Troubleshooting

Using CLI Data

This section describes the show and clear commands that are used for troubleshooting.

show subscriber

This section describes the show subscriber commands for the existing subscribers sessions.

Table 1: show subscriber Command Output Description

Field	Description
|	Output modifiers.
all	Displays all the existing subscriber sessions.
supi	Displays subscriber sessions based on SUPI ID.
gnodeb-id	Displays the gnodeb-id of the session.

clear subscriber

This section describes the clear subscriber commands for the existing subscribers sessions.

Table 2: clear subscriber Command Output Description

Field	Description
|	Output modifiers.
all	Clears all the subscriber sessions.

Field	Description
gnodeb-id	Clears the sessions that have the specified gnodeb-id.
supi	Clears the sessions based on the SUPI value.

Logs

Feature Description

AMF utilizes the common logging framework to generate logs from its microservices.

The supported log levels are:

- Error
- Warn
- Info
- Debug
- Trace

Note Warn level logging takes place during production.

Error

These errors are fatal errors, which can impact service for multiple subscribers. Examples errors are as follows:

- Node discovery of SBA fails after query from NRF and local configuration
- Mandatory IE missing in an NGAP message
- Memory cache startup errors
- Endpoint not found

Warn

These errors impact few specific call-flows majorly, but not blockers of functionality. Example errors are as follows:

- Node discovery of SBA fails but we have more options to retry.
- Mandatory IE missing in a NAS message
- RPC timeout
- Procedural timeout

- Validation failure (not critical)

  Example: Registration rejected as Registration request message received registration type as the Reserved registration type.

- External entity sending unexpected or negative response

  Example: Handover Cancel, Hand over Failure, or Initial Context Setup Failure

- Unexpected value of objects maintained by AMF

  Example: NIL value of transaction

- Unable to fetch a subscriber

Info

This log level purpose is to know information for cause. Examples are as follows:

- Procedural outcome Example: Disabling of ICSR for Registration
- Collision abort, cleanup, suspend, or continue.

Debug

This log level purpose is to get debug messages. Example messages are as follows:

- All external exchanged messages

  Example: Sending Registration accept to UE.

- State machine changes
- Collision detailed logging

Trace

This log level purpose is to get content of all external tracing messages. Example messages are as follows:

- Registration request message
- N1N2 transfer message

How it Works

This section describes how this feature works.

Log Tags

Use log tags to tag the logs for specific procedures which are part of a flow or an event. Enabling of AMF logging takes place at different log levels for different log tags.

Name	Purpose	Example Log tags
AMF service	To capture procedures.	• LogTagReg • LogTagPDU, and so on
Protocol Endpoint	To capture on the interface.	• LogTagNas • LogTagNgap • LogTagNonUE
Rest Endpoint	To capture on the interface.	• LogTagN11 • LogTagN14 • LogTagNRF • LogTagN11OrN14 (N1NMsgTransfer can come from N14/N11 interfaces) and so on

Frequently Encountered Scenarious

Geo-Replication Pod in Pending State

This section describes how to correct geo-replication pod conflict in case of shared hardware setup.

Problem

After completing Day1 configuration on AMF, when you deploy AMF and SMF on the same mode, the geo-replication pod is in pending state.

The following table lists the ports configured use by geo-replication pod. The port numbers are for reference purpose only.

Note The default base port is 15000. You can change the default base port.

Table 3: Ports Configured for Geo-replication Pod

15000	INFRA_PROMETHEUS_PORT
15001	PPROF_EP_PORT
15002	INFRA_ADMIN_PORT
15003	IPC_EP_PORT
15004	GEO_KEEPALIVED_PORT

15005	INFRA_DIAG_PORT

Resolution

1. Change the default base port for geo-pod from 15000 to other available port range.

   instance instance-id *<instance_id>* **endpoint geo internal base-port start** *<new_port>*

   Note <instance_id> should match the <local_instance_id>.

   Configure the relevant keepalive port in SMI config. (base_port + 4) is required only in case of GR setup.

2. To verify that the new port change configuration is reflecting, run the following command.

   ```
   kubectl describe pod georeplication-pod-0 -n cn | grep -i port
   ```

3. SSH to the server where geo-pod is running and run the following command.

   ```
   sudo netstat -plan | grep grpod | grep <port_range> | grep -v
   ```