SecMaster

Best Practices

Issue	01
Date	2023-06-20

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. All rights reserved.

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

Trademarks and Permissions

HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Contents

1 Operation Guide to Data Transfer

1.1 Scenario

SecMaster can access cloud service logs by default. Beyond that, SecMaster also provides log collection management. With this function, you can collect, parse, and transfer logs, query logs in a visualized manner, and build threat models.

During this process, you need to install an agent to enable the communication between SecMaster and the target ECS. You also need to install the Logstash component for data access, parsing, and transfer.

Currently, you can use either of the following methods for data access in SecMaster:

- **Quick Data Access with the Default Parser in SecMaster**
- **Data Access with a Custom Parser**

1.2 Constraints

There are some restrictions on using SecMaster log collection management:

- Currently, the data collection agent can run only on Linux servers running EulerOS of certain versions. For details, see **Supported OSs**.
- During agent installation, only IAM accounts can be used for viewing information on the console.

Supported OSs

Currently, the data collection agent can run only on EulerOS Linux servers on x86_64 architecture.

Table 1-1 Supported EulerOS versions

Version	ECS OS Version
EulerOS 2.5	EulerOS 2.5 64bit for Tenant 20210227 (40 GB) EulerOS 2.5 64bit for Tenant 20220321 base 2.5.11 (40 GB) EulerOS 2.5 64bit for Tenant 20220906 base 2.5.12 (40 GB) EulerOS 2.5 64bit for Tenant 20221130 base 2.5.13 (40 GB) Public-CAD-EulerOS-BaseTemplate-2.5.9-x86_64-Standard (dedicated for making resources and not supporting password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.5.11-x86_64-Standard (dedicated for making resources and not supporting password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.5.12-x86_64-Standard (dedicated for making resources and not supporting password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.5.13-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.5.14-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB)
EulerOS 2.9	Public-CAD-EulerOS-BaseTemplate-2.9.6-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.9.7-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.9.8-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.9.9-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.9.10-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB)
EulerOS 2.10	Public-CAD-EulerOS-BaseTemplate-2.10.5-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.10.6-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.10.7-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB)

1.3 Quick Data Access with the Default Parser in SecMaster

This chapter walks you through how to collect ECS logs in UDP mode, how to parse collected logs using the default parser configured for collectors, and how to send the parsed data to a SecMaster pipeline. After data access, you can query the information on the **Security Analysis** page.

Prerequisite

You have obtained the IAM account and its password for logging in to the console.

Step 1: Buy an ECS

For details, see **Purchasing an ECS**.

⚠ CAUTION

Currently, the data collection agent can run only on EulerOS Linux servers on x86_64 architecture. When purchasing an ECS, select an OS version SecMaster supports by referring to **Supported OSs**.

Figure 1-1 Selecting an OS version

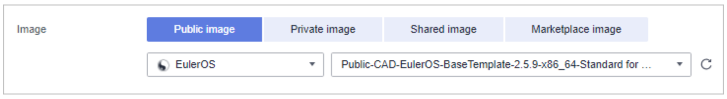


Image: Public image

EulerOS

Public-CAD-EulerOS-BaseTemplate-2.5.9-x86_64-Standard for ...

Step 2: Create a Node and Install the Agent on the Node

The agent is a client software that maintains the communication between SecMaster and an ECS. It can deliver commands and report heartbeat data.

For details about how to install an agent on an ECS, see **Installing the Agent**.

For details about how to add a node, see **Creating a Node**.

Step 3: Configure Components

Logstash is an open-source data collection engine that provides the real-time pipeline function. Logstash can dynamically collect data from different sources, convert the data, and output the data to different destinations.

For details about how to configure components, see **Configuring Components**.

Step 4: (Optional) Create a Pipeline

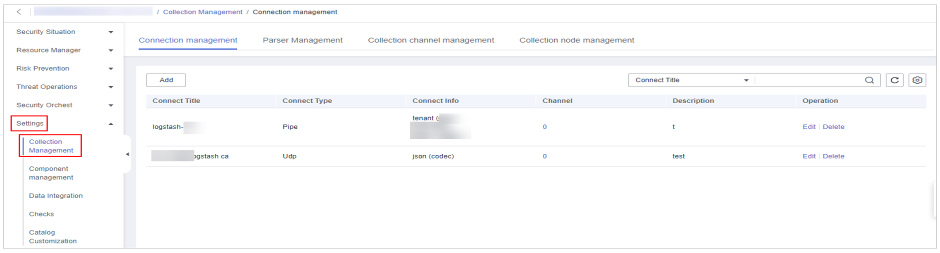
You need to add a pipeline for storing incoming data. For details, see **Creating a Pipeline**.

Step 5: Create a Data Connection Source and Destination

Create a data connection, including the data source and the data destination where the parsed data is transferred to.

1. Go to the SecMaster console.
2. In the navigation pane, choose **Workspace** > **Management**. In the workspace list, click the name of the target workspace.
3. In the navigation pane on the left, choose **Settings** > **Collection Management**.

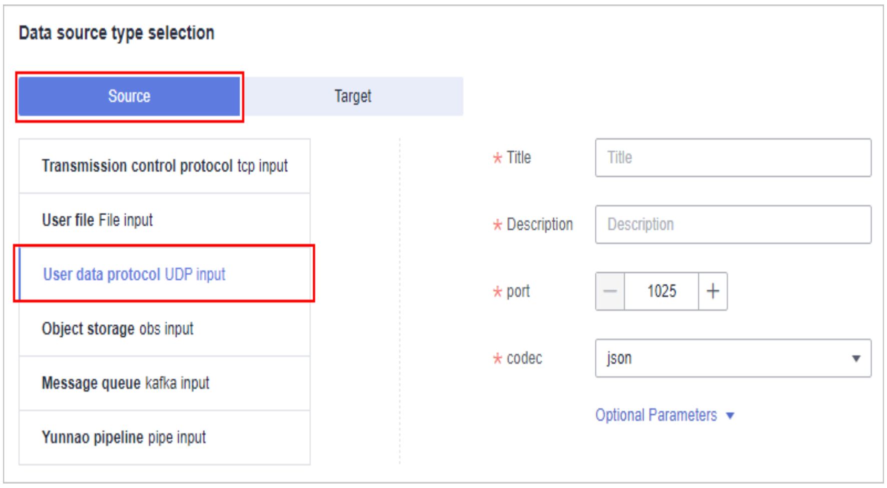
Figure 1-2 Collection Management



Connect Title	Connect Type	Connect Info	Channel	Description	Operation
logstash-[redacted]	Pipe	tenant ([redacted]	0	t	Edit | Delete
[redacted]ogstash ca	Udp	json (codec)	0	test	Edit | Delete

4. Add a data connection source.
   a. On the **Connection management** page, click **Add**.
   b. On the **Source** tab page, select **User data protocol UDP input** as the source of the data source type and set UDP parameters.

Figure 1-3 Data source


Data source type selection
Source
Target
Transmission control protocol tcp input
User file File input
User data protocol UDP input
Object storage obs input
Message queue kafka input
Yunnao pipeline pipe input
Optional Parameters

* Title: Title

* Description: Description

* port: 1025

* codec: json

Table 1-2 Data source parameters

Parameter	Description
Title	Name of the data connection source.
Description	A brief description of the data connection source.

Parameter	Description
Port	Set the port over which you want to collect the data.
codec	Set the encoding format. You can select **json** or **plain**.
Optional Parameters	Customize other optional parameters.

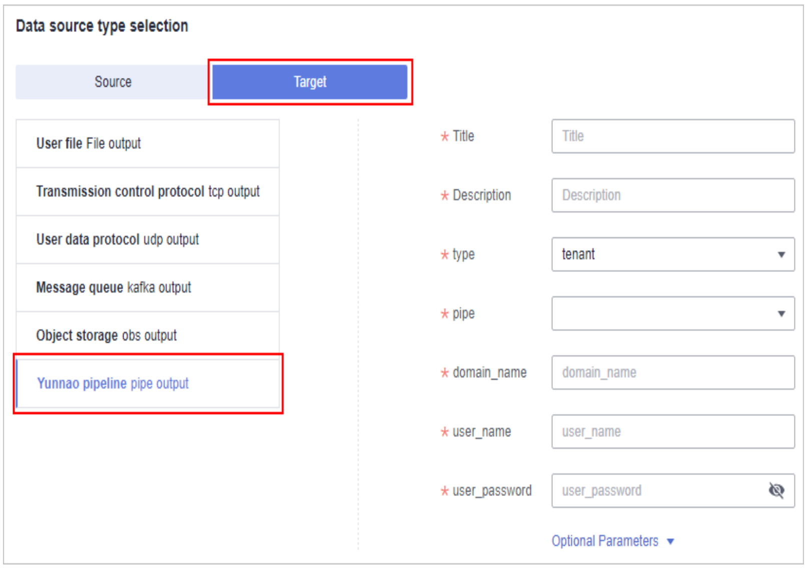
c. After the setting is complete, click **Confirm** in the lower right corner of the page.

5. Add a data connection destination.

a. On the **Collection Management** page, click the **Connection management** tab. On the displayed page, click **Add**.

b. Click the **Destination** tab. Then, select **Yunnao pipeline output** for the data source type and configure the pipeline information.

Figure 1-4 Data source access destination



Data source type selection

Source
Target
User file File output
Transmission control protocol tcp output
User data protocol udp output
Message queue kafka output
Object storage obs output
Yunnao pipeline pipe output

* Title: Title
* Description: Description
* type: tenant
* pipe:
* domain_name: domain_name
* user_name: user_name
* user_password: user_password

Table 1-3 Data source access destination parameters

Parameter	Description
Title	Name of the data source destination.
Description	A brief description of the data connection destination.
type	Select **tenant**.
pipe	Select the name of the pipeline created in **Step 4: (Optional) Create a Pipeline**.

Parameter	Description
domain_name	Enter the account that creates the IAM user.
User_name	Enter the IAM username.
Password	Enter the password of the IAM user.
Optional Parameters	Customize other optional parameters.

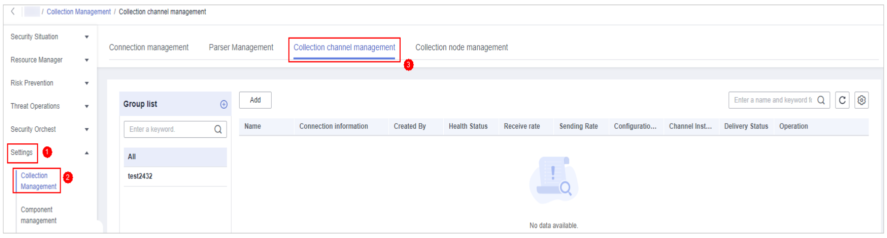
c. After the setting is complete, click **Confirm** in the lower right corner of the page.

Step 6: Add a Collection Channel

A collection channel connects the input, parsing, and output to form a pipeline and delivers the pipeline to collection nodes where the agent and Logstash are installed. In doing this, the data access and transfer process can then start.

1. Go to the SecMaster console.
2. In the navigation pane, choose **Workspace** > **Management**. In the workspace list, click the name of the target workspace.
3. In the navigation pane on the left, choose **Settings** > **Collection Management**. On the **Collection Management** page, click the **Collection Channels** tab.

Figure 1-5 The collection channel management page is displayed.



4. Add a channel group.

   a. On the collection channel management page, click ⊕ on the right of the **Group list**.

   b. Enter a group name and click ✓.

5. On the right of the group list, click **Add**.
6. On the **Basic Configuration** page, configure basic information.

Table 1-4 Basic configuration parameters

Parameter		Description
Basic Information	Title	The collection channel name you customize.
	Channel grouping	Select the group created in 4.

Parameter		Description
	Description	(Optional) Enter the description of the collection channel.
Source Configuration	Source Name	Select the source created in **Step 5: Create a Data Connection Source and Destination**.
Destination Configuration	Destination Name	Select the destination created in **Step 5: Create a Data Connection Source and Destination**.

7. After the basic configuration is complete, click **Next** in the lower right corner of the page.
8. On the **Parser Configuration** page, select **Fast access**.

   In quick access mode, all raw logs are stored in the message field.
9. After the parser is configured, click **Next** in the lower right corner of the page.
10. On the **Select Node** page, click **Add**. In the **Add Node** dialog box displayed, select a node that has the agent and Logstash installed and click **Confirm**.
11. After the node is selected, click **Next** in the lower right corner of the page.
12. On the **Channel Details Preview** page, confirm the configuration and click **OK**.

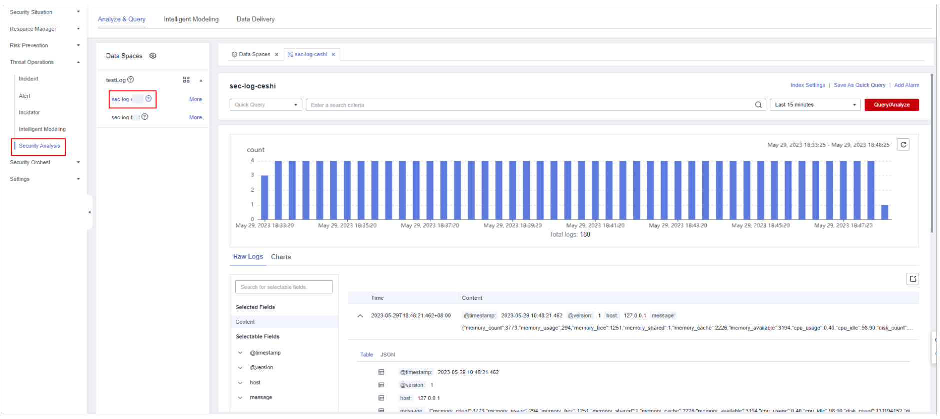
After the collection channel is added, the pipeline will be delivered. Refresh the page. If the health status is **Normal**, the delivery is complete.

Step 7: Query and Analyze

As logs are transferred to SecMaster, you can query logs in SecMaster after data access completes.

1. Go to the SecMaster console.
2. In the navigation pane, choose **Workspace** > **Management**. In the workspace list, click the name of the target workspace.
3. In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**.
4. Select the SecMaster pipeline added in **Step 4: (Optional) Create a Pipeline**. Then, you can view the parsed log data on SecMaster.

Figure 1-6 Analyze & Query



2023-05-29T18:48:21.462+08:00 @timestamp: 2023-05-29 10:48:21.462 @version: 1 host: 127.0.0.1 message:
{"memory_count":3773,"memory_usage":294,"memory_free":1251,"memory_shared":1,"memory_cache":2226,"memory_available":3194,"cpu_usage":0.40,"cpu_idle":98.90,"disk_count":...

@timestamp: 2023-05-29 10:48:21.462
@version: 1
host: 127.0.0.1

1.4 Data Access with a Custom Parser

This chapter describes how to parse ECS logs SecMaster collects in UDP mode into JSON format and how to transfer the parsed data to a SecMaster pipeline. After the data access, you can query information on the **Security Analysis** page and build threat models based on parsed logs.

Prerequisites

You have obtained the IAM account and its password for logging in to the console.

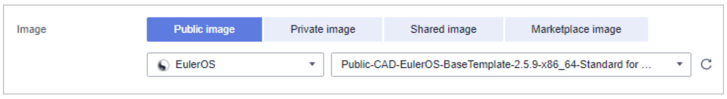
Step 1: Buy an ECS

For details, see **Purchasing an ECS**.

CAUTION

Currently, the data collection agent can run only on EulerOS Linux servers on x86_64 architecture. When purchasing an ECS, select an OS version SecMaster supports by referring to **Supported OSs**.

Figure 1-7 Selecting an OS version



EulerOS
Public-CAD-EulerOS-BaseTemplate-2.5.9-x86_64-Standard for ...

Step 2: Create a Node and Instal the Agent on the Node

The agent is a client software that maintains the communication between SecMaster and an ECS. It can deliver commands and report heartbeat data.

For details about how to install an agent on an ECS, see **Installing the Agent**.

For details about how to add a node, see **Creating a Node**.

Step 3: Configure Components

Logstash is an open-source data collection engine that provides the real-time pipeline function. Logstash can dynamically collect data from different sources, convert the data, and output the data to different destinations.

For details about how to configure components, see **Configuring Components**.

Step 4: (Optional) Create a Pipeline

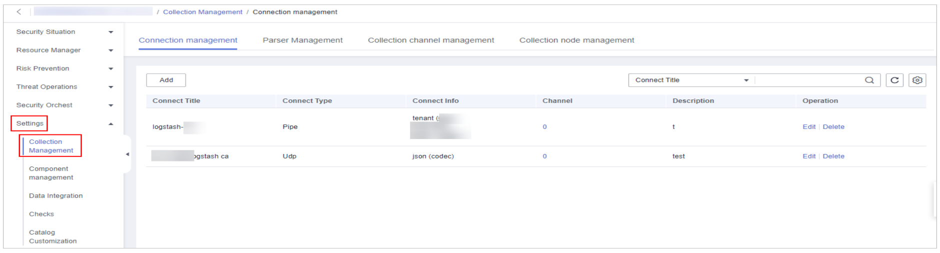
You need to add a pipeline for storing incoming data. For details, see **Creating a Pipeline**.

Step 5: Create a Data Connection Source and Destination

Create a data connection, including the data source and the data destination where the parsed data is transferred to.

1. Go to the SecMaster console.
2. In the navigation pane, choose **Workspace** > **Management**. In the workspace list, click the name of the target workspace.
3. In the navigation pane on the left, choose **Settings** > **Collection Management**.

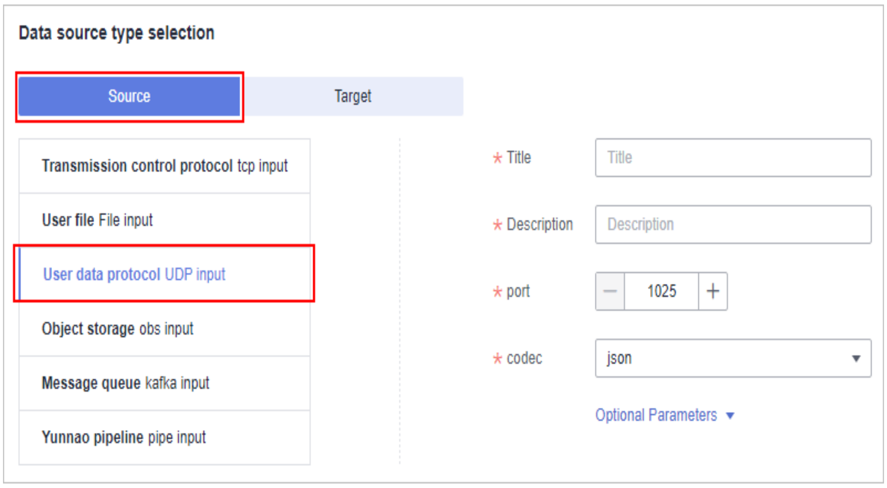
Figure 1-8 Collection Management



Connect Title	Connect Type	Connect Info	Channel	Description	Operation
logstash-[redacted]	Pipe	tenant ([redacted]	0	t	Edit | Delete
[redacted]ogstash ca	Udp	json (codec)	0	test	Edit | Delete

4. Add a data connection source.
   a. On the **Connection management** page, click **Add**.
   b. On the **Source** tab page, select **User data protocol UDP input** as the source of the data source type and set UDP parameters.

Figure 1-9 Data source parameters


Data source type selection
Source
Target
Transmission control protocol tcp input
User file File input
User data protocol UDP input
Object storage obs input
Message queue kafka input
Yunnao pipeline pipe input
Optional Parameters

* Title: Title
* Description: Description
* port: 1025
* codec: json

Table 1-5 Data source parameters

Parameter	Description
Title	Name of the data connection source.
Description	A brief description of the custom data connection source.
Port	Set the port over which you want to collect the data.
codec	Set the encoding format. You can select **json** or **plain**.
Optional Parameters	Customize other optional parameters.

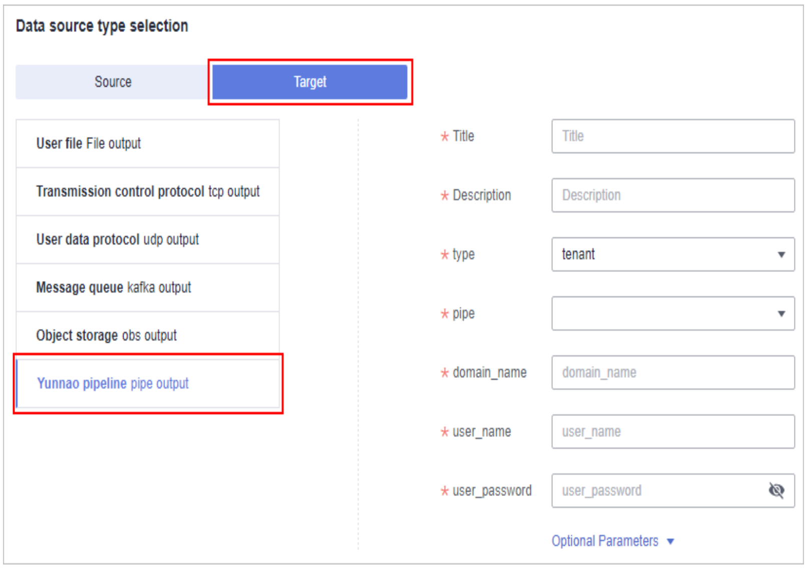
c. After the setting is complete, click **Confirm** in the lower right corner of the page.

5. Add a data connection destination.

a. On the **Collection Management** page, click the **Connection management** tab. On the displayed page, click **Add**.

b. Click the **Destination** tab. Then, select **Yunnao pipeline output** for the data source type and configure the pipeline information.

Figure 1-10 Data source access destination



Data source type selection
Source
Target
User file File output
Transmission control protocol tcp output
User data protocol udp output
Message queue kafka output
Object storage obs output
Yunnao pipeline pipe output
* Title
Title
* Description
Description
* pipe
* domain_name
domain_name
* user_name
user_name
* user_password
user_password
Optional Parameters ▾

* type: tenant

Table 1-6 Data source access destination parameters

Parameter	Description
Title	Name of the data source destination.

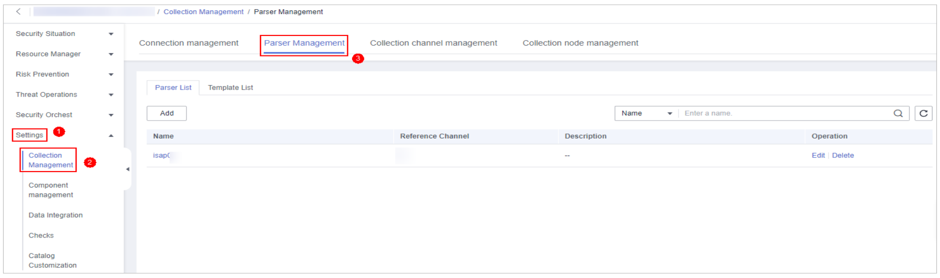
Parameter	Description
Description	A brief description of the data connection destination.
type	Select **tenant**.
pipe	Select the name of the pipeline created in **Step 4: (Optional) Create a Pipeline**.
domain_name	Enter the account that creates the IAM user.
User_name	Enter the IAM username.
Password	Enter the password of the IAM user.
Optional Parameters	Customize other optional parameters.

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

Step 6: Configure a Parser

1. Go to the SecMaster console.
2. In the navigation pane, choose **Workspace** > **Management**. In the workspace list, click the name of the target workspace.
3. In the navigation pane on the left, choose **Settings** > **Collection Management** > **Parser Management** tab.

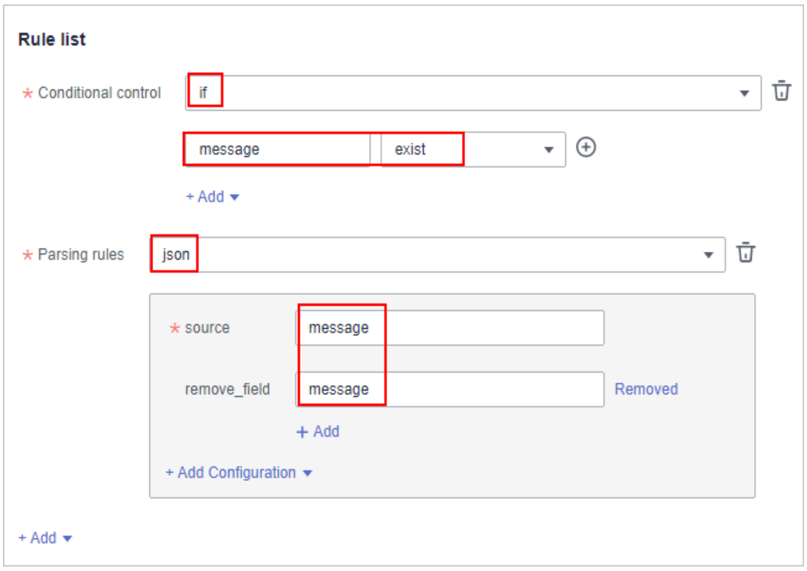
Figure 1-11 Accessing the parser management page



Name	Reference Channel	Description	Operation
isap(		--	Edit | Delete

4. On the **Parser Management** page, click **Add**. On the displayed page, set parameters and add a collection channel.
   - **Name**: Set a parser name.
   - (Optional) **Description**: Enter the parser description.
   - **Rule list:** Set parsing rules for the parser. Click **Add** and select a rule type.
     - **Conditional control**: Select the **if** condition to check whether the log exists.
     - **Parsing rules**: Select **json** to remove the original field (message).

Figure 1-12 Rule list



Rule list

* Conditional control: if

message | exist

+ Add

* Parsing rules: json

* source: message

remove_field: message Removed

+ Add

+ Add Configuration

+ Add

5. Click **OK** in the lower right corner of the page.

Step 7: Add a Collection Channel

A collection channel connects the input, parsing, and output to form a pipeline and delivers the pipeline to collection nodes where the agent and Logstash are installed. In doing this, the data access and transfer process can then start.

1. Add a channel group.
   a. On the collection channel management page, click ⊕ on the right of the **Group list**.
   b. Enter a group name and click ✓.
2. On the right of the group list, click **Add**.
3. On the **Basic Configuration** page, configure basic information.

Table 1-7 Basic configuration parameters

Parameter		Description
Basic Information	Title	The collection channel name you customize.
	Channel grouping	Select the group created in **1**.
	Description	(Optional) Enter the description of the collection channel.
Source Configuration	Source Name	Select the source created in **Step 5: Create a Data Connection Source and Destination**.

Parameter		Description
Destination	Destination Name	Select the name of the data destination created in **Step 5: Create a Data Connection Source and Destination**.

4. After the basic configuration is complete, click **Next** in the lower right corner of the page.
5. On the parser configuration page, select the parser configured in **Step 6: Configure a Parser**.
6. After the parser is configured, click **Next** in the lower right corner of the page.
7. On the **Select Node** page, click **Add**. In the **Add Node** dialog box displayed, select a node that has the agent and Logstash installed and click **Confirm**.
8. After the node is selected, click **Next** in the lower right corner of the page.
9. On the **Channel Details Preview** page, confirm the configuration and click **OK**.

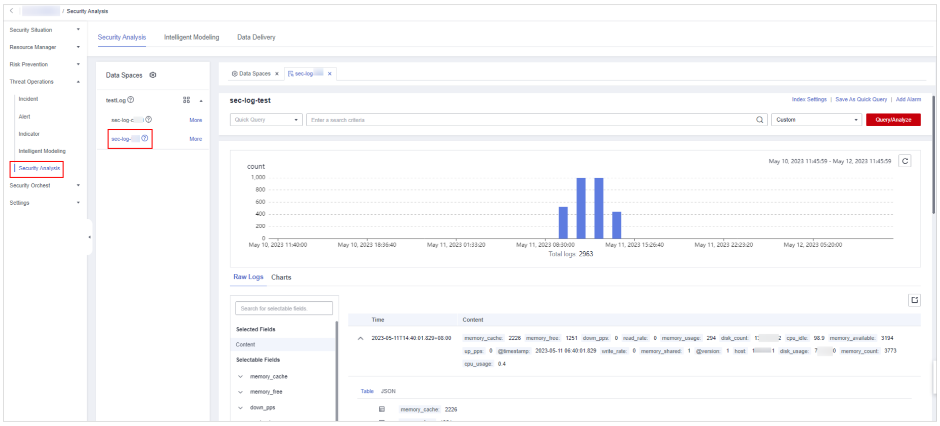
After the collection channel is added, the pipeline will be delivered. Refresh the page. If the health status is **Normal**, the delivery is complete.

Step 8: Query and Analyze

As logs are transferred to SecMaster, you can query logs in SecMaster after data access completes.

1. Go to the SecMaster console.
2. In the navigation pane, choose **Workspace** > **Management**. In the workspace list, click the name of the target workspace.
3. In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**.
4. Select the SecMaster pipeline added in **Step 4: (Optional) Create a Pipeline**. Then, you can view the parsed log data on SecMaster.

Figure 1-13 Security Analysis



Time	Content
2023-05-11T14:40:01.829+08:00	memory_cache: 2226 memory_free: 1251 down_pps: 0 read_rate: 0 memory_usage: 294 disk_count: 1[redacted]2 cpu_idle: 98.9 memory_available: 3194 up_pps: 0 @timestamp: 2023-05-11 06:40:01.829 write_rate: 0 memory_shared: 1 @version: 1 host: 1[redacted]1 disk_usage: 7[redacted]0 memory_count: 3773 cpu_usage: 0.4

memory_cache: 2226

A Change History

Released On	Description
2023-06-20	This issue is the first official release.