NAIE
V200R020C50

Fault Identification & Root Cause Localization

Issue 01
Date 2020-06-30
1 Documentation Guide

Documents including Introduction, Quick Start, FAQs, API Reference, and Glossary are given to help customers learn and use the fault identification and root cause localization service in order to customize site-oriented models.

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>This document describes the positioning, application scenarios, functions, benefits, and restrictions of the fault identification and root cause localization service.</td>
</tr>
<tr>
<td>Quick Start</td>
<td>This document describes how to use the fault identification and root cause localization service to quickly generate fault identification and root cause localization models, helping users quickly get familiar with and use the fault identification and root cause localization service.</td>
</tr>
<tr>
<td>FAQs</td>
<td>This document provides answers to frequently asked questions (FAQs) for users of the fault identification and root cause localization service.</td>
</tr>
<tr>
<td>Glossary</td>
<td>This document describes the product terms related to the fault identification and root cause localization service.</td>
</tr>
<tr>
<td>API Reference</td>
<td>This document describes the APIs of the fault identification and root cause localization service, including the description, syntax, parameter description, examples, and other information.</td>
</tr>
</tbody>
</table>
2.1 Introduction to Fault Identification and Root Cause Locating

Algorithms and technologies, such as big data and AI, are used to process alarm flows on the live network in real time, and to aggregate alarms, identify faults, and locate root causes in a timely and accurate manner. Network alarm flow data, such as wireless access, transmission, and power and environment data, is interconnected to obtain network fault information and identify root alarms. Trouble tickets can be compressed and delivered precisely, helping O&M engineers efficiently perform O&M.

2.2 Application Scenarios

RAN Fault Identification and Root Cause Locating

Faults frequently occur on the RAN in the telecom field. Devices and network management systems (NMSs) continuously report a large amount of alarm data. However, cross-domain alarm correlation, fault identification, and root cause locating are difficult. Trouble tickets may be repeatedly and ineffectively dispatched. Some trouble tickets may not be handled. As a result, O&M efficiency is low. This service aims to resolve the preceding issues. Based on the real-time alarm flow and topology data, this service aggregates alarms, quickly identifies faults, and accurately locates the root causes of faults.

2.3 Product Features

Toggling Alarm Filtering

Real-time live network toggling alarms are identified and filtered, which does not affect the identification and handling of common faults.
Alarm Aggregation
Fault alarms are aggregated based on intelligent fault duration prediction and topology relationships.

Fault Identification
Root causes are located and faults are identified based on fault propagation diagrams, other algorithms, and aggregated alarm data. Both single-domain and cross-domain faults can be accurately identified.

Fault Rectification
Whether the identified faults are rectified is determined in real time based on the reported alarm clearance data. No trouble tickets need to be dispatched for rectified faults.

Fault Association
Subsequent alarm association identifies faults on the same NE in different periods. Only original faults need to be handled. Faults around the same time or in a similar topology are automatically associated to facilitate trouble ticket combination.

Incremental Recommendation on Propagation Relationships
Alarm propagation correlations can be periodically trained and recommended based on new alarm data. Users can select, accept, and apply the correlations for fault identification.

2.4 Product Values

Accurate Fault Identification
A suitable fault identification process and efficient aggregation and identification algorithms accurately identify and locate faults. The fault check rate reaches 100%. The fault check accuracy reaches 95%.

Easy to Use
RAN fault propagation diagrams are constantly updated. After topology data configuration, users can identify and locate faults by interconnecting with real-time alarm streams.

Continuous Optimization
New alarm propagation correlations can be automatically learned online. These correlations can be manually identified and are applicable to live-network inference, facilitating continuous incremental learning and improving service performance.
Various Functions

Toggling alarm filtering, alarm aggregation, fault identification, fault rectification, subsequent alarm association, incremental recommendation, and other built-in functions support fault identification and locating.

2.5 Restrictions

Data Restrictions

Network alarms must contain information such as the accurate occurrence time, device where the alarms are generated, and alarm names. In addition, the alarms can be mounted to the NEs in the topology. For details about the alarm data format, see the related API document.

The topology relationship between devices must be determined, including: topology relationships between base stations and transmission NEs, and between transmission NEs; power supply relationship between the power and environment and base stations, and between the power and environment and transmission NEs. For details about the topology data format, see the related API document.

Alarm Propagation Relationship Restrictions

Experts are required in the inference based on new alarm propagation relationships after the service is launched.

Scenario Restrictions

This service applies to the RAN.

2.6 Basic Concepts

B

BTS

A Base Transceiver Station (BTS) terminates the radio interface. It allows transmission of traffic and signaling across the air interface. The BTS includes the baseband processing, radio equipment, and the antenna.

G

TE Association

The system recommends TEs that have similar topologies and occur around the same time to users.

I

IP RAN
An IP radio access network (RAN) is a network that uses IP technology to achieve data backhaul on a radio access network.

**Associated TE**

If an original TE that occurs closest to the time when the current TE occurs is not deleted from the historical TEs of the root NE, the current TE is associated to this original TE.

**POW**

Value of the NeType field in the alarm data file. This value indicates power and environment devices that power wireless base stations and transmission network elements on the radio access network.

**PTN**

Value of the NeType field in the alarm data file. This value indicates the devices which data passes through from a base station to the core network.

**TRANS**

Value of the NeType field in the alarm data file. This value indicates transmission devices on the radio access network.

**Topology**

A topology displays the logical layout of the components of a computer system or network and their interconnections.

**Original TE**

Original TE and secondary TE occurring on the same NE in different time periods are considered the same fault. After the original TE fault is rectified, the secondary TE fault is automatically rectified.

### 2.7 Service Dependencies

**ModelArts Service**

The NAIE platform uses the ModelArts service provided by the Huawei public cloud system to implement data preprocessing and large-scale distributed model training.
IAM Service

The NAIE platform uses the Identity and Access Management (IAM) service provided by the Huawei public cloud system to implement unified identity authentication and permission management.

API Gateway

The NAIE platform must interconnect with the unified API gateway provided by the Huawei public cloud system. The API gateway provides a unified entrance for users to invoke NAIE cloud service APIs. APIs provided by the NAIE cloud service for tenants must be registered with the API gateway before being released.

Relationship with the OBS

The NAIE platform uses the Object Storage Service (OBS) to store data and model backup and snapshots, achieving secure, reliable, and low-cost storage.

Relationship with the CCE

The NAIE platform uses the Cloud Container Engine (CCE) to deploy models as online services, satisfying requirements for high concurrency and elastic scaling.

2.8 Billing Description

Billing Items

The fault identification and root cause locating service is charged based on the number of alarms and service subscription duration set during the subscription. The billing items include the number of alarms, as described in Table 2-1.

<table>
<thead>
<tr>
<th>Billing Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of alarms</td>
<td>The fault identification and root cause locating service is charged based on the number of alarms and service subscription duration set during the subscription. You will be charged for the service after the subscription. If you do not use the service, unsubscribe from it in a timely manner to avoid unnecessary fees.</td>
</tr>
</tbody>
</table>

Billing Mode

Pay-per-use mode is used. Fees are charged based on the number of alarms and service subscription duration set during the subscription.

Billing formula: Unit price x Number of alarm steps x Service subscription duration. The billing step is 50,000 alarm events per day.
Changing Billing Mode

Fees are charged for the fault identification and root cause locating service after the subscription. Users can unsubscribe from or re-subscribe to the service as required. No service change configuration is involved.

Renewal

Users can recharge their accounts in time as required to ensure that the fault identification and root cause locating service can be used properly.

Expiration and Overdue Payment

If you do not renew your subscription on time, the cloud platform provides a grace period and a retention period. The grace period and retention period depend on the customer level. For details, see Grace Period and Retention Period.

If the account is not recharged after the retention period expires, the resources are cleared.

2.9 Accessing Fault Identification and Root Cause Locating Service

Step 1 Enter https://console-intl.huaweicloud.com/naie/ in the address box of a browser on a user PC and press Enter to access the AI marketplace.

Step 2 Click Sign In in the upper right corner to access the login page.

Step 3 Select IAM User Login and enter the account name, IAM user name, and password, as shown in Figure 2-1.

You can also log in using an account. Change the password after the first successful login and change the password periodically.
Figure 2-1 Logging in as an IAM user

Step 4 Click Log In to access the AI marketplace.

Step 5 Choose AI Services > Model Service > Telco Domain AI Model Service > Fault Identification and Root Cause Locating. The fault identification and root cause locating service introduction page is displayed.

Step 6 Click Enter Service. The fault identification and root cause locating service page is displayed.

----End

2.10 Change History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-06-30</td>
<td>Added section &quot;Billing Description.&quot;</td>
</tr>
<tr>
<td>2020-03-30</td>
<td>Optimized the entire document.</td>
</tr>
<tr>
<td>2019-12-30</td>
<td>Released this document officially for the first time.</td>
</tr>
</tbody>
</table>
3 Quick Start

3.1 Prerequisites

3.2 Subscribing to the Fault Identification and Root Cause Locating Service

Step 1  Enter https://console-intl.huaweicloud.com/naie/ in the address box of a browser on a user PC and press Enter to access the AI marketplace.

When you access the AI marketplace for the first time, the Access Authorization page is displayed. Click Authorize.

Step 2  Click Log In in the upper right corner. The login page is displayed, as shown in Figure 3-1.
Step 3  Enter the tenant name and password, and click Log In to enter the AI marketplace.

Change the password after the first successful login and change the password periodically.

Step 4  Choose AI Services > Model Service > Telco Domain AI Model Service > Fault Identification and Root Cause Locating. The fault identification and root cause locating service introduction page is displayed.

Step 5  Click Buy Now. The page shown in Figure 3-2 is displayed.

You can click Learn about billing details to better understand the resources, specifications, and price information provided by the fault identification and root cause locating service. In addition, when you use a specific resource, the fault identification and root cause locating service displays an eye-catching charging prompt on the page.

The parameters are described as follows:

- Region: HUAWEI CLOUD region that provides services.
- Alarm Number: Average number of alarms generated per day. Set this parameter based on the site requirements.
3.3 Accessing Fault Identification and Root Cause Locating Service

**Step 1** Enter [https://console-intl.huaweicloud.com/naie/](https://console-intl.huaweicloud.com/naie/) in the address box of a browser on a user PC and press Enter to access the AI marketplace.

**Step 2** Click Sign In in the upper right corner to access the login page.

**Step 3** Select IAM User Login and enter the account name, IAM user name, and password, as shown in Figure 3-3.

You can also log in using an account. Change the password after the first successful login and change the password periodically.
Figure 3-3 Logging in as an IAM user

Step 4 Click Log In to access the AI marketplace.

Step 5 Choose AI Services > Model Service > Telco Domain AI Model Service > Fault Identification and Root Cause Locating. The fault identification and root cause locating service introduction page is displayed.

Step 6 Click Enter Service. The fault identification and root cause locating service page is displayed.

---End

3.4 Project Management

Data assets in a domain must be isolated. A project contains corresponding data assets and the alarm information of the corresponding domain. Multi-project management is introduced. Each project stores only the data assets of the project. Data is isolated during fault identification and root cause locating.

Step 1 Log in to the fault identification and root cause locating service. The project management list is displayed on the homepage by default, as shown in Figure 3-4.

By default, the system initializes a default project. Some sample data is preconfigured in the project for reference.
Figure 3-4 Project management list

![Project Management List Screen](image)

**Step 2** Click **Create** to create a project, as shown in **Figure 3-5**.

Figure 3-5 Creating a project

![Create Project Screen](image)

**Step 3** You can perform the following operations on the project:

- ✗: Edit project information. The default project cannot be edited.
- ❌: Delete the project.
- ☑: View project information and manage the project, as shown in **Figure 3-6**.
In the upper left corner of the project details page, click on the right of the project name to return to the project management list page.

Figure 3-6 Viewing the project

3.5 Monitoring Overview

The fault identification and root cause locating service provides comprehensive fault monitoring functions.

Step 1  Click in the Operation column corresponding to the target project.

The Monitoring Overview page is displayed. You can view the trouble event (TE) overview, as shown in Figure 3-7. Table 3-1 describes the statistics. The statistics are updated dynamically.

Figure 3-7 Monitoring overview page
### Table 3-1 Monitoring overview parameters

<table>
<thead>
<tr>
<th>Statistical chart name</th>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Uncleared TEs</td>
<td>Number of currently uncleared TEs</td>
<td></td>
</tr>
<tr>
<td>TE statistics on the current day</td>
<td>TE quantity curve on the current day</td>
<td></td>
</tr>
<tr>
<td>TE statistics of this week</td>
<td>TE quantity curve of the current week</td>
<td></td>
</tr>
<tr>
<td>Top 5 fault statistics</td>
<td>Top 5 faults in all historical faults</td>
<td></td>
</tr>
<tr>
<td>Top 5 fault root causes</td>
<td>Top 5 root alarms of all historical faults</td>
<td></td>
</tr>
<tr>
<td>Top 5 fault symptoms</td>
<td>Top 5 symptom alarms of all historical faults</td>
<td></td>
</tr>
<tr>
<td>TE recovery rate (%)</td>
<td>Percentage of cleared TEs based on the <strong>TE clearing policy</strong> configured on the <strong>System Configurations &gt; Parameter Configuration</strong> page.</td>
<td></td>
</tr>
<tr>
<td>TE recovery duration (min)</td>
<td>Duration from the TE generation time to the TE clearance time. The two curves indicate the maximum and average recovery durations at the current time, respectively.</td>
<td></td>
</tr>
<tr>
<td>TE generation duration (min)</td>
<td>Duration from the generation time of the first TE alarm to that of the last TE alarm. The two curves indicate the maximum and average TE generation durations at the current time, respectively.</td>
<td></td>
</tr>
</tbody>
</table>

---End

### 3.6 Fault Dashboard

The fault identification and root cause locating service provides comprehensive fault monitoring functions. You can view TEs and TE details on the fault dashboard page.

**Step 1** Click 📅 in the **Operation** column corresponding to the target project.

**Step 2** Choose **Fault dashboard** from the navigation pane.

The **Fault dashboard** page is displayed, as shown in **Figure 3-8**. The parameters are described as follows:

- **Auto refresh period**: Page refresh interval. Select a value from the drop-down list box as required.
- **Filter Criteria**: Set the TE filtering criteria and click **Query**. The TE information meeting the filtering criteria is displayed.
- TE information display area: You can click in the upper right corner of the page to switch to the list display mode.

**Figure 3-8** Fault dashboard

**Step 3** Click a TE diagram. The **TE Details** page is displayed, as shown in **Figure 3-9**.

1. **TE information**: The number of NEs (radio base stations, transmission NEs, and power and environment devices) involved in the TE, root NEs, total number of alarms, root alarms, and symptom alarms are displayed. Click on the right of **TE information** to view all alarms of the current TE.

2. **NE topology links**: You can check the TE fault scenario. Click an NE. Then, all alarms and rules of the NE are displayed on the right.

3. **Information about the selected NE**: The name of the selected NE and the number of NE alarms are displayed. Click on the right of **Select NE Info** to view all alarms of the selected NE.

4. The alarm and rule information of the selected NE are displayed.
Step 4  Click **Switch to Activity Rule** in the upper right corner of the page. The page shown in **Figure 3-10** is displayed.

You can add or delete rule lines.

- **Delete a rule**: Select a rule line and click **Delete** to delete the rule line.
- **Add a rule**: Click **Add Rules**. Then, click a start alarm and drag a line to an end alarm.
Step 5 If you want to restore the modified rules to the original ones, click **Switch to Historical Rule**. Then, the modification does not take effect. If you want the modification to take effect, click **Save**.

Step 6 Click **Secondary relationship** in the upper right corner of the page. You can view the list of all secondary and original TEs related to the current TE, as shown in **Figure 3-11**.

Secondary TE and original TE are considered the same fault occurring in different time periods. If the original TE is rectified, the secondary TE is automatically rectified.

Click **Details** on the right of a TE. The **TE Details** dialog box of the TE is displayed. Click **Back** in the upper right corner of the **TE Details** dialog box. You can return the **TE Details** page.
Figure 3-11 Secondary relationships

Secondary relationship

- Current TE: Unresolved
  Root alarm:NE_COMMU_BREAK; Symptom alarm:NE Is Disconnected
  2019/12/26 09:00:17

- Secondary TE1: Unresolved
  Root alarm:LTI1; Symptom alarm:LTI1
  2019/12/26 09:00:31

- Secondary TE2: Unresolved
  Root alarm:NE_COMMU_BREAK; Symptom alarm:NE Is Disconnected
  2019/12/26 09:01:05

- Secondary TE3: Unresolved
  Root alarm:MW_LOF; Symptom alarm:LAG_MEMBER_DOWN
  2019/12/26 09:02:43

Step 7 Click Associated TEs on the TE Details page. The Associated TEs page is displayed.

You can view all TEs associated with the current TE. You can click the button in the red box shown in Figure 3-12 to switch the TE display mode.

Associated TEs involve TEs that occur in the same time period and have similar topologies.

Figure 3-12 Associated TEs

-----End
3.7 Fault Propagation Diagram

3.7.1 Managing Alarm Propagation Relationships

You can easily view and edit alarm propagation relationships.

**Step 1**  
On the menu bar, click **Fault Propagation Diagram** and choose **Management**.

The alarm propagation relationship management page is displayed, as shown in **Figure 3-13**. The page is described as follows:

- Drop-down list box in the upper left corner: Switch to display single-NE or cross-NE alarm propagation relationships.
- Filtering criteria: Set search criteria. Set the alarm title to screen out propagation relationships containing specific alarms. Set the NE type to screen out alarm propagation relationships of NEs of the specific type. After the filtering criteria are set, click **Query** on the right of the page for the settings to take effect.
- Number of propagation relationships: The number of current alarm propagation relationships on the page and that of all alarm propagation relationships are displayed.
- Alarm propagation relationship diagram: The icon indicates the NE type. The text below the icon indicates the alarm name. The line direction indicates the alarm propagation relationship. One line indicates one propagation relationship.

**Figure 3-13 Management page**

**Step 2**  
Click **Import Rules** in the upper right corner of the page. The **Import** dialog box is displayed.
Click **Download rule sample file** to download and modify the example file. After the modification is complete, upload the file. You can view the imported data on the **Management** page.

**Figure 3-14** Import dialog box

![Import dialog box](image)

**Step 3** You can perform the following operations on the propagation diagram.
- Add a propagation relationship: Click **Add Rules** in the upper left corner of the page. Click a start alarm and draw a line to another alarm with a propagation relationship.
- Edit a propagation relationship: Click a propagation relationship line. Click **Edit Rules** displayed in the upper left corner of the page. In the displayed **edit** dialog box, set the confidence value.
- Delete a propagation relationship: Click a propagation relationship line. Click **Delete** displayed in the upper left corner of the page.

**Step 4** After the modification is complete, click **in the upper right corner of the page to save the modification.**

**Step 5** If the propagation diagram content is correct, click **More** in the upper right corner of the **Management** page and choose **Release activity rules** to publish the propagation diagram.

After the publication is complete, the propagation diagram is published as a version, facilitating the search and backtracking of historical propagation diagrams.

**Step 6** After the propagation diagram is published, click **More** and choose **Application version rules.**

You can apply the propagation diagram to live-network inference as required.

**Step 7** If a full propagation diagram is not published, click **More** and choose **Delete activity rules** to delete the full propagation diagram.
Step 8  Click More and choose Restore version rules. The Restore version rules dialog box is displayed, as shown in Figure 3-15. Historical versions obtained by propagation diagram publication are displayed in the dialog box. Select a historical version and click Restoration rules to restore the historical version. You can further perform operations in this section on the historical version.

Figure 3-15 Restoring a propagation diagram

---End

3.7.2 Recommended Alarm Propagation Relationships

If Automatic mining period is set on the System Configurations > Parameter Configuration page, alarm propagation relationships obtained by the automatic mining period running model are displayed in a list on this page. You can check whether the propagation relationships are correct based on actual services.

Step 1  On the menu bar, click Fault Propagation Diagram and choose Recommended. The fault propagation diagram recommendation page is displayed, as shown in Figure 3-16. The page is described as follows:

- Filtering criteria: Set the propagation diagram type, root alarm type, symptom alarm type, and other information as required. Support indicates the occurrence frequency of the current alarm propagation relationships. Click Query to display screened-out data.
- Fault propagation diagram list: One raw displays one alarm propagation relationship, including information such as the root alarm, symptom alarm, occurrence frequency, and confidence.
Step 2  You can perform the following operations on a recommended alarm propagation relationship.

- If the alarm propagation relationship is correct, click ✅ in the Operation column. In the displayed Note dialog box, click OK. The alarm propagation relationship is saved to the database.
- If the root alarm and symptom alarm of the alarm propagation relationship are reversed, click ⬅️ in the Operation column. In the displayed Note dialog box, click OK. The alarm propagation relationship is corrected and saved to the database.
- If the propagation relationship is incorrect, click ⬇️ in the Operation column. In the displayed Note dialog box, click OK. The alarm propagation relationship is deleted.

Step 3  To apply saved alarm propagation relationships to live-network inference, you need to perform propagation diagram publication and appliance on the Fault Propagation Diagram > Management page. For details, see Managing Alarm Propagation Relationships.

----End

3.8 Data Access

The fault identification and root cause locating service aims to use intra-NE and inter-NE alarm compression and fault identification on the radio access network (including power and environment, base stations, and transmission NEs) to accurately dispatch trouble tickets and achieve the goal of one fault having one trouble ticket. The relationships between power and environment, base stations, and transmission NEs are as follows:

- Power and environment devices power base stations and transmission NEs.
Transmission NEs are NEs close to base stations. Therefore, you need to import the following data on the data access page:

- Service path file: Service topology relationship file of base stations and transmission NEs. Currently, only local upload is supported.
- Power supply relationship file: Topology relationship file for power and environment devices to power base stations and transmission NEs. Currently, only local upload is supported.
- Alarm file: Alarm aggregation file of base stations, power and environment, and transmission NEs. Data can be imported in three methods, including local upload, subscription and import of alarm dataset files published using the dataset service, and API-based data access. You can import alarm data flows using one of the methods.

**Topology File Upload from the Local PC**

**Step 1** Click in the Operation column corresponding to the target project.

**Step 2** Choose Data Access from the navigation pane.

The Data Access page is displayed, as shown in **Figure 3-17**.

**Figure 3-17** Data access page

**Step 3** Click on the right of Service path file to select a topology file from the local PC, as shown in **Figure 3-18**.

You can click Download Service Topology Example on the right to download the service topology example file. Click to view the data description of the service topology file.
**Figure 3-18 Importing data**

**Step 4** Click “…” on the right of **Power supply relationship file** to select a power supply relationship file from the local PC, as shown in **Figure 3-18**.

You can click **Download Power Supply Topology Example** on the right to download the power supply topology example file. Click 📄 to view the data description of the power supply topology file.

**Step 5** Click **Upload Topology** to upload the service topology and power supply topology example files.

**Step 6** The **Data Interfaces** function is provided for topology files. Topology data can be imported directly using interfaces. Click **Data Interfaces**. The interface invoking information and example packet are displayed, as shown in **Figure 3-19**.

**Figure 3-19 Data interface**

----End

**Alarm File Upload from the Local PC**

Alarm data is imported by local upload.

**Step 1** On the **Data Access** page, select **Local Upload** for **Data Source** in the **Alarm file interface** area, as shown in **Figure 3-17**.
**Figure 3-20** Alarm file upload from the local PC

**Step 2** Click on the right of **Alarm file** to select an alarm file from the local PC. You can click **Download Example File** on the right to download the alarm example file. Use the icon to view the naming requirements and data description of the alarm file.

**Step 3** Click **Upload Alarm** to upload the alarm file.

---End

**Alarm Data Import from the Data Catalog**

In the data catalog–based method, an alarm dataset subscribed to in the dataset service is imported. In this section, the alarm file subscribed to in the dataset service is only the example file. In practice, you need to publish a dataset in the data lake and subscribe to the dataset.

**Step 1** On the **Data Access** page, select **Data Catalog** for **Data Source** in the **Alarm file interface** area, as shown in **Figure 3-21**.

**Figure 3-21** Data import from the data catalog

**Step 2** Click **Data Catalog**.

The **Data Catalog** dialog box is displayed, as shown in **Figure 3-22**.

---End
Step 3  Click **Subscribe to New Data** in the upper right corner of the **Data Catalog** dialog box.

The dataset service is accessed, as shown in **Figure 3-23**. You can access the dataset service only after subscribing to the dataset service.
Step 4  In the navigation pane, click **Cross-Domain Comprehensive Service Analysis**. All datasets published in the current catalog are displayed on the right.

Step 5  Click **Alarm Example Data Table**.

The data details page is displayed, as shown in **Figure 3-24**. You can view the dataset details on the dataset details page.

![Figure 3-24 Dataset details page](image)

**Figure 3-24 Dataset details page**

Step 6  Click **Subscribe** in the upper right corner of the page.

The **Subscribe** dialog box is displayed, as shown in **Figure 3-25**.

![Figure 3-25 Subscription dialog box](image)

**Figure 3-25 Subscription dialog box**

Step 7  Click **Subscribe Now**. In the displayed **Confirm** dialog box, click **OK**.

You can go to the **Personal Center** page to view the alarm file approval progress. The current file is an example file and is automatically approved after the subscription. Otherwise, you need to wait for the approval by the asset administrator of the data lake.
Figure 3-26 Viewing the subscription progress

**Step 8** After the subscription is successful, return to the fault identification and root cause locating service page, as shown in Figure 3-27.

Click **Refresh** in the upper left corner of the dialog box. The subscribed alarm example dataset is displayed. Select the example dataset and click **Import**.

Figure 3-27 Data catalog

API-based Alarm Data Access

**Step 1** To obtain authentication information over the public cloud IAM interface, enter the tenant name, user name, password, and project ID. The user token information is returned.
**Step 2** Invoke the alarm data access interface.

**POST**

```
POST https://iam.cn-north-1.myhuaweicloud.com/v3/auth/tokens
```

<table>
<thead>
<tr>
<th>Params</th>
<th>Authorization</th>
<th>Headers</th>
<th>Body</th>
<th>Pre-request Script</th>
<th>Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td></td>
<td>(1)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Request address:** `https://console.huaweicloud.com/domainconsole/cdflapigw/inference/{serviceId}?region=cn-north-1`. *serviceId* indicates the service ID. Set it as required.
- **x-access-address:** URL for invoking a service. Currently, the value can be `/replayer/v1.0/alarm/cdfl/batch` or `/replayer/v1.0/alarm/cdfl/single`.
- **X-Auth-Token:** token value obtained in Step 1

**Request packet:** JSON message body. For details about the packet example, see "Alarm Access API" in API Reference.

---

***End***
3.9 System Configuration

Basic Configurations

Set the model input parameters and automatic mining period of the fault identification and root cause locating service.

**Step 1**  Click in the Operation column corresponding to the target project.

**Step 2**  Choose System Configurations from the navigation pane.

The Parameter Configuration page is displayed, as shown in Figure 3-28. Table 3-2 describes the parameters.

**Figure 3-28 Parameter configuration**

**Table 3-2 Parameter configuration**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Playback multiple</td>
<td>This parameter is required when you use an alarm file to simulate a real-time alarm flow. It indicates the multiple of sent file alarm data compared with the real-time alarm flow. The value ranges from 1 to 48. Example: The alarm file contains alarm data for three months. It takes three months to infer and generate all TEs by default. If the inference needs to be completed within one week, set the playback multiple to 12. In this case, the duration for traversing the file alarm data is shortened by 1/12.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **TE clearing policy**          | Policy for clearing existing TEs. The options are as follows (multiple options can be selected):  
- **Clear root alarms**: A TE is automatically cleared when its root alarms are cleared.  
- **Clear symptom alarms**: A TE is automatically cleared when its symptom alarms are cleared.  
- **Clear by proportion**: A TE is automatically cleared when a certain proportion of alarms in the TE are cleared. The value ranges from 0 to 1, excluding 0. |
| **Dynamic step prediction parameter** | Parameters required for service alarm aggregation. The options are as follows:  
- **Initial Step Size**: Initial step. If the interval between two alarms is less than the step, the service considers that the two alarms are correlated and aggregates them. The value ranges from 60,000 to 1,800,000 (one minute to half an hour).  
- **Step Length Waiting Multiple**: Waiting time = Step x Value of this parameter. If no new correlated alarm is generated within the waiting time, the alarm aggregation ends. The value ranges from 1 to 5.  
- **Step Learning Rate**: This parameter is used to update the step. The value ranges from 0 to 1, excluding 0. |
| **Automatic mining period**     | The system periodically performs rule mining, displays the mining results, and integrates the rules applicable to service faults into the database.  
If the alarm compression or aggregation rules stored in the database of the fault identification and root cause locating service cannot meet service requirements, you can set **Automatic mining period** to periodically discover new rules and integrate them into the database. |
| **Maximum packaging duration**  | Maximum waiting time for alarm set aggregation. If the waiting time exceeds the threshold, the alarm set aggregation is forcibly stopped and root cause identification starts. |

**Step 3** Click **Save** in the upper right corner of the page for the parameter configurations to take effect.

The system starts online real-time inference based on imported data and configured parameters and displays generated TE information on the **Fault dashboard** page in real time.

----End
Advanced Parameter Settings

Set Data preprocessing configuration Sample Files, Toggling rule configuration file, and Diagnosis rule configuration file.

**Step 1** Expand Advanced Parameter Settings on the Parameter Configuration page, as shown in Figure 3-29.

You can download the example files in the upper right corner to view the file format details.

**Figure 3-29 Advanced parameter settings**

Step 2 Set Data preprocessing configuration Sample Files, Toggling rule configuration file, and Diagnosis rule configuration file, and click Upload File to upload the files respectively.

----End

Label Management

The fault identification and root cause locating service compresses alarms based on the model parameters configured by users. The generated TE information is displayed on the Monitoring Overview page.

Label addition is supported on the File Configuration page. Each label is a user-defined attribute for TE filtering. For example, if you set a label to contain major alarms that you concern and select this label for TE filtering on the Monitoring Overview page, the page displays only TEs containing the alarms in the label. In this way, invalid trouble tickets are reduced and invalid analysis by monitoring personnel is reduced. The user-defined content in the label may also be time periods, NE names, NE levels (you can set the NE level), and other data.

**Step 1** Expand Advanced Parameter Settings on the Parameter Configuration page.

**Step 2** Click Add Label in the upper right corner of the Label Management area.

The Add Label dialog box is displayed, as shown in Figure 3-30.

The parameters are described as follows:

- **Label Name:** Set this parameter based on the filtering scenario. For example, the Major alarm label is used to filter out useless alarms.
Label Content: Label content used for TE filtering. You can click Download Content Template to download the example file and view the JSON data format.

Figure 3-30 Adding a label

Add Label

* Label Na.. Major alarm

* Label Co... function filterbyAllAlarmTitle(te){var alarmTitles = {};alarmTitles['OML'] = 1;alarmTitles['GSM'] = 1;alarmTitles['GSM'] = 1;alarmTitles['GSM'] = 1;alarmTitles['OML Fault'] = 1;alarmTitles['CSL Fault'] = 1;alarmTitles['GSM Cell out of Service'] = 1;alarmTitles['GSM Local Cell Unusable'] = 1;alarmTitles['GSM Local Cell Blocked'] =

Download Content Template

Cancel OK

Step 3  Click OK.

----End

3.10 Change History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-03-30</td>
<td>Added section &quot;Subscribing to the Fault Identification and Root Cause Locating Service&quot;. Changed the service UI, optimized service functions, and updated all documents.</td>
</tr>
<tr>
<td>2019-12-30</td>
<td>Released this document officially for the first time.</td>
</tr>
</tbody>
</table>
4 API Reference

4.1 Before You Start

This document provides guidance for NAIE service development and test personnel to manage service resources using APIs of the NAIE fault identification and root cause locating service.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand the API components and interface list.</td>
<td>Before You Start</td>
</tr>
<tr>
<td>Prepare for using interfaces.</td>
<td>Overview</td>
</tr>
<tr>
<td>Understand the representational state transfer (REST) message body and usage.</td>
<td>Environment Preparation</td>
</tr>
<tr>
<td>Understand interface usage.</td>
<td>Alarm Access</td>
</tr>
</tbody>
</table>

4.2 Overview

Table 4-2 describes the APIs provided by the fault identification and root cause locating service.

<table>
<thead>
<tr>
<th>Type</th>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root cause locating and analysis</td>
<td>API for accessing the alarm data service</td>
<td>This API is used to access third-party raw alarm data APIs.</td>
</tr>
</tbody>
</table>
4.3 Environment Preparation

4.3.1 Obtaining Request Authentication

APIs are invoked in token authentication mode. Common requests are authenticated using tokens.

Token Authentication

If you use a token for authentication, you must obtain the user’s token and add X-Auth-Token to the request message header of the service API when invoking an API.

**Step 1** Send `POST https://IAM endpoint/v3/auth/tokens`. Obtain the IAM endpoint and region name in the message body.

If the service area name is **All**, select the IAM cn-north-1 endpoint.

The following is a request example.

```json
{
  "auth": {
    "identity": {
      "methods": [
        "password"
      ],
      "password": {
        "user": {
          "name": "username",
          "password": "password",
          "domain": {
            "name": "domainname"
          }
        }
      }
    },
    "scope": {
      "project": {
        "name": "cn-north-1aaa" //Assume that the area name is cn-north-1aaa.
      }
    }
  }
}
```

**Step 2** Obtain the token. For details, see section "Obtaining User Token" in Identity and Access Management API Reference. The value of **X-Subject-Token** in the response header is the token value.

**Step 3** Invoke a service API, add X-Auth-Token to the message header, and set the value of X-Auth-Token to the token obtained in step 2.

----End
4.3.2 Obtaining the Project ID and Tenant ID

A project ID (project_id or tenant_id because both of them have the same meaning in this document) is required for some URLs when invoking an API. Therefore, you need to obtain a project ID on the console before invoking an API. To obtain the project ID, perform the following steps:

**Step 1** Register and log in to the management console.

**Step 2** Click the username and select **Basic Information** from the drop-down list.

**Step 3** On the **Basic Information** page, click **Manage**.

**Step 4** On the **My Credential** page, view project IDs in the project list.

**Figure 4-1** Viewing the project ID

---End

4.4 Alarm Access

4.4.1 REST API Overview

**Function**

This API sends alarm data to the trouble ticket system.

**URI**

The URI format is as follows:
/replayer/v1.0/alarm/cdfl/batch

**Table 4-3** describes the parameters.
Table 4-3 Parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory or Not</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alarms:</td>
<td>Yes</td>
<td>List&lt;RawAlarm&gt;</td>
<td>Public cloud alarm dataset</td>
</tr>
</tbody>
</table>

Request

The following is a request example:

```plaintext
POST https://xxx/replayer/v1.0/alarm/cdfl/batch
{
  alarms:
  [  
    {
      "serialId":"103707929.0",
      "normId":"bts:Battery Not In Position",
      "title":"Battery Not In Position",
      "alarmSource":"094660_PDKOPIUTARA_MBTS",
      "severity":"0",
      "raiseTime":"1566445244308",
      "reportTime":"1566445244308",
      "clearFlag":"true",
      "clearTime":"1566445244308",
      "neId":"bts_095772",
      "neType":"bts",
      "neSubType":"NodeB",
      "neLocation":"eNodeB =NJ_GL_HW_Yincheng Square1_FL_M, Operator index=0, Location=Nanjing, AlarmCounty=Gulou District, FirstOccurrence=1564823820"
    }
  ]
}
```

Table 4-4 describes the parameters.

Table 4-4 Parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory or Not</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alarms:</td>
<td>Yes</td>
<td>List&lt;RawAlarm&gt;</td>
<td>Public cloud alarm dataset</td>
</tr>
</tbody>
</table>

Table 4-5 describes the fields.
### Table 4-5 Field description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Type</th>
<th>Mandatory or Not</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>serialId</td>
<td>Unique alarm serial ID</td>
<td>String</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>normId</td>
<td>Alarm normalization flag</td>
<td>String</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>title</td>
<td>Alarm name</td>
<td>String</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>alarmSource</td>
<td>Alarm source, which is used for information display</td>
<td>String</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>severity</td>
<td>Alarm severity</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>raiseTime</td>
<td>Alarm generation time</td>
<td>Long</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>reportTime</td>
<td>Alarm reporting time</td>
<td>Long</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>clearFlag</td>
<td>Alarm clearance flag</td>
<td>Boolean</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>clearTime</td>
<td>Alarm clearance time</td>
<td>Long</td>
<td>This parameter is mandatory when clearFlag is set to true.</td>
<td>-</td>
</tr>
<tr>
<td>neId</td>
<td>Logical NE ID, which must be set to the value of NE_NAME for the topology interface.</td>
<td>String</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>neType</td>
<td>NE type</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>neSubType</td>
<td>NE subtype</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>neLocation</td>
<td>Location information</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
</tbody>
</table>

### Response

- Success response example: {"code":"0"}
- Failed response example: {"code":"1"}

### Return Value

Table 4-6 describes the return values.
### Table 4-6 Return Value

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory or Not</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>code</td>
<td>Yes</td>
<td>int</td>
<td>Whether an exception occurs. The value 1 indicates yes. The value 0 indicates no.</td>
</tr>
<tr>
<td>desc</td>
<td>No</td>
<td>String</td>
<td>Exception description</td>
</tr>
</tbody>
</table>

### 4.4.2 Java Code Example

The Spring Boot framework is used to add the corresponding POM dependency.

```xml
<dependency>
  <groupId>com.fasterxml.jackson.core</groupId>
  <artifactId>jackson-databind</artifactId>
  <version>${jackson.version}</version>
</dependency>

<dependency>
  <groupId>org.apache.httpcomponents</groupId>
  <artifactId>httpclient</artifactId>
  <version>${httpclient.version}</version>
</dependency>

<dependency>
  <groupId>org.apache.httpcomponents</groupId>
  <artifactId>httpasyncclient</artifactId>
  <version>${httpasyncclient.version}</version>
</dependency>

<dependency>
  <groupId>org.apache.httpcomponents</groupId>
  <artifactId>httpmime</artifactId>
  <version>4.5.6</version>
</dependency>

<dependency>
  <groupId>org.springframework</groupId>
  <artifactId>spring-orm</artifactId>
  <version>${spring.version}</version>
</dependency>

<dependency>
  <groupId>org.springframework</groupId>
  <artifactId>spring-context</artifactId>
  <version>${spring.version}</version>
</dependency>

<dependency>
  <groupId>org.springframework</groupId>
  <artifactId>spring-aop</artifactId>
  <version>${spring.version}</version>
</dependency>

<dependency>
  <groupId>org.springframework</groupId>
  <artifactId>spring-tx</artifactId>
  <version>${spring.version}</version>
</dependency>

<dependency>
  <groupId>org.springframework</groupId>
  <artifactId>spring-web</artifactId>
  <version>${spring.version}</version>
</dependency>
```
application.properties configuration items are as follows:

iamUrl=https://IP: Port/v3/auth/tokens
password=xxxxxxxxx
domainName=xxxxxxxxx
name=xxxxxxxxx
projectId=e078xxxxxxxxx
receiverUrl=https://IP: Port/cdflapigw/inference/v1.0/xxxxxxxxx

The Java core code is as follows:

package com.huawei.softcom.ai.smartorder.replayer.file2rest;

import com.fasterxml.jackson.databind.ObjectMapper;
import org.apache.http.config.Registry;
import org.apache.http.config.RegistryBuilder;
import org.apache.http.conn.ssl.SSLConnectionSocketFactory;
import org.apache.http.impl.nio.conn.PoolingNHttpClientConnectionManager;
import org.apache.http.impl.nio.reactor.IOReactorConfig;
import org.apache.http.nio.conn.ssl.SSLIOSessionStrategy;
import org.apache.http.nio.reactor.IOReactorException;
import org.apache.http.ssl.SSLContextBuilder;
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import org.springframework.beans.factory.annotation.Autowired;
import org.springframework.beans.factory.annotation.Value;
import org.springframework.http.*;
import org.springframework.stereotype.Component;
import org.springframework.web.client.RestTemplate;
import javax.net.ssl.SSLContext;
import java.io.IOException;
import java.security.KeyManagementException;
import java.security.KeyStoreException;
import java.security.NoSuchAlgorithmException;
import java.text.MessageFormat;
import java.util.*;
import java.util.concurrent.ExecutorService;
import java.util.concurrent.Executors;
import java.util.concurrent.LinkedBlockingQueue;

@Component("restAlarmSender ")
public class RestAlarmSender {
    private static final Logger logger = LoggerFactory.getLogger(RestAlarmSender.class);

    @Value("${receiverUrl:null}")
    private String receiverUrl;

    @Value("${batchSendSize:null}")
    private int batchSendSize;

    private String token;

    @Value("${iamUrl}")
    private String iamUrl;

    @Value("${password}")
    private String password;

    @Value("${domainName}")
    private String domainName;

    @Value("${name}")
    private String name;

    @Value("${projectId}")
    private String projectId;

    @Autowired
    private RestTemplate restTemplate;

    private LinkedBlockingQueue<RawAlarm> alarmsToSend = new LinkedBlockingQueue<>();

    CloseableHttpAsyncClient httpclient = initHttpAsyncClient();

    private static HttpClientContext context = HttpClientContext.create();

    ObjectMapper mapper = new ObjectMapper();

    public RestAlarmSender() {
        ExecutorService executorService = Executors.newSingleThreadExecutor();
        executorService.execute(this::sendAlarmsByBatch);
    }

    private void getToken(){
        String url = iamUrl;
        HttpHeaders headers = new HttpHeaders();
        headers.setContentType(MediaType.APPLICATION_JSON);
        String json = "{"\"auth\":{\"identity\":{\"password\":{\"user\":{\"password":\"" + password + ",
                                      \"domain\":{\"name\":"" + domainName + ",\"scope\":{\"project\":{\"id\":"" + projectId + ",\"id\"}"}}}}},
                      \"methods\":{\"\"}}};
        HttpEntity<String> httpEntity = new HttpEntity<>(json, headers);
        try {
            ResponseEntity<String> response = restTemplate.exchange(url, HttpMethod.POST, httpEntity,
                                                                      String.class);
            logger.info(response.getBody());
            token = response.getHeaders().get("X-Subject-Token").get(0);
        } catch (Exception e) {
            logger.error("config URL error ." + e.getMessage());
        }
    }

    public void sendRawAlarm(RawAlarm alarm) {
        // add to send queue
        alarmsToSend.add(alarm);
    }
}
private void sendAlarmsByBatch() {
    while (!Thread.currentThread().isInterrupted()) {
        try {
            // blocking if empty
            RawAlarm first = alarmsToSend.take();
            List<RawAlarm> alarmList = new ArrayList<>();
            alarmList.add(first);
            while (!alarmsToSend.isEmpty() && alarmList.size() < batchSendSize) {
                alarmList.add(alarmsToSend.take());
            }
            postAlarms(alarmList);
        } catch (InterruptedException ex) {
            logger.error(String.format(Locale.ENGLISH, "Sending alarms interrupted %s", ex.getMessage()));
            Thread.currentThread().interrupt();
        }
    }
}

private void postAlarms(List<RawAlarm> alarms) {
    HttpPost httpPost = new HttpPost(receiverUrl);
    if (null == token) {
        getToken();
    }
    httpPost.setHeader("Content-Type", "application/json");
    httpPost.setHeader("x-access-address", "/replayer/v1.0/alarm/cdfl/batch");
    httpPost.setHeader("X-Auth-Token", token);
    try {
        String alarmStr = mapper.writeValueAsString(alarms);
        StringEntity entity = new StringEntity(alarmStr, "UTF-8");
        httpclient.start();
        httpclient.execute(httpPost, context, new FutureCallback<HttpResponse>() {
            @Override
            public void completed(HttpResponse result) {
                logger.info(MessageFormat.format("Sending alarm successfully, url:{0}, number of " + "alarms: {1}", receiverUrl, alarms.size()));
            }
            @Override
            public void failed(Exception e) {
                logger.error(MessageFormat.format("Sending alarm unsuccessfully, url:{0}, message: {1}", receiverUrl, e.getMessage()));
            }
            @Override
            public void cancelled() {
                // todo
            }
        });
    } catch (IOException e1) {
        logger.error(MessageFormat.format("Sending alarm unsuccessfully, url:{0}, IOException", receiverUrl));
    } catch (Exception e) {
        logger.error(MessageFormat.format("Sending alarm unsuccessfully, url:{0}, message: {1}", receiverUrl, e.getMessage()));
    }
}
### 4.4.3 Kafka Access

#### Function

Alarm data access supports real-time Kafka alarm data access, identifies root causes, and exports fault information.

#### Kafka Configurations

*Table 4-7* shows the Kafka configurations.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory or Not</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kafka.server</td>
<td>Yes</td>
<td>String</td>
<td>Kafka service address</td>
</tr>
<tr>
<td>kafka.alarm.topic</td>
<td>Yes</td>
<td>String</td>
<td>Kafka message topic</td>
</tr>
<tr>
<td>kafka.alarm.group.id</td>
<td>Yes</td>
<td>String</td>
<td>Kafka group</td>
</tr>
</tbody>
</table>

#### Data Format of Each Record

*Table 4-8* shows the format of each data record.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Type</th>
<th>Mandatory or Not</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>serialId</td>
<td>Unique alarm serial ID</td>
<td>String</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>normId</td>
<td>Alarm normalization flag</td>
<td>String</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>title</td>
<td>Alarm name</td>
<td>String</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>alarmSource</td>
<td>Alarm source, which is used for information display</td>
<td>String</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>severity</td>
<td>Alarm severity</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>raiseTime</td>
<td>Alarm generation time</td>
<td>Long</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>reportTime</td>
<td>Alarm reporting time</td>
<td>Long</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>clearFlag</td>
<td>Alarm clearance flag</td>
<td>Boolean</td>
<td>Yes</td>
<td>-</td>
</tr>
</tbody>
</table>
4.5 Fault Information Export

4.5.1 REST API Overview

Function

After the alarm data is identified, the corresponding fault information is generated. Fault information needs to be delivered to the downstream for processing. Each receiver needs to define a fault output interface.

URI

The URI format is as follows:

http://{IP}:{PORT}/te/receiver/normal

Table 4-9 describes the parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory or Not</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>Yes</td>
<td>String</td>
<td>IP address of the fault receiving service</td>
</tr>
<tr>
<td>PORT</td>
<td>Y</td>
<td>String</td>
<td>Port for the fault receiving service</td>
</tr>
</tbody>
</table>
### Table 4-10 Input parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory or Not</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>troubleEventVO</td>
<td>Yes</td>
<td>String</td>
<td>Fault model output</td>
</tr>
</tbody>
</table>

### Table 4-11 Field description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Type</th>
<th>Mandatory or Not</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>serialId</td>
<td>TE serial number, which is unique.</td>
<td>String</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>raiseTime</td>
<td>TE generation time</td>
<td>Long</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>clearFlag</td>
<td>TE clearance flag</td>
<td>Boolean</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>neList</td>
<td>TE NE list</td>
<td>List&lt;NetworkElementVO&gt;</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>title</td>
<td>TE name</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>clearTime</td>
<td>TE clearance time</td>
<td>Long</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>rcResult</td>
<td>Diagnosis information</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>measures</td>
<td>Handling suggestions</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>troubleCauseFeedback</td>
<td>Feedback</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>primaryTe</td>
<td>Original TE serial number when the current TE is an associated TE</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>teGroupId</td>
<td>ID of the group associated with a TE.</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>directConnection</td>
<td>Topology information</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>filterRuleId</td>
<td>Group information</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>teUrl</td>
<td>RUL that points to TE details</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
</tbody>
</table>
### Table 4-12 Description of fields in the NetworkElementVO model

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Type</th>
<th>Mandatory or Not</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>neId</td>
<td>Unique ID of an NE in the topology information</td>
<td>String</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>name</td>
<td>NE name</td>
<td>String</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>neType</td>
<td>NE type, for example, [pow, trans, bts]</td>
<td>String</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>rootFlag</td>
<td>Whether it is a root NE.</td>
<td>Boolean</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>alarmList</td>
<td>Alarm list</td>
<td>List&lt;AlarmVO&gt;</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>neSubType</td>
<td>NE subtype</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>physicalNeId</td>
<td>Physical site ID</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>neStatus</td>
<td>Site status (0: normal; 1: engineering)</td>
<td>Integer</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>neVendor</td>
<td>NE vendor</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>neVendorCode</td>
<td>NE vendor code</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>neLocation</td>
<td>NE location information</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>neLocationCode</td>
<td>NE location code</td>
<td>String</td>
<td>No</td>
<td>-</td>
</tr>
</tbody>
</table>

### Table 4-13 Description of fields in the AlarmVO model

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Type</th>
<th>Mandatory or Not</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>serialId</td>
<td>Alarm serial number generated by the device</td>
<td>String</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>title</td>
<td>Alarm type name</td>
<td>String</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>normId</td>
<td>Alarm type normalization flag</td>
<td>String</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>clearFlag</td>
<td>Alarm clearance flag</td>
<td>Boolean</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>raiseTime</td>
<td>Alarm occurrence time</td>
<td>Long</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Type</td>
<td>Mandatory or Not</td>
<td>Example</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>rootFlag</td>
<td>Whether the alarm is a root alarm on the NE.</td>
<td>Boolean</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>featureFlag</td>
<td>Whether the alarm is a symptom alarm on the NE.</td>
<td>Boolean</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>emsSerialId</td>
<td>Alarm sequence number generated by the integrated EMS</td>
<td>String</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>clearTime</td>
<td>Alarm clearance time</td>
<td>Long</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>alarmId</td>
<td>Original alarm type ID</td>
<td>String</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>severity</td>
<td>Alarm severity</td>
<td>String</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>reportTime</td>
<td>Time when an alarm is reported to the level-1 NMS</td>
<td>Long</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>alertKey</td>
<td>Location information</td>
<td>String</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

### 4.5.2 REST API Example

The following is an example of the REST API:

```json
{
    "clearFlag": false,
    "clearTime": 0,
    "directConnection": "["fromNeId":"Taicang Xinhuxi Gaojing Base Station Equipment Room","toNeId":"HA3460-Suzhou New Lake West Gaojing /P","topoType":"POW_DIRECT","topoLevel":"L1"],
["fromNeId":"HA3460-Suzhou New Lake West Gaojing /P","toNeId":"SZ_TC_HW_New Lake West Gaojing Remote New Chuanqun North Base Station Equipment Room_FL_BBU","topoType":"UP2DOWN_DIRECT","topoLevel":"L1"],
["fromNeId":"HA3460-Suzhou New Lake West Gaojing /P","toNeId":"SZ_TC_HW_New Lake West Gaojing Remote Telecom New Lake Bali Bridge base station equipment room_FL_BBU","topoType":"POW_DIRECT","topoLevel":"L1"],
"filterRuleId": "001,003",
"neList": [
    {
        "alarmList": [
            {
                "alarmId": "0",
            }
        ]
    }
}
```
"alterKey": "HA3460-Suzhou Xinhuxi Gaojing (070629)/P/1-0.2-AND1EM8F 0/2-3, Location=Suzhou, AlarmCounty=Taicang, FirstOccurrence=1566426484",
"arriveTime": 1575873932360,
"clearFlag": false,
"clearTime": 0,
"emsSerialId": "2287680093_276720302_1850564167_531778074",
"feature": true,
"normId": "trans: The physical port is Down.",
"raiseTime": 1566426484000,
"reportTime": 1575873773925,
"root": true,
"serialId": "380024994",
"severity": "Major",
"title": "The physical interface is Down."
},
{
"alarmId": "0",
"alterKey": "HA3460-Suzhou Xinhuxi Gaojing (070629)/P/1-0.2-AND1EM8F 0/2-2, Location=Suzhou, AlarmCounty=Taicang, FirstOccurrence=1566426484",
"arriveTime": 1575873932360,
"clearFlag": false,
"clearTime": 0,
"emsSerialId": "674294076_3046322036_1921508736_3547714930",
"feature": true,
"normId": "trans: The physical port is Down.",
"raiseTime": 1566426484000,
"reportTime": 1575873773925,
"root": true,
"serialId": "380024974",
"severity": "Major",
"title": "The physical interface is Down."
},
{
"alarmId": "0",
"alterKey": "HA3460-Suzhou Xinhuxi Gaojing (070629)/P/1-0.2-AND1EM8F 0/2-1, Location=Suzhou, AlarmCounty=Taicang, FirstOccurrence=1566426484",
"arriveTime": 1575873932360,
"clearFlag": false,
"clearTime": 0,
"emsSerialId": "191293479_3645668405_2991936724_2928622693",
"feature": true,
"normId": "trans: The physical port is Down.",
"raiseTime": 1566426484000,
"reportTime": 1575873773925,
"root": true,
"serialId": "380024967",
"severity": "Major",
"title": "The physical interface is Down."
},
{
"alarmId": "0",
"alterKey": "HA3460-Suzhou Xinhuxi Gaojing (070629)/P/1-0.1-AND1EM8T 0/1-1, Location=NAIE Fault Identification & Root Cause Localization 4 API Reference

49

Issue 01 (2020-06-30) Copyright © Huawei Technologies Co., Ltd.

"alarmId": "0",
"alterKey": "HA3460-Suzhou Xinhuxi Gaojing (070629)/P/1-0.1-AND1EM8T 0/1-1, Location=Suzhou, AlarmCounty=Taicang, FirstOccurrence=1566426484",
"arriveTime": 1575873932360,
"clearFlag": false,
"clearTime": 0,
"emsSerialId": "435013940_3375083456_1545460862_3612364305",
"feature": true,
"normId": "trans: The physical port is Down.",
"raiseTime": 1566426484000,
"reportTime": 1575873773925,
"root": true,
"serialId": "380024950",
"severity": "Major",
"title": "The physical interface is Down."
4.6 Change History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-03-30</td>
<td>Added the following sections about alarm access APIs:</td>
</tr>
<tr>
<td></td>
<td>● Java Code Example</td>
</tr>
<tr>
<td></td>
<td>● Kafka Access</td>
</tr>
<tr>
<td></td>
<td>Added the fault information export API and section &quot;Fault Information Export.&quot;</td>
</tr>
<tr>
<td>Date</td>
<td>Change Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>2019-12-30</td>
<td>This is the first official release.</td>
</tr>
</tbody>
</table>
5 FAQs

5.1 What Data Do Users Need to Provide

This service aggregates, identifies, and locates faults based on real-time alarm data generated on the live network. This service depends on the following data on the corresponding network:

- Real-time alarm flow: Alarm data reported by NEs and NMSs on the live network (including wireless access, transmission, and power and environment domains) is sent to the service in real time through RESTful APIs.
- Topology data: topology data of the live network, including NE service connections, power supply relationships between the power and environment monitoring system and base stations, and power supply relationships between the power and environment monitoring system and transmission NEs. Topology data can be uploaded locally on the system configuration page. If the customer network topology changes frequently, you are advised to periodically update the topology path file.

5.2 What Is the Result of Fault Identification and Root Cause Locating

The fault identification and root cause locating result of this service includes the following aspects:

- Alarms generated in a certain period are aggregated and considered the same fault. Users do not need to handle scattered alarms.
- This service identifies the root NEs, root alarms, and symptom alarms for aggregated alarms. You only need to handle the root alarm on the root NE to rectify the fault.
- This service also provides many functions for identified TEs, such as clearance check, subsequent TE association, and correlated TE association, which facilitates combined processing for the same type of faults and avoids repeated processing.

You can choose Fault Monitoring > Board to experience the preceding function.
5.3 Change History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-03-30</td>
<td>This issue does not include any changes.</td>
</tr>
<tr>
<td>2019-04-30</td>
<td>This is the first official release.</td>
</tr>
</tbody>
</table>
B 

**BTS**

A Base Transceiver Station (BTS) terminates the radio interface. It allows transmission of traffic and signaling across the air interface. The BTS includes the baseband processing, radio equipment, and the antenna.

G 

**TE Association**

The system recommends TEs that have similar topologies and occur around the same time to users.

I 

**IP RAN**

An IP radio access network (RAN) is a network that uses IP technology to achieve data backhaul on a radio access network.

J 

**Associated TE**

If an original TE that occurs closest to the time when the current TE occurs is not deleted from the historical TEs of the root NE, the current TE is associated to this original TE.

P 

**POW**

Value of the NeType field in the alarm data file. This value indicates power and environment devices that power wireless base stations and transmission network elements on the radio access network.
Value of the NeType field in the alarm data file. This value indicates the devices which data passes through from a base station to the core network.

**T**

**TRANS**

Value of the NeType field in the alarm data file. This value indicates transmission devices on the radio access network.

**Topology**

A topology displays the logical layout of the components of a computer system or network and their interconnections.

**Y**

**Original TE**

Original TE and secondary TE occurring on the same NE in different time periods are considered the same fault. After the original TE fault is rectified, the secondary TE fault is automatically rectified.