SecMaster

Best Practices

Issue 04
Date 2025-01-22

Contents

1 Log Access and Transfer Operation Guide

1.1 Solution Overview

You can use SecMaster to collect security logs on and off the cloud, as well as transfer security logs from SecMaster to a third-party system and product.

Table 1-1 Log access and transfer scenarios

Scenario	Operation Guide
Enabling SecMaster to collect logs on Huawei Cloud	For details, see **Enabling Log Access**.
Enabling SecMaster to transfer logs from SecMaster to a third-party system or product	Refer to the procedure in this guide.
Enabling SecMaster to collect security logs off Huawei Cloud	Refer to the procedure in this guide.

Log Collection Principles

The log collector node works as an intermediate node. It collects, uploads, and delivers logs between SecMaster and the tenant server.

Figure 1-1 SecMaster log collection principles
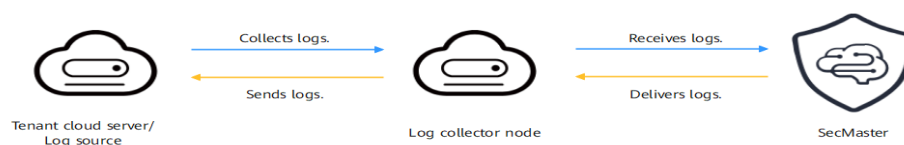
Basic Concepts

This part describes basic concepts and functions of the log collection.

- Log collection component Logstash: collects and transfers logs.
- Component controller (isap-agent): manages log collection component Logstash and other components.
- **Log collector node**: **collects logs, transfers logs to SecMaster, and transfers logs out of SecMaster.**

  A log collector node is an ECS with the SecMaster component controller installed. The component controller has the log collection component installed. Only one log collector node is required for a tenant.

Figure 1-2 Architecture of the log collector node

- Collector: custom Logstash. A collector node is a custom combination of Logstash+ component controller (isap-agent).
- Connector: A connector is a basic element for Logstash. It defines the way Logstash receives source data and the standards it follows during the process. Each connector has a source end and a destination end. 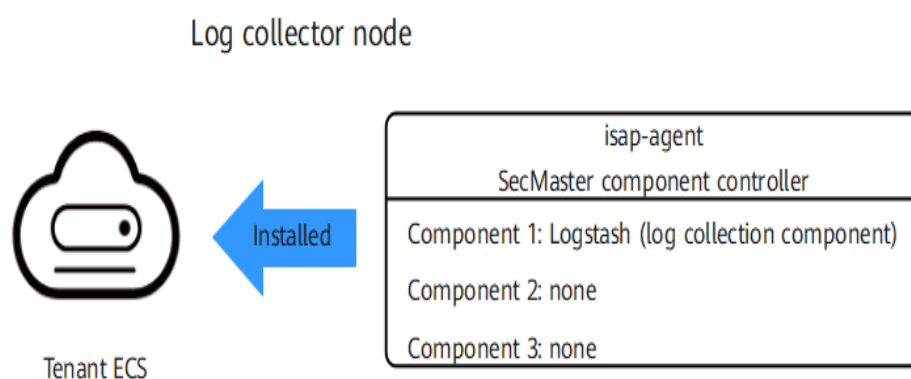Source ends and destination ends are used for data inputs and outputs, respectively. The SecMaster pipeline is used for log data transmission between SecMaster and your devices.
- Parser: A parser is a basic element for configuring custom Logstash. Parsers mainly work as filters in Logstash. SecMaster preconfigures varied types of filters and provides them as parsers. In just a few clicks on the SecMaster console, you can use parsers to generate native scripts to set complex filters for Logstash. In doing this, you can convert raw logs to the format you need.
- Collection channel: A collection channel is equivalent to a Logstash pipeline. Multiple pipelines can be configured in Logstash. Each pipeline consists of the input, filter, and output parts. Pipelines work independently and do not affect each other. You can deploy a pipeline for multiple nodes. A pipeline is considered one collection channel no matter how many nodes it is configured for.

Transmission Protocols and Log Formats Supported

Table 1-2 Transmission protocols and log formats supported

Scenario	Protocol	Log Format
Log access to SecMaster	TCP	JSON, syslog, and plain
	UDP	JSON, syslog, and plain
	OBS	JSON and plain
	Kafka	JSON and plain
	SecMaster	JSON and plain
	ElasticSearch CSS	JSON and plain
Transferring logs out from SecMaster	TCP	json
	UDP	json
	Kafka	json
	OBS	json
	SecMaster	json

1.2 Resource Planning

Account

A non-administrator IAM account that has the SecMaster data collection management permission.

ECS Specifications

The following table lists the specifications of the tenant cloud server (ECS) where the collector (isap-agent + Logstash) is installed.

Table 1-3 ECS specifications

vCPUs	Memory	System Disk Size	Data Disk Size	Collector Capacity (Reference)
4	8 GiB	50 GiB	100 GiB	4,000 EPS @ 500 B
8	16 GiB	50 GiB	100 GiB	10,000 EPS @ 500 B
16	32 GiB	50 GiB	100 GiB	20,000 EPS @ 500 B

vCPUs	Memory	System Disk Size	Data Disk Size	Collector Capacity (Reference)
32	64 GiB	50 GiB	100 GiB	40,000 EPS @ 500 B
64	128 GiB	50 GiB	100 GiB	80,000 EPS @ 500 B
Specifications description: ● 4000 EPS@500B: The log collector can process 4000 events per second. Condition: The size of an event is not larger than 500 bytes. ● **Minimum ECS specifications**: **vCPUs**: **2**; **Memory: 4 GB**; **System disk**: **50 GB**; **Data disk**: **100 GB**. ● Architecture requirements: Currently, the log collection component controller (isap-agent) can run only on Linux x86 ECSs. More will be supported in the future. ● OS (image): There is no restriction. Huawei Cloud EulerOS is recommended. ● The log volume usually increases in proportion to the server specifications. You are advised to increase the log volume based on the specifications in the table. If there is huge pressure on a collector, you can deploy multiple collectors and manage them centrally through collection channels. This can distribute the log forwarding pressure across collectors.				

Log Access Limit

No limits. You can enable log access for as many security logs as your resources can handle.

1.3 Process Flow

This topic walks you through on how SecMaster collects security logs from third-party (non-Huawei Cloud) systems or products, as well as how it transfers security logs from SecMaster to third-party systems or products. The procedure is as follows.

Figure 1-3 Log transfer process
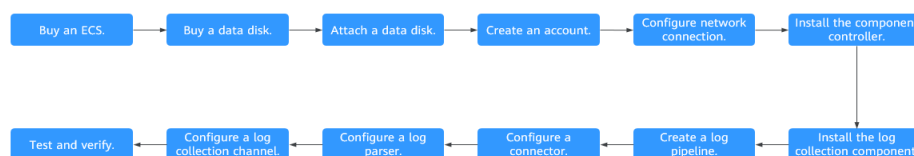
This section describes the process of transferring logs in and out SecMaster.

Table 1 Log transfer process

Procedure	Description
(Optional) Step 1: Buy an ECS	Install the log collector.
(Optional) Step 2: Buy a Data Disk	Ensure that there is enough space to run the log collector.
(Optional) Step 3: Attach a Data Disk	Ensure that there is enough space to run the log collector.
Step 4: Create a Non-administrator IAM Account	Use this account to access SecMaster for the log collector on the tenant side.
Step 5: Configure Network Connection	Connect the tenant VPC to the SecMaster network.
Step 6: Install the Component Controller (isap-agent)	Manage the log collector node (ECS) on SecMaster.
Step 7: Install the Log Collection Component (Logstash)	Configure the log collection process.
(Optional) Step 8: Creating a Log Storage Pipeline	**This step is required when you transfer security logs from non-Huawei Cloud systems to SecMaster. Skip this step if you only need to transfer Huawei Cloud logs to a third-party system or product.** Create a log storage location (pipeline) in SecMaster for log storage and analysis.
Step 9: Configure a Connector	Set the parameters of the log source and destination ends. Complete this step based on your needs: ● **Transferring Third-Party Security Logs to SecMaster** ● **Transferring Security Logs from SecMaster to a Third-Party System or Product**
(Optional) Step 10: Configure a Log Parser	Configure a log parser to convert source logs to the required data type in codeless mode.
Step 11: Configure a Log Collection Channel	Connect all function components to ensure that SecMaster and the log collector work properly.
Step 12: Test and Verify	Check whether log access is successful.

1.4 Procedure

1.4.1 (Optional) Step 1: Buy an ECS

This topic walks you through how to buy an ECS for installing the log collector.

To collect data, you need to prepare an ECS and install the log collector on the ECS. Make sure the ECS has at least 50 GB of memory. If you already have an ECS that meets the requirements, skip this step.

Prerequisites

You have obtained the IAM administrator account information.

## Buying an ECS

Step 1 View the ECS information.

1. Log in to the console as the IAM administrator.

2. Click ![icon] in the upper left corner of the management console, select a region or project, click ![icon] in the upper left corner of the page, and choose **Compute** > **Elastic Cloud Server**.

3. On the ECS list page, click the name of the target ECS to go to its details page.

4. View ECS details about **AZ**, **Specifications**, **Image**, **System Disk**, and **Data Disk**.

Figure 1-4 Viewing ECS Information
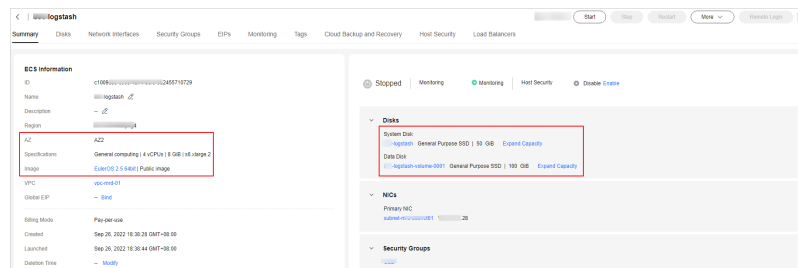
5. Check whether the ECS system disk size is 50 GB or above.

    –   If yes, skip **(Optional) Step 1: Buy an ECS** and go to **(Optional) Step 2: Buy a Data Disk**.

    –   If no, go to **Step 2** and buy an ECS.

Step 2 Go back to the **Elastic Cloud Server** page and click **Buy ECS** in the upper right corner of the page.

Step 3 On the ECS purchase page, configure parameters.

Table 1-4 Parameters for purchasing an ECS

Parameter		Description
Basic Configuration		Configure **Billing Mode** and **Region** based on your service requirements. If there are no special requirements for **AZ**, just select **Random**.
Instance	CPU Architecture	Select **x86**. Currently, the log collector component controller (isap-agent) can only run on Linux ECSs running the x86 architecture.
	Search Filters	Select an instance that meets the requirements as required. Minimum requirements: **2vCPUs** and **4 GiB Memory**.
OS	Image	You are advised to select **Public image** > **Huawei Cloud EulerOS** and then select the specific image as required. **Do not select** images whose names contain "**dedicated for making resources and not support password injection**" because such images cannot be logged in to using passwords. After selecting an image, set **Host protection (HSS)** if needed.
Storage & Backup	System Disk	Minimum requirements for **System Disk**: **50 GiB**. Select a system disk that meets the requirements.
	Data Disk	Minimum requirements for **Data Disk**: **100 GiB**. Click **Add Data Disk** and select a data disk that meets the requirements.
	Enable backup	Configure those parameters based on your service needs.
Network	VPC	Configure those parameters based on your service needs.
	Primary NIC	After the configuration, **record** the selected **VPC and subnet** information, which will be used later.
Security Group		Configure this parameter as required.
Public Network Access		Configure this as required.

Parameter	Description
Instance Management	Configure this parameter based on your needs. After the configuration, record the settings for **ECS Name**, **Username**, and **Password**.
Advanced Settings	Configure parameters as required.
Quantity	Configure this parameter as needed.

Step 4 Check the configurations, select the agreement, and click **Submit**.

Step 5 On the order page, select a payment method and complete the payment.

----End

1.4.2 (Optional) Step 2: Buy a Data Disk

This topic describes how to buy a data disk for the log collector.

An idle data disk with capacity not less than 100 GB is required for the ECS you plan to install the log collector. This data disk is used for collection management. The data disk must be in the same AZ as the ECS.

If you have purchased and configured a data disk based on **(Optional) Step 1: Buy an ECS**, skip this step. Otherwise, follow the steps in this topic to buy a data disk.

Buying a Data Disk

Step 1 Query the data disk information.

1. Log in to the console as the IAM administrator.

2. Click ▣ in the upper left corner of the management console, select a region or project, click ▤ in the upper left corner of the page, and choose **Storage** > **Elastic Volume Service**.

3. On the **Disks** tab, click the name of an EVS disk to go to tis details page.

4. View the **Name**, **AZ**, **Capacity (GiB)**, and **Function** of an EVS disk.

Figure 1-5 Data disk information
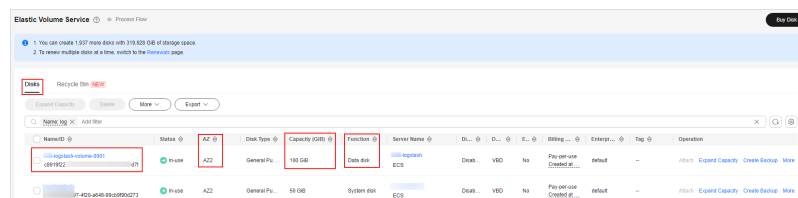
5. Check whether the data disk is in the same AZ as the existing ECS and whether the disk capacity is 100 GB or the above.

   – If yes, skip this step and go to **(Optional) Step 3: Attach a Data Disk**.

   – If no, go to **Step 2** and purchase a data disk.

Step 2 Return to the EVS page and click **Buy Disk** in the upper right corner of the page.

Step 3 On the displayed page, set the disk purchase parameters.

Table 1-5 Parameters for purchasing a disk

Parameter	Description
Region	Select the region the same as the one you specified for the ECS in **(Optional) Step 1: Buy an ECS**.
AZ	Select the AZ you selected for the ECS you bought in **(Optional) Step 1: Buy an ECS**.
Attach To Server	Select **Now**, click **Select Server**, and select the ECS purchased in **(Optional) Step 1: Buy an ECS** or other ECS you prepared, and click **OK**.
Billing Mode	Select a billing mode based on your needs. You are advised to select the same billing mode for the data disk and the ECS it is used for.
Data Source	Configure this parameter based on your needs.
Disk Specifications	- Disk type: Set it as required. - Capacity (GiB): Minimum capacity for the **data disk** is 100 GiB. Select a data disk that meets the requirements.
Selected Specifications	This area displays the configuration information of the selected disk. No configuration is required.
Automatic Backup	Configure this parameter based on your needs.
More	Configure this parameter based on your needs.
Enterprise Project	Configure this parameter as required. If there is no special requirement, select the **default** enterprise project.
Disk Name	Configure this parameter as required.
Quantity	Configure this parameter as required.

Step 4 Check the configurations and click **Next**.

Step 5 Complete the purchase as prompted.

⚠️ **CAUTION**

You do not need to initialize the disk after the purchase. This will be done automatically during **Network Connection Configuration**.

----End

1.4.3 (Optional) Step 3: Attach a Data Disk

This topic describes how to attach a data disk to an ECS.

You need to attach a data disk to the ECS used for the log collector to make sure there is enough space for running the log collector.

- Scenario 1: You have purchased an ECS and a data disk that meet the requirements by referring to **(Optional) Step 1: Buy an ECS** and the disk has been attached to the ECS.

- Scenario 2: You already have an ECS that meets the requirements (not purchased by referring to **(Optional) Step 1: Buy an ECS**), and a data disk that meets the requirements and is purchased based on **(Optional) Step 2: Buy a Data Disk**. The data disk has been attached to the ECS during the purchase.

Attaching a Data Disk

Step 1 If you have an ECS and a data disk that meet the requirements, check whether the data disk has been attached to the ECS.
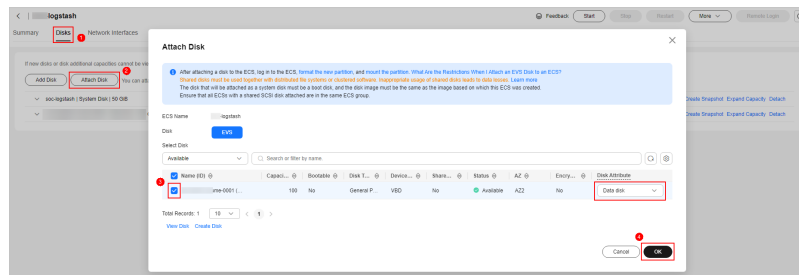
1. Log in to the console as the IAM administrator.

2. Click ⬚ in the upper left corner of the management console, select a region or project, click ☰ in the upper left corner of the page, and choose **Compute** > **Elastic Cloud Server**.

3. On the ECS list page, click the name of the target ECS to go to its details page.

4. Click the **Disks** tab and check whether the required data disk has been attached to the ECS.

   – If it has been attached, skip this step and go to **Step 4: Create a Non-administrator IAM User**.

   – If it has not been attached, go to **Step 2**.

Figure 1-6 Attached data disks
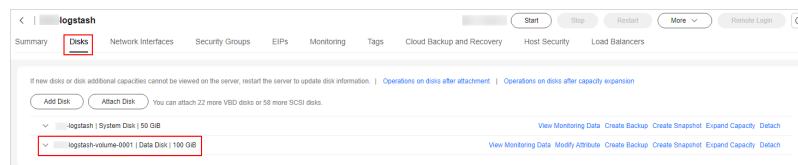
Step 2 On the **Disks** tab, click **Attach Disk**. In the displayed dialog box, select the data disk that meets the conditions and click **OK**.

Figure 1-7 Attaching a disk

----End

1.4.4 Step 4: Create a Non-administrator IAM User

This topic walks you through how to create a non-administrator IAM user.

IAM authentication is used for tenant log collection. So you need to create an IAM user (machine-machine account) with the minimum permission to access SecMaster APIs. MFA must be disabled for the IAM user. This user is used to log in to the log collector on the tenant side and access SecMaster.

Creating a Non-administrator IAM User

Step 1 Log in to the console as the IAM 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 **Tenant collection**.
   – **Description**: Enter a description.

3. Click **OK**.

Step 4 Assign permissions to the user group.

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.
   – **Policy Name**: Set this parameter to **Least permission policy for tenant collection**.
   – **Policy View**: Select **JSON**.
   – **Policy Content**: Copy the following content and paste it in the text box.
     ```
     {
         "Version": "1.1",
         "Statement": [
             {
                 "Effect": "Allow",
                 "Action": [
                     "secmaster:workspace:get",
                     "secmaster:node:create",
     ```

```
                         "secmaster:node:monitor",
                         "secmaster:node:taskQueueDetail" ,
                         "secmaster:node:updateTaskNodeStatus"
                    ]
                }
            ]
        }
```

3. 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 **Tenant collection** created in **Step 3**.

2. On the **Permissions** tab, click **Authorize**.

3. On the **Select Policy/Role** page, search for and select the **Least permission policy for tenant collection** 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**.

Step 6 Create a user.

1. In the navigation pane on the left on the IAM console, choose **Users**. Then, click **Create User** in the upper right corner.

2. Set basic user information.

Table 1-6 Basic user information

Parameter		Description
User Details		Custom configuration. Record the IAM **Username** you configure. The username is required later.
Access Type	Programmatic access	Select this parameter.
	Management console access	Deselect this parameter.
Credential Type	Access key	Select this parameter.
	Password	Select this parameter. After selecting the **Password** parameter, select **Set by user**, and set a password. Record the IAM user password you set. This password is required later.

3. Click **Next**.

4. Search for and select the **Tenant collection** user group created in **Step 3**, and click **Create** in the lower right corner.

Step 7 Verify that no virtual MFA devices are associated to the user.

1. In the navigation pane on the left on the IAM console, choose **Users**. Then, click the user created in **Step 6**.

2. Click the **Security Settings** tab and ensure that the status of **Virtual MFA Device** is **Unbound**.

Step 8 View the domain account information of the IAM user.

1. Hover over the username in the upper right corner and select **My Credentials** from the drop-down list.

2. On the **API Credentials** page, view and record the account name, which is the domain account for installing the isap-agent.

Figure 1-8 Account Name
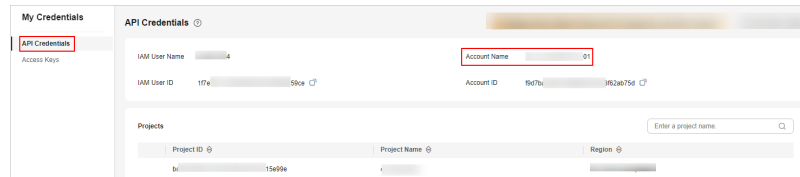
----**End**

1.4.5 Step 5: Configure Network Connection

Before collecting data, you need to establish the network connection between the tenant VPC and SecMaster.

Configuring Networks

Step 1 You have enabled the paid SecMaster and created a workspace.

For details, see **Buying SecMaster** and **Creating a Workspace**.

Step 2 Log in to the management console.

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 1-9 Workspace management page
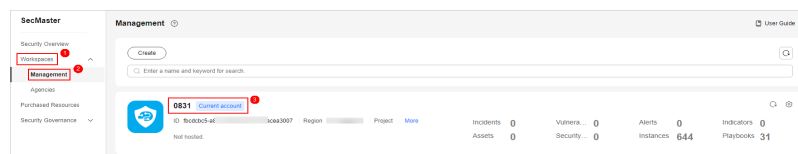
Step 5 In the navigation pane on the left, choose **Settings** > **Components**.

Figure 1-10 Node management page
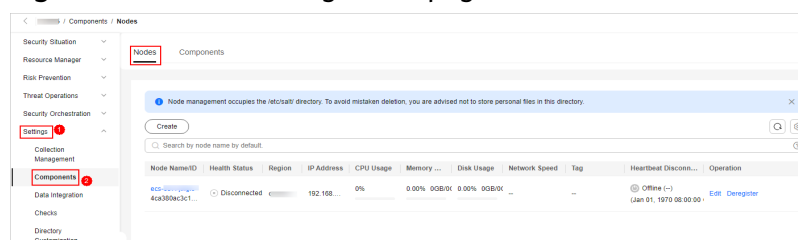
Step 6 On the **Nodes** tab, click **Create**. The **Create Node** page is displayed on the right.

**Step 7** On the **Create Node** page, configure a channel.

Figure 1-11 Create Node
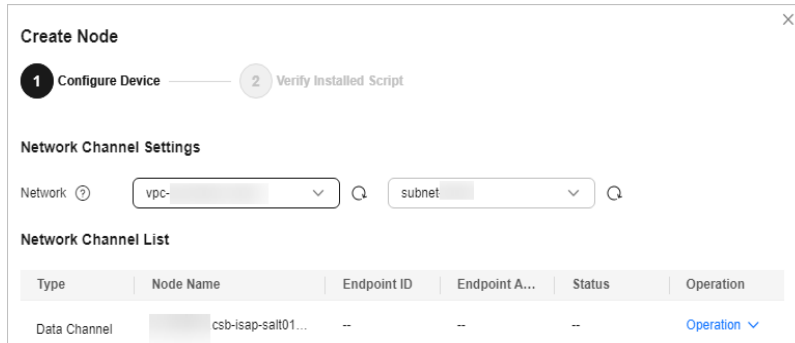
1. In the **Network Channel Settings** area, select the VPC and subnet you recorded in **(Optional) Step 1: Buy an ECS**.

2. In the network channel list, click **Config** in the **Operation** column of each channel. In the displayed confirmation dialog box, click **Confirm**.

    If all channels are accepted, the network channel configuration is complete.

Figure 1-12 Network channels configured
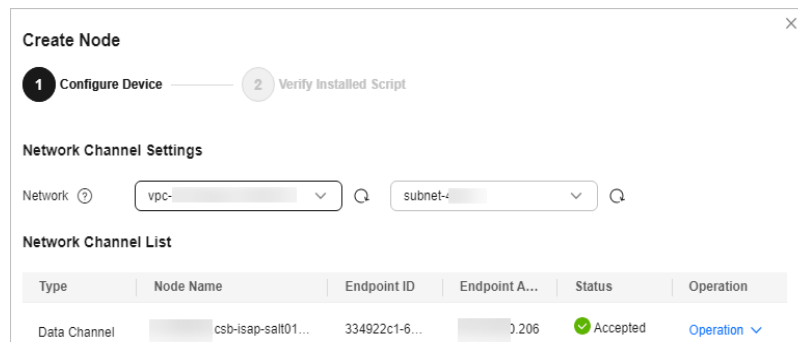
📖 **NOTE**

VPC endpoints you use for log collection are billed. For details about pricing, see **Billing Overview**.

If you no longer need to collect log data, you need to manually release the VPC endpoints used. For details, see **Deleting a VPC Endpoint**.

----End

1.4.6 Step 6: Install the Component Controller (isap-agent)

This topic describes how to install the SecMaster controller (isap-agent) and manage the log collector node (ECS) on SecMaster.

Installing the Component Controller

Step 1   When you finish **Step 5: Configure Network Connection**, on the page displayed, click **Next** in the lower right corner. The **Script Installation Verification** page is displayed.
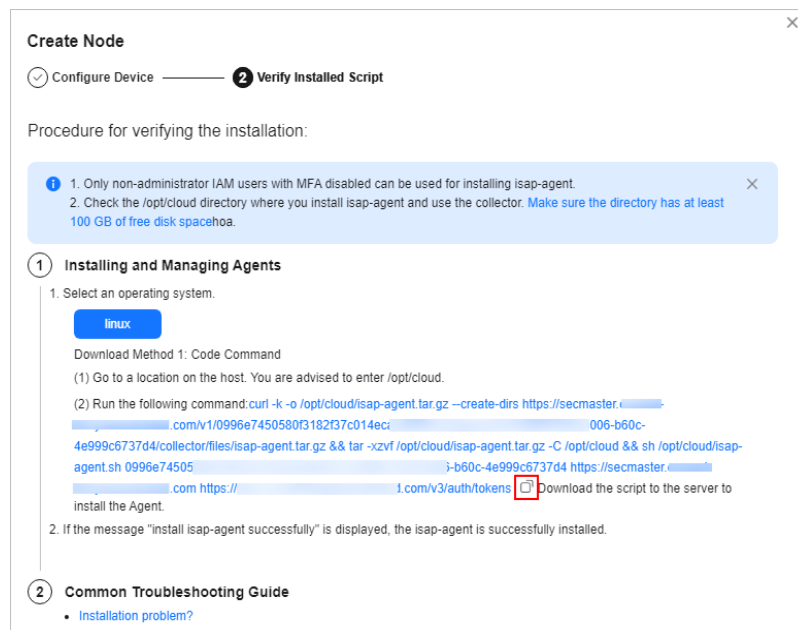
Step 2   Click ⬜ to copy the command for installing the component controller.

Figure 1-13 Copying the installation command

Step 3   Install the component controller.

1. Remotely log in to the ECS prepared in **(Optional) Step 1: Buy an ECS**.

   – Go 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 **Logging In to an ECS 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 command copied in **Step 2** as user **root** to install the controller on the ECS.

3. Enter the domain name, username, and password of the machine-machine account created in **Step 4: Create a Non-administrator IAM User** as prompted.

4. If **install isap-agent successfully** is displayed, the component controller is installed.

Figure 1-14 Installation succeeded

If the installation fails, rectify the fault by referring to **Troubleshooting the Component Controller Installation Failure**. If the system displays a message indicating that the memory is insufficient, rectify the fault by referring to **Partitioning a Disk**.

Step 4 After confirming that the installation has been completed, return to the page for adding nodes (**Step 2**) and click **Confirm** in the lower right corner of the page.

You can view new nodes on the **Nodes** tab.

Figure 1-15 New nodes added

----**End**

1.4.7 Step 7: Install the Log Collection Component (Logstash)

This topic describes how to install the SecMaster log collection component (Logstash) and configure the log collection process.

Installing the Log Collection Component

Step 1 Log in to the management console.

Step 2 Click ≡ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 1-16 Workspace management page

Step 4 In the navigation pane on the left, choose **Settings** > **Components**. Then, select the **Components** tab.

Figure 1-17 Accessing the Components tab
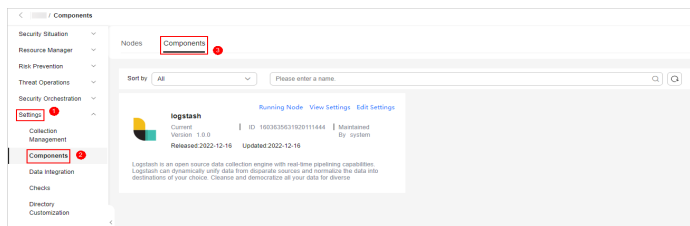
Step 5 On the **Components** tab page, click **Edit Settings** in the upper right corner of the component to be viewed. The configuration management page of the component is displayed on the right.

Step 6 In the **Node Configuration** area, click **Add** in the upper left corner of the node list. In the **Add Node** dialog box displayed, select the ECS node prepared in **(Optional) Step 1: Buy an ECS** and click **OK**.
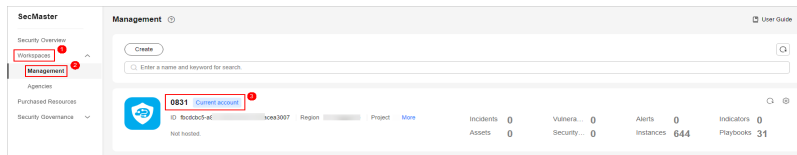
Step 7 On the **Configuration Management** page, click **Save and Apply** in the lower right corner.

Wait for a period of time. When the component status changes to **Applied completed**, the Logstash collector has been installed on the current node.

Figure 1-18 Configuration completed
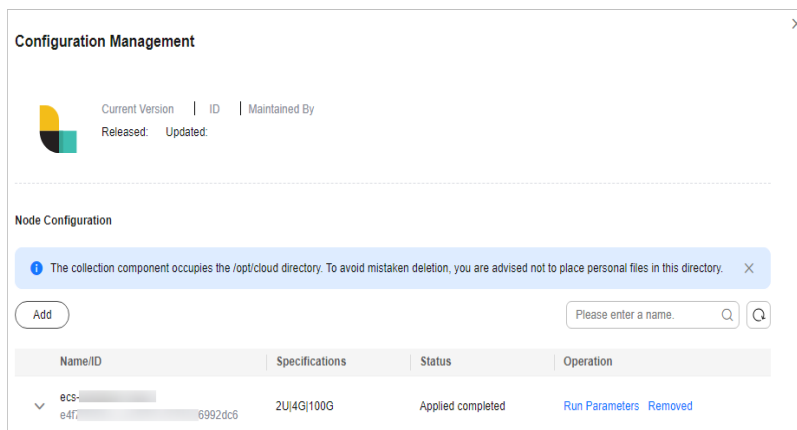
----**End**

1.4.8 (Optional) Step 8: Creating a Log Storage Pipeline

This topic describes how to create a log storage location (pipeline) in SecMaster for log storage and analysis.

This step is required when you transfer security logs from non-Huawei Cloud systems to SecMaster. Skip this step if you only need to transfer Huawei Cloud logs to a third-party system or product.

Creating a Log Storage Pipeline

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 1-19 Workspace management page
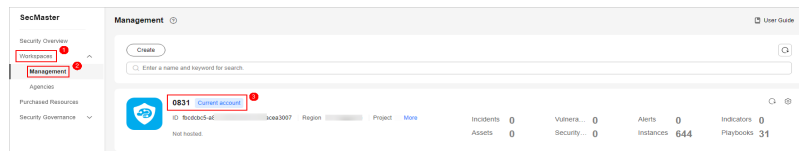
Step 4 In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

Figure 1-20 Accessing the Security Analysis tab page
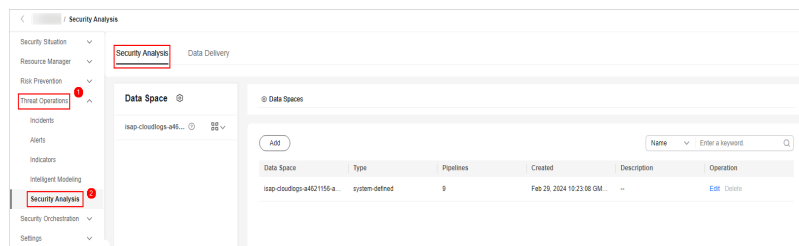
Step 5 Create a data space.

1. In the upper left corner of the data space list, click **Add**. The **Add Data Space** panel is displayed on the right.

   Figure 1-21 Add Data Space
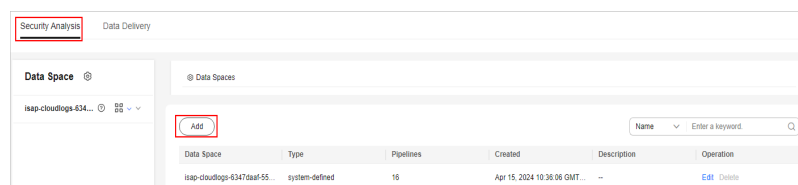
2. On the **Add Data Space** panel, set the parameters for the new data space.

Table 1-7 Parameters for adding a data space

Parameter	Description
Data Space	Enter a data space name. The name must meet the following requirements: – The name can contain 5 to 63 characters. – The value can contain letters, numbers, and hyphens (-). The name cannot start or end with a hyphen (-) or contain consecutive hyphens (-). – The name cannot be the same as any other data space name on Huawei Cloud.
Description	(Optional) Remarks of the data space.

3. Click **OK**.

Step 6 In the data space navigation tree on the left, click ⊞ on the right of the data space name created in **Step 5** and select **Create Pipeline**.

Figure 1-22 Creating a pipeline
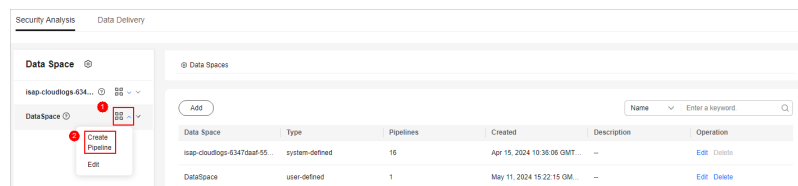
Step 7 On the **Create Pipeline** page, configure pipeline parameters. For details about the parameters, see **Table 1-8**.

Table 1-8 Creating a pipeline

Parameter	Description
Data Space	Data space to which the pipeline belongs, which is generated by the system by default.
Pipeline Name	Name of the pipeline. The name must meet the following requirements: ● The name can contain 5 to 63 characters. ● The value can contain letters, numbers, and hyphens (-). The name cannot start or end with a hyphen (-) or contain consecutive hyphens (-). ● The name must be unique in the data space.

Parameter	Description
Shards	The number of shards of the pipeline. The value ranges from 1 to 64.
	An index can potentially store a large amount of data that exceeds the hardware limits of a single node. To solve this problem, Elasticsearch subdivides your index into multiple pieces called shards. When creating an index, you can specify the number of shards as required. Each shard is in itself a fully-functional and independent "index" that can be hosted on any node in the cluster.
Lifecycle	Life cycle of data in the pipeline. The value ranges from 7 to 180.
Description	Remarks on the pipeline. This parameter is optional.

Step 8 Click **OK**

After the pipeline is created, you can click the data space name to view the created pipeline.

----End

1.4.9 Step 9: Configure a Connector

This topic describes how to configure the source and destination for log collection. Perform the following operations based on the scenario:

- **Transferring Third-Party Security Logs to SecMaster**
- **Transferring Security Logs from SecMaster to a Third-Party System or Product**

Transferring Third-Party Security Logs to SecMaster

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 1-23 Workspace management page
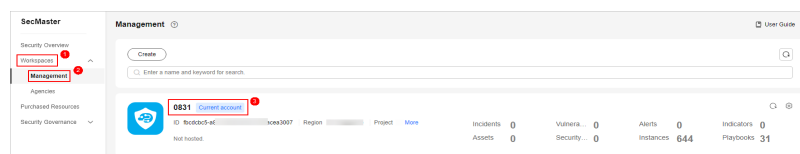
Step 4 In the navigation pane on the left, choose **Settings** > **Collections**.

Figure 1-24 Accessing the connection management page
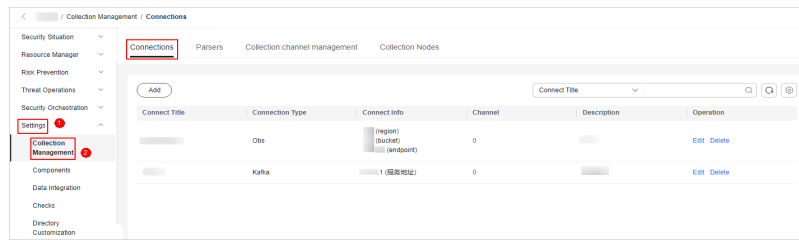
Step 5 Add a source for the data connection.

1. On the **Connections** tab, click **Add**.

2. Configure the data connection source details.

Figure 1-25 Source

The following uses UDP and TCP as examples. For more connection types, see **Rules for Configuring Connectors**.

– Connection type: UDP

Table 1-9 Log source

Parameter	Description
Connection Method	Select **Source**.
Connection Type	Select **UDP**.
Title	Name of the data connection source.
Description	Customize the data source description.
Port	Retain the default value.
Codec	Retain the default value.
Advanced Settings	No configuration is required.

– Connection type: TCP

Table 1-10 Log source

Parameter	Description
Connection Method	Select **Source**.
Connection Type	Select **TCP**.
Title	Name of the data connection source.
Description	Customize the data source description.
Port	Retain the default value. Ensure that the port number is different from those used by other sources.
Codec	If the original log format is not JSON, select **Plain**.
Packet label	No configuration is required.

3. After the setting is complete, click **Confirm** in the lower right corner of the page.

Step 6 Add a destination for the data connection.

1. On the **Connections** tab, click **Add**.

2. Configure the data connection destination details.

Figure 1-26 Destination

Table 1-11 Log transfer destination

Parameter	Description
Connection Method	Select **Destination**.
Connection Type	Select **SecMaster**.
Title	Customize the destination name of the data connection.
Description	Description of the connection destination.
Type	User-defined log destination type.

Parameter	Description
Pipe	Select the name of the pipeline created in **(Optional) Step 8: Creating a Log Storage Pipeline**.
Domain_name	Enter the domain account information of the IAM user used to log in to the console.
User_name	Enter the user information of the IAM user used to log in to the console.
Password	Enter the password of the current login IAM user.
Advanced Settings	No configuration is required.

3. After the setting is complete, click **Confirm** in the lower right corner of the page.

----End

Transferring Security Logs from SecMaster to a Third-Party System or Product

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 1-27 Workspace management page
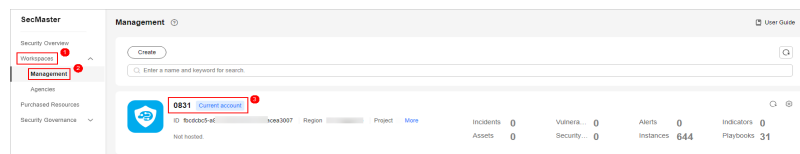
Step 4 In the navigation pane on the left, choose **Settings** > **Collections**.

Figure 1-28 Accessing the connection management page
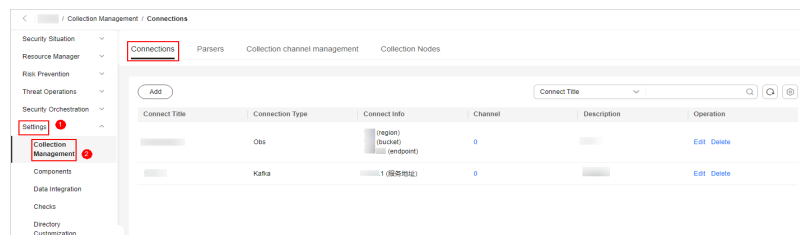
Step 5 Add a source for the data connection.

1. On the **Connections** tab, click **Add**.

2. Configure the data connection source details.

Figure 1-29 Data sources

Table 1-12 Log source

Parameter	Description
Connection Method	Select **Source**.
Connection Type	Select **SecMaster**.
Title	Customize the destination name of the data connection.
Description	Description of the connection destination.
Type	User-defined log destination type.
Pipe	Select the name of the pipeline created in **(Optional) Step 8: Creating a Log Storage Pipeline**.
Domain_name	Enter the domain account information of the IAM user used to log in to the console.
User_name	Enter the user information of the IAM user used to log in to the console.
Password	Enter the password of the current login IAM user.
Advanced Settings	No configuration is required.

3. After the setting is complete, click **Confirm** in the lower right corner of the page.

Step 6 Add a destination for the data connection.

On the **Connections** page, click **Add** and configure data connection destination parameters.

Set this parameter based on the site requirements. For more connection types, see **Connector Rules**.

----End

1.4.10 (Optional) Step 10: Configure a Log Parser

This topic describes how to configure a log parser to convert the log format in a codeless manner.

SecMaster provides log parser (rule) templates. You can use them directly. If the log parser (rule) templates cannot meet your log conversion requirements, you can create custom log parsers (rules).

- **Method 1: Using a Template**
- **Method 2: Creating a Custom Parser**

Method 1: Using a Template

The following example shows how to parse **DBAPPSecurity WAF logs**.

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 1-30 Workspace management page
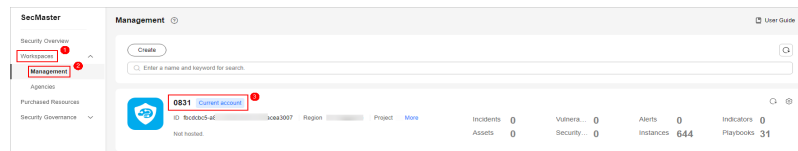
Step 4 In the navigation pane on the left, choose **Settings** > **Collections**. Then, select the **Parsers** tab.

Figure 1-31 Accessing the Parsers tab
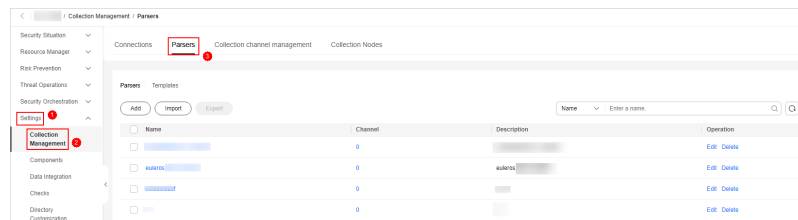
Step 5 On the **Parsers** tab page, click the **Templates** tab.

Step 6 On the template list page, locate the row that contains **Analysis of Anheng WAF log** and click **Create by Template** in the **Operation** column.

Step 7 On the **Create Parser** page, set parameters.

Table 1-13 Parameters for adding a parser

Parameter		Description
Basic Information	Name	Parser name, which is automatically generated by the system based on the template and can be changed.
	Description	Parser description, which is automatically generated by the system based on the template and can be modified.
Rules		Parsing rules, which are automatically generated by the system based on the template. You can edit them as needed.
		To add a rule, click **Add**, select a rule type, and set parameters based on the selected rule.
		● **Parsing rule**: Select parsing rules for the parser. For details about the parameters, see **Parser Rules**.
		● **Conditional control**: Select the conditions for the parser. You can select **If**, **Else**, or **Else if**.

Step 8 Click **OK** in the lower right corner of the page.

----End

Method 2: Creating a Custom Parser

If the log parser (rule) templates cannot meet your log conversion requirements, you can create custom log parsers (rules).

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 1-32 Workspace management page
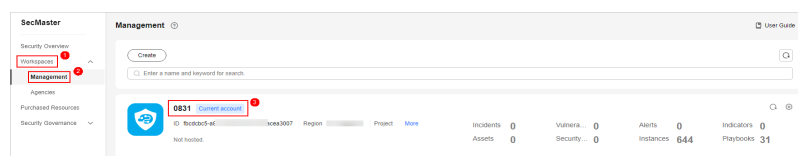
Step 4 In the navigation pane on the left, choose **Settings** > **Collections**. Then, select the **Parsers** tab.

Figure 1-33 Accessing the Parsers tab
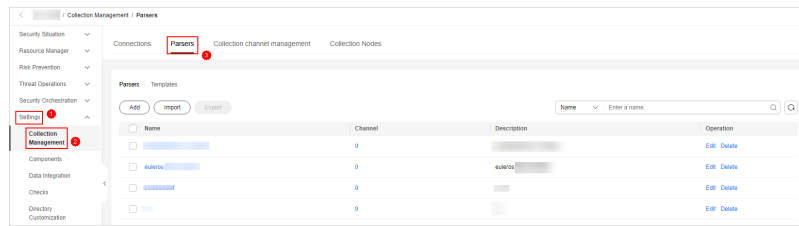
Step 5   On the **Parsers** tab, click **Add**.

Step 6   On the **Create Parser** page, set parameters.

Table 1-14 Parameters for adding a parser

Parameter		Description
Basic Information	Name	Set the parser name.
	Description	Enter the parser description.
Rules		Set the parsing rule of the parser. The procedure is as follows:
		1. Click **Add** and select a rule type.
		– **Parsing rule**: Select parsing rules for the parser. For details about the parameters, see **Parser Rules**.
		– **Conditional control**: Select the conditions for the parser. You can select **If**, **Else**, or **Else if**.
		2. Set parameters based on the selected rule.

Step 7   Click **OK** in the lower right corner of the page.

----End

1.4.11 Step 11: Configure a Log Collection Channel

This topic describes how to configure a log collection channel and connect functional components to let SecMaster and the log collector work properly.

Configuring a Log Collection Channel

Step 1   Log in to the management console.

Step 2   Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

**Step 3**   In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 1-34 Workspace management page
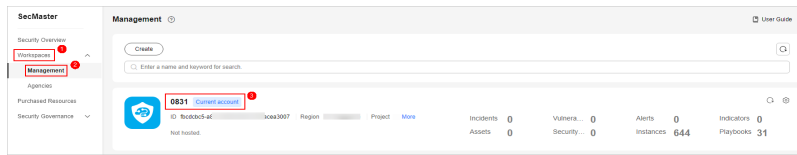
Step 4 In the navigation pane on the left, choose **Settings** > **Collections**. Then, select the **Collection Channels** tab.

Figure 1-35 Collection channel management tab page
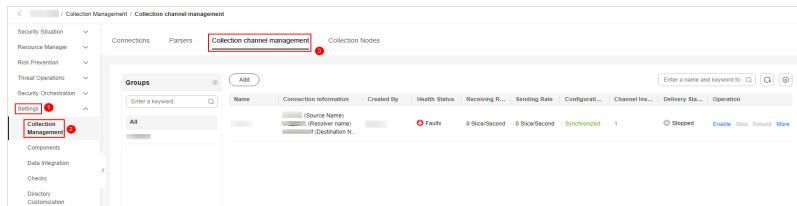
Step 5 Add a log collection channel group.

  1. On the **Collection Channels** tab, click ⊕ on the right of **Groups**.

  2. Enter a group name and click ✔.

Step 6 Create a log collection channel.

  1. On the right of the group list, click **Add**.

  2. In the **Configure Basic Configuration** step, configure basic information.

Table 1-15 Basic configuration parameters

Parameter		Description
Basic Information	Title	The collection channel name you customize.
	Channel grouping	Select the group created in **Step 5**.
	(Optional) Description	Enter the description of the collection channel.
Configure Source	Source Name	Select the name of the log source added in **Step 9: Configure a Connector**. After you select a source, the system automatically generates the information about the selected source.
Destination Configuration	Destination Name	Select the name of the log destination added in **Step 9: Configure a Connector**. After you select a destination, the system automatically generates the information about the selected destination.

3. Click **Next** in the lower right corner of the page.

4. On the displayed **Configure Parser** page, select the parser configured in **(Optional) Step 10: Configure a Log Parser** and click **Next** in the lower right corner of the page.

   If no parsers are configured, you can select **Quick access Parser** to add raw logs to the collection channel list.

5. On the **Select Node** page, click **Create**. In the **Add Node** dialog box displayed, select the ECS node created in **(Optional) Step 1: Buy an ECS** and click **OK**.

Figure 1-36 Selecting a node
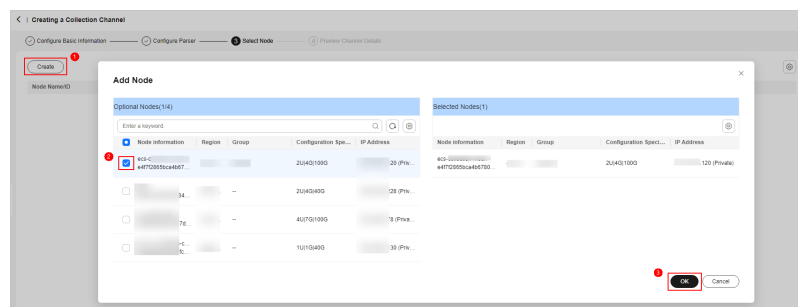
Step 7 Click **Next** in the lower right corner of the page.

Step 8 On the **Preview Channel Details** page, confirm the configuration and click **Save and Execute**.

On the **Collection Channels** tab, if the health status of a collection channel is **Normal**, the collection channel is successfully delivered.

Figure 1-37 Collection channels configured
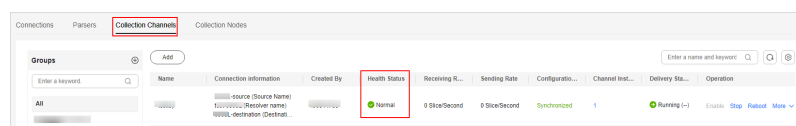
----End

1.4.12 Step 12: Verify Log Access and Transfer

This topic describes how to test and verify that non-Huawei Cloud logs can be transferred to SecMaster.

Table 1-16 Test and verification scenario description

Scenario	Verification Method
Enabling SecMaster to collect logs on Huawei Cloud	Go to the **Security Analysis** page on the SecMaster console and check whether there are logs of cloud services with log access enabled.

Scenario	Verification Method
Enabling SecMaster to transfer logs from SecMaster to a third-party system or product	Check whether logs are transferred to the third-party system or product.
Enabling SecMaster to collect security logs off Huawei Cloud	Verify the log access by referring to this section.

Verification

Step 1 View data in the collection channel on the SecMaster console.

1. Log in to the management console.

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

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

Figure 1-38 Workspace management page
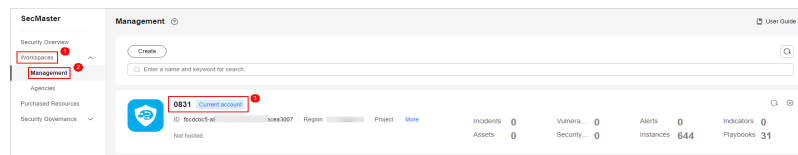
4. In the navigation pane on the left, choose **Settings** > **Collections**. Then, select the **Collection Channels** tab.

Figure 1-39 Collection channel management tab page
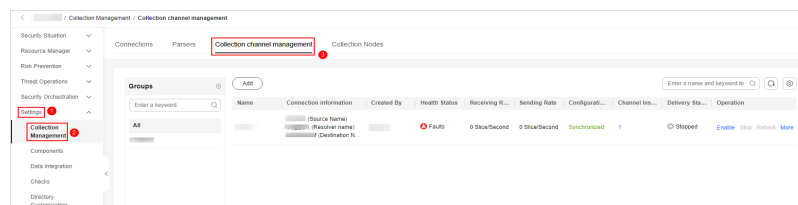
5. On the **Collection Channels** tab, click the setting button in the upper right corner of the table and select **Received** and **Sent**.

Figure 1-40 Parameters
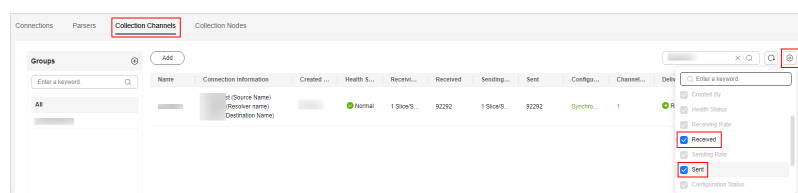
6. In the table, view the monitoring information of the corresponding collection channel. If there is data in the **Received** and **Sent** columns, the log access is successful.

Figure 1-41 Viewing the log access status

Step 2 Check data in the security analysis log pipeline on the SecMaster console.

Step 3 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click the name of the pipeline created in **Creating a Log Storage Pipeline**.

Figure 1-42 Pipeline data page
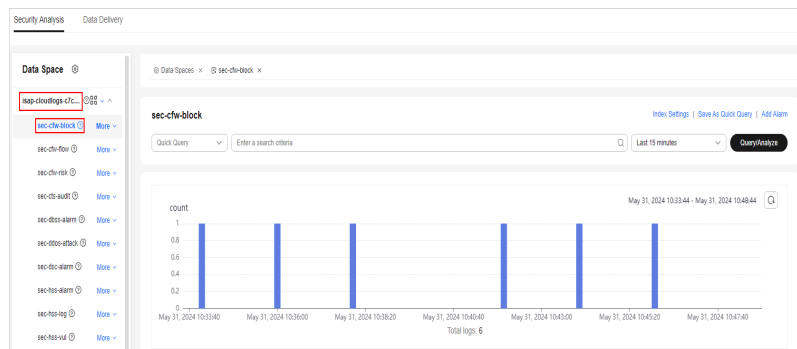
Step 4 If data is displayed in the log pipeline, the log access is successful.

----End

2 Credential Leakage Response Solution

Incident Type: Credential Leakage

Credential leakage means that the identity authentication information, such as the username, password, API key, and access token, of an individual or organization is obtained or disclosed by an unauthorized third party when the individual or organization uses online services, such as cloud services, social media platforms, and emails. This may occur in many cases, including but not limited to phishing, malware, social engineering, and system vulnerabilities. Once credentials are disclosed, attackers may use them to access sensitive data, perform illegal transactions, or damage the system, which severely affects services.

Response Solution

To address the preceding issues, Huawei Cloud launched the SecMaster service. SecMaster is a next-generation cloud native security operation platform. Based on years of cloud security experience of Huawei Cloud, it enables integrated and automatic security operations through cloud asset management, security posture management, security information and event management, security orchestration and automatic response, cloud security overview, simplified cloud security configuration, configurable defense policies, and intelligent and fast threat detection and response.

Incident Response Process

Step 1 **Identify whether identity credentials are compromised or disclosed**.

1. If you receive any of the following messages, check your identity credentials for damage or leakage:
   - Alerts or metrics from cloud services (such as CCM, SecMaster, and CTS) and external monitoring systems;
   - Prompt messages from the contractor or third-party service provider;
   - Findings through internal or external security inspections;
   - Internal system messages;
   - Information anonymously reported to you;
   - Information you receive in other ways. For example, an attacker may use leaked credentials to steal your data and modify your public-facing resources.

2. Make sure a service ticket or case has been submitted for the incident. If no service tickets or cases are submitted, submit one manually.

3. Determine and record the impact on end users.

   No matter whether this scenario has direct impact on users, record the survey result in the ticket or case related to the incident.

4. For automatically created service tickets or cases, identify real alerts or abnormal metrics.

   For example, an alert or abnormal metric in CTS may be generated because there are unsafe IAM settings or IAM credential leaks. It may also be a billing alert triggered when your billing cost exceeds a predefined threshold.

5. Locate the leaked credential set.

   – If a service ticket or case is created, check whether the user/role name, user/role ID, or access key ID has been recorded in the ticket or case.

   – If the alert is generated by SecMaster baseline inspection, you can view the baseline inspection result on the console and find the access key ID of the affected credential. For details, see **Viewing the Baseline Inspection Result**.

   – If the alert is reported by CTS, you can view the result in the incident list on the console. The resource name is the access key. The **Credential** field contains **access_key_id**, **account_id**, **user_name**, and other information.

6. Determine when credentials may be compromised or leaked. Any API operation performed after this time shall be considered malicious, and any resource created after this time shall be considered leaked.

7. If your application is interrupted, identify the possible incidents that cause the interruption. If the interruption is not related to a credential leak, check the deployment pipeline to see if any changes were made before the incident. You can use CTS to view logs of all account activities.

8. Communicate incidents:

   – Determine stakeholder roles based on the organization's incident response plan.

   – Notify relevant stakeholders, including legal personnel, technical teams, and developers, and ensure that they are added to the service ticket and war rooms for continuous updates.

9. Communicate incidents with external parties.

   – Ensure that your legal counsel is aware of the situation and keep them in the loop of internal stakeholders for any updates, especially updates for external communications.

   – Add colleagues responsible for public or external communication to the service ticket so that they can receive regular status updates about the incident and fulfill their communication responsibilities.

   – If your jurisdiction has regulations that require the reporting of such incidents, ensure that the person responsible for notifying the local or federal law enforcement agency in your organization also receives a notification of the incident/is added to the service ticket. Consult your legal counsel and law enforcement for guidance on the collection and preservation of evidence and regulatory authorities. Your report may help analyze similar activities or help others, even if it is not required by

regulations to report to open databases, government agencies, or non-governmental organizations.

Step 2 **Contain incidents**.

You can disable compromised credentials or revoke permissions related to these credentials to prevent the use of compromised credentials to call APIs.

1. Disable the compromised credentials identified in **Step 1**.

   a. If the user credentials are permanent IAM user credentials, delete them on the IAM console. For details, see **Deleting an IAM User**.

   b. If the user credentials are temporary credentials obtained from IAM, they can be associated with the IAM role. To disable these functions, perform the following steps:

      i. Cancels all sessions of the current role. If the attacker obtains a new temporary security credential and continues the attack, go to **Step 2.1.b.ii**.

      ii. Delete all IAM policies added to the role, modify existing policies to block all access, or modify the policy of the role to prevent attackers from taking the role.

      Credentials are still valid for a specified period of time after being issued. After the trust policy is modified, the credentials can still be used within the validity period. **Step 2.1.b.i** and **Step 2.1.b.ii** will prevent all users, including any legitimate users or applications, from using credentials obtained by taking on roles.

2. You can view the credentials that are continuously used on the CTS console within about 30 minutes, regardless of access keys, IAM users, or roles, and confirm that the compromised credentials have been disabled.

Step 3 **Eradicate incidents**.

You need to check which API operations are performed and which resources are created, deleted, or modified after the credential is damaged, and take measures to eliminate the impact.

1. Use your preferred monitoring tool to access CTS and collect all API operations performed by the damaged credential. The log collection time is from the damage time to the current time.

   – If you use a third-party tool (such as Splunk) to collect CTS logs, obtain logs from the tool.

   – If you send logs to OBS instead of using a third-party tool, you can use LTS to collect, query, and store logs.

2. On the LTS console, query all API operations performed after the credential is damaged or leaked.

3. Pick out the API calls that may:

   – Access sensitive data, for example, OBS Object.

   – Create resources, such as databases and cloud servers.

   – Creates resources, including EC auto scaling groups.

   – Create or modify permissions, and check API methods including but not limited to CreateUser, CreateRole, AssumeRole*, Get*Token, Attach*Policy, *Image*, *Provider, Tag*, Create*, Delete* and Update*.

- Delete affected cloud resources.

- Modify affected cloud resources.

4. Based on the result of the previous step, identify any applications that might have been affected. Obtain the ID or tag information of each affected resource and notify the resource owner.

5. If additional credentials (such as IAM users and roles) are created, disable and delete all credentials of these resources based on the **Step 2.1**.

6. Repeat **Step 3.1** to **Step 3.5** to check for and handle all additional credentials.

Step 4 **Recover from incident**.

1. Restore the modified resource.

- If the resource can be destroyed and replaced, a new resource is added.

- If the resource cannot be replaced, perform either of the following operations:

- Restore a resource from a backup.

- New resources are prepared and configured in the application infrastructure, and damaged resources are isolated and removed from the application infrastructure.

- Destroy damaged resources or continue to isolate them for evidence.

- Restore the deleted resource.

i. Check the application to which the resource belongs. If the resource tag is not listed in the CTS service item and the resource is supported by the cloud, check the configuration.

ii. If the deleted resource can be restored from a backup, restore it directly. If the deleted resource cannot be restored from a backup, obtain the resource configuration from CMDB, provision the resource again, and configure it in the infrastructure of the application.

Step 5 **Complete post-incident activities**.

- Investigate and collect evidence on certain compromised resources, analyze the attack methods used by attackers on the compromised resources, and check whether additional risks and risk mitigation measures need to be taken for related resources or applications.

a. For any compromised resources that have been segregated for further analysis, forensic activities are performed on those resources and the findings are incorporated into ex post facto reporting.

b. Ensure that the CMDB is correctly updated to reflect the current status of all affected resources and applications.

- Review the incident itself and its response, determine which measures are effective and which are not, update the improvement process based on the information, and record the investigation results.

----End