ROMA Connect

Troubleshooting Guide

Issue	01
Date	2025-01-20

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks 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 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.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Common Data Integration Tasks

1.1 Garbled Characters Are Displayed When Data Is Written to MRS Hive at the Destination

Cause Analysis

When a task is created, the storage type of the destination is inconsistent with that specified during table creation.

For example, the storage type is set to text file during table creation, whereas the storage type of the destination is set to RCFile during task creation.

Solution

Change the storage type of the destination to the same as that specified during table creation.

1.2 All Data Is Written to the First Field of MRS Hive

Cause Analysis

Column separators are used during table creation.

Solution

Run the following command in the database to set the separator:

alter table *Table name* set serdeproperties('field.delim'='*Separator*')

1.3 An Error Message Is Displayed at the Destination Indicating Task Execution Times Out

Cause Analysis

The task name contains more than 64 characters, and the first 64 characters of multiple scheduled task names are the same.

Solution

Reduce the task name length to fewer than 64 characters or change the task names with the same first 64 characters to different values.

1.4 Error Message "could only be written to 0 of the 1 minReplication nodes. There are 2 datanode(s) running and 2 node(s) are excluded in this operation" Is Reported at the Destination During Data Integration from MySQL to MRS Hive

Cause Analysis

All HDFS cluster nodes are bound to EIPs. When an MRS Hive data source is created, EIPs are used as all IP addresses in the uploaded configuration file, and IP addresses and hostnames are configured in Hosts. However, when the file is uploaded, the IP address of the node returned by the HDFS master node is an intranet IP address. As a result, the connection fails and therefore the FDI task fails to be executed.

Solution

Add the **dfs.client.use.datanode.hostname** configuration item to the **hdfs-site.xml** file uploaded during MRS Hive data source creation and set its value to **true**. Then, upload the modified configuration file and create the MRS Hive data source again.

1.5 Error Message "Illegal mix of collations for operation 'UNION'" Is Displayed at the Source Database During MySQL-to-MySQL Data Integration

Cause Analysis

According to the data source view at the source, union is used in the view definition statement. However, the encoding of the fields on both sides of union is inconsistent.

Solution

Use CONVERT to unify the encoding for fields, for example, CONVERT (ID USING utf8) AS ID.

1.6 Data May Be Lost When Incremental Data Collection Is Performed from the Source MySQL on an Hourly Basis

Cause Analysis

The source database uses **createtime** to record the time when data is inserted and uses **updatetime** to record the time when data is updated. During task creation, **Timestamp** is set to **updatetime**. However, the value of **updatetime** is earlier than that of **createtime** in the source database. When the task is executed, the time specified **updatetime** is not within the incremental collection period. As a result, some data cannot be collected.

Solution

Change the value of **updatetime** in the source database or use **createtime** as the timestamp field during task creation.

1.7 Error Message "401 unauthorized" Is Displayed at the Source During API-to-MySQL Data Integration

Cause Analysis

The possible causes are as follows:

- **Security Authentication** is set to **None** during API creation, whereas **Authentication Mode** is set to **AppKey Auth** during data source creation.
- **Security Authentication** is set to **App** during API creation, whereas **Authentication Mode** is set to **AppKey Auth** and **App Authentication Type** is set to **Secret** during data source creation.

Solution

You can perform the following operations to tore solve this issue:

- Select **None** for **Authentication Mode** when creating a data source.
- Change **App Authentication Type** to **Default**.

1.8 Error Message "cannot find record mapping field" Is Displayed at the Destination During Kafka-to-MySQL Data Integration

Cause Analysis

According to the mapping configuration, the length of the field type at the source exceeds the length limit of the field type at the destination or a field configured in mapping information does not exist in the source data.

Solution

Check whether the field type matches the field in the mapping configuration, whether the field length exceeds the limit, and whether the field exists. If not, modify the field configuration.

1.9 Error Message "connect timeout" Is Displayed at the Source During Scheduled API-to-MySQL Data Integration

Cause Analysis

There are six nodes on the data plane. Two of them cannot connect to the IP address of the API data source.

Solution

This is a network problem. Contact VPC custom service to locate the fault.

1.10 FDI Fails to Obtain Data During Real-Time Kafka-to-MySQL Data Integration Although Data Exists in MQS Topics

Cause Analysis

The address configured for the data source is not the MQS address of the instance. Therefore, the FDI task cannot collect data although messages exist in MQS of the instance.

Solution

Check the task configuration and data source configuration and change the data source configuration to the correct MQS address.

1.11 Value of the Source Field of the tinyint(1) Type Is Changed from 2 to 1 at the Destination During Scheduled MySQL-to-MySQL Data Integration

Cause Analysis

The MySQL driver automatically identifies tinyint(1) as the bit type. Therefore, the field value is changed to 1 at the destination.

Solution

Change **Connection Mode** to **Professional** for the MySQL data source and add **tinyInt1isBit=false** to the end of the character string, for example, **jdbc:mysql://ip:port/database?tinyInt1isBit=false**.

1.12 "The task executes failed.Writer data to kafka failed" Is Reported When the Kafka Destination Is Used over the Public Network

Possible Cause

When the destination data source is Kafka using the public network, the scheduled task reports the "The task executes failed.Writer data to kafka failed" error due to network exceptions.

Solution

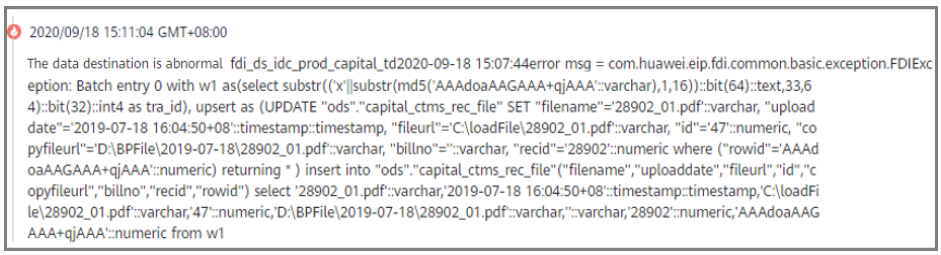
Wait until the next task scheduling, or stop the task and then restart it.

2 Composite Data Integration Tasks

2.1 Data Fails to Be Written Because the RowId Field Type Is Incorrectly Configured in the Destination Table

Cause Analysis

When the RowId mode is used to collect Oracle table data, an error is reported because the table field type is incorrectly configured.



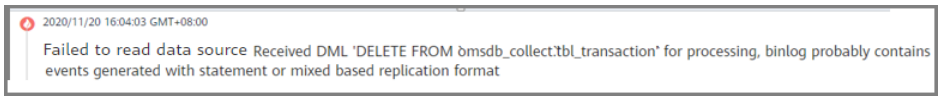
Solution

Modify the table field type. The row ID is 18 characters of letters and digits. The destination field must be of the character type.

2.2 Error Message "binlog probably contains events generated with statement or mixed based replication forma" Is Displayed When the Binlog of the MySQL Database Is Read

Symptom

A composite task fails to be executed, and the error message "binlog probably contains events generated with statement or mixed based replication forma" is displayed.



Solution

This problem is caused by a bug in the current Debezium version. You must upgrade the MySQL database.

For a composite task, delete the configuration of the table first. After the task is started, the data is skipped. After the task is successfully executed, configure the table again and collect data again.

2.3 Data Still Fails to Be Written After an FDI Task Failure Is Rectified

Cause Analysis

When the writer writes data to a database, it consumes data from a topic in Kafka. After the data is successfully saved to the database, the writer submits the consumption offset to Kafka. If an exception occurs when data is written, the consumption offset is not submitted. After the fault is rectified, restart the task to process the data that fails to be saved to the database again. Therefore, if the data does not meet the requirements of the destination after the task configuration is modified, the task still fails to be executed.

Solution

You can use any of the following methods to rectify the fault:

- As data in a Kafka topic will age six hours later, wait until the dirty data is cleared and then start the task.

- Delete the original task and create a task. In this way, topics in Kafka will be deleted and dirty data will be cleared.
- For a composite task, delete the table and start the task. Wait until the Writer consumes the data in this table and then add the table to collect data again.

2.4 Camel Fails to Access the Database Because Table Names Contain Garbled Characters

Cause Analysis

The parameters used for accessing the database are incorrect. As a result, the composite task fails to be started and finally the task is terminated.

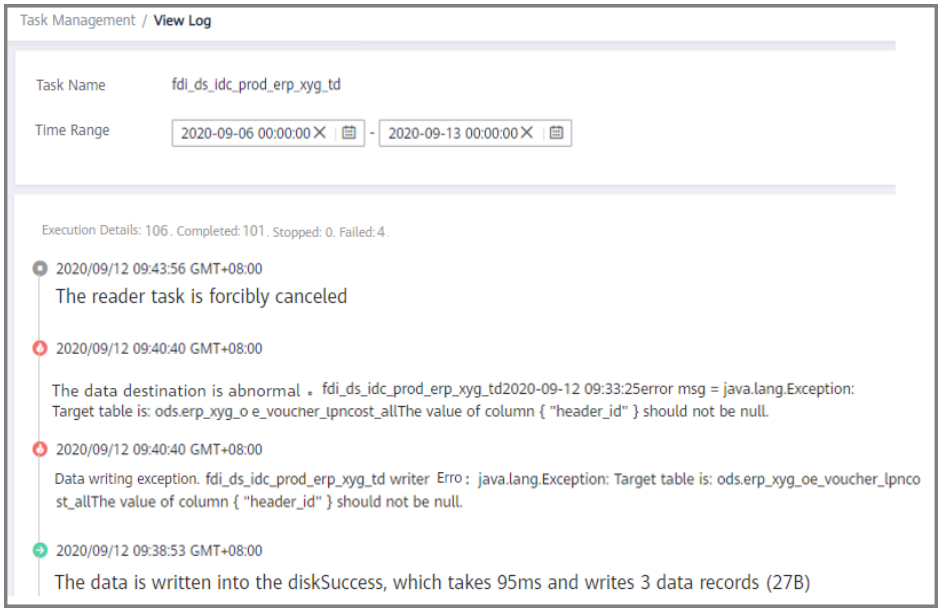
Solution

Check whether garbled characters exist in table names in the database. If yes, contact the database administrator, delete the tables whose names contain garbled characters, and restart the task.

2.5 Inserted Data Violates the Non-null Constraint

Cause Analysis

The task fails to be executed. The following information is displayed in the log:



Solution

Perform the following operations to resolve the issue:

- This field in the source table is set to null, but is set to a non-null value in the destination table. To resolve this issue, modify the field attributes in the source and destination tables to ensure consistency.
- A redundant table mapping is configured during task creation. Therefore, data in the source table with a similar name is collected to the destination table. As a result, empty data is written to the field. To resolve this issue, correctly configure the table mapping.
- In the redo logs generated by the Oracle database, the **WHERE** condition is missing in the field of the UPDATE statement. As a result, the value of this field is missing. To resolve this issue, add the **WHERE** condition to the field of the UPDATE statement.

2.6 FDI Task Fails to Be Executed Because DWS Changes to the Read-only State

Cause Analysis

When the DWS disk space reaches the threshold, for example, 80%, or data skew occurs in some tables with a large amount of data, the DWS cluster becomes read-only. On the FDI side, all tasks for accessing DWS stopped abnormally at a certain time point.

Solution

Handle the read-only issue of DWS. After the database service is restored, directly start the FDI task if the task is stopped for less than 6 hours. If the task is stopped for more than 6 hours, data in the channel has expired. In this case, reset the synchronization progress and start the task again. If there are tables whose data has not been fully collected before a full data task is stopped, data of these tables will be collected all over again.

In addition, analyze the causes of the read-only state for database development optimization, or expand the disk space to prevent the problem from recurring.

2.7 Data Write to DWS Becomes Slower

Cause Analysis

Data write in seconds is normal. If it takes more than 5 seconds to write thousands of data records, the performance deteriorates.

Solution

If a DWS table is frequently accessed, the write performance deteriorates. In this case, optimize DWS, for example, periodically use the **analyze** plan table and **VACUUM FULL**.

3 Data Sources

3.1 Data Source Connection Failed

1. Check whether the data source configuration is correct. For example, check whether the database name and password are correct.
2. Check whether the data source IP address and FDI are in the same VPC. If no, create a VPC peering connection first.

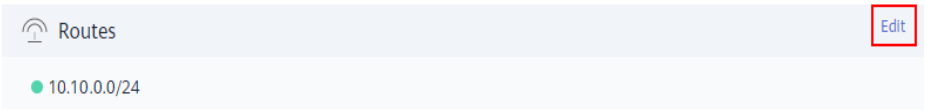
   For details about how to create a VPC peering connection, see **VPC Peering Connection**.
3. Check whether the connection port is enabled on the data source server firewall.
4. Check whether the IP address of the FDI data plane is added to the IP address whitelist of the data source server.
5. Check whether the data source IP address is the IP address of the customer's data center or private network. If yes, establish a VPN connection first.

   For details about how to create a VPN connection, see **Buying a VPN Connection**
6. Check whether the route from FDI to the data source is added.

   If the IP address is a private network address and is not in the 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16 network segment, add a route on the **Instances** page.

   a. Log in to the ROMA Connect console. On the **Instances** page, click **View Console** next to a specific instance.

   b. In the **Routes** area, click **Edit**, click **Add Address**, add a route, and click **Save**.



7. Check whether the security group is bypassed.
   a. Log in to the ROMA Connect console. On the **Instances** page, click **View Console** next to a specific instance.
   b. In the **Security Group** area, click the security group name, for example, **default**, to access the security group console.

   c. On the **Outbound Rules** tab page, check whether the IP address configured for the data source is in the destination list.

      If the destination IP address is 0.0.0.0/0, all IP addresses are allowed. If no rule is available, click **Add Rule** and add the configured IP address to the outbound rule.

3.2 MRS Hive Data Source Connection Failed

Cause Analysis

The possible causes are as follows:

- The private IP address specified in the MRS Hive configuration file cannot communicate with the IP address of the FDI data plane. As a result, the connection fails.
- **HDFS URL** is set to the **root** directory **hdfs:///hacluster**, but the user of the machine-machine account does not have the administrator permissions. As a result, the connection fails.

Solution

- Bind an EIP to the MRS Hive server and change the IP address in the configuration file to the EIP. Then, add the **dfs.client.use.datanode.hostname** configuration item to the **hdfs-site.xml** fil, and set the value to **true**.
- Change **Machine-machine Username** to the name of a user with the administrator permission or change **HDFS URL** to a directory on which the user has sufficient permissions.

If the connection still fails after the preceding operations are performed, rectify the fault by referring to **Data Source Connection Failed**.

3.3 FTP Data Source Connection Failed

Cause Analysis

The connection mode used by the server is different from that specified for the FTP data source. For example, the active connection mode is used by the server, whereas the connection mode of the FTP data source is set to **Passive**.

Solution

Modify the connection mode to ensure that the connection mode of the server is the same as that of the data source.

If the connection still fails after the preceding operation is performed, rectify the fault by referring to **Data Source Connection Failed**.

3.4 OBS Data Source Connection Failed

Cause Analysis

The possible causes are as follows:

- The data source address is not set to the endpoint address.
- The AK/SK and bucket name are incorrect.

Solution

- Change the data source address to the endpoint address.
- Enter the correct AK/SK and bucket name.

If the connection still fails after the preceding operations are performed, rectify the fault by referring to **Data Source Connection Failed**.

3.5 Kafka Data Source Connection Failed

Cause Analysis

Enable SSL is set to **Yes** when the connection address is an MQS intranet address and both **MQS SASL_SSL** and **Intra-VPC Plaintext Access** are enabled.

Solution

Change **Enable SSL** to **No**.

If the connection still fails after the preceding operation is performed, rectify the fault by referring to **Data Source Connection Failed**.

4 Service Integration

4.1 Backend Service Fails to Be Invoked

Cause Analysis

The possible causes are as follows:

- The backend service address is incorrect.
- The timeout duration is incorrect.

  If a backend service fails to return a response within the configured timeout duration, APIC displays a message indicating that the backend service fails to be invoked.
- The security group of the Elastic Cloud Server (ECS) on which the backend service is deployed cannot be accessed.

Solution

- Change the backend service address in the API definition.
- Increase the backend timeout duration in the API definition.
- Ensure that the inbound and outbound ports and protocols configured for services are correct.

4.2 Error Message "No backend available" Is Displayed When an API Is Called

Cause Analysis

The possible causes are as follows:

- The backend service cannot be accessed.
- The required port is not enabled in the ECS security group.

Solution

- Modify the backend service.
- Enable the required port in the ECS security group.

4.3 Error Message "The API does not exist or has not been published in an environment" Is Displayed When an API Is Called Using JavaScript

Cause Analysis

The possible causes are as follows:

- The API is not published in an environment.
- The URL to be accessed is different from that in the API details.
- The API uses the OPTIONS method for cross-domain requests. However, CORS is not enabled and **OPTIONS** is not selected for **Method** during API creation.

Solution

- Publish the API in an environment.
- Modify the URL to ensure that the URL is the same as that in the API details. If a slash (/) is missing after the URL, the API cannot be matched.

  Example: **http://example.com/test/** and **http://example.com/test** match different APIs.
- Enable CORS and select **OPTIONS** for **Method** when creating the API.

4.4 Common Errors Related to IAM Authentication Information

When an API using IAM authentication is called, the following IAM authentication error may be encountered:

- **Incorrect IAM authentication information: verify aksk signature fail**

- **Incorrect IAM authentication information: AK access failed to reach the limit,forbidden**
- **Incorrect IAM authentication information: decrypt token fail**
- **Incorrect IAM authentication information: Get secretKey failed**

Incorrect IAM authentication information: verify aksk signature fail

```
{
  "error_msg": "Incorrect IAM authentication information: verify aksk signature fail, ......
  "error_code": "APIC.0301",
  "request_id": "******"
}
```

Possible Cause

The signature algorithm is incorrect, and the signature calculated by the client is different from that calculated by ROMA Connect.

Solution

1. Obtain the canonicalRequest calculated by ROMA Connect.

   Obtain the canonicalRequest calculated by API Gateway from the following error information:

   ```
   {
     "error_msg": "Incorrect IAM authentication information: verify aksk signature fail,canonicalRequest:PUT|/v2/******/instances/******/configs/||authorization:SDK-HMAC-SHA256 Access=******, SignedHeaders=authorization;content-length;content-type;host;x-project-id;x-sdk-date, Signature=******|content-length:84|content-type:application/json;charset=UTF-8|host:******|x-project-id:******|x-sdk-date:20201117T072119Z||authorization;content-length;content-type;host;x-project-id;x-sdk-date|******",
     "error_code": "APIC.0301",
     "request_id": "******"
   }
   ```

   Replace vertical bars (|) with line breakers to change the error information as follows:

   ```
   {
     "error_msg": "Incorrect IAM authentication information: verify aksk signature fail,canonicalRequest:PUT
   /v2/******/instances/******/configs/

     authorization:SDK-HMAC-SHA256 Access=******, SignedHeaders=authorization;content-length;content-type;host;x-project-id;x-sdk-date, Signature=******
     content-length:84
     content-type:application/json;charset=UTF-8
     host:******
     x-project-id:******
     x-sdk-date:20201117T072119Z

     authorization;content-length;content-type;host;x-project-id;x-sdk-date
   ******",
     "error_code": "APIC.0301",
     "request_id": "******"
   }
   ```

2. Obtain the canonicalRequest calculated by the client by printing logs or using debug interrupts. The following table describes the functions used to calculate the canonicalRequest in the SDKs of different languages.

Table 4-1 Functions for calculating canonicalRequest in the SDKs of common languages

Language	Location
Java (earlier than 3.1.0)	Sign function in com.cloud.sdk.auth.signer.DefaultSigner.class of **libs/java-sdk-core-*.jar**
Java (3.1.0 or later)	Sign function in com.cloud.sdk.auth.signer.Signer.class of **libs/java-sdk-core-*.jar**
cpp	Signer::createSignature function in **signer.cpp**.
csharp	Sign function in **signer.cs**
c	sig_sign function in **signer.c**
go	Sign function in **signer.go**
js	Signer.prototype.Sign function in **signer.js**
php	Sign function in **signer.php**
python	Sign function in **signer.py**

3. Check whether the domain name, method, protocol, path, query strings, headers, and body parameters of canonicalRequest obtained in **1** are the same as those obtained in **2**.
   - If they are different, the common causes are as follows:
     - Some HTTP clients automatically add **charset=utf-8** to the signature header content-type.
     - The user used a proxy to forward requests. The URL, query strings, headers, and body in the request forwarded by the proxy to ROMA Connect are inconsistent with those signed by the client.
     - Some HTTP clients automatically ignore the body of requests that use the GET or DELETE method.
     - Some earlier version SDKs do not allow special characters in URLs.
     - Some earlier version SDKs do not support query strings that contain a key with multiple values, for example, **?a=1&a=2**.
     - Some earlier version SDKs do not allow query strings in URLs.
     - The user-agent header in the actual request is different from the signed user-agent header.
     - Multiple headers with the same name exist.
     - Multiple query strings with the same name exist.
     - The cannonicalRequest contains the authorization header, which conflicts with the signature header.

- If they are consistent, check whether the AppSecret or SK is correct.

  Common cause: The AppSecret or SK contains unnecessary spaces.

Incorrect IAM authentication information: AK access failed to reach the limit,forbidden

```
{
  "error_msg": "Incorrect IAM authentication information: AK access failed to reach the limit,forbidden." .....
  "error_code": "APIC.0301",
  "request_id": "******"
}
```

Possible Cause

- The AK/SK signature is incorrectly calculated. Resolve the problem by referring to **Incorrect IAM authentication information: verify aksk signature fail**.
- The SK corresponding to the AK does not match.
- AK/SK authentication fails for more than five consecutive times, and the AK/SK pair is locked for five minutes. (Authentication requests are rejected within this period).
- The token has expired during token authentication.

Incorrect IAM authentication information: decrypt token fail

```
{
  "error_msg": "Incorrect IAM authentication information: decrypt token fail",
  "error_code": "APIC.0301",
  "request_id": "******"
}
```

Possible Cause

The token cannot be parsed for IAM authentication of the API.

Solution

- Check whether the token is correct.
- Check whether the token has been obtained in the environment where the API is called.

Incorrect IAM authentication information: Get secretKey failed

```
{
"error_msg": "Incorrect IAM authentication information: Get secretKey failed,ak:******,err:ak not exist",
"error_code": "APIC.0301",
"request_id": "******"
}
```

Possible Cause

The AK used for IAM authentication of the API does not exist.

Solution

Check whether the AK is correct.

4.5 A Message Is Displayed Indicating that the Certificate Chain Is Incomplete When You Add a Certificate

Cause Analysis

Generally, a certificate file issued by an intermediate agency contains multiple certificates, for example, a server certificate and a certificate chain in PEM format. This message may be generated when not all of the certificates are combined to form a complete certificate.

Solution

Combine all certificates to form a complete certificate and then fill it in. A server certificate must be placed before the certificate chain in a complete certificate file. The following shows the procedure:

1. Use Notepad to open all PEM certificate files.
2. Paste the **server certificate** before the certificate chain.

   Pay attention to the instructions that come with the certificates. The general rules are as follows:

   - No empty line between certificates.
   - Format of the certificate chain:

     -----BEGIN CERTIFICATE-----

     -----END CERTIFICATE-----

     -----BEGIN CERTIFICATE-----

     -----END CERTIFICATE-----

5 Device Integration

5.1 Error Message "java.lang.IllegalArgumentException: {IP address}_{timestamp}" Is Displayed During Demo Running

Cause Analysis

No EIP has been bound to the ROMA Connect instance.

Solution

Bind an EIP to the ROMA Connect instance and then run the demo again.

5.2 Failed to Connect to ROMA Connect Using the MQTTBox Client

Possible Cause

The possible causes are as follows:

- The **MQTT Client Id**, **Host**, **Username**, and **Password** in the connection configuration are incorrect.
- **Append timestamp to MQTT client id?** is selected.

Solution

- On the **MQTT CLIENT SETTINGS** page, check whether **MQTT Client Id**, **Host**, **Username**, and **Password** are correctly configured.

- Unselect **Append timestamp to MQTT client id?**