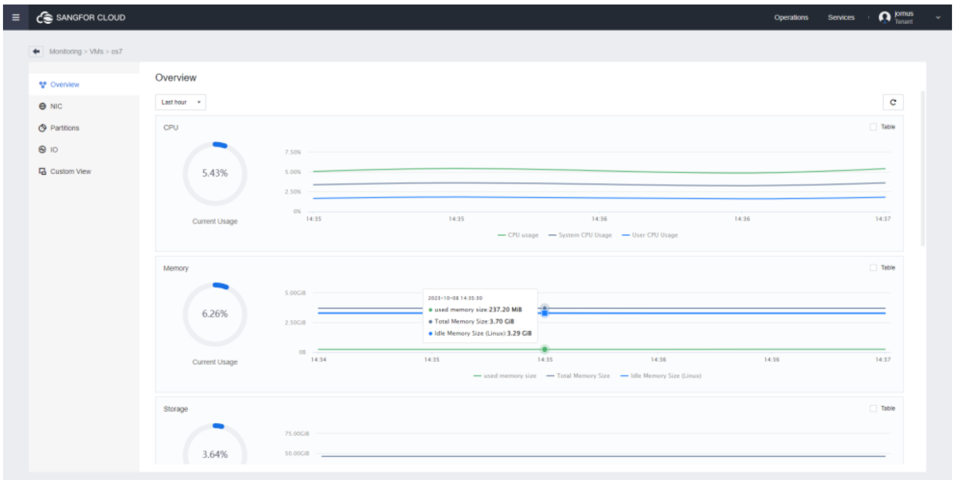
Download

The following commands can be executed in Command Prompt. To execute them in PowerShell, please add . / to the beginning of the commands.



```
[root@localhost ~]# curl -kf4 -m 30 -X GET https://aops.local.cloud.scp:8888/api/download/aops-agent-service-linux-amd64 -H 'x-a
gent-id: 4191342464610' -o aops-agent-service-linux-amd64 && chmod +x aops-agent-service-linux-amd64 && ./aops-agent-service-lin
ux-amd64 --control install --version e4ec59b6 --agentId 4191342464610
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 7204k  100 7204k    0     0  9198k      0 --:--:-- --:--:-- --:--:-- 9185k
download aops-super-agent successful.
register aops-super-agent service successful.
start aops-super-agent service successful.
[root@localhost ~]# _
```

2. Click the virtual machine name, and the tenant can obtain the VM's actual information in real-time.

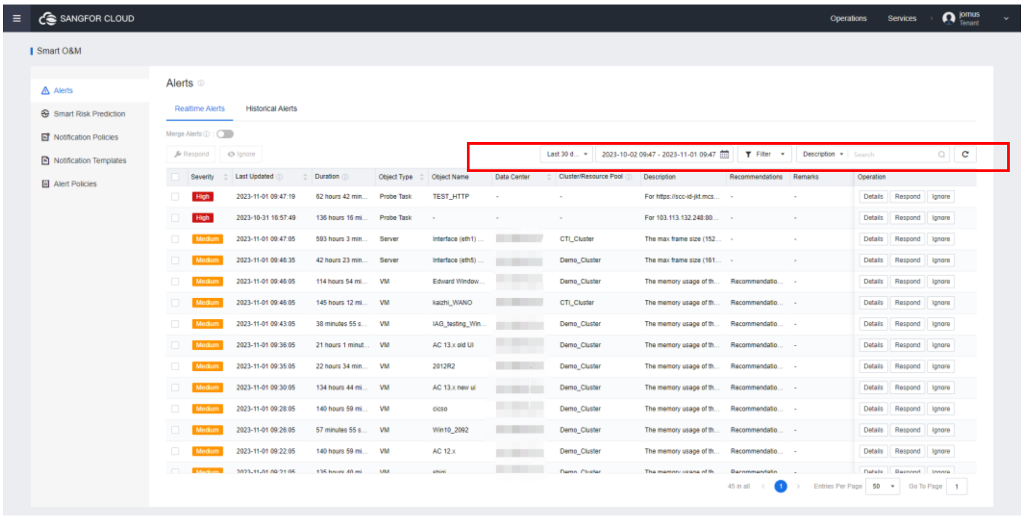


1.5 Smart O&M

The console will monitor the platform and virtual machines in real-time based on the alert policies. All alerts will be recorded. Tenants can view recent alerts or historical alerts as needed to troubleshoot and locate abnormalities.

1.5.1 View Alert

View alert issues in **Smart O&M > Alert**. You can filter the alert as shown below.



2023-10-02 09:47 - 2023-11-01 09:47

Severity	Last Updated	Duration	Object Type	Object Name	Data Center	Cluster/Resource Pool	Description	Recommendations	Remarks	Operation
High	2023-11-01 09:47:19	62 hours 42 min...	Probe Task	TEST_HTTP	-	-	For https://scc-id-jkt.mcs...	-	-	Details Respond Ignore
High	2023-10-31 16:57:49	136 hours 16 mi...	Probe Task	-	-	-	For 103.113.132.248:80...	-	-	Details Respond Ignore
Medium	2023-11-01 09:47:05	593 hours 3 min...	Server	Interface (eth1) ...	[redacted]	CTI_Cluster	The max frame size (152...	-	-	Details Respond Ignore
Medium	2023-11-01 09:46:35	42 hours 23 min...	Server	Interface (eth5) ...	[redacted]	Demo_Cluster	The max frame size (161...	-	-	Details Respond Ignore
Medium	2023-11-01 09:46:05	114 hours 54 mi...	VM	Edward Window...	[redacted]	Demo_Cluster	The memory usage of th...	Recommendatio...	-	Details Respond Ignore
Medium	2023-11-01 09:46:05	145 hours 12 mi...	VM	kaizhi_WANO	[redacted]	CTI_Cluster	The memory usage of th...	Recommendatio...	-	Details Respond Ignore
Medium	2023-11-01 09:43:05	38 minutes 55 s...	VM	IAG_testing_Win...	[redacted]	Demo_Cluster	The memory usage of th...	Recommendatio...	-	Details Respond Ignore
Medium	2023-11-01 09:36:05	21 hours 1 minut...	VM	AC 13.x old UI	[redacted]	Demo_Cluster	The memory usage of th...	Recommendatio...	-	Details Respond Ignore
Medium	2023-11-01 09:35:05	22 hours 34 min...	VM	2012R2	[redacted]	Demo_Cluster	The memory usage of th...	Recommendatio...	-	Details Respond Ignore
Medium	2023-11-01 09:30:05	134 hours 44 mi...	VM	AC 13.x new ui	[redacted]	Demo_Cluster	The memory usage of th...	Recommendatio...	-	Details Respond Ignore
Medium	2023-11-01 09:28:05	140 hours 59 mi...	VM	cicso	[redacted]	Demo_Cluster	The memory usage of th...	Recommendatio...	-	Details Respond Ignore
Medium	2023-11-01 09:26:05	57 minutes 55 s...	VM	Win10_2092	[redacted]	Demo_Cluster	The memory usage of th...	Recommendatio...	-	Details Respond Ignore
Medium	2023-11-01 09:22:05	140 hours 59 mi...	VM	AC 12.x	[redacted]	Demo_Cluster	The memory usage of th...	Recommendatio...	-	Details Respond Ignore
Medium	2023-11-01 09:21:05	135 hours 40 mi...	VM	shini	[redacted]	Demo_Cluster	The memory usage of th...	Recommendatio...	-	Details Respond Ignore

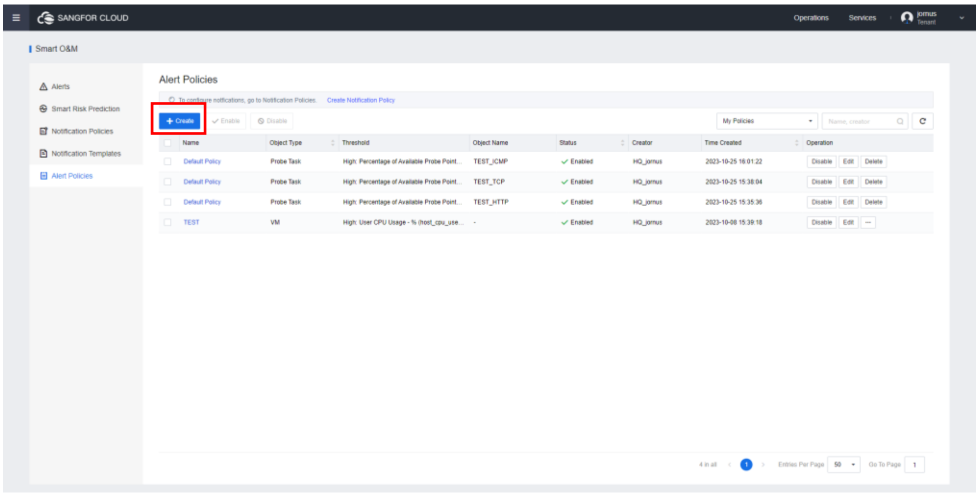
45 in all 1 Entries Per Page 50 Go To Page 1

1.5.2 Alert Policies

Tenants can create, edit, enable, disable, and delete alert policies on the **Alert**

Policies page.

1. Log in to MCS, navigate to **Smart O&M > Alert > Alert Policies**, and click **Create**. The probe task will be considered a default alert policy.

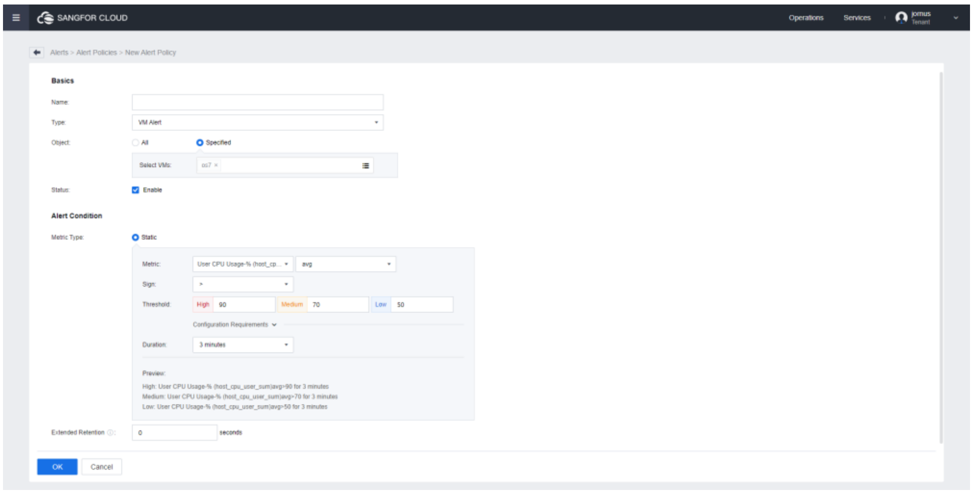


Alert Policies

To configure notifications, go to Notification Policies. Create Notification Policy

Name	Object Type	Threshold	Object Name	Status	Creator	Time Created	Operation
Default Policy	Probe Task	High: Percentage of Available Probe Point...	TEST_ICMP	✓ Enabled	HQ_jomus	2023-10-25 16:01:22	Disable Edit Delete
Default Policy	Probe Task	High: Percentage of Available Probe Point...	TEST_TCP	✓ Enabled	HQ_jomus	2023-10-25 15:38:04	Disable Edit Delete
Default Policy	Probe Task	High: Percentage of Available Probe Point...	TEST_HTTP	✓ Enabled	HQ_jomus	2023-10-25 15:35:36	Disable Edit Delete
TEST	VM	High: User CPU Usage - % (host_cpu_use...	-	✓ Enabled	HQ_jomus	2023-10-08 15:39:18	Disable Edit ···

2. Configure **Basics** and **Alert Condition** according to requirements.


SANGFOR CLOUD
Operations
Services
jomus
Tenant
Alerts > Alert Policies > New Alert Policy
Configuration Requirements
OK
Cancel

Basics

Name:

Type: VM Alert

Object: ○ All ● Specified

Select VMs: os7 ×

Status: ☑ Enable

Alert Condition

Metric Type: ● Static

Metric: User CPU Usage-% (host_cp... avg

Sign: >

Threshold: High 90 Medium 70 Low 50

Duration: 3 minutes

Preview:

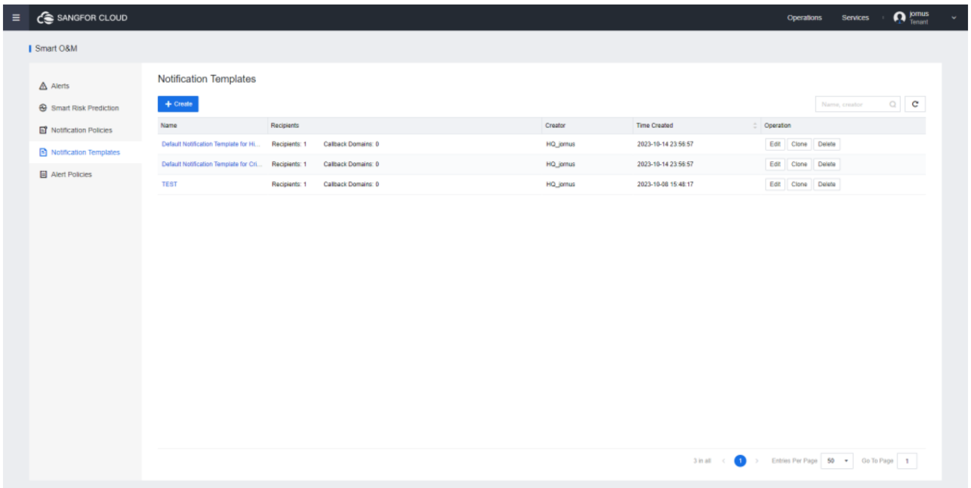
High: User CPU Usage-% (host_cpu_user_sum)avg>90 for 3 minutes
Medium: User CPU Usage-% (host_cpu_user_sum)avg>70 for 3 minutes
Low: User CPU Usage-% (host_cpu_user_sum)avg>50 for 3 minutes

Extended Retention: 0 seconds

1.5.3 Notification Policies

Tenants can **create, edit, enable, disable,** and **delete** notification policies on the **Notification Policies** page.

1. Log in to the MCS, navigate to **Smart O&M > Alert > Notification Template,** and click **Create**.

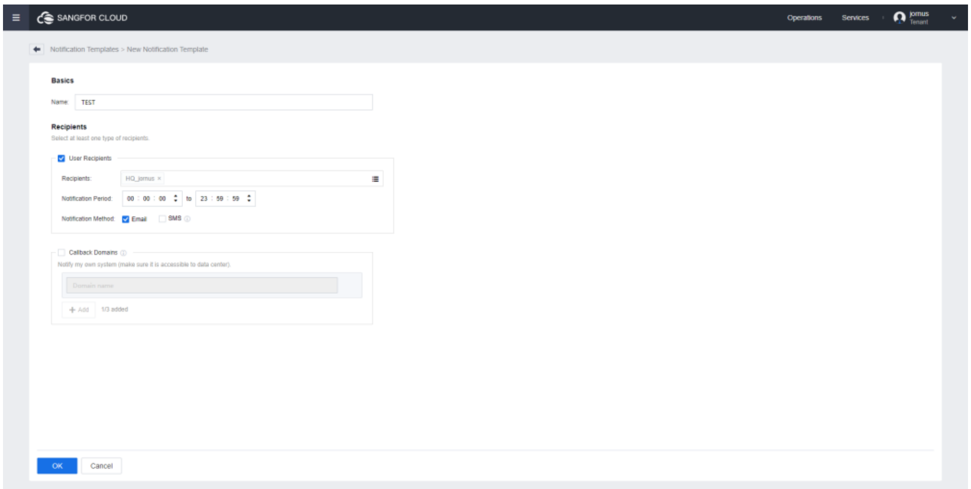


Notification Templates

Name	Recipients		Creator	Time Created	Operation
Default Notification Template for Hi...	Recipients: 1	Callback Domains: 0	HQ_jomus	2023-10-14 23:56:57	Edit Clone Delete
Default Notification Template for Cri...	Recipients: 1	Callback Domains: 0	HQ_jomus	2023-10-14 23:56:57	Edit Clone Delete
TEST	Recipients: 1	Callback Domains: 0	HQ_jomus	2023-10-08 15:48:17	Edit Clone Delete

3 in all ‹ 1 › Entries Per Page 50 Go To Page 1

2. Configure **Basics** and **Recipients** according to requirements.



Basics

Name: TEST

Recipients

Select at least one type of recipients.

☑ User Recipients

Recipients: HQ_jomus ×

Notification Period: 00 : 00 : 00 to 23 : 59 : 59

Notification Method: ☑ Email □ SMS

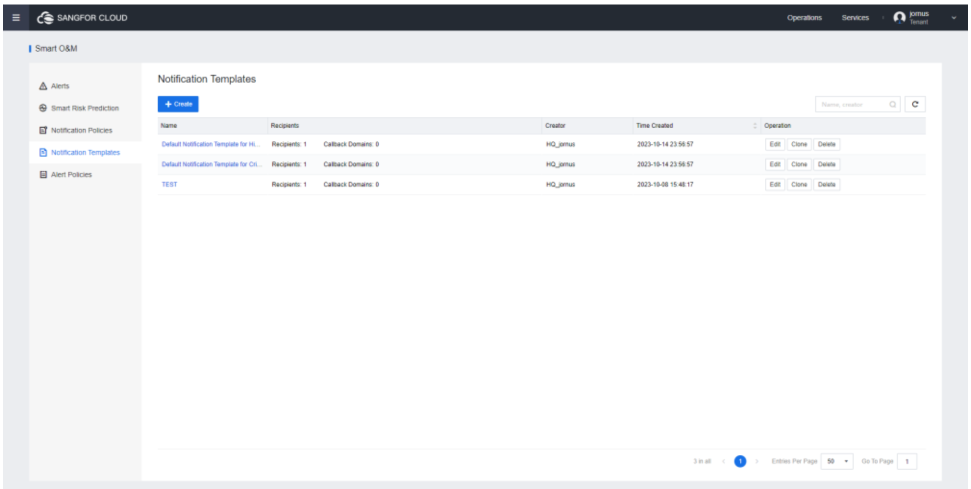
□ Callback Domains

Notify my own system (make sure it is accessible to data center).

Domain name

1/3 added

3. Click **OK** to complete the configuration of templates.

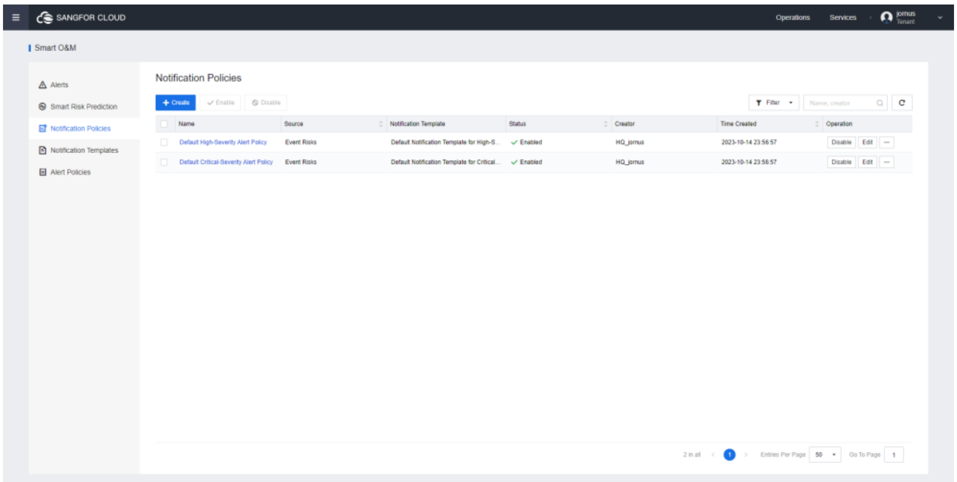


Notification Templates

Name	Recipients		Creator	Time Created	Operation
Default Notification Template for Hi...	Recipients: 1	Callback Domains: 0	HQ_jomus	2023-10-14 23:56:57	Edit Clone Delete
Default Notification Template for Cri...	Recipients: 1	Callback Domains: 0	HQ_jomus	2023-10-14 23:56:57	Edit Clone Delete
TEST	Recipients: 1	Callback Domains: 0	HQ_jomus	2023-10-08 15:48:17	Edit Clone Delete

3 in all ‹ 1 › Entries Per Page 50 Go To Page 1

4. In **Notification Policies**, click **Create**.



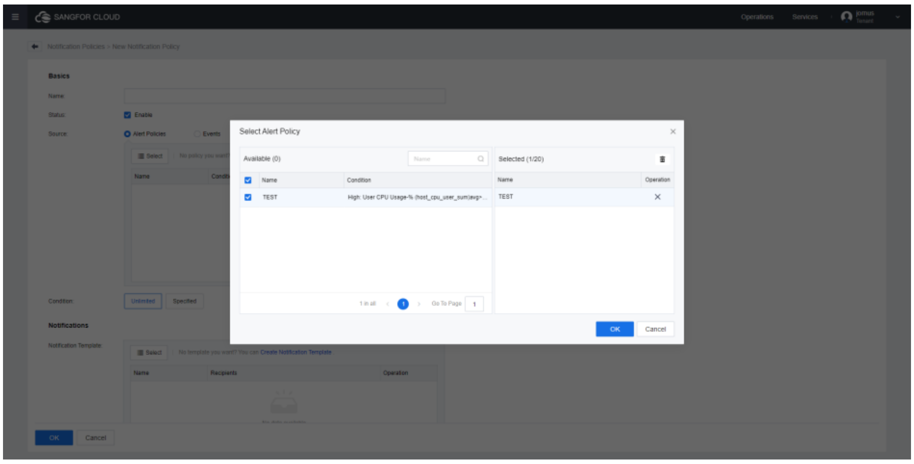
Notification Policies

Name	Source	Notification Template	Status	Creator	Time Created	Operation
Default High-Severity Alert Policy	Event Risks	Default Notification Template for High-S...	✓ Enabled	HQ_jomus	2023-10-14 23:56:57	Disable Edit ···
Default Critical-Severity Alert Policy	Event Risks	Default Notification Template for Critical...	✓ Enabled	HQ_jomus	2023-10-14 23:56:57	Disable Edit ···

5. Configure the options according to your needs.

Select **Source** as **Alert Policies:**

a. Click **Select** to choose the recently created alert policies.



Status: ☑ Enable

Source: ● Alert Policies ○ Events

Select Alert Policy

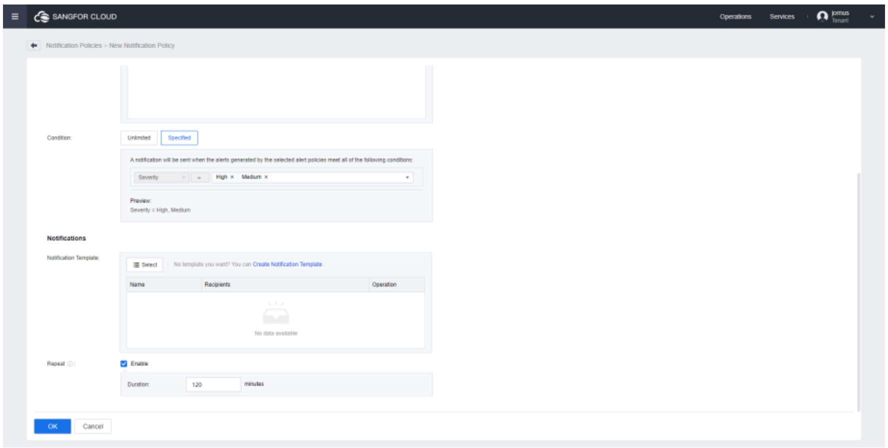
Available (0)

☑	Name	Condition
☑	TEST	High: User CPU Usage-% (host_cpu_user_sum)avg>...

Selected (1/20)

Name	Operation
TEST	×

b. In **Condition**, set it as **Unlimited** or **specify the alert severity**.


SANGFOR CLOUD
Operations
Services
jomus
Tenant
Notification Policies > New Notification Policy
Unlimited
Specified
Notifications
Select
No template you want? You can Create Notification Template
No data available
OK
Cancel

Condition: Specified

A notification will be sent when the alerts generated by the selected alert policies meet all of the following conditions:

Severity = High × Medium ×

Preview:
Severity = High, Medium

Notification Template:

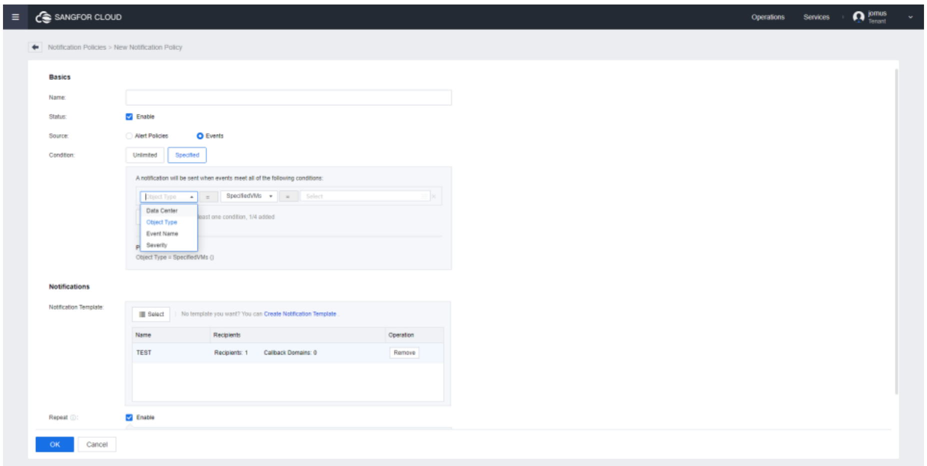
Name	Recipients	Operation

Repeat: ☑ Enable

Duration: 120 minutes

Select **Source** as **Event Risks:**

a. In **Condition**, select **Unlimited** or **Specified** according to different conditions. Alert notifications will be triggered based on the selected event.



Notification Policies > New Notification Policy

Basics

Name:

Status: ☑ Enable

Source: ○ Alert Policies ● Events

Condition: Unlimited [✓ Specified]

A notification will be sent when events meet all of the following conditions:

Object Type = SpecifiedVMs = Select

...east one condition, 1/4 added

Object Type = SpecifiedVMs ()

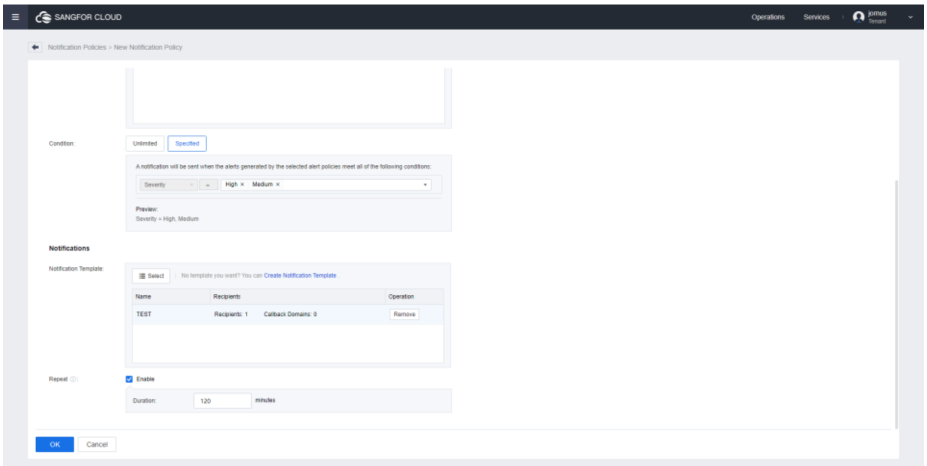
Notifications

Notification Template: Select | No template you want? You can Create Notification Template .

Name	Recipients		Operation
TEST	Recipients: 1	Callback Domains: 0	Remove

Repeat: ☑ Enable

b. In the **Notification Template,** select the notification templates that we just created.



Notification Policies > New Notification Policy

Condition: Unlimited [✓ Specified]

A notification will be sent when the alerts generated by the selected alert policies meet all of the following conditions:

Severity = High × Medium ×

Preview:
Severity = High, Medium

Notifications

Notification Template: Select | No template you want? You can Create Notification Template .

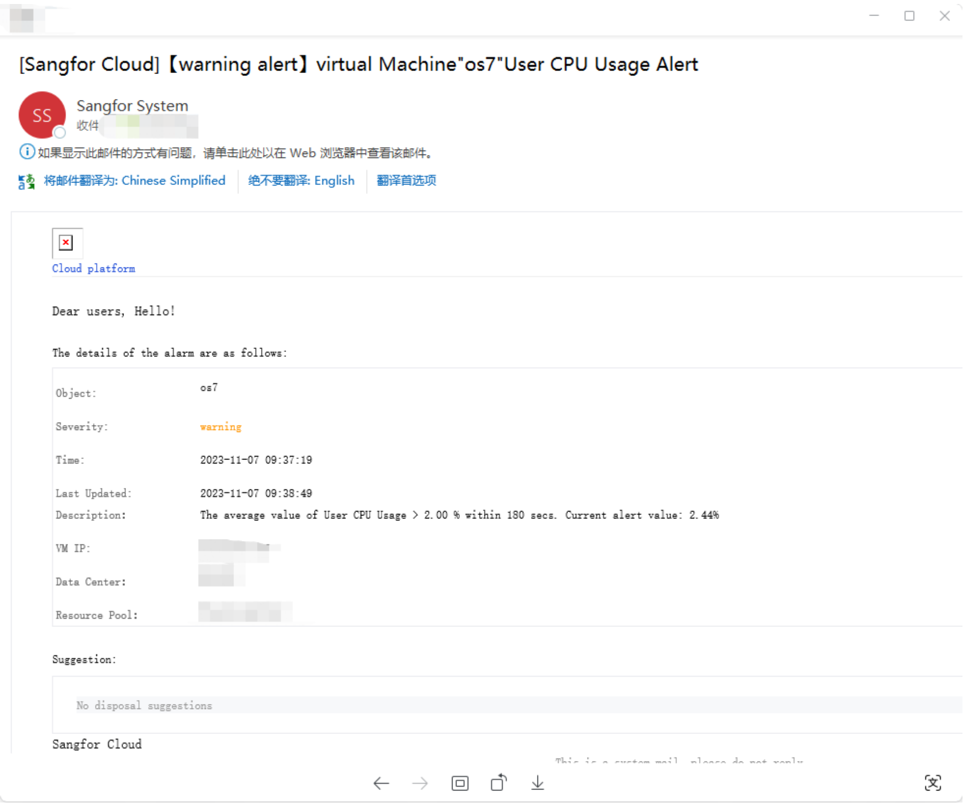
Name	Recipients		Operation
TEST	Recipients: 1	Callback Domains: 0	Remove

Repeat: ☑ Enable

Duration: 120 minutes

c. Click **OK** to complete the configuration.

6. An example of an alert is shown below.



[redacted]

[Sangfor Cloud]【warning alert】virtual Machine"os7"User CPU Usage Alert

SS Sangfor System
收件 [redacted]

ⓘ如果显示此邮件的方式有问题，请单击此处以在 Web 浏览器中查看该邮件。

将邮件翻译为: Chinese Simplified | 绝不要翻译: English | 翻译首选项

Cloud platform

Dear users, Hello!

The details of the alarm are as follows:

Object:	os7
Severity:	warning
Time:	2023-11-07 09:37:19
Last Updated:	2023-11-07 09:38:49
Description:	The average value of User CPU Usage > 2.00 % within 180 secs. Current alert value: 2.44%
VM IP:	[redacted]
Data Center:	[redacted]
Resource Pool:	[redacted]

Suggestion:

No disposal suggestions

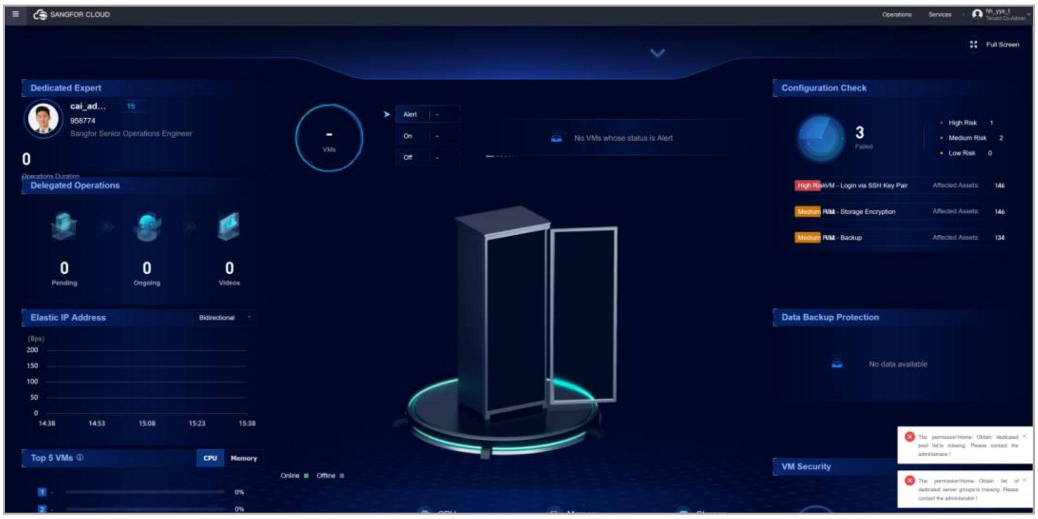
Sangfor Cloud

This is a system mail, please do not reply

1.6 Tenant Co-Admin Monitoring

The monitor displayed for the tenant co-admin is the same as that for the tenant if the tenant allocates related permissions, such as the homepage, dedicated cloud monitor, and monitoring permissions, to the tenant co-admin.

If permissions are not allocated to the tenant co-admin, no data is available on the monitor for the tenant co-admin.



High Risk	VM - Login via SSH Key Pair	Affected Assets:	146
Medium	VM - Storage Encryption	Affected Assets:	146
Medium	VM - Backup	Affected Assets:	134

The permission'Home: Obtain dedicated pool list'is missing. Please contact the administrator !

The permission'Home: Obtain list of dedicated server groups'is missing. Please contact the administrator !

Relevant data will be available if the following permissions are allocated to the tenant co-admin:

Home: Obtain the list of dedicated resource pools

Home: Obtain the dedicated resource pool overview

Home: Obtain the overview of physical resources of the dedicated resource pool

Home: Obtain the data backup protection information of the dedicated resource pool

Home: Obtain the intelligent security protection information of the dedicated resource pool

Home: Obtain the security information of VMs in the dedicated resource pool

Home: Obtain the server list

Home: Obtain the server details

Home: Obtain the list of dedicated server groups

Home: Obtain the dedicated server group overview

Home: Obtain the list of elastic IPs of the dedicated server group

Home: Obtain the overview of physical resources of the dedicated server group

Home: Obtain the data backup protection information of the dedicated server group

Home: Obtain the intelligent security protection information of the dedicated server group

Home: Obtain the security information of VMs in the dedicated server group

Home: Obtain the VM list

Home: Obtain the information of the dedicated expert and MSP

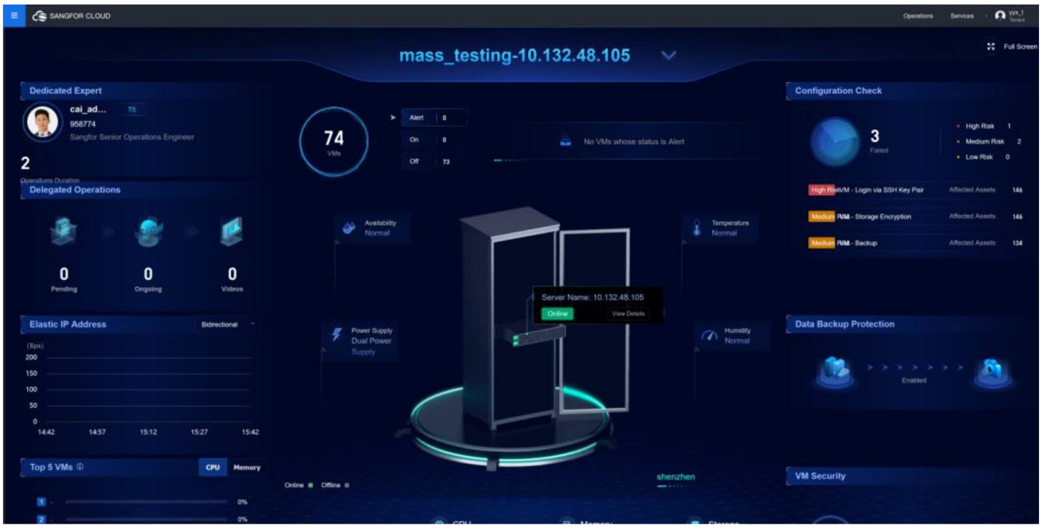
Home: Obtain the information of delegated operations service

Home: Obtain the configuration check information of VMs

Operations Center: Obtain the list of elastic IPs and bandwidth

O&M - Monitoring and Alert: View the trend graph of monitoring data

O&M - Monitoring and Alert: View the latest monitoring data


SANGFOR CLOUD
Operations
Services
Full Screen
mass_testing-10.132.48.105
Dedicated Expert
cai_ad...
958774
Sangfor Senior Operations Engineer
2
Operations Duration
Delegated Operations
0
Pending
0
Ongoing
0
Videos
Elastic IP Address
Bidirectional
(Bps)
200
150
100
50
0
14:42
14:57
15:12
15:27
15:42
Top 5 VMs
CPU
Memory
1
2
0%
0%
74
VMs
Alert 0
On 0
Off 73
No VMs whose status is Alert
Availability
Normal
Temperature
Normal
Power Supply
Dual Power
Supply
Humidity
Normal
Server Name: 10.132.48.105
Online
View Details
Online
Offline
shenzhen
Configuration Check
3
Failed
High Risk 1
Medium Risk 2
Low Risk 0
High Risk VM - Login via SSH Key Pair
Affected Assets: 146
Medium RM - Storage Encryption
Affected Assets: 146
Medium RM - Backup
Affected Assets: 134
Data Backup Protection
Enabled
VM Security