Failure and Error Handling Support

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
Introduced local cause code support for the ims-vops-failure condition.	2022.02.0
First introduced.	2022.01.0

Feature Description

AMF supports the error handling for the following interfaces:

- SBI—AMF interaction across various 5G NF's
- REST-EP—AMF interaction to NGAP, and NAS (towards UE)

AMF validates the syntax and semantic errors for each attribute during SBI message validation. It evaluates the mandatory, conditional, and optional attributes in the following:

- NGAP content
- NAS content
- Each SBI interface message

Note You can define the local cause code-mapping values for Mobility-Management, while rejecting the NAS messages under failure scenarios.

Validation of the NGAP and NAS optional IEs aren't supported.

How it Works

This section describes how this feature works.

Error Handling on SBI Interface

AMF supports the failure handling for SBI interfaces to continue or to terminate the call. This failure handling is supported as per the actions defined under each service, message-type, and status code.

NRF library provides the failure handling template for each NF to handle statistical and dynamical endpoint information. This library integrates with the REST endpoint to handle SBI message requests or responses.

AMF performs failure handling in the following scenarios:

- When the remote SBI endpoint responds with HTTP error code, it performs the retry procedure as per the failure handling template configuration.
- When the remote SBI endpoint does not respond within the timeout value, it considers it as an error and proceeds with failure handing.
- When failure is detected, the REST endpoint checks for retry count in the Failure Handing profile and performs retries.
- When retries are exhausted or retries aren't configured, it performs the failure action as configured.

Retransmit happens to the same configured URI.

You can configure response timeout under Failure Handling profile. The default timeout value is 2000 ms.

When multiple status codes are received, the number of retries defined for the first received status code is considered.

For terminate process, the UE context is cleared without any peer communication.

Note

- AMF supports the primary, secondary, and tertiary IP addresses that are defined in NF-client profile. If the primary address returns an error or times out, try the secondary address. If the secondary address returns an error or times out, try the tertiary address.
- `Retry-and-ignore` is supported only for the SMSF interface.

The peer NFs send cause codes to the AMF for each SBI interface. The AMF handles these cause codes received from any SBI interface in each response message as per UE context.

Table 3: SBI Supported Failure Actions

Parameter	Failure Action
continue	• Continues the session • Rejects the call
terminate	• Terminates the session • Rejects the call
retry-and-terminate	Perform retry as configured, • If retries are not exhausted, continues the session and the call. • If retries are exhausted, terminates the session and rejects the call.
retry-and-continue	Perform retry as configured, • If retries are not exhausted, continues the session and the call. • If retries are exhausted, terminates the session and rejects the call.
retry-and-ignore	Perform retry as configured, • If retry is passed, continues the session, and continues the call. • If retries are exhausted, continues the session, and continues the call (provided no dependency).

SBI Supported Interfaces and Messages

Table 4: SBI Supported Interfaces and Messages

Interface	Messages
AMF	Service: namf-comm • AmfCommUeContextTransfer • AmfCommUeContextTransferUpdate • AmfCommCreateUeContext
AUSF	Service: nausf-auth • AusfAuthenticationReq • AusfAuthenticationCfm
PCF	Service: npcf-am-policy-control • PcfAmfPolicyControlCreate • PcfAmfPolicyControlDelete
SMF	Service: nsmf-pdusession • SmfSmContextCreate • SmfSmContextUpdate • SmfSmContextDelete
SMSF	Service: nsmsf-sms • SmsfActivationReq • SmsfDeactivationReq • SmsfSendSms
UDM	Service: nudm-sdm • UdmSubscriptionReq • UdmUnSubscriptionReq Service: nudm-uecm • UdmRegistrationReq • UdmDeRegistrationReq

SBI Message Validation

AMF performs the message validation for the SBI interfaces.

Table 5: Handling of Inbound Request Messages

Action	Inbound Request Message
Lookup	• Performs look up for the presence of mandatory or conditional attributes. • REST endpoint fills the appropriate cause code and sends to the peer NF when inbound message isn't qualified. • REST endpoint doesn't forward the failure request process to the AMF-service pod.
Validation	• Validates syntax and semantic errors in mandatory or conditional attributes. • REST endpoint fills the appropriate cause code and sends to the peer NF, when any failure of message parsing or decoding occurs. • REST endpoint doesn't forward the failure request process to the AMF-service pod.
Optional Attributes	• Validates optional attributes in SBI messages. • Checks the syntax and semantic errors of optional attributes present in the SBI message. • REST endpoint ignores the validation of failed optional attributes and forwards the request to the AMF-service pod. The AMF-service pod handles the requested message as per the call model.

Note Validation of incoming inbound request message from UDM, SMF, and SMSF to AMF is supported on the REST endpoint.

Error handling on NGAP and NAS

NGAP error handling:

- Mandatory IE's presence and length checks are performed for the NGAP message validation.

NAS error handling:

- Mandatory IE's presence and length checks are performed for NAS message validation. Conditional IE validations for NAS are also performed.

Local Cause Code Mapping

You can ignore the default EPS Mobility Management (EMM) cause code and configure a preferred EMM cause code to send to a UE in response to a procedural failure.

For example, you can instruct the AMF to return one of the six different EMM cause codes other than the default value, when the AMF receives an authentication error from an AUSF. A list local cause code mappings are created at the global configuration level. A desired list name is specified in the Call Control Profile or in the AMF services or both.

The order of Cause Code selection is as follows:

- Call Control Profile
- AMF Services
- Default

You can configure the local cause codes either or both in the AMF-service or in the Call Control profile.

Table 6: Local Cause Code Mapping condition and 5GMM Cause Codes, on page 6 explains the local cause code-mapping conditions, and 5GMM cause codes with its default value.

Table 6: Local Cause Code Mapping condition and 5GMM Cause Codes

Local Cause Code Mapping Condition	5GMM Cause Codes
`auth-failure`	• `illegal-ms` • `no-suitable-cells-in-tracking-area` • `plmn-not-allowed` • `restricted-service-area` • `roaming-not-allowed-in-this-tracking-area` • `tracking-area-not-allowed` Default Value: `illegal-ms`
`clear-subscriber`	• `plmn-not-allowed` • `5GS-services-not-allowed` • `no-suitable-cells-in-tracking-area` • `restricted-service-area` • `roaming-not-allowed-in-this-tracking-area` • `tracking-area-not-allowed` Default Value: `plmn-not-allowed`

Local Cause Code Mapping Condition	5GMM Cause Codes
ctxt-xfer-fail	• ue-identity-not-derived • no-suitable-cells-in-tracking-area • plmn-not-allowed • restricted-service-area • roaming-not-allowed-in-this-tracking-area • tracking-area-not-allowed Default Value: ue-identity-not-derived
ims-vops-failure	• redirection-to-epc-required • no-suitable-cells-in-tracking-area Default Value: redirection-to-epc-required
peer-node-unknown	• ue-identity-not-derived • no-suitable-cells-in-tracking-area • plmn-not-allowed • restricted-service-area • roaming-not-allowed-in-this-tracking-area • tracking-area-not-allowed Default Value: ue-identity-not-derived
registration-restriction	• plmn-not-allowed • 5GS-service-not-allowed • no-suitable-cells-in-tracking-area • restricted-service-area • roaming-not-allowed-in-this-tracking-area • tracking-area-not-allowed Default Value: plmn-not-allowed

Local Cause Code Mapping Condition	5GMM Cause Codes
rat-type-restriction	• plmn-not-allowed • no-suitable-cells-in-tracking-area • restricted-service-area • roaming-not-allowed-in-this-tracking-area • tracking-area-not-allowed Default Value: plmn-not-allowed
restricted-zone-code	• no-suitable-cells-in-tracking-area • 5GS-services-not-allowed • plmn-not-allowed • restricted-service-area • roaming-not-allowed-in-this-tracking-area • tracking-area-not-allowed Default Value: no-suitable-cells-in-tracking-area
udm-unavailable	• no-suitable-cells-in-tracking-area • plmn-not-allowed • restricted-service-area • roaming-not-allowed-in-this-tracking-area • tracking-area-not-allowed Default Value: no-suitable-cells-in-tracking-area

Feature Configuration

Configuring this feature involves the following steps:

1. Local Cause Code Mapping at Global Configuration—This configuration supports the commands to configure local cause code mapping at Global configuration. For more information, see Configuring the Local Cause Code Mapping at Global Configuration, on page 9.
2. Local Cause Code Mapping under Call Control Policy Configuration. —This configuration supports the commands to configure local cause code mapping under Call Control Policy. For more information, see Configuring the Local Cause Code Mapping under Call Control Policy, on page 9.
3. Local Cause Code Mapping under AMF Service Configuration—This configuration supports the commands to configure local cause code mapping under AMF-service. For more information, see Configuring the Local Cause Code Mapping under AMF Service, on page 10.

Configuring the Local Cause Code Mapping at Global Configuration

To configure this feature, use the following configuration:

```
config
   local-cause-code-map name cause_code_map_name cause_code_type cause-code-5gmm
 cause_code_5gmm_type
   end
```

NOTES:

- **local-cause-code-map name** *cause_code_map_name cause_code_type*—Specify a name for Cause Code Map.

  The *cause_code_type* includes one of the following:

  - `auth-failure`—UE authentication failure
  - `clear-subscriber`—UE subscriber clear condition type
  - `ctxt-xfer-fail`—Context transfer failure between AMF and MME
  - `ims-vops-failure`—IMS voice-centric UE registration failure
  - `peer-node-unknown`—No response from peer node
  - `rat-type-restriction`—Restriction with RAT type
  - `registration-restriction`—Restriction with Registration
  - `restricted-zone-code`—Restricted zone code
  - `udm-unavailable`—UDM not available

  cause-code-5gmm *cause_code_5gmm_type*—Specify the *cause_code_5gmm_type*. For the values of *cause_code_5gmm_type*, see *Local Cause Code Mapping condition and 5GMM Cause Codes* table.

Configuration Example

The following are the example configurations.

```
config
   local-cause-code-map name lc1 auth-failure cause-code-5gmm
no-suitable-cells-in-tracking-area
   end
```

```
config
   local-cause-code-map name lc2 ctxt-xfer-fail cause-code-5gmm restricted-service-area
   end
```

```
config
   local-cause-code-map name example ims-vops-failure { no-suitable-cells-in-tracking-area
 | redirection-to-epc-required }
   end
```

Configuring the Local Cause Code Mapping under Call Control Policy

```
config
   call-control-policy policy_name
```

```
local-cause-code-map cause_code_map_name
end
```

NOTES:

- **call-control-policy** *policy_name*—Specify the Call Control Policy name.
- **local-cause-code-map** *cause_code_map_name*—Specify the *cause_code_map_name* which is configured at *Configuring the Local Cause Code Mapping at Global Configuration*.

Configuration Example

The following is an example configuration.

```
config
   amf-global
      call-control-policy ccp1
         local-cause-code-map lc1
         end
```

Configuring the Local Cause Code Mapping under AMF Service

To configure this feature, use the following configuration:

```
config
   amf-services service_name
      local-cause-code-map cause_code_map_name
      end
```

NOTES:

- **local-cause-code-map** *cause_code_map_name*—Specify the *cause_code_map_name* which is configured at Configuring the Local Cause Code Mapping at Global Configuration, on page 9 .

Configuration Example

The following is an example configuration.

```
config
   amf-services amf
      local-cause-code-map lc2
      end
```

Failure Handling Template

Configuring the response timeout for failure handling involves the following steps:

- Response Timeout Configuration at Endpoint—This configuration provides the commands to configure response timeout at endpoint. For more information, see Configuring the Response Timeout at Endpoint, on page 11.
- Response Timeout Configuration at Failure Profile—This configuration provides the commands to configure response timeout at failure profile level. For more information, see Configuring the Response timeout at Failure Profile, on page 12.

The following is an example of the failure handling template configuration for the AUSF. This configuration is similar for all other interfaces.

Configuring the Response Timeout at Endpoint

To configure the response timeout at endpoint level, use the following configuration:

```
config
   profile nf-client nf-type name_of_nf_type
      ausf-profile profile_name
         locality locality_name
            service name type service_name
               responsetimeout timeout_value
               end
```

NOTES:

- **profile nf-client nf-type** *name_of_nf_type*—Specify the NF.
- **ausf-profile** *profile_name*—Specify a name for AUSF profile.
- **locality** *locality_name*—Specify a name for locality.
- **service name type** *service_name*—Specify a name for service type.
- **responsetimeout** *timeout_value*—Specify the timeout value in seconds. Must be an integer.

Configuration Example

The following is an example configuration.

```
config
   profile nf-client nf-type ausf
      ausf-profile AUP1
         locality LOC1
            service name type nausf-auth
               responsetimeout 2000
               end
```

Configuration Verification

To verify the configuration:

```
show running-config profile nf-client nf-type ausf | details
profile nf-client nf-type ausf
 ausf-profile AUP1
  locality LOC1
   priority 30
   service name type nausf-auth
    responsetimeout 2000
    endpoint-profile EP1
     capacity   30
     priority   1
     uri-scheme http
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 209.165.200.229
      primary ip-address port 9047
      secondary ip-address ipv4 209.165.200.229
      secondary ip-address port 9047
      tertiary ip-address ipv4 209.165.200.229
```

```
      tertiary ip-address port 9047
     exit
    exit
   exit
  exit
 exit
exit
```

Configuring the Response timeout at Failure Profile

When the request is failed and the failure profile is selected, the response time is considered from the failure handling profile.

To configure the response timeout at failure profile level, use the following configuration:

```
config
   profile nf-client-failure nf-type name_of_nf_type
      profile failure-handling failure_handling_name
         service name type service_name
            responsetimeout timeout_value
            end
```

NOTES:

- **profile nf-client-failure nf-type** *name_of_nf_type*—Specify the NF.
- **profile failure-handling** *failure_handling_name*—Specify a name for failure handling.
- **service name type** *service_name*—Specify a name for service type.
- **responsetimeout** *timeout_value*—Specify the timeout value in seconds. Must be an integer.

Configuration Example

The following is an example configuration:

```
config
   profile nf-client-failure nf-type ausf
      profile failure-handling FH1
         service name type nausf-auth
            responsetimeout 1000
            end
```

Configuration Verification

To verify the configuration:

```
show running-config profile nf-client-failure nf-type ausf | details
profile nf-client-failure nf-type ausf
 profile failure-handling FH1
  service name type nausf-auth
   responsetimeout 1000
   message type AusfAuthenticationReq
    status-code httpv2 503
     retry               3
     retransmit          2
     retransmit-interval 25
     action              retry-and-terminate
    exit
   exit
   message type AusfAuthenticationCfm
    status-code httpv2 503
```

```
     retry               3
     retransmit          2
     retransmit-interval 25
     action              retry-and-terminate
    exit
   exit
  exit
 exit
exit
```

Behavior for Multiple Failure Cause Code Configuration

If multiple status codes return one after another matches the failure handling profile, the following known behavior is observed:

- Example—When retry count is configured and retransmit value is not configured.

```
config
  profile nf-client-failure nf-type smsf
   profile failure-handling FH5
    service name type nsmsf-sms
     responsetimeout 1000
     message type SmsfActivationReq
      status-code httpv2 500
       retry  3
       retransmit-interval 2000
       action retry-and-ignore
      exit
      status-code httpv2 504
       retry  2
       retransmit-interval 2000
       action retry-and-ignore
       end
```

  For the example mentioned,

  - If AMF receives 500 response for the first try, then it performs a second retry.
  - In the second retry, if AMF gets 504 response, AMF tries twice.
  - When this retry count (for 504 response) is exhausted, AMF doesn't resume the retry count for first one (500 response).
  - The maximum retries depend on the maximum number of endpoints configured (primary, secondary, tertiary) or NRF discovered ones.

- Example—When retry count and retransmit value are configured.

```
config
  profile nf-client-failure nf-type smsf
   profile failure-handling FH5
    service name type nsmsf-sms
     responsetimeout 1000
     message type SmsfActivationReq
      status-code httpv2 504
       retransmit 3
       retry 2
       action retry-and-terminate
       end
```

  For the example mentioned,

  - If both retransmit value and retry count are configured, retransmit happens first and then retry.

Retransmmission is done thrice and if it fails, retry to done for secondary endpoint.

If retry returns 504 response, retransmmission is done three times and if it fails, retry is done for tertiary endpoint.

Note Retries are always done to another endpoint, while retransmmission is done always to same endpoint.