SecMaster

FAQs

Issue 09

Date 2025-08-08

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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 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)	Server security	HSS detects host security risks, executes protection policies, and synchronizes related alerts and protection data to SecMaster.	Ensures host security.	**HSS Functions**
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**

1.2 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

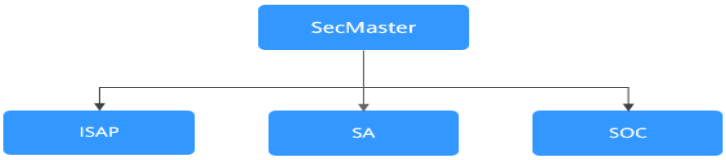
Item		Common Function	Difference
Asset security	Server	Both can display the overall security posture of servers.	• SecMaster synchronizes server risk data from HSS and then displays overall server security posture. • HSS scans accounts, ports, processes, web directories, software information, and automatic startup tasks on servers and displays server security posture.
	Websites	-	• SecMaster checks and scans the overall security posture of website assets from different dimensions. • HSS does not support this function.
Vulnerability	Emergency vulnerability notices	-	• SecMaster synchronizes security notices from Huawei Cloud. You can obtain security information in a timely manner. • HSS does not support this function.

Item		Common Function	Difference
	Server vulnerabilities	Both can display server scanning results and support server vulnerability management.	• 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	-	• 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.
	Unsafe settings	-	• 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.

1.3 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.

1.4 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, SecMaster 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, see **Enabling Log Access** and **Log Data Collection**.

2 About Purchase and Specifications Change

2.1 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 2-1 describes the host quota configuration.

Table 2-1 ECS quota description

Parameter	Description
ECS Quota	The maximum number of servers that require protection. The total ECS quota must be greater than or equal to the total number of servers within your account. This value cannot be changed to a smaller one after your purchase is complete. **NOTE** • 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 quota whenever your server quantity increases.

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 SecMaster 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/Roles**. 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"
            "iam:permissions:checkRoleForAgencyOnDomain"
            "iam:permissions:checkRoleForAgencyOnProject"
            "iam:permissions:checkRoleForAgency"
            "iam:roles:listRoles"
         ]
```



```
        }
    ]
}
```

c. Click **OK**.

2. Add project-level permissions.

a. In the navigation pane on the left, choose **Permissions** > **Policies/Roles**. 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, 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 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 **Edition Upgrade**.
- Buy a value-added package: For details, see **Purchasing Value-Added Packages**.
- Increase ECS quotas: For details, see **Increasing the Quota**.

2.4 How Do I Upgrade SA to SecMaster?

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.

SecMaster is an upgraded version of SA. New functions and version iteration will be performed in SecMaster. If you are using SA, SecMaster is recommended for your use in the future.

Precautions

- Only the upgrade from SA to SecMaster is supported. The change from SecMaster to SA is not supported.
- During the upgrade, your SA quota will be allocated to different regions for SecMaster during the upgrade. Before the upgrade, make sure you know how you want SecMaster to take over your SA quota. Note that the SA purchase channel will be unavailable later.
- After the upgrade, SA and SecMaster share the same lifecycle. However, as for you pay-per-use SA subscriptions, you still need to go to the SA console for cancelling or renewing the subscription.

- After the upgrade, change operations cannot be performed in SecMaster. If you need to perform operations such as version upgrade or quota increase, perform the operations in SA.

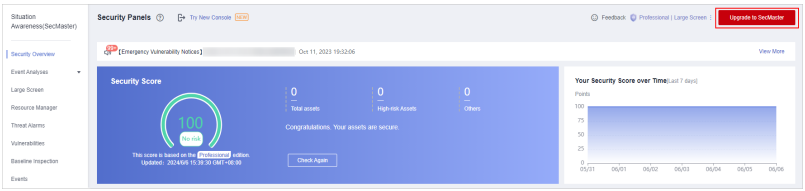
Upgrading SA to SecMaster

Step 1 Log in to the SecMaster console.

Step 2 In the upper left corner of the page, click ☰ and choose **Security & Compliance** > **Situation Awareness**.

Step 3 In the upper right corner of the page displayed, click **Upgrade to SecMaster**.

Figure 2-1 Upgrade to SecMaster



Step 4 On the **Upgrade to SecMaster** page, configure parameters.

- **Edition Mapping**: The system has automatically synchronized the edition mappings between SA and SecMaster (edition, billing mode, or large screen). No manual configuration is required.
- **Allocate Quota**: Allocate all SA quotas to SecMaster based on your needs.

Step 5 Click **Upgrade Now**.

After the upgrade is complete, you can use SecMaster. Go to SecMaster: Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**. For more details, see SecMaster Introduction.

----End

3 Security Situation

3.1 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.

Updating the Security Score

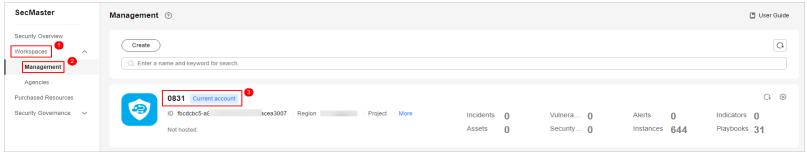
Step 1 **Log in to the SecMaster console.**

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 3-1 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 **Threats** > **Alerts**. On the displayed page, handle the alert.

Step 8 After handling unsafe settings, vulnerabilities, or alerts, go back to the **Situation Awareness** > **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 details, see **Security Score**.

3.2 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.

3.3 Why Is Data Inconsistent or Not Displayed on the Security Overview Page?

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.

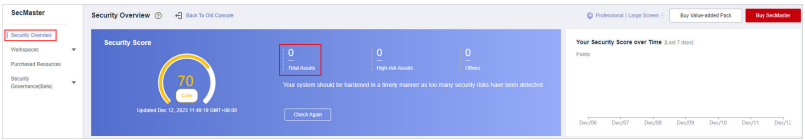
So you can go to the corresponding service (WAF or HSS) to view and handle latest alerts.

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 3-2 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.

4 Risk Prevention

4.1 What Is the Difference Between a Baseline and a Vulnerability?

Baseline Inspection

A baseline is a critical cloud security configuration that defines the minimum security requirements for system and service management. It establishes standardized settings across service, application, OS, and component configurations. SecMaster provides baseline inspection. This feature can scan cloud services for risks in key configuration items, report scan results by category, generate alerts for incidents, and provide hardening suggestions and guidelines.

- For details about the built-in check items supported by SecMaster, see **Built-in Check Items**.
- For more details about baseline inspection, see **Overview**.
- The following table lists the compliance packs built in SecMaster.

Table 4-1 SecMaster Built-in Compliance Packs

Compliance Pack	Description	Applicable Region	Category	Domain
Cloud Security Compliance Check 1.0	This compliance pack automates the assessment of your data security posture across four key areas: identity and access management, infrastructure security, data protection, and backup integrity. It helps you efficiently identify data security issues.	Global	Industry standards	Network security
DJCP 2.0 Level 3 Requirements	This compliance pack provides check items and guidelines to help you evaluate your data security management. It also suggests improvements based the level 3 requirements of China's national standard GB/T 22239-2019 information security technology — Baseline for classified protection of cybersecurity.	China	National standards	Network security

Compliance Pack	Description	Applicable Region	Category	Domain
Network Security	This compliance pack offers automated security checks aligned with international best practices. It enables cloud customers to identify threats and risks across key assets—including cloud servers, web applications, object storage, and data security centers—enhancing overall network security capabilities.	Global	Industry standards	Network security
Huawei Cloud Security Configuration	This compliance pack automates security configuration checks for IAM, monitoring, compute (container and cloud server), network, storage, and data services against cloud security benchmarks, helping you establish and maintain a secure cloud foundation.	Global	Industry standards	Network security

Compliance Pack	Description	Applicable Region	Category	Domain
GDPR	The *General Data Protection Regulation (GDPR)* is a comprehensive data privacy law established by the European Union to safeguard individuals' personal data and ensure its secure processing. It mandates that all organizations processing EU citizens' personal data must ensure transparent, lawful, and secure data processing practices.	European Union	Regional laws	Data protection
OS Configuration Baseline	This compliance pack checks password complexity policies, common weak passwords, and configurations. It can detect insecure password configurations and risky configurations in key software on servers, and provide rectification suggestions for detected risks, helping you correctly handle risky configurations on servers.	Global	Industry standards	Operating systems (OSs)

Compliance Pack	Description	Applicable Region	Category	Domain
Common Weak Password Detection	This check compares passwords used by accounts with common weak passwords defined in a library and reminds users to change detected weak passwords.	Global	Industry standards	Operating systems (OSs)
Password Complexity Policy Detection	A password complexity policy specifies the rules that user passwords must comply with to improve password security and defend against brute-force attacks. This feature checks the password complexity policies in Linux and provides suggestions to help improve password security.	Global	Industry standards	Operating systems (OSs)
PCI-DSS	The *Payment Card Industry Data Security Standard (PCI DSS)* is a global security standard jointly formulated by five major payment card brands (Visa, Mastercard, American Express, Discover, and JCB) to protect payment card data and prevent data leaks and frauds.	Global	Industry standards	Data security

Compliance Pack	Description	Applicable Region	Category	Domain
NIST SP 800-53	*NIST SP 800-53* provides a comprehensive security control framework for organizations to identify, assess, and manage information security risks.	Global	Industry standards	Data security

Vulnerabilities

A vulnerability is a defect or weakness in operating systems, security policies, or software. Attackers may exploit these defects or weaknesses to damage system, steal data, interrupt services, or cause other security problems. SecMaster can integrate vulnerability scan results from Host Security Service (HSS) and vulnerability data you import into SecMaster, so that you can quickly locate vulnerable assets and fix vulnerabilities. For more details, see **Vulnerability Management Overview**.

4.2 How Do I Handle Vulnerabilities?

1. **View vulnerability details**.
2. **Fix vulnerabilities** one by one by vulnerability severity.
   - For a Windows server, you need to restart it after you fix its vulnerabilities.
   - For a Linux server, you need to restart it after you fix its kernel vulnerabilities.
3. **Verify the vulnerability fix**.

4.3 Why Is an Alert Still Reported After I Fixed a Vulnerability?

If you **fix a vulnerability** on the SecMaster console and a message is displayed indicating that the vulnerability fails to be fixed, possible causes are as follows:

Linux Servers

- No Yum sources have been configured.

  In this case, configure a Yum source suitable for your Linux OS. Then, fix the vulnerability again.

- The Yum source does not have the latest software upgrade package.

  Switch to the Yum source that has the corresponding software package, configure the Yum source, and then fix the vulnerability.

- The intranet cannot connect to the Internet.

  To fix vulnerabilities online, you need to connect to the Internet and use external Yum sources. If your server cannot access the Internet, or the external yum sources cannot provide stable services, you can use a Huawei Cloud **image source**.

- The old kernel version remains.

  Old kernel versions often remain on servers after an upgrade. You can run a fix command to check whether the kernel version in use meets the vulnerability requirements. After confirming that the kernel version is correct, you can ignore the vulnerability alert on the **Risk Prevention** > **Vulnerabilities** page on the console. For details, see **Ignoring a Vulnerability**. You are not advised to delete the old kernel versions.

  Table 4-2 Commands for verifying fixes

OS	Fix Command
CentOS/Fedora /Euler/Red Hat/Oracle	**rpm -qa | grep** *Software_name*
Debian/Ubuntu	**dpkg -l | grep** *Software_name*
Gentoo	**emerge --search** *Software_name*

- The server is not restarted after the kernel vulnerability is fixed.

  After the kernel vulnerability is fixed, you need to restart the server, or the vulnerability alert will still be reported.

4.4 Do I Need to Restart a Server After Its Vulnerabilities Are Fixed?

After you fix Windows OS vulnerabilities or Linux kernel vulnerabilities, you need to restart servers for the fix to take effect, or you will receive the alert over and over again. For other types of vulnerabilities, you do not need to restart servers after fixing them.

4.5 What Is the Sequence of Fixing Vulnerabilities in Batches?

Vulnerabilities in Linux software are fixed based on the sequence of vulnerabilities listed on the console.

When fixing Windows OS vulnerabilities, fix the vulnerabilities that require pre-installed patches first. Other Windows OS vulnerabilities are fixed based on the sequence of vulnerabilities listed on the console.

5 Threat Management

5.1 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.

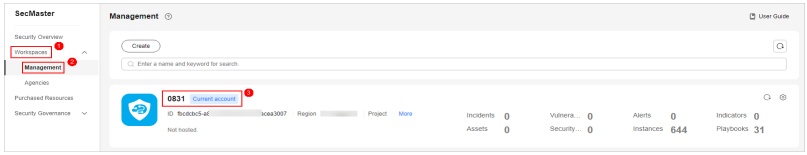
Step 1 **Log in to the SecMaster console.**

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 5-1 Workspace management page



Step 5 In the navigation pane on the left, choose **Threats** > **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**.

5.2 How Do I Check the Storage Space Used by All Logs?

SecMaster allows you to view the storage space used by all logs in **Security Reports**. You can check log analysis in a security report:

- In a **daily security report**, you can check the total log volume for the previous day in the log analysis area.
- In a **weekly security report**, you can check the total log volume for the previous week in the log analysis area.
- In a **monthly security report**, you can check the total log volume for the previous month in the log analysis area.

For details, see **Viewing a Security Report**.

6 Data Integration

6.1 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 6-1 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
Intrusion Prevention System (IPS)	Attack logs	nip-attack	7 to 30 days
Managed Threat Detection (MTD)	Alarm logs	mtd-alarm	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
Cloud Trace Service (CTS)	CTS logs	cts-audit	7 to 30 days

Cloud Service	Log Description	Log	Log Lifecycle
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

7 Data Collection

7.1 Why Did the Component Controller Fail to Be Installed?

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 **Which Commands Are Commonly Used for the Component Controller?**

Possible Cause 1: The Network Between the ECS Where You Want to Install isap-agent and the OBS Bucket Storing the Agent Is Disconnected

Figure 7-1 Disconnected network between the target ECS and OBS bucket

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.
  a. Log in to the OBS management console.
  b. In the navigation pane on the left, choose **Buckets**. On the displayed page, click the name of the target bucket.
  c. On the displayed details page, download the installation script and installation package.
  d. Use a remote management tool, such as SecureFX or WinSCP, to log in to the server.
  e. Upload the installation package to the **/opt/cloud** directory on the server.

Possible Cause 2: Insufficient Disk Space on the ECS

Figure 7-2 Insufficient disk space

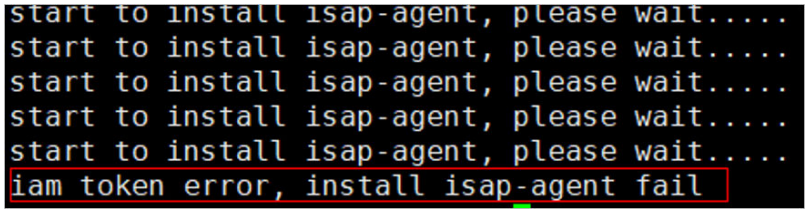
Solution

Clear the disk to reserve sufficient space.

Possible cause 3: Failed to Obtain IAM Tokens

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

Figure 7-3 Obtaining IAM token failed



Troubleshooting and solution

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

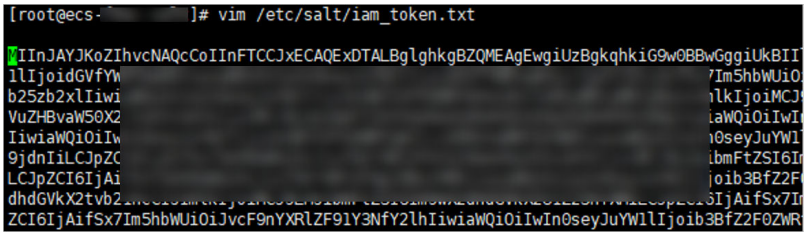
   Figure 7-4 Username and password of an IAM user

   - If any of them or both of them are incorrect, run the installation command with correct information again.
   - If they are correct, go to **2**.

2. 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 **3**.

   Figure 7-5 Checking files

- If a message is displayed indicating that the file does not exist, contact technical support.

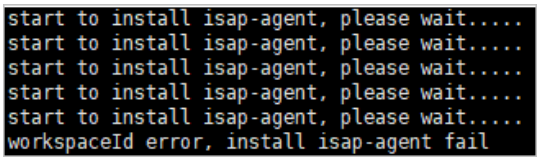
3. Run a **ping** command to check whether the server is reachable. If it is unreachable, enable the communication.

Figure 7-6 Checking the network

Possible Cause 4: Failed to Verify the Workspace ID

If the information shown in the following figure is displayed, the workspace ID verification failed.

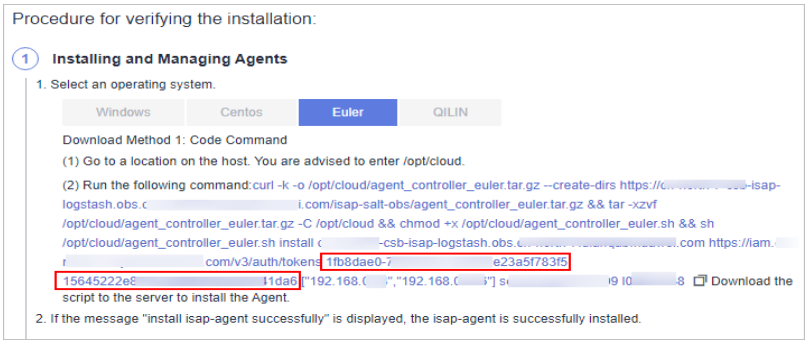
Figure 7-7 Workspace ID verification failed



Solution

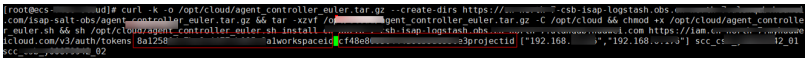
1. Log in to the SecMaster console.
2. In the navigation pane on the left, choose **Workspaces**. In the workspace list, click the name of the target workspace.
3. In the navigation pane on the left, choose **Log Audit** > **Components**. On the displayed page, click the target node.
4. Check workspace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

Figure 7-8 Parameters on the console



5. Check whether the workspace ID and project ID in the command are the same as those in the file in **4**.

Figure 7-9 Parameter information in the command

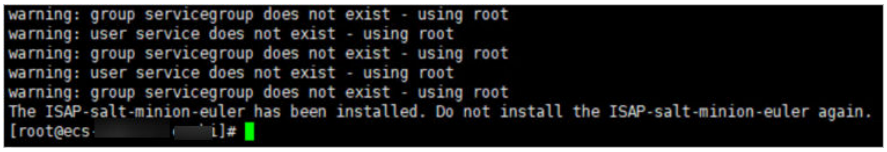


6. Use a valid workspace ID and project ID to run the command again.

Possible Cause 5: isap-agent Installed Repeatedly When isap-agent Has Already Been Installed

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

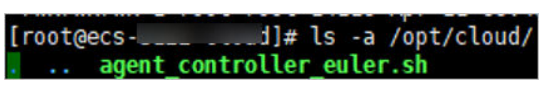
Figure 7-10 Agent already installed



Solution

1. (Optional) Method 1: Deregister the node on the management console.
   a. Log in to the SecMaster management console.
   b. In the navigation pane on the left, choose **Workspaces**. In the workspace list, click the name of the target workspace.
   c. In the navigation pane on the left, choose **Log Audit** > **Components**. On the displayed **Nodes** tab, locate the row that contains the target node and click **Deregister** in the **Operation** column.
   d. In the displayed dialog box, click **OK**.
2. (Optional) Method 2: Run a script command to uninstall component controller isap-agent.
   a. Use a remote management tool, such as SecureFX or WinSCP, to log in to the server.
   b. Run the **sh /opt/cloud/agent_controller_euler.sh uninstall** command to uninstall the component controller.
3. Check whether the uninstallation is complete.
   a. Use a remote management tool, such as SecureFX or WinSCP, to log in to the server.
   b. (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 7-11 Script file

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

      Figure 7-12 Checking isap-agent details

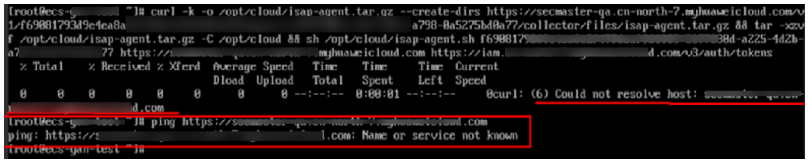
CAUTION

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

Possible Cause 6: Disconnected Network Between ECS and DNS

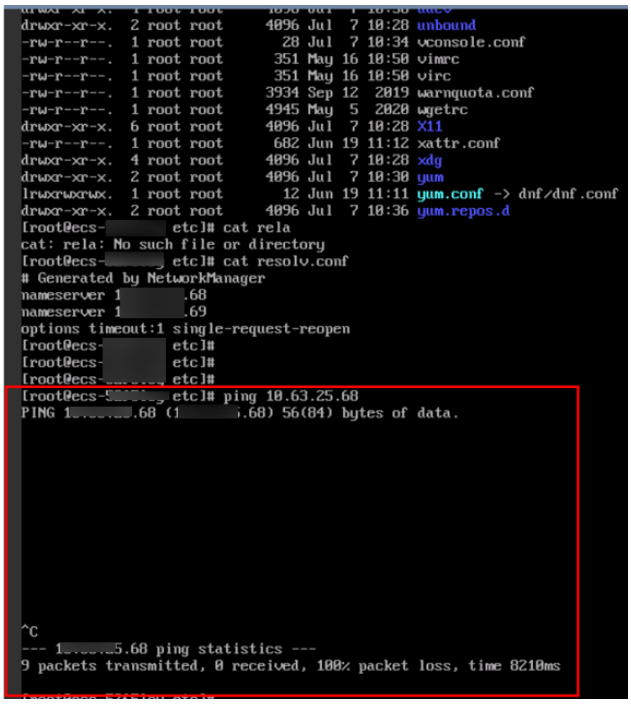
During the isap-agent installation, the message "Could not resolve host:*******" is displayed.

Figure 7-13 Error message indicating that the network between the ECS and DNS is disconnected



The installation failed because the network between the ECS and DNS was disconnected.

Figure 7-14 Disconnected network between the target ECS and DNS



Solution

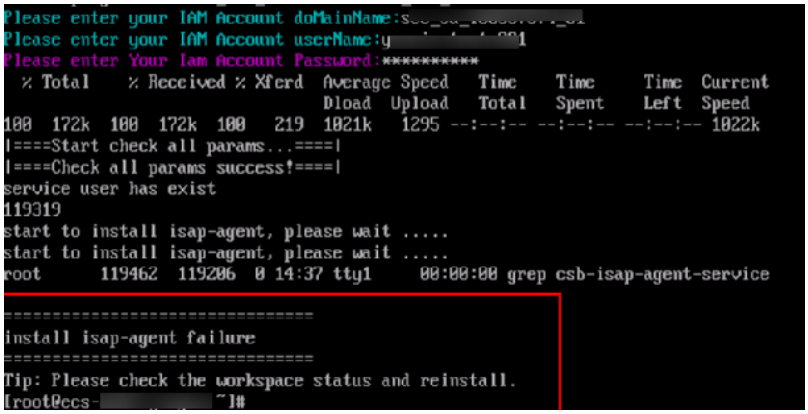
In the VPC the ECS belongs to, enter the correct DNS resolution address. For details, see **How Do I Change the DNS Server Address of an ECS?**

Possible Cause 7: The Workspace Does Not Exist or the Account Lacks Permission.

During the isap-agent installation, the following information is displayed:

```
install isap-agent failure

Tip: Please check the workspace status and reinstall
```

Figure 7-15 Error message indicating that the workspace does not exist or the account lacks permission



Solution

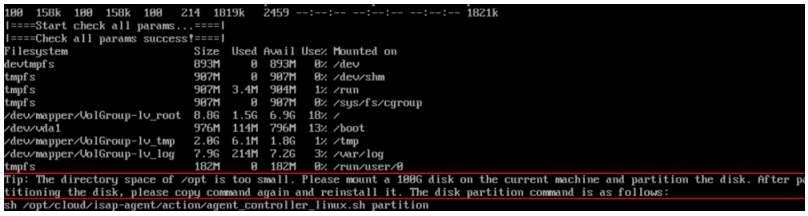
1. Check whether the workspace has been created.
2. Check whether the SecMaster machine-machine account that has the minimum permission is correctly configured.

   For details, see **Creating a Non-administrator IAM User**.

Possible Cause 8: Disk Not Partitioned

During the isap-agent installation, the message "The directory space of /opt is too small" is displayed.

Figure 7-16 Disk not partitioned



Solution

1. Run the following command on the installation page:

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

   For details, see **Partitioning a Disk**.
2. Reinstall isap-agent.

   For details, see **Installing the Component Controller**.

7.2 How Are Collection Node or Collection Channel Faults Handled?

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 to reached 100%.

Figure 7-17 Collection node fault

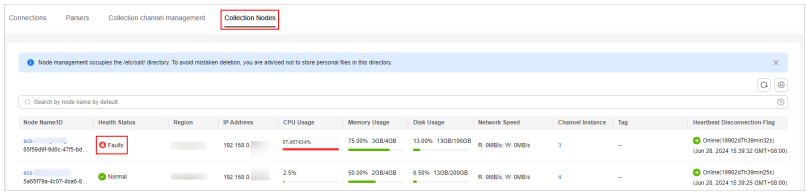
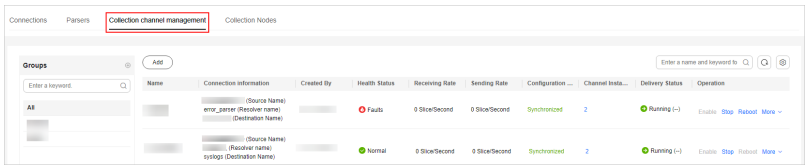


Figure 7-18 Collection channel fault



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

1. Remotely log in to the ECS where the collection node resides.
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 7-19 Status

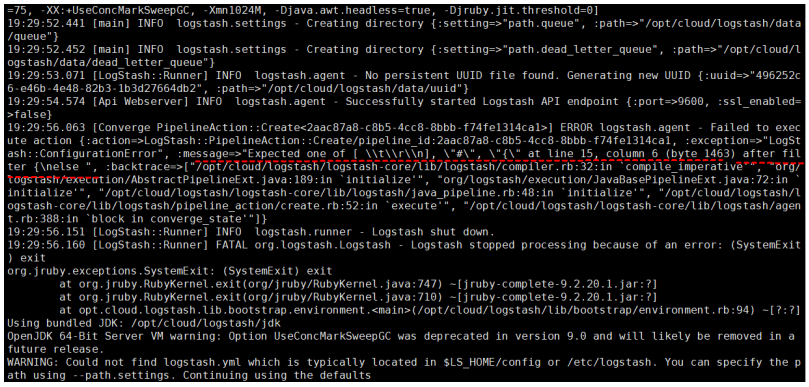
```
top - 19:21:09 up 8 days, 29 min,  2 users,  load average: 1.04, 0.29, 0.13
Tasks:  84 total,   1 running,  83 sleeping,   0 stopped,   0 zombie
%Cpu(s): 95.8 us,  3.7 sy,  0.0 ni,  0.5 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  3879596 total,   532820 free,  1234536 used,  2112240 buff/cache
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 7-20 Collector run log



4. Run the following command to switch to the directory where the collection channel configuration file is stored:

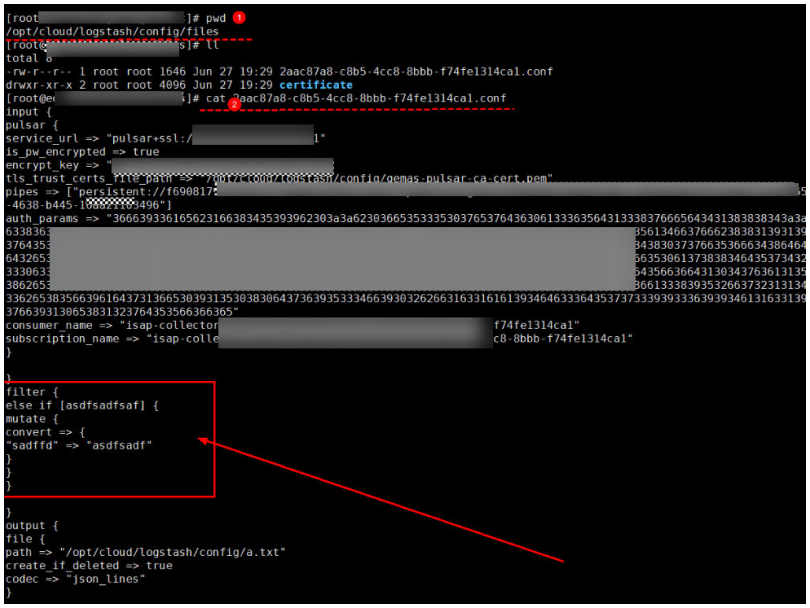
   cd /opt/cloud/logstash/config/files

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 7-21 Filter exceptions



Solution

Step 1 Log in to the SecMaster console and access the target workspace.

Step 2 In the navigation pane on the left, choose **Log Audit** > **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 7-22 Configurations of an abnormal parser

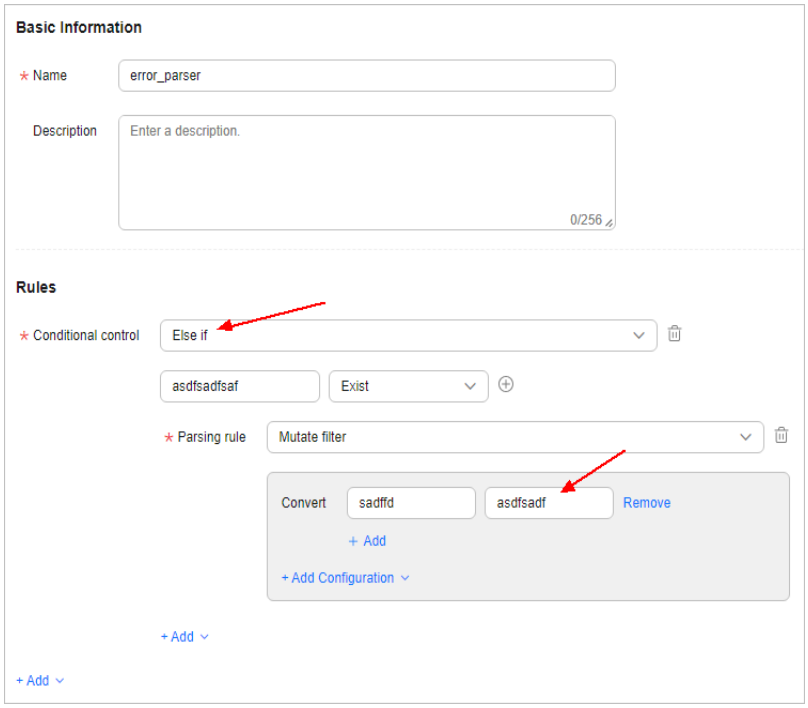
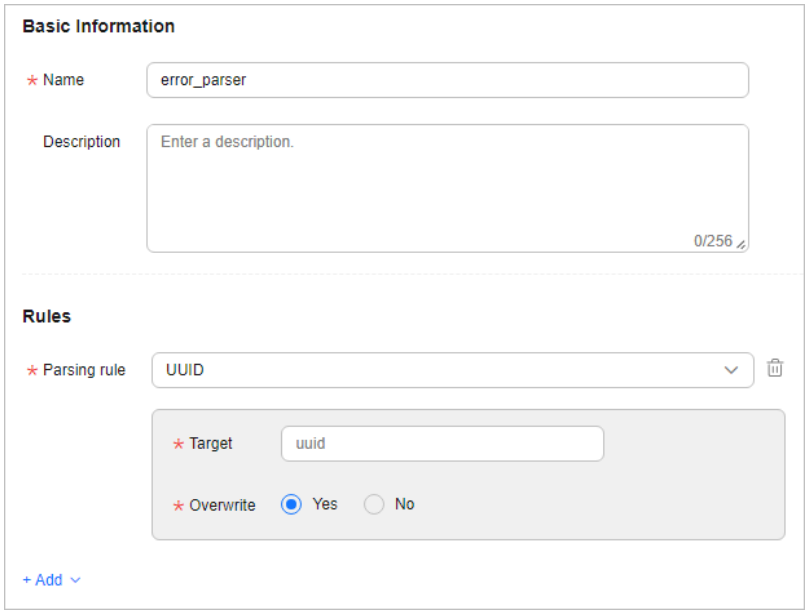


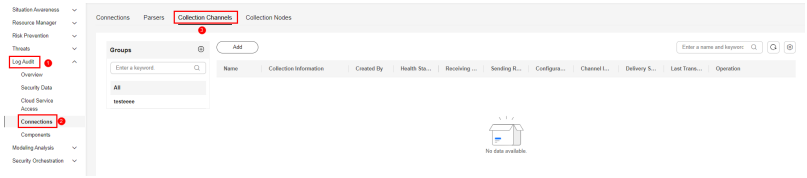
Figure 7-23 Modifying the parser configuration



Step 4 Click **OK**.

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

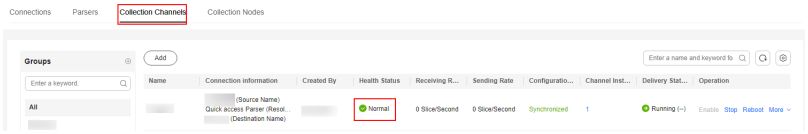
Figure 7-24 Restarting a collection channel



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

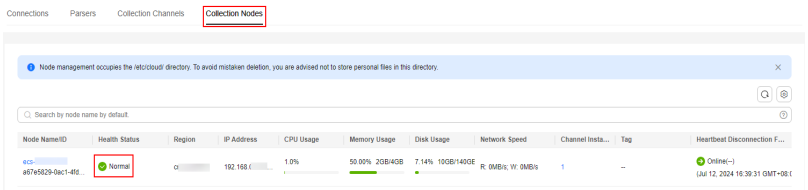
- After the restart is complete, go to the **Collection Channels** tab and check the health status of the target collection channel.

  Figure 7-25 Health status of a collection channel

- Select the **Collection Nodes** tab. On the page displayed, check the health status of the target collection node.

  Figure 7-26 Health status of a collection node

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

----End

7.3 Which Commands Are Commonly Used 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.

7.4 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 **Billing Overview**.

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:

Releasing ECS and VPC Endpoint Resources

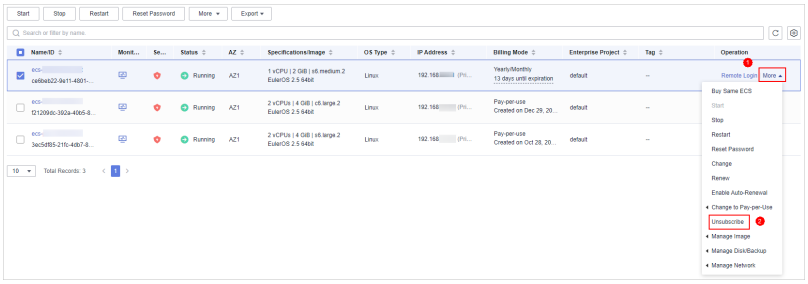
Step 1 **Log in to the SecMaster console.**

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 7-27 Unsubscribing from an ECS

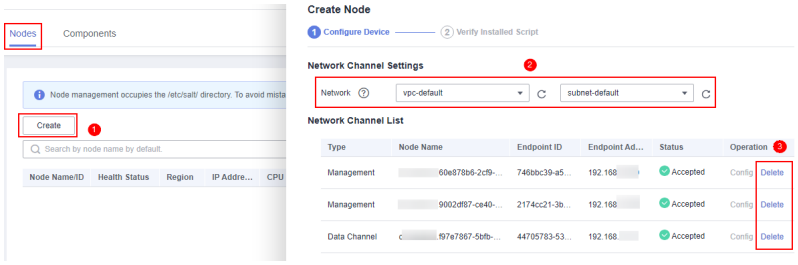


3. In the dialog box displayed, unsubscribe from or delete the ECS as prompted.

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 **Log Audit** > **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**.

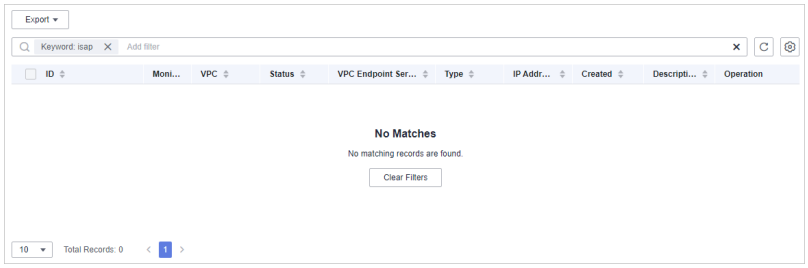
   Figure 7-28 Deleting a node



   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.

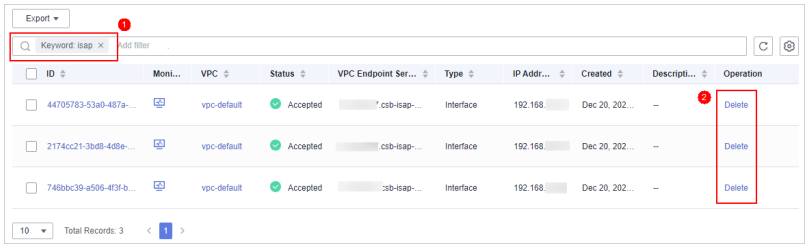
- If no, go to **Step 4.7**.

Figure 7-29 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 7-30 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

8 Permissions Management

8.1 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**.

8.2 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.

Granting Permissions to an IAM User

Step 1 **Log in to the SecMaster console** as an 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, 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

9 Regions and AZs

9.1 What Are Regions and AZs?

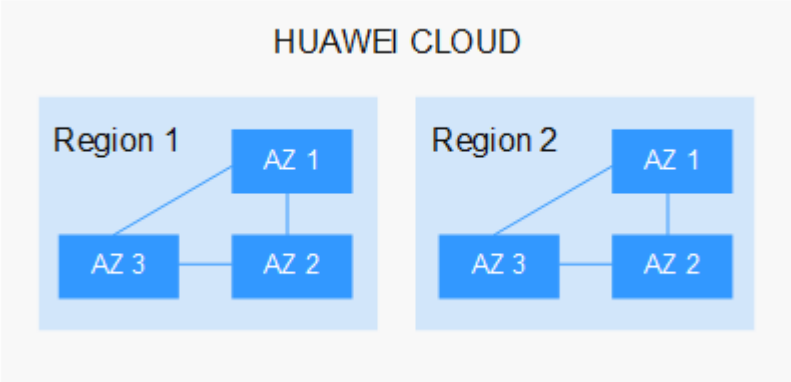
Concepts

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 9-1 shows the relationship between regions and AZs.

Figure 9-1 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.

When selecting a region, consider the following factors:

- Location

  You are advised to select a region close to you or your target users. This reduces network latency and improves access rate. However, Chinese mainland regions provide basically the same infrastructure, BGP network quality, as well as operations and configurations on resources. Therefore, if you or your target users are in the Chinese mainland, you do not need to consider the network latency differences when selecting a region.

  - If you or your target users are in the Asia Pacific region (excluding the Chinese mainland), select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If you or your target users are in Africa, select the **AF-Johannesburg** region.
  - If you or your target users are in Europe, select the **EU-Paris** region.
- Resource price

  Resource prices may vary in different regions. For details, see **Product Pricing Details**.

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.

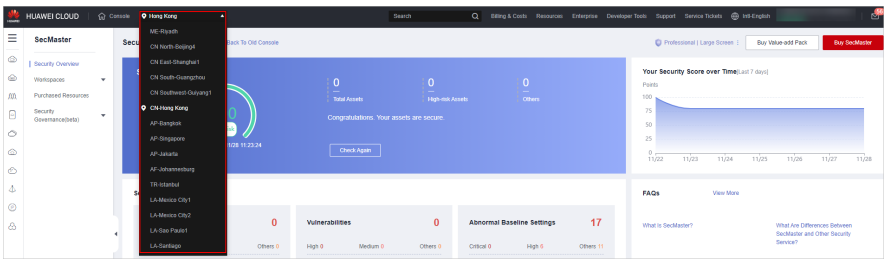
Regions and Endpoints

Before using an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.

9.2 Why Is the Region Selection Box Displayed for Global-Level Projects?

SecMaster is a global project. However, a region selection box is displayed on the console.

Figure 9-2 Region selection box



With the region selection box displayed, you can:

- Switch to another region anytime you want.

  If log in to a region where SecMaster is not available, you can switch to any of other regions where SecMaster has been deployed.

- Manage all data centrally.

  To manage data centrally, SecMaster divides regions into compliance zones. Only data in the same compliance zone can be aggregated. The specific compliance zones in SecMaster are as follows:

  Table 9-1 Compliance zones

Region Name	SecMaster Compliance Zone
CN North-Beijing4	Chinese Mainland
CN North-Ulanqab1	
CN East-Shanghai1	
CN East-Shanghai2	
CN South-Guangzhou	
CN South-Shenzhen	
CN Southwest-Guiyang1	
CN North-Ulanqab-Auto1	CN North-Ulanqab-Auto1
CN-Hong Kong	CN-Hong Kong
AP-Bangkok	AP-Bangkok
AP-Singapore	AP-Singapore

Region Name	SecMaster Compliance Zone
AP-Jakarta	AP-Jakarta
TR-Istanbul	European website
LA-Mexico City2	LA-Mexico City2
LA-Sao Paulo1	LA-Sao Paulo1
ME-Riyadh	ME-Riyadh

