

SecMaster

FAQs

Issue 03
Date 2024-10-30



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Product Consulting	1
1.1 Why Is There No Attack Data or Only A Small Amount of Attack Data?	1
1.2 Where Does SecMaster Obtain Its Data From?	1
1.3 What Are the Dependencies and Differences Between SecMaster and Other Security Services?	2
1.4 What Are the Differences Between SecMaster and HSS?	3
1.5 What Are the Relationships and Differences Between SecMaster and SA?	5
1.6 Why Cannot the Total ECS Quota Be Less Than the Number of Existing ECSs?	6
1.7 Can I Use SecMaster Across Accounts?	6
1.8 How Do I Update My Security Score?	7
1.9 How Do I Handle a Brute-force Attack?	8
1.10 Issues About Data Synchronization and Data Consistency	9
1.11 How Do I Grant Permissions to an IAM User?	10
1.12 How Long Are Logs Stored in SecMaster?	11
2 Purchase Consulting	13
2.1 How Do I Change SecMaster Editions or Specifications?	13
2.2 How Do I Obtain Permissions to Purchase SecMaster?	13
2.3 How Do I Release an ECS or VPC Endpoint?	15
3 About Data Collection Faults	18
3.1 Component Controller Installation Failure	18
3.2 Collection Node or Collection Channel Faults	22
3.3 Common Commands for the Component Controller	25
4 Regions and AZs	27
4.1 What Are Regions and AZs?	27

1 Product Consulting

1.1 Why Is There No Attack Data or Only A Small Amount of Attack Data?

SecMaster can detect a variety of attacks on cloud assets and presents them objectively.

If your assets are exposed little to the Internet (risks such as open ports and weak passwords can be exploited by attackers), it is less likely that they will be attacked. So there will be no or little security data in SecMaster.

If you believe that SecMaster fails to reflect the attack status of your system, feel free to provide feedback to our customer service.

1.2 Where Does SecMaster Obtain Its Data From?

SecMaster utilizes threat data collected from cloud-based threats and Huawei cloud services. Through big data mining and machine learning, it analyzes and presents threat trends while providing protection suggestions.

- SecMaster collects data from network traffic and security device logs to present the security status of assets and generate corresponding threat alerts using AI analysis.
- Additionally, SecMaster aggregates alarm data from other security services, such as Host Security Service (HSS) and Web Application Firewall (WAF). Based on obtained data, SA then performs big data mining, machine learning, and intelligent AI analysis to identify attacks and intrusions, helping you understand the attack and intrusion processes and providing related protection suggestions.

By analyzing security data that covers every aspect of your services, SecMaster makes it easier for you to understand comprehensive security situation of your services and make informed decisions and handle security incidents in real time.

For details about how to access data, see [Accessing Data](#).

1.3 What Are the Dependencies and Differences Between SecMaster and Other Security Services?

SecMaster can work with other security services such as WAF, HSS, Anti-DDoS, and DBSS.

- **How SecMaster Works With Other Services**

SecMaster is a security management service that depends on other security services to provide threat detection data so that it can analyze security threat risks, display the global security threat posture, and provide informed suggestions.

Other security services report detected threats to SecMaster and SecMaster aggregates the received data to display the global security posture.

- **Differences Between SecMaster and Other Security Services**

SecMaster: It is only a visualized threat detection and analysis platform and does not implement any specific protective actions. It must be used together with other security services.

Other security services display the event data detected by themselves only. They can take specific protective actions, but cannot display global threat posture.

Table 1-1 describes the differences between SecMaster and other security protection services.

Table 1-1 Differences between SecMaster and other services

Service	Category	Dependency and Difference	Protected Object	Function
SecMaster	Security management	SecMaster focuses on the global security threat and attack situation, analyzes threat data generated by several security services and cloud security threats, and provides protection suggestions.	Display the global security threat attack situation.	SecMaster Functions
Anti-DDoS	Network security	Anti-DDoS detects and defends against abnormal DDoS attack traffic, and synchronizes attack logs and defense data to SecMaster.	Ensure enterprise service stability.	Anti-DDoS Features
Host Security Service (HSS)	Host security	HSS detects host security risks, executes protection policies, and synchronizes related alerts and protection data to SecMaster.	Ensures host security.	HSS Functions

Service	Category	Dependency and Difference	Protected Object	Function
WAF	Application security	WAF checks website service traffic in multiple dimensions. It can defend against common attacks and block threats to website. Intrusion logs and alert data are synchronized to SecMaster to present the network-wide web risk situation.	Ensure availability and security of web applications.	WAF Functions
DBSS	Data security	DBSS protects and audits database access behaviors. Related audit logs and alert data are synchronized to SecMaster.	Ensure the security of databases and assets on the cloud.	DBSS Service Overview

1.4 What Are the Differences Between SecMaster and HSS?

Service Positioning

- SecMaster is a next-generation cloud native security operations platform. Based on years of Huawei Cloud experience in cloud security, it enables integrated and automatic security operations through cloud asset management, security posture management, security information and incident management, security orchestration and automatic response, cloud security overview, simplified cloud security configuration, configurable defense policies, and intelligent and fast threat detection and response.
- Host Security Service (HSS) is designed to protect server workloads in hybrid clouds and multi-cloud data centers. It protects servers and containers and prevents web pages from malicious modifications.

In short, SecMaster presents the comprehensive view of security posture, and HSS secures servers and containers.

Function Differences

- SecMaster collects security data (including detection data of security services such as HSS, WAF, and Anti-DDoS) on the entire network and provides capabilities such as cloud asset management, security posture management, security information and incident management, security orchestration, and automatic response, helping you implement integrated and automatic security operations management.
- HSS uses technologies such as AI, machine learning, and deep algorithms to analyze server risks through agents installed on protected servers. It delivers inspection and protection tasks through the console. You can manage the security information reported by the Agent through the HSS console.

Table 1-2 Differences between SecMaster and HSS

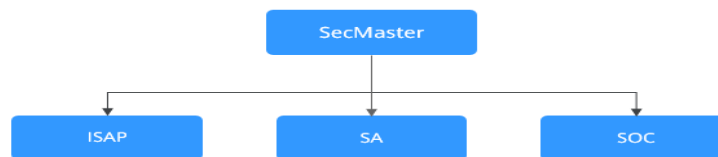
Item		Common Function	Difference
Asset security	Server	Both can display the overall security posture of servers.	<ul style="list-style-type: none"> • SecMaster synchronizes server risk data from HSS and then displays overall server security posture. • HSS scans accounts, ports, processes, web directories, software information, and automatic startup tasks on servers and displays server security posture.
	Websites	-	<ul style="list-style-type: none"> • SecMaster checks and scans the overall security posture of website assets from different dimensions. • HSS does not support this function.
Vulnerability	Emergency vulnerability notices	-	<ul style="list-style-type: none"> • SecMaster synchronizes security notices from Huawei Cloud. You can obtain security information in a timely manner. • HSS does not support this function.
	Server vulnerabilities	Both can display server scanning results and support server vulnerability management.	<ul style="list-style-type: none"> • SecMaster synchronizes server vulnerability data from HSS and allows you to manage server vulnerabilities in SecMaster. • HSS allows you to manage Linux, Windows, Web-CMS, and application vulnerabilities. It also gives you an overview of vulnerabilities in real time, including vulnerability scan details, vulnerability statistics, vulnerability types and distributions, your top 5 vulnerabilities, and the top 5 risky servers.
Baseline inspection	Cloud service baseline	-	<ul style="list-style-type: none"> • SecMaster can help you check key configurations of Huawei Cloud services you enabled based on built-in checks that are included in Cloud Security Compliance Check 1.0 and Network Security. • HSS does not support this function.

Item		Common Function	Difference
	Unsafe settings	-	<ul style="list-style-type: none"> SecMaster does not support this function. HSS checks your baseline settings, including checking for weak passwords, and reviewing security policies and configuration details. HSS provides an overview of your configuration security rating, the top 5 configuration risks, detected weak passwords, and the top 5 servers with weak passwords configured.

1.5 What Are the Relationships and Differences Between SecMaster and SA?

Huawei Cloud provides SecMaster and Situation Awareness (SA) services. Their relationships and differences are as follows.

Figure 1-1 SA and SecMaster



SecMaster integrates Situation Awareness (SA), Intelligent Security Analysis Platform (ISAP), and Security Operations Center (SOC).

- SecMaster is Huawei's next-generation cloud-native security operations center.
 Combined with Huawei Cloud years of experience in security and based on cloud-native security capabilities, SecMaster provides cloud asset management, security posture management, security information and incident management, security orchestration, automatic responses, and other functions, helping you implement integrated and automatic security operations management.
- Situation Awareness (SA) is a security management and situation analysis platform of Huawei Cloud.
 It gives you a comprehensive overview of your global security situation by leveraging the big data analysis technologies, making it easier for you to analyze attack events, threat alarms, and attack sources.
- Intelligent Security Analysis Platform (ISAP) is a data middle-end system for security operations analysis and modeling.

It supports collection of cloud service security logs, data retrieval, and intelligent modeling and provides professional security analysis capabilities to protect cloud workloads, applications, and data.

- Security Operations Center (SOC) is an operations platform that quickly responds to risky elements, threats, and vulnerabilities during security operation activities on the cloud. It works with the Security Operations, Analytics, and Response (SOAR) system to orchestrate, automate, manage, and control security risks on the cloud.

SOC provides a workbench entry based on a complete security operations service framework. You can use SOC to centrally manage security assets and policies, orchestrate automated responses, and handle security operations workflows.

1.6 Why Cannot the Total ECS Quota Be Less Than the Number of Existing ECSs?

The total ECS quota is the total number of hosts that are authorized to receive detections. When buying SecMaster, ensure that the total ECS quota is greater than or equal to the total number of hosts under the current account. Otherwise, threats may not be detected in a timely manner if unauthorized hosts are attacked, increasing risks such as data leakage.

[Table 1-3](#) describes the host quota configuration.

Table 1-3 ECS quota description

Parameter	Description
ECS Quota	<p>The maximum number of ECSs that require protection from SecMaster.</p> <p>The total ECS quota must be greater than or equal to the total number of hosts within your account. This value cannot be changed to a smaller one after your purchase is complete.</p> <p>NOTE</p> <ul style="list-style-type: none"> • The maximum ECS quota cannot exceed 10,000. • If some of your ECSs are not protected by SecMaster, threats to them cannot be detected in a timely manner, which may result in security risks, such as data leakage. To prevent this, increase the ECS quota upon an increase of the host asset quantity.

1.7 Can I Use SecMaster Across Accounts?

Yes.

Workspace agency allows for security operations across accounts. To be specific, you can centrally view asset risks, alerts, and incidents in workspaces entrusted by other users.

For details, see [Workspace Agency](#).

1.8 How Do I Update My Security Score?

SecMaster checks your asset health in real time, evaluates the overall security posture, and gives a security score. A security score helps you quickly understand the overall status of unprocessed risks to your assets.

After asset security risks are fixed, manually ignore or handle alerts and update the alert status in the alert list. The risk severity can be down to a proper level accordingly. Your security score will be updated after you refresh the alert status and check your environment again.

Procedure



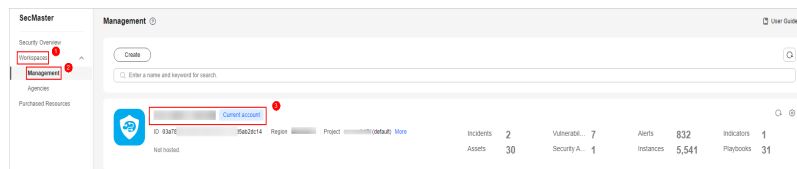
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner of the page and choose **Security & Compliance > SecMaster**.
- Step 4** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 1-2 Workspace management page



- Step 5** In the navigation pane on the left, choose **Risk Prevention > Baseline Check**. On the baseline check page displayed, handle the baseline check items that fail the check.
- Step 6** In the navigation pane on the left, choose **Risk Prevention > Vulnerabilities**. On the vulnerability management page displayed, handle the vulnerabilities.
- Step 7** In the navigation pane on the left, choose **Threat Operations > Alerts**. On the displayed page, handle the alert.
- Step 8** After handling unsafe settings, vulnerabilities, or alerts, go back to the **Security Situation > Situation Overview** page and click **Check Again**. After the check, the security score will be updated.

NOTE

It takes some time for a check to finish. You can refresh the page to get the new security score five minutes after you start the recheck.

----End

For more details about security score, see [Security Score](#).

1.9 How Do I Handle a Brute-force Attack?

Brute-force attacks are common intrusion behavior. Attackers guess and try login usernames and passwords remotely. When they succeed, they can attack and control systems.

SecMaster works with HSS to receive alerts for brute force attacks detected by HSS and centrally display and manage alerts.

Handling Alerts

HSS uses brute-force detection algorithms and an IP address blacklist to effectively prevent brute-force attacks and block attacking IP addresses. Alerts will be reported.

If you receive an alert from HSS, log in to the HSS console to confirm and handle the alert.


- If your host is cracked and an intruder successfully logs in to the host, all hosts under your account may have been implanted with malicious programs. Take the following measures to handle the alert immediately to prevent further risks to the hosts:
 - a. Check whether the source IP address used to log in to the host is trusted immediately.
 - b. Change passwords of accounts involved.
 - c. Scan for risky accounts and handle suspicious accounts immediately.
 - d. Scan for malicious programs and remove them, if any, immediately.
- If your host is cracked and the attack source IP address is blocked by HSS, take the following measures to harden host security:
 - a. Check the source IP address used to log in to the host and ensure it is trusted.
 - b. Log in to the host and scan for OS risks.
 - c. Upgrade the HSS protection capability if it is possible.
 - d. Harden the host security group and firewall configurations based on site requirements.


For details, see [How Do I Handle a Brute-force Attack Alarm?](#)

Marking Alerts

After an alert is handled, you can mark the alert.

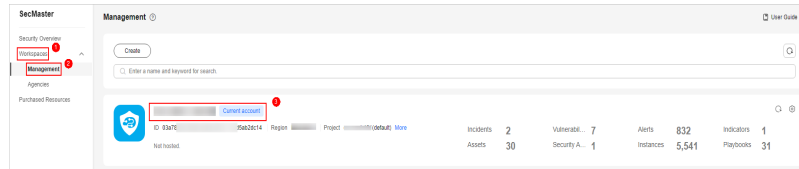
Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Security & Compliance > SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 1-3 Workspace management page



Step 5 In the navigation pane on the left, choose **Threat Operations > Alerts**.

Step 6 On the **Alert** tab, select **Brute-force attacks** and refresh the alert list.

Step 7 Delete the non-threat alerts.

----End

For details, see [Viewing Alerts](#).

1.10 Issues About Data Synchronization and Data Consistency

Why Is the Data in SecMaster Inconsistent with That in WAF or HSS?

SecMaster aggregates all historical alert data reported by WAF and HSS, but WAF and HSS display real-time alert data. So data in SecMaster is inconsistent with that in WAF and HSS.

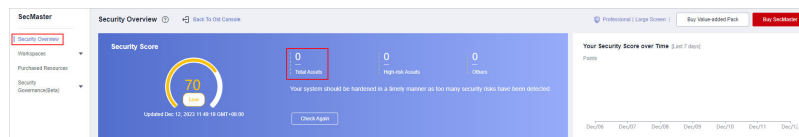
So you can go to the corresponding service (WAF or HSS) to view and handle latest alerts.

Why Is Zero Displayed for Total Assets on the Security Overview Page?

Symptom

A workspace was added and asset information was synchronized to and displayed on the **Resource Manager** page in the workspace, but the total number of assets on the **Security Overview** page is still 0.

Figure 1-4 Zero assets reported on the Security Overview page



Cause

SecMaster synchronizes asset details **every hour on the hour** after you create a workspace and synchronize asset information to the **Resource Manager** page.

Solution

Check the asset quantity after the very beginning of the next hour.

1.11 How Do I Grant Permissions to an IAM User?

If you want to authorize an IAM user to operate the SecMaster service, you need to use the primary account to grant permissions to the user.

Procedure

Step 1 Log in to the console as the administrator.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance > Identity and Access Management**.

Step 3 Create a user group.

1. In the navigation pane on the left, choose **User Groups**. On the displayed page, click **Create User Group** in the upper right corner.
2. On the **Create User Group** page, specify user group name and description.
 - **Name:** Set this parameter to **SecMaster_ops**.
 - **Description:** Enter a description.
3. Click **OK**.

Step 4 Create a custom policy.

1. In the navigation pane on the left, choose **Permissions > Policies/Roles**. In the upper right corner of the displayed page, click **Create Custom Policy**.
2. Configure a policy.
 - a. **Policy Name:** Set this parameter to **SecMaster_FullAccess**.
 - b. **Policy View:** Select **JSON**.
 - c. **Policy Content:** Copy the following content and paste it in the text box.

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "secmaster:*:*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

- a. Click **OK**.

Step 5 Assign permissions to the created user group.

1. In the navigation pane on the left, choose **User Groups**. On the displayed page, click **SecMaster_ops**.
2. On the **Permissions** tab page, click **Authorize**.
3. On the **Select Policy/Role** page, search for and select the **SecMaster_FullAccess** policy, and click **Next**.
4. Set the minimum authorization scope. Select **All resources** for **Scope**. After the setting is complete, click **OK**.

You can view the authorization record after the authorization is added.

----End

1.12 How Long Are Logs Stored in SecMaster?

SecMaster can aggregate logs from many cloud products, such as WAF, HSS, and OBS. After the log aggregation, SecMaster can query and analyze the data and perform intelligent modeling.

The following table lists how long SecMaster stores logs of cloud products.

Table 1-4 Log access supported by SecMaster

Cloud Service	Log Description	Log	Log Lifecycle
Web Application Firewall (WAF)	Attack logs	waf-attack	7 to 30 days
	Access logs	waf-access	
SecMaster	Compliance baseline log	secmaster-baseline	7 to 10 days
Object Storage Service (OBS)	Access logs	obs-access	7 to 15 days
Intrusion Prevention System (IPS)	Attack logs	nip-attack	7 to 30 days
Identity and Access Management (IAM)	Audit logs	iam-audit	7 to 30 days
Host Security Service (HSS)	HSS alarms	hss-alarm	7 to 30 days
	HSS vulnerability scan results	hss-vul	7 days
	HSS security logs	hss-log	7 to 15 days
Data Security Center (DSC)	Alarm logs	dsc-alarm	7 to 30 days
Anti-DDoS	Attack logs	ddos-attack	7 to 30 days
Database Security Service (DBSS)	Alarm logs	dbss-alarm	7 to 30 days
Cloud Trace Service (CTS)	CTS logs	cts-audit	7 to 30 days
Cloud Firewall (CFW)	Access control logs	cfw-block	7 to 30 days
	Traffic logs	cfw-flow	7 to 15 days
	Attack event logs	cfw-risk	7 to 30 days

Cloud Service	Log Description	Log	Log Lifecycle
API Gateway (APIG)	Access logs	apig-access	7 to 30 days

2 Purchase Consulting

2.1 How Do I Change SecMaster Editions or Specifications?

You can upgrade the SecMaster edition, increase ECS quotas, and buy a value-added package.

NOTICE

- The standard edition can only be billed on a yearly or monthly basis.
- Only one edition can be used within an account. Purchasing some asset quotas in the standard edition and other asset quotas in the professional edition is not supported.
- The **Large Screen**, **Intelligent Analysis**, and **Security Orchestration** in the value-added packages are plus features of the standard and professional editions. To use them, purchase the standard or professional edition first.

-
- Upgrade the edition: For details, see [Editon Upgrade](#).
 - Buy a value-added package: For details, see [Purchasing Value-Added Packages](#).
 - Increase ECS quotas: For details, see [Increasing the Quota](#).

2.2 How Do I Obtain Permissions to Purchase SecMaster?

If a message indicating insufficient permission is displayed when you purchase SecMaster, obtain the permission by following the procedure below.

Procedure

- Step 1** Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance > Identity and Access Management**.

Step 3 (Optional) Create a user group.

If the **SecMaster_ops** user group has been created, skip this step.

1. In the navigation pane on the left, choose **User Groups**. On the displayed page, click **Create User Group** in the upper right corner.
2. On the **Create User Group** page, specify user group name and description.
 - **Name:** Set this parameter to **SecMaster_ops**.
 - **Description:** Enter a description.
3. Click **OK**.

Step 4 Assign permissions to the user group.

1. Add global permissions.
 - a. In the navigation pane on the left, choose **Permissions > Policies**. In the upper right corner of the displayed page, click **Create Custom Policy**.
 - b. Configure a policy.

- **Policy Name:** Enter a policy name.
- **Policy View:** Select **JSON**.
- **Policy Content:** Copy the following content and paste it in the text box.

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:permissions:checkRoleForAgency",
        "iam:agencies:listAgencies",
        "iam:permissions:grantRoleToAgencyOnDomain",
        "iam:agencies:createAgency",
        "iam:permissions:grantRoleToAgency",
        "iam:permissions:grantRoleToAgencyOnProject"
      ]
    }
  ]
}
```

- c. Click **OK**.
2. Add project-level permissions.
 - a. In the navigation pane on the left, choose **Permissions > Policies**. In the upper right corner of the displayed page, click **Create Custom Policy**.
 - b. Configure a policy.

- **Policy Name:** Enter a policy name.
- **Policy View:** Select **JSON**.
- **Policy Content:** Copy the following content and paste it in the text box.

```
{
  "Version": "1.1",
```

```

"Statement": [
  {
    "Action": [
      "bss:order:pay",
      "bss:unsubscribe:update",
      "bss:order:view",
      "bss:balance:view",
      "bss:order:update",
      "ecs:cloudServers:list",
      "bss:renewal:view",
      "bss:renewal:update",
      "secmaster:*:*"
    ],
    "Effect": "Allow"
  }
]

```

c. Click **OK**.

Step 5 Assign permissions to the created user group.

1. In the navigation pane on the left, choose **User Groups**. On the displayed page, click **SecMaster_ops**.
2. On the **Permissions** tab page, click **Authorize**.
3. On the **Select Policy/Role** page, search for and select the policy added in **Step 4** and click **Next**.
4. Set the minimum authorization scope. Select **All resources** for **Scope**. After the setting is complete, click **OK**.
5. Verify the authorization. The policy will be listed on the page.

Step 6 Add the operation account to the user group.

1. In the navigation pane on the left, choose **User Groups**.
2. Locate the row that contains the **SecMaster_ops** user group, and click **Manage User** the **Operation** column.
3. In the displayed **Manage User** dialog box, select users you want to add.
4. Click **OK**.

----End

2.3 How Do I Release an ECS or VPC Endpoint?


To enable log data collection, you are required to buy ECSs for collecting logs and configure VPC endpoints for establishing connections with and managing collection nodes.

- ECSs are billed. For details about ECS pricing, see [Billing Overview](#).
- VPC endpoints are billed. For details, see [VPC Endpoint User Guide](#).

If you no longer need log data collection or unsubscribe from SecMaster, you need to manually release the ECSs and VPC endpoints you create for log data collection, or they will continue to be billed. Perform the following steps:

Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 Release the ECS used for log data collection.


1. In the upper left corner of the page, click  and choose **Compute > Elastic Cloud Server**.
2. In the resource list, locate the row that contains the target ECS, choose **More > Unsubscribe** or **More > Delete** in the **Operation** column.

Figure 2-1 Unsubscribing from an ECS



3. In the dialog box displayed, unsubscribe from or delete the ECS as prompted.

Step 4 Release the VPC endpoints used to connect and manage collection nodes.


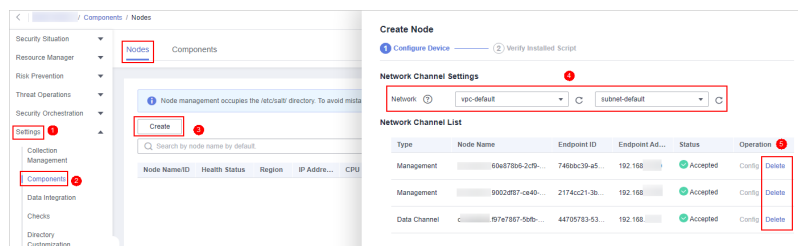
1. Click  in the upper left corner of the page and choose **Security & Compliance > SecMaster**.
2. In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
3. In the navigation pane on the left, choose **Settings > Components**.
4. Deregister a node.
 - a. On the **Nodes** tab, locate the row that contains the target node and click **Deregister** in the **Operation** column.
 - b. In the displayed dialog box, click **OK**.
5. Delete the VPC endpoint.
 - a. On the **Nodes** page, click **Create**. On the **Create Node** slide-out panel, select a network node.
 - b. In the network channel list, click **Delete**.

Figure 2-2 Deleting a node



c. In the displayed dialog box, click **OK**.


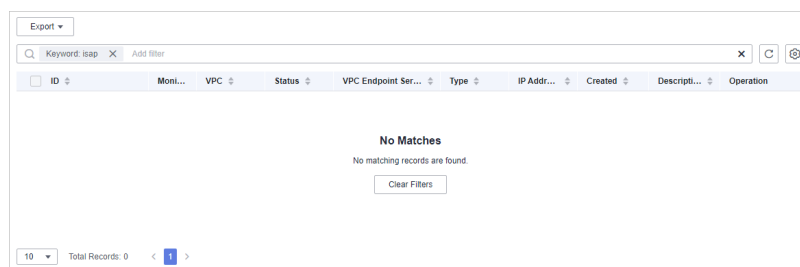
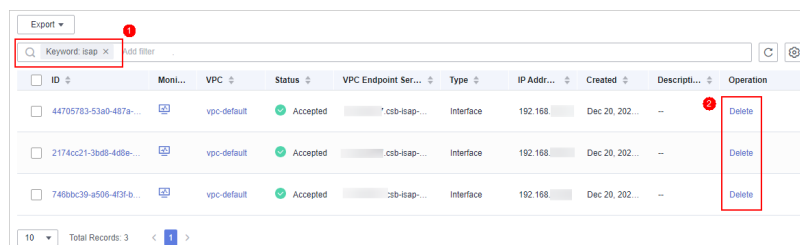
6. Check whether there are unreleased VPC endpoints created by SecMaster for log data collection.
 - a. In the upper left corner of the page, click  and choose **Networking > VPC Endpoint**.
 - b. In the VPC endpoint search box, enter **isap** and press **Enter** to search for VPC endpoints related to SecMaster data collection.
 - c. Check whether there are unreleased VPC endpoints created by SecMaster for log data collection.
 - If no, go to [Step 4.7](#).

Figure 2-3 Deleting a VPC endpoint



- If yes, locate the row that contains the target VPC endpoint and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.

Figure 2-4 Deleting a VPC endpoint



Then, go to [Step 4.7](#).

7. Check whether there are any VPC endpoints related to SecMaster are still being charged.
 - If yes, contact technical support.
 - If no, no further action is required.

----End

3 About Data Collection Faults

3.1 Component Controller Installation Failure

A component controller (isap-agent) needs to be installed on ECSs for security data collection. If the installation fails, you can fix the fault by following the instructions provided in this section.

For details about common commands used during troubleshooting, see [Common Commands for the Component Controller](#).

Possible Causes

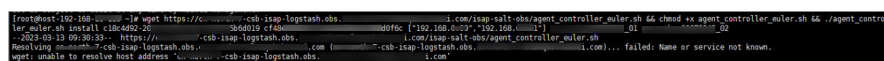
The possible causes are as follows:

- The network between the ECS where you want to install component controller isap-agent and the OBS bucket storing the agent is disconnected.
- The disk space of the ECS server is insufficient.
- Failed to obtain the IAM token.
- Failed to verify the workspace ID.
- The component controller isap-agent has been installed. The system attempts to install it again.

Locating the Cause and Fixing the Failure

- **The network between the ECS where you want to install component controller isap-agent and the OBS bucket storing the agent is disconnected.**

Figure 3-1 Disconnected network between the server and OBS



```
[root@host-192-168-0-20 ~]# wget https://cscb-isap-logstash.obs.amazonaws.com/isap-salt-obs/agent_controller_euler.sh 66 chood ex agent_controller_euler.sh 66 ./agent_control
ler_euler.sh install c18c4d92-2c3b5d019 cf484848ad0f2c [192.168.0.20] [192.168.0.20]
[2024-10-30 09:28:25] https://cscb-isap-logstash.obs.amazonaws.com/isap-salt-obs/agent_controller_euler.sh
Resolving cscb-isap-logstash.obs.amazonaws.com (cscb-isap-logstash.obs.amazonaws.com)... failed: Name or service not known.
wget: unable to resolve host address 'cscb-isap-logstash.obs.amazonaws.com'
```

Solution

- (Optional) Method 1: Connect the ECS to OBS.

- (Optional) Method 2: Manually download the installation script and installation package to the local PC, and upload the installation package to the **/opt/cloud** directory on the server.
 - i. Log in to the OBS management console.
 - ii. In the navigation pane on the left, choose **Buckets**. On the displayed page, click the name of the target bucket.
 - iii. On the displayed details page, download the installation script and installation package.
 - iv. Use a remote management tool, such as SecureFX or WinSCP, to log in to the server.
 - v. Upload the installation package to the **/opt/cloud** directory on the server.
- **The disk space of the ECS is insufficient.**

Figure 3-2 Insufficient disk space

```
[root@host-192.168... ~]# wget https://obssec-mrd-datas.obs-sec-mrd-datas.obs.com/salt/salt-minion-euler.zip
2023-09-13 09:33:03 -- https://obssec-mrd-datas.obs-sec-mrd-datas.obs.com/salt/salt-minion-euler.zip
Resolving obssec-mrd-datas.obs-sec-mrd-datas.obs.com (obssec-mrd-datas.obs-sec-mrd-datas.obs.com)... 200.0.80.29
Connecting to obssec-mrd-datas.obs-sec-mrd-datas.obs.com (obssec-mrd-datas.obs-sec-mrd-datas.obs.com)|200.0.80.29|443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 91255430 (87M) [application/zip]
Saving tar: salt-minion-euler.zip.31
100% [
```

Solution

Clear the disk to reserve sufficient space.

- **Failed to obtain the IAM token.**

- **Symptoms**

If information shown in the following figure is displayed in the log, the call to obtain IAM token failed.

Figure 3-3 IAM token failure

```
start to install isap-agent, please wait....
start to install isap-agent, please wait....
start to install isap-agent, please wait....
start to install isap-agent, please wait....
start to install isap-agent, please wait....
iam token error, install isap-agent fail
```

- **Troubleshooting and Solution**

- i. Check whether the IAM account or username in the command is correct.

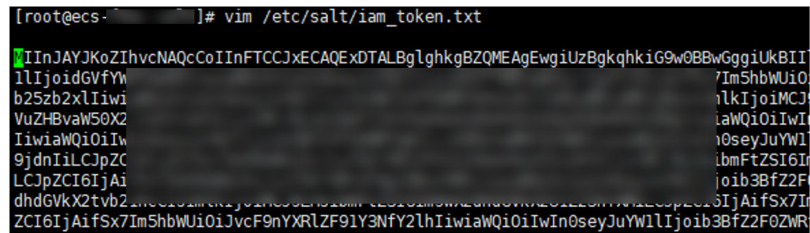
Figure 3-4 Username and password of an IAM user

```
[root@ecs-52fd-cloud]# curl -k -o /opt/cloud/agent_controller_euler.tar.gz --create-dirs https://... -csb-isap-logstash.obs-sec-mrd-datas.obs.com/isap-salt-obs-agent_controller_euler.tar.gz && tar -xzf /opt/cloud/agent_controller_euler.tar.gz -C /opt/cloud && sh /opt/cloud/agent_controller_euler.sh install ... -csb-isap-logstash.obs-sec-mrd-datas.obs.com https://iam.obs-sec-mrd-datas.obs.com/v3/auth/tokens 8a12588d-7... 4d8 cf48e 35ce392d9ffc [192.168... 192.168... 6]
01:
```

- o If any of them or both of them are incorrect, run the installation command with correct information again.
- o If they are correct, go to **ii**.
- ii. Run the **vim /etc/salt/iam_token.txt** command to check whether the **/etc/salt/iam_token.txt** file exists.

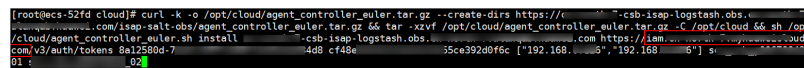
- If the information shown in the following figure is displayed, the directory exists. Go to [iii](#).

Figure 3-5 Checking files



- If a message is displayed indicating that the file does not exist, contact technical support.
- iii. Run the **ping** command to check whether the server is reachable. If it is unreachable, enable the communication.

Figure 3-6 Checking the network

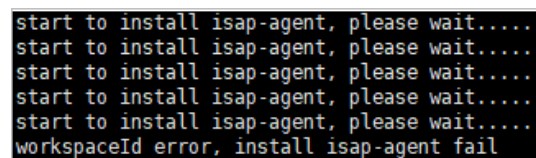


- **Failed to verify workspace ID.**

- **Symptoms**

If the information shown in the following figure is displayed, the Workspace ID verification fails.

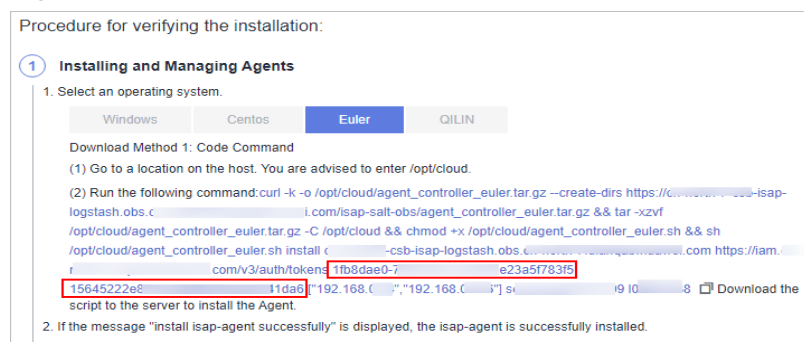
Figure 3-7 Workspace ID verification failure



- **Solution**

- Log in to the SecMaster management console.
- In the navigation pane on the left, choose **Workspaces**. In the workspace list, click the name of the target workspace.
- In the navigation pane on the left, choose **Settings > Components**. On the displayed page, click the target node.
- Check workspace ID and project ID in the command output.

Figure 3-8 Parameters on the console



- v. Check whether the workspace ID and project ID in the command are the same as those in the file in [iv](#).

Figure 3-9 Parameter information in the command

```
[root@ecs-...ud]# curl -k -o /opt/cloud/agent_controller_euler.tar.gz --create-dirs https://...csb-isap-logstash.obs...huawei.com/isap-salt-obs/agent_controller_euler.tar.gz && tar -zxvf /opt/cloud/agent_controller_euler.tar.gz -C /opt/cloud && chmod +x /opt/cloud/agent_controller_euler.sh && sh /opt/cloud/agent_controller_euler.sh install --workspaceid=...csb-isap-logstash.obs...iam.cn...cloud.com/v3/auth/tokens 8a125e...alworkspaceid=...c149e8...projectid=[192.168...192.168...] scc_c...42_01
```

- vi. Use the correct workspace ID and project ID to run the command again.
- **The component controller isap-agent has been installed. The system attempts to install it again.**

– **Symptoms**

If the information shown in the following figure is displayed, the Agent has been installed.

Figure 3-10 Agent installed already

```
warning: group servicegroup does not exist - using root
warning: user service does not exist - using root
warning: group servicegroup does not exist - using root
warning: user service does not exist - using root
warning: group servicegroup does not exist - using root
The ISAP-salt-minion-euler has been installed. Do not install the ISAP-salt-minion-euler again.
[root@ecs-...i]#
```

– **Solution**

- i. (Optional) Method 1: Logging out the node on the management console.
 - 1) Log in to the SecMaster management console.
 - 2) In the navigation pane on the left, choose **Workspaces**. In the workspace list, click the name of the target workspace.
 - 3) In the navigation pane on the left, choose **Settings > Components**. On the displayed **Nodes** tab, locate the row that contains the target node and click **Deregister** in the **Operation** column.
 - 4) In the displayed dialog box, click **OK**.
- ii. (Optional) Method 2: Run a script command to uninstall component controller isap-agent.
 - 1) Use a remote management tool, such as SecureFX or WinSCP, to log in to the server.
 - 2) Run the **sh /opt/cloud/agent_controller_euler.sh uninstall** command to uninstall the component controller.
- iii. Check whether the uninstallation is complete.
 - 1) Use a remote management tool, such as SecureFX or WinSCP, to log in to the server.
 - 2) (Optional) Method 1: Run the **ls -a /opt/cloud/** command to view the files in the **/opt/cloud** directory. If the information shown in the following figure is displayed (including only the script file), the uninstallation is complete.

Figure 3-11 Script file

```
[root@ecs-...i]# ls -a /opt/cloud/
.. agent_controller_euler.sh
```


- (Optional) Method 2: Run the **salt-minion --version** command. If the following information is displayed, the uninstallation is complete.

Figure 3-12 Checking isap-agent details

```
[root@ecs-]# salt-minion --version
-bash: salt-minion: command not found
```

CAUTION

It takes some time to deregister a node. Do not install the Agent until you confirm that the node has been deregistered.

3.2 Collection Node or Collection Channel Faults

Symptom

The component controller isap-agent periodically reports the collection node status and collection channel health status. Despite a delay of about one minute, the **Health Status** of a collection node or collection channel was still displayed as **Faulty** 3 minutes after the collection channel is delivered, and the CPU usage or memory usage of the server is about reached 100%.

Figure 3-13 Collection node fault

Node Name/ID	Health Status	Region	IP Address	CPU Usage	Memory Usage	Disk Usage	Network Speed	Channel Instance	Tag	Heartbeat/Disconnection Flag
44c-19902c7b386c231 595589f-9820-4719-0d	Faulty		192.168.0.1	97.00%	308M/4GB	13.00% 12GB/100GB	R: 0MB/s; W: 0MB/s	3	-	Online: 19902c7b386c231 (Jun 28, 2024 15:39:32 GMT+08:00)
44c-19902c7b386c231 5655718-4207-0a65-6	Normal		192.168.0.1	2.5%	58.00% 208M/4GB	6.50% 13GB/200GB	R: 0MB/s; W: 0MB/s	4	-	Online: 19902c7b386c231 (Jun 28, 2024 15:39:25 GMT+08:00)

Figure 3-14 Collection channel fault

Groups	Name	Connection Information	Created By	Health Status	Receiving Rate	Sending Rate	Configuration	Channel Instance	Delivery Status	Operations
All	eml_sender (Source Name)	eml_sender (Receiver Name)		Faulty	0 Slice/Second	0 Slice/Second	Synchronized	2	Running (-)	Enable Stop Restart More
	syslog (Source Name)	syslog (Receiver Name)		Normal	0 Slice/Second	0 Slice/Second	Synchronized	2	Running (-)	Enable Stop Restart More

Possible Causes

The configured connector or parser has syntax or semantic errors. As a result, the collector cannot run properly and restarts over and over again. The CPU and memory are exhausted.

Fault Location

- Remotely log in to the ECS where the collection node resides.

- Log in to the ECS console, locate the target server, and click **Remote Login** in the **Operation** column to log in to the server. For details, see [Login Using VNC](#).
 - If your server has an EIP bound, you can also use a remote management tool, such as PuTTY or Xshell, to log in to the server and install the component controller on the server as user **root**.
2. Run the following command to check the OS running status:
top
- If the following information is displayed, the Java process in the ECS uses a large number of CPU resources.

Figure 3-15 Status

```
top - 19:21:09 up 8 days, 29 min, 2 users, load average: 1.04, 0.29, 0.13
Tasks: 84 total, 1 running, 83 sleeping, 0 stopped, 0 zombie
%Cpu(s): 95.8 us, 3.7 sy, 0.0 ni, 0.5 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 3879596 total, 532820 free, 1234536 used, 2112240 buff/cache
KiB Swap: 0 total, 0 free, 0 used, 2295348 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
29442	root	20	0	4731800	1.0g	15528	S	190.3	27.9	0:44.63	java
29245	root	20	0	353640	30420	16508	S	0.7	0.8	0:00.23	dockerd
29425	root	20	0	11780	5464	2740	S	0.7	0.1	0:00.02	containerd-shim
9	root	20	0	0	0	0	S	0.3	0.0	1:41.10	rcu_sched
23490	root	20	0	830056	9704	4360	S	0.3	0.3	0:02.47	csb-isap-agent-

3. Run the following command to view the collector run logs:
docker logs isap-logstash -f
- According to the logs, the filter (parser) configuration of the current collection channel is incorrect, as shown in the following figure.

Figure 3-16 Collector run log

```
-f75 -XX:+UseConcMarkSweepGC, -Xmn1024M, -Djava.awt.headless=true, -Dirubyjit.threshold=0]
19:29:52.441 [main] INFO logstash.settings - Creating directory {setting=>"path.queue", :path=>"/opt/cloud/logstash/data/queue"}
19:29:52.452 [main] INFO logstash.settings - Creating directory {setting=>"path.dead_letter_queue", :path=>"/opt/cloud/logstash/data/dead_letter_queue"}
19:29:53.071 [LogStash::Runner] INFO LogStash.agent - No persistent UUID file found. Generating new UUID {uuid=>"496252c6-e46b-4e48-82b3-1b3d27664db2", :path=>"/opt/cloud/logstash/data/uuid"}
19:29:54.574 [Api Webserver] INFO LogStash.agent - Successfully started Logstash API endpoint {port=>9600, :ssl_enabled=>false}
19:29:56.063 [Converge PipelineAction::Create<2aac87a0-c8b5-4cc8-8bbb-f74fe131dca1>] ERROR LogStash.agent - Failed to execute action {action=>LogStash::PipelineAction::Create/pipeline_id:2aac87a0-c8b5-4cc8-8bbb-f74fe131dca1, :exception=>"LogStash::ConfigurationError", :message=>"Expected one of [\\t\\n\\r\\n], \\s*, \\s* at line 15, column 6 (byte 1463) after filter {name " ", :backtrace=>["/opt/cloud/logstash/logstash-core/lib/logstash/compiler.rb:32:in 'compile_imperative'", "/opt/cloud/logstash/execution/AbstractPipelineExt.java:189:in 'initialize'", "/opt/cloud/logstash/execution/JavaBasePipelineExt.java:72:in 'initialize'", "/opt/cloud/logstash/logstash-core/lib/logstash/java_pipeline.rb:48:in 'initialize'", "/opt/cloud/logstash/logstash-core/lib/logstash/pipeline_action/create.rb:52:in 'execute'", "/opt/cloud/logstash/logstash-core/lib/logstash/agent.rb:388:in 'block in converge_state'"]}}
19:29:56.151 [LogStash::Runner] INFO LogStash.runner - Logstash shut down.
19:29:56.160 [LogStash::Runner] FATAL org.logstash.Logstash - Logstash stopped processing because of an error: (SystemExit) exit
org.jruby.exceptions.SystemExit: (SystemExit) exit
  at org.jruby.RubyKernel.exit(org/jruby/RubyKernel.java:747) ~[jruby-complete-9.2.20.1.jar:7]
  at org.jruby.RubyKernel.exit(org/jruby/RubyKernel.java:710) ~[jruby-complete-9.2.20.1.jar:7]
  at opt.cloud.logstash.lib.bootstrap.environment.<main>(</opt/cloud/logstash/lib/bootstrap/environment.rb:94> ~[?:7])
Using bundled JDK: /opt/cloud/logstash/jdk
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
WARNING: Could not find logstash.yml which is typically located in $LS_HOME/config or /etc/logstash. You can specify the path using --path.settings. Continuing using the defaults
```

4. Run the following command to switch to the directory where the collection channel configuration file is stored:
cd /opt/cloud/logstash/config/files
5. Run the following command to check whether the filter part is abnormal:
cat Configuration file name
- If the information shown in the following figure is displayed, the current filter is abnormal.

Figure 3-17 Filter exceptions

```

[root@... ~]# pwd
/opt/cloud/logstash/config/files
[root@... ~]# ll
total 0
-rw-r--r-- 1 root root 1646 Jun 27 19:29 2aac87ab-c8b5-4cc8-8bbb-f74fe1314ca1.conf
drwxr-xr-x 2 root root 4096 Jun 27 19:29 certificate
[root@... ~]# cat 2aac87ab-c8b5-4cc8-8bbb-f74fe1314ca1.conf
input {
  pulsar {
    service_url => "pulsar+ssl://[redacted]:1"
    is_pw_encrypted => true
    encrypt_key => [redacted]
    tls_trust_certs_file_path => "/opt/cloud/logstash/config/gomas-pulsar-ca_cert.pem"
    pipes => ["persistent://[redacted]:4638-b445-10[redacted]496"]
    auth_params => {"366639336165623166383435393962303a3a62303665353335303765376436306133363564313338376665643431383838343a3a
6338363
3764353
6432653
3338633
3862653
336265383366396164373136653039313530383064373639353334663930326266316331616139346463336435373733393933363939346131633139
3766393138653831323764353566366365"}
    consumer_name => "isap-collector"
    subscription_name => "isap-collector-f74fe1314ca1-c8-8bbb-f74fe1314ca1"
  }
}
filter {
  else if [asdfsadsaf] {
    mutate {
      convert => {
        "sadffd" => "asdfsadf"
      }
    }
  }
}
output {
  file {
    path => "/opt/cloud/logstash/config/a.txt"
    create_if_deleted => true
    codec => "json_lines"
  }
}

```

Solution

- Step 1 Log in to the SecMaster console and access the target workspace.
- Step 2 In the navigation pane on the left, choose **Settings > Collections**. Then, select the **Parsers** tab.
- Step 3 Click **Edit** in the **Operation** column of the row containing the target parser. On the edit page, delete the incorrect configuration and configure it again.

Figure 3-18 Configurations of an abnormal parser

Basic Information

* Name:

Description:

Rules

* Conditional control: Else if

Exist

* Parsing rule: Mutate filter

Convert: Remove

+ Add

+ Add Configuration

+ Add

Figure 3-19 Modifying the parser configuration

The screenshot shows a configuration form with two main sections: 'Basic Information' and 'Rules'.
Basic Information:
 - **Name:** A text input field containing 'error_parser'.
 - **Description:** A text area with the placeholder 'Enter a description.' and a character count '0/256' at the bottom right.
Rules:
 - **Parsing rule:** A dropdown menu showing 'UUID' with a trash icon to its right.
 - **Target:** A text input field containing 'uuid'.
 - **Overwrite:** Radio buttons for 'Yes' (selected) and 'No'.
 At the bottom left of the form is a '+ Add' button with a dropdown arrow.

Step 4 Click **OK**.

Step 5 Click the **Collection Channels** tab, locate the target connection channel, and click **Restart** in the **Operation** column.

Step 6 Check the status of the collection channel and collection node.

- After the restart is complete, go to the **Collection Channels** tab and check the health status of the target collection channel.
- Select the **Collection Nodes** tab. On the page displayed, check the health status of the target collection node.

If the **Health Status** of the collection channel and collection node is **Normal**, the fault has been rectified.

----End

3.3 Common Commands for the Component Controller

Here are some commands you may need to troubleshoot the installation failure of the component controller isap-agent.

- Restart

sh /opt/cloud/isap-agent/action/agent_controller_linux.sh restart

Note: This command will stop and then restart the isap-agent process. You can use command to restart isap-agent if isap-agent fails start or the process does not exist due to a node fault.

- Start

sh /opt/cloud/isap-agent/action/agent_controller_linux.sh start

Note: You can use this command to start isap-agent if isap-agent breaks down but the automatic startup time for disaster recovery does not arrive.

- Stop

sh /opt/cloud/isap-agent/action/agent_controller_linux.sh stop

You can use this command to stop isap-agent. This command will clear the scheduled automatic startup check settings to stop the isap-agent process.

- Checking processes

ps -ef|grep isap-agent

You can use this command to check whether isap-agent is installed on the current host.

- Checking logs

tail -100f /opt/cloud/isap-agent/log/run.log

You can use this command to query the latest 100 lines of logs of the isap-agent service to locate exceptions.

- Disk partitions

sh /opt/cloud/isap-agent/action/agent_controller_linux.sh partition

When you install the collector on a node, you can use this command to partition disks you attach to the node.

4 Regions and AZs

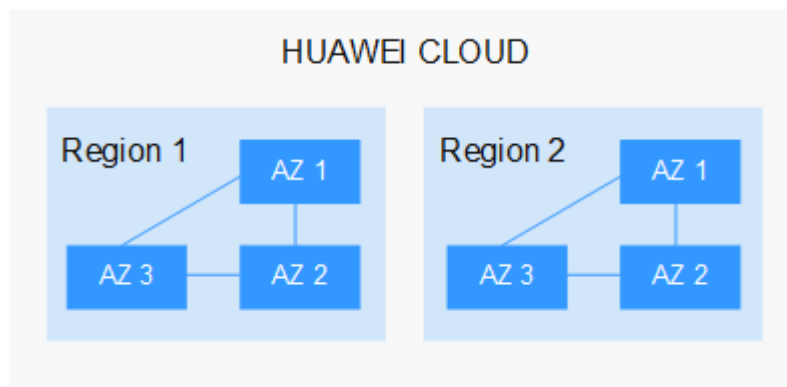
4.1 What Are Regions and AZs?

Concepts

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided from the dimensions of geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, compute, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to facilitate the construction of cross-AZ high-availability systems.

[Figure 4-1](#) shows the relationship between regions and AZs.

Figure 4-1 Relationship between regions and AZs

Huawei Cloud provides services in many regions around the world. You can select regions and AZs as needed.

Selecting a Region

If you or your users are in Europe, select the **EU-Dublin** region.

Selecting an AZ

When determining whether to deploy resources in the same AZ, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs in the same region.
- For low network latency, deploy resources in the same AZ.